# Global Information Assurance Certification Paper

# SANS GIAC Certified Firewall Analyst Practical Assignment

GCFW Version 1.7

Authored by:
Benjamin Lam

Date submitted: November 27, 2002

## Assignment 1 Security Architecture



## Assignment 2 Security Policy and Tutorial

## Assignment 3: Verify the Firewall Policy



## Assignment 4 Design Under Fire



## Reference

# Assignment 1 Security Architecture

## User Requirement

The network security infrastructure for Enterprise is required to design. The design should fulfill the following business operation and requirements

a) The total revenue of last financial year was US$ 5 million dollars without on-line sales.
b) The expected sales amount through Internet is 40% of the revenue of last year. Also since the customer can purchase product anytime and anywhere, it is expected to have 20% increment of sales. So the total expected sales amount through Internet is 2 + 1 = US$ 3 million dollars.
c) Protect internal back-end systems in which a lot of confidential and sensitive data that must not be disclosed illegally or retrieved by the competitors is stored.
d) Only a subset of data in internal database is needed to be viewed or updated by suppliers and partners.
e) Sales force only need to access internal mail and database server when they are out of office.
f) Teleworkers need to access internal systems for urgent maintenance work when they are out of office.
g) Internet access should be provided to the internal staff. Usage of Internet access should be business related only.
h) Not all the staff need the Internet access services due to their job natures.
i) The Internet Web access activities should be logged for auditing purpose.
j) 7x24 on-line buying non-stop Web service should be provided for the public.
k) All services or connections should be entirely through Internet.
l) A secure way should be provided for the suppliers and partners to provide and retrieve the information.
m) A secure way should be provided for sales force to access internal database and mail server to retrieve the information of product and mail.
n) A secure way should also be provided for teleworkers.
o) All sensitive information through Internet must be encrypted.

## How each group communicates with Enterprise

1) *Internal staff* can access the Internet Web server. Since not all staff has business need to access the Internet, authentication is required. They also can send Internet e-mail.
2) The *customer* can only access Web servers located in the public zone of the external firewall to browse and search the Web content and buy product online anytime & anywhere.
3) The *suppliers & partners* can provide/retrieve information to GIAC by two ways.
   i) Through the *VPN*. Only the *ftp server* located in the security zone of the VPN/firewall gateway can be accessed. Two-factor authentication will be required for accessing the ftp server.
   *ii)* Through the *secure Web interface*. They can only access the *public Web servers.*

4) *Sales force* of GIAC can access the *internal mail and database servers* through *VPN.* Also two-factor authentication will be required.
5) *Teleworkers of Enterprise* can access the internal systems through VPN. Also two-factor authentication will be required.

**The services and protocols used for communication of each group and Enterprise**

1) The **internal staff** can access the Internet through proxy server with LDAP authentication. Only **FTP,HTTP** and **HTTPS** will be permitted. The internal mail server can send **SMTP** email to Internet.
2) Two services will be set up in Web servers, **HTTP & HHTPS** for **customers.** HTTP will be used for Web browsing or searching. Once customers want to buy product online, HTTPS will be used.
3) The **suppliers and partners** can access the **Web** server by specific **TCP port 543 with SSL enabled** if their network infrastructure do not support VPN tunneling.
   OR they can access the ftp server protected by the firewall/VPN gateway **through VPN**. Only **FTP** will be permitted.
   For Web access, they must provide their public IP address used for outgoing traffics.
   Two-factor authentication is required for both methods.
4) **Sales force** can access the internal database and mail server **through VPN**. **SQLPLUS** and **POP3** services are used. Two-factor authentication is required.
5) **Teleworkers** can access the internal systems **through VPN**. **telnet** and **ftp** services are used. Two-factor authentication is required.

The high-level security policies are defined according to above requirements. And a two-tier firewall infrastructure is designed to protect the GIAC Enterprise network. Please refer to the figure 1 for details.

## Network Diagram

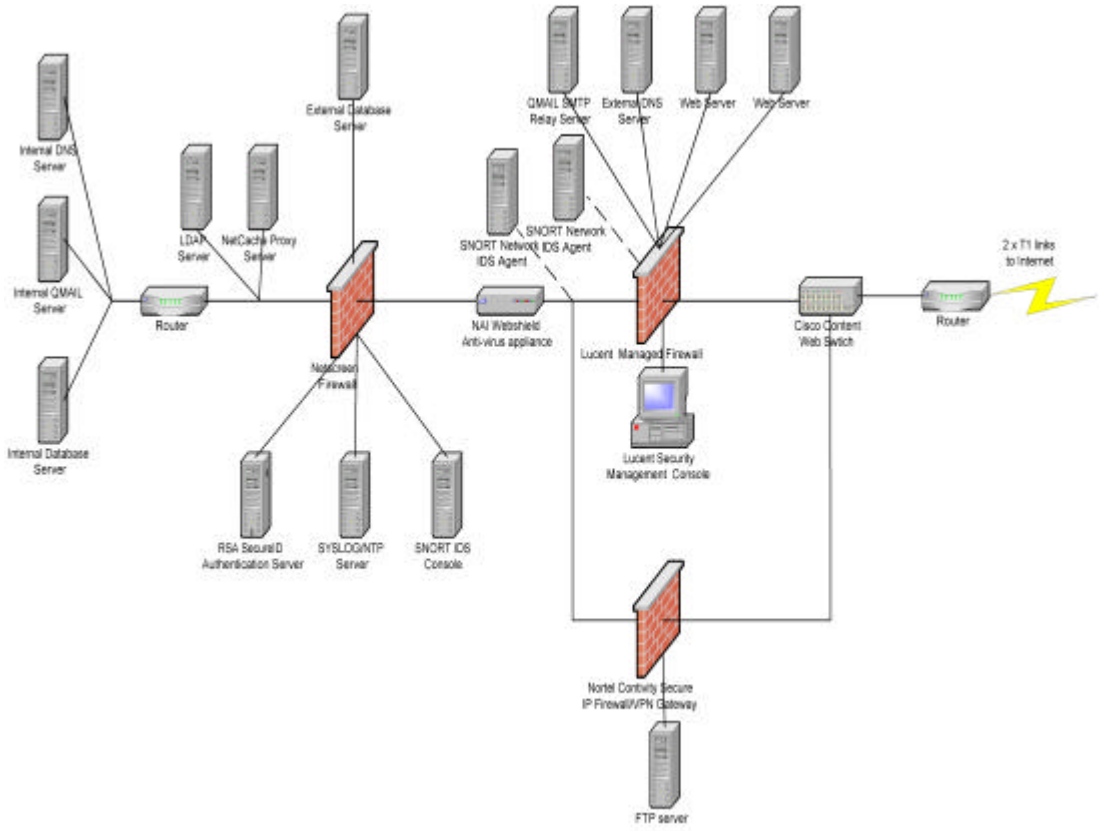



Figure 1. Network Diagram

## High level technical policies

1) Public can only access the Web server in the public access zone of external firewall.
2) Only HTTP and HTTPS service requests should be allowed from outside world into the Web server.
3) Only server providing services (such as Web, SMTP relay and DNS etc) for public will be located in the public zone of external firewall. Servers that do not need to have direct connection with public world (such as database, Syslog/NTP server etc) should be protected by internal firewall.
4) Web server can only access the external database server protected by the internal firewall.
5) The GIAC internal back-end database server will access external database server in the security zone of the internal firewall to retrieve and update the data periodically. Only single direction traffic from internal to external should be allowed.
6) Direct access from the Web server into the GIAC internal network is not allowed.
7) Direct access from Outside World into the GIAC internal network is also not allowed except the teleworker and salesman using VPN.
8) Secure Sockets Layer (SSL)v3 should be used to provide secure communications at the transport level.
9) X.509v3 certificate that supports data communication should be used

whenever public key encryption is adopted.

10) The listening port of running services in servers should be static not dynamic.
11) Virus scanning for the email, ftp and Web service should be implemented.
12) OS of all servers in the security network infrastructure should be "hardened".

## Overview of the Solutions

1) Using hardware based purpose-built appliance if the product is available on the market. Since it can eliminate performance degrade due to the overhead of the general-purpose operating system. It also eliminates the security holes typically found in the general-purpose OS.
2) Using **two-tier firewall infrastructure** to increase the protection to the internal network.
3) **Internet mail relay** is implemented to handle the incoming SMTP mail. It prevents the direct connection between the internal SMTP server and Internet world.
4) Implement the **split DNS approach** to separate the Internal and public IP information. Thus, the outsider can only obtain the virtual public IP address.
5) Implementing NAI virus scanning e-ppliance. Actually, it is an application proxy of FTP, HTTP and SMTP. It will act as a **proxy layer** between two firewalls in addition to the primary function virus scanning.
6) Proxy caching server is used for internal staff accessing the Internet. LDAP authentication is required. The proxy server can log all URL visited.
7) Three different brand names of firewall are used.
8) **External database server** is implemented. It should only host the data necessary for the suppliers and partners. Full replication of internal database to external database is not recommended. If the public Web server is compromised, only the data in external database will be reached by the compromised system. Such arrangement will increase the level of protection of internal database.
9) Time sync server is implemented. The time stamps of security devices are very important to correlate the network events and activities. Time sync server is used to sync the time stamps.
10) Nortel Contivity Secure IP Services Gateway is used for **firewall/VPN gateway**. It provides **additional security protection** after the traffic is decrypted. The detailed explanation on why using such product will be described later. Moreover, VPN users and public users are separated by two firewalls. If server or firewall on one side is being hacked and even be compromised, the other side will not be affected immediately.
11) Implementing Cisco layer 7 Web switch. It mainly serves two functions. a) It can **protect against the DOS attack** of servers located in the public zone. b) It can provide the load balancing on two or more Web servers. It also provides the auto fail-over when one server is down or maintenance work is required. No software client or agent is needed to install on the server.
12) Implementing network based intrusion detection system. The **IDS** will be configured in **"stealth mode"**. This means that IDS will have two interfaces: one for monitoring and another one for reporting. No IP address and protocol stack will be bound to the monitoring interface.

**Perimeter Defense component in design**

*1) External Firewall - Lucent Firewall Brick 201.*

a) It operates as layer 2 switch making it invisible to outside world and eliminating the possibility to be hacked or cyber attacked.
b) hardware based firewall appliance
c) Each interface has its own set of policy. It means that if a permitted traffic from one interface to the other is required to configure, it does not succeed when only one interface's policy has been modified. Both policies correspond to two interfaces must be changed. Although it will increase the administrative workload little bit, it eliminates the "single fault" human error of misconfiguring the policy that allows the deny traffic to pass through the firewall.
d) ICSA certified firewall
e) 150 Mbps clear text throughput. It is enough as the throughput of internal and Internet gateway is only 100 Mbps.

2) *Internal Firewall - Netscreen-204*

a) hardware based firewall appliance
b) ICSA certified firewall
c) Attack protection(such as SYN attack, Ping of Death, IP spoofing, Tear drop attack) on any interfaces.
d) 400 Mbps clear text throughput. It is enough as the throughput of internal and Internet gateway is only 100 Mbps.

*3) Firewall/VPN Gateway – Nortel Contivity Secure IP Services Gateway 1700*

a) Stateful inspection firewall
b) hardware based firewall appliance
c) ICSA certified firewall and VPN gateway
d) Support split tunneling
e) It can prioritize traffic by IP, users, groups and VPN tunnels.

*4) Virus scanning and proxy layer- NAI Webshield e250*

a) McAfee's anti-virus software is preloaded on the Solaris. Although it cannot eliminate the possibility from being hacked through the vulnerabilities of OS, the time for recovering after the machine crash is minimized as it is not necessary to re-install the OS and the application.
b) Actually, it is an application proxy of FTP, HTTP and SMTP services. It can provide additional function as the proxy layer between two firewalls.
c) The virus signature update can be scheduled at most frequency once a day.
d) The manufacturer release new virus signature once a week at normal condition.

*5) Web service load balancing and DOS protection - Cisco CSS 11000 Series Content Service Switches*

a) It provides a load balancing of the Web servers.
b) It provides a auto fail-over when one server is down

c) It provides a DOS protection. It can prevent Syn flood, LAND, Smurf and ping of death attack.
d) One of the methods to detect whether the Web server is up is to check against the file integrity of home page. If the hash value is different, the web server is declared to be down. The outside world cannot access this server again. This feature can be used to detect whether the home page has been defaced and disconnected with the web server from Internet, although it is not the primary purpose.
e) It provides NAT function.
f) It provides routing function.

*6) Internet Mail Relay - Qmail*

Qmail is an Internet Mail Transfer Agent (MTA) for UNIX/LINUX operating systems. It is designed for high security. When comparing with Sendmail, another MTA for UNIX/LINUX, the vulnerabilities found are much fewer.

*7) Proxy Server - NetCache proxy server*
a) hardware based proxy appliance
b) Disk cache capacity is 72 GB
c) It provides replication by caching the frequently accessed Internet Web content. It can reduce the network traffic and increase the response time.

8) Web server – Sun One Web server 6.0 with SP4 run on Solaris 8.

9) *Two factor Authentication*. RSA SecureID authentication server run on Win 2000 server

10) *Internal Authentication for Internet access* - Sun One directory server 5.1 run on Solaris 8

11) *Internal and border routers* - Cisco 2620 router

12) Central firewall log and time sync system - Syslog/NTP server (LINUX based)

13) External DNS server – BIND 9.2.1 run on Solaris 8

14) Network based intrusion detection system – SNORT 2.0 run on Red Hat LINUX 7.3.

**IP Assignment**

| **Server** | **Real IP** | **Virtual IP** |
|---|---|---|
| External Web server 1 | 172.16.1.10/24 | 201.70.246.164/28 |
| External Web server 2 | 172.16.1.11/24 | 201.70.246.164/28 |
| External SMTP relay | 172.16.1.12/24 | 201.70.246.165/28 |
| External DNS server | 172.16.1.13/24 | 201.70.246.163/28 |

| | | |
|---|---|---|
| SYSLOG/NTP server | 172.16.3.10/24 | Nil |
| SecureID Auth server | 172.16.3.11/24 | Nil |
| Network IDS console | 172.16.3.12/24 | Nil |
| Monitoring interface of network IDS agents | 172.16.3.13/24 | Nil |
| | 172.16.3.14/24 | Nil |
| External database server | 172.16.4.10/24 | Nil |
| Trust interface of internal firewall | 172.16.5.1/24 | Nil |
| Untrust interface of internal firewall | 172.16.2.1/24 | Nil |
| Trust interface of Webshield anti-virus tools | 172.16.5.2/24 | Nil |
| Untrust interface of Webshield anti-virus tools | 172.16.1.2/24 | 201.70.246.167/28 |
| Trust interface of firewall/VPN gateway | 172.16.1.3/24 | Nil |
| Untrust interface of firewall/VPN gateway | 201.70.246.166/28 | Nil |
| Managed IP of external firewall | 172.16.1.4/24 | Nil |
| Lucent Security Management Server | 172.16.1.5/24 | Nil |
| Cisco Content Switch | 202.70.246.162/28 | Nil |
| External Router Ethernet Interface | 202.70.246.161/28 | Nil |

Virtual internal IP range assigned to the sale force group using VPN
172.17.1.1 – 172.17.1.254 network mask 255.255.255.0
Virtual internal IP range assigned to the teleworker group using VPN
172.18.1.1 – 172.18.1.254 network mask 255.255.255.0

**Cost/benefit justification**

| | |
|---|---|
| Cisco router | US$2,000 x 2 |
| 10/100M autosense switch | US$1,200 x 4 |
| Content switch | US$28,000 x 1 |
| LMF (including the management console) | US$9,000 x 1 |
| Nortel firewall/VPN gateway | US$10,000 x 1 |
| Netscreen firewall | US$13,000 x 1 |
| NAI Virus scanning | US$13,000 x 1 |
| Proxy server | US$11,000 x 1 |
| Web server (UNIX based) | US$11,000 x 2 |
| Qmail server (UNIX based) | US$3,000 x 1 |
| LDAP server (UNIX based) | US$3,200 x 1 |
| Directory server, License | US$2 per entry |
| DNS server (UNIX based) | US$3,000 x 1 |
| ftp server (LINUX based) | US$1,500 x 1 |
| Syslog/NTP server (LINUX based) | US$1,500 x 1 |
| RSA server (including the agents for ftp | |

| | |
|---|---|
| And Web server) | US$9,000 x 1 |
| Secured token | US$120 per user |
| Notebook for console administration | US$1,300 x 1 |
| Network based IDS (1 console, 2 agents) | US$ 4,500 |

Total estimated costs including hardware, software, installation and basic configuration (OS hardening and firewall policy implementation not included) for building the security network is US$ 156,000. (It is assumed that about 1,000 internal staff need to access the Internet and about 100 salesmen & teleworkers need to access the internal network through VPN with two-factor authentication. The suppliers and partners will pay for their own SecureID token.)
14 man-days will be purchased for OS hardening and firewall policy implementation.
Total estimated costs is 156,000 + 14 * 1,000 = US$170,000.

Assumed that the lifetime of the network infrastructure is 3 years. So it will be used to protect the value about 3,000,000 * 3 = US$ 9 million dollars. (The increment per year does not take into account.)
The proportion of protected value in percentage is 170,000/9,000,000 = 1.89%. It is justified to implement the Enterprise security infrastructure.

# Assignment 2 Security Policy and Tutorial

## General Guideline for implementing policies/ruleset

Everything is denied but which specially is permitted. This is known as implicit deny any. It is critical to pay attention to the order of ACL or ruleset as all devices proposed in the design will process each ACL or ruleset in up-down sequence against traffic and apply the action specified in the policy to the first matching policy on the list. Also, the policies should be arranged from the most specific to the most general. Only the required services will be permitted to pass through the router/firewall.

Tutorial on how to implement the policy of external firewall will be given as the implementation of the policy or ruleset is different from other devices. Normally, only one set of policy needs to be defined for other devices. The number of policies need to be defined are equal to the number of LAN interfaces.

## Border router access list (incoming traffic from Internet to router)

access-list 101 deny IP 201.70.246.160 0.0.0.15 any log _____line 1
access-list 101 permit UDP any host 201.70.246.163 eq 53 _____line 2
access-list 101 permit TCP any host 201.70.246.164 eq http _____line 3
access-list 101 permit TCP any host 201.70.246.164 eq https _____line 4
access-list 101 permit TCP any host 201.70.246.164 eq 543 _____line 5
access-list 101 permit TCP any host 201.70.246.165 eq smtp _____line 6
access-list 101 permit UDP any host 201.70.246.166 eq 500 _____line 7
access-list 101 permit ESP any host 201.70.246.166 _____line 8
access-list 101 permit IP any host 201.70.246.167 established_____line 9
access-list 101 deny IP any any log_____line 10

## Border router access list (outgoing traffic to Internet)

access-list 102 permit IP 201.70.246.160 0.0.0.15 any _____line 1
access-list 102 deny IP any any log_____line 2

## Explanation of ACL of router

access-list 101 (applied to the WAN link interface to ISP)

For line 1, it is prevention against intruders IP spoofing of the Enterprise Public IP address. It must be the first line in order to filter and drop such packet. If it is placed in line 2 for example, any spoofed packets with destination IP 201.70.246.163 and UDP port 53 can bypass the ACL.

For line 10, actually it can be omitted if the traffic dropped by the router is not necessary to be logged as the ACL of Cisco router is "Everything is denied but which specially is permitted". Setting this rule is for the logging purpose. Moreover, it must be the last line. If it is placed before any permitted traffic rules, permitted packet will be dropped by this denied rule anyway.

For line 2 to 5, they are for the Web, external DNS and SMTP traffic. These rules can be placed in a different order since they are for different services and there is no conflict between them. But bear in mind that they must be

placed between line 1 and 10.

For line 7 & 8, they are ACL for VPN users. Line 7 is for the IKE protocol key exchange. Line 8 is for the ESP protocol of VPN. These rules can also be placed in different order since they are for different services and no conflict between them. But bear in mind that they must be placed between line 1 and 10.

For line 9 it is the permitted rule for the established TCP connection of outgoing traffic from Enterprise to Internet after a TCP three-way handshake is successful. 201.70.246.167 is the virtual public IP for Internet access and outgoing SMTP mail. These rules can also be placed in different order since they are for different services and no conflict between them. But bear in mind that they must be placed between line 1 and 10.

*access-list 102 (applied to the ethernet interface connected to content switch)*
Actually, it is egress filtering that only allows packet that the source IP with public IP range of Enterprise leaving the router to Internet.

**External Firewall**

| Source | Destination | Service | Action | Log |
|---|---|---|---|---|
| 1) supplier/partner Group | Web servers | TCP port 543 | permit | Yes |
| 2) Web server | ACE server | UDP port 5500 | permit | Yes |
| 3) Web server | DB server in internal firewall | sqlplus,ftp | permit | Yes |
| 4) Mgt console | NTP server | ntp | permit | Yes |
| 5) SMTP mail relay | Webshield external interface | smtp | permit | Yes |
| 6) Webshield external interface | Public zone & Mgt console | ftp,smtp | deny | Yes |
| 7) Webshield external interface | any | ftp,http,https, smtp | permit | Yes |
| 8) any | SMTP mail relay | smtp | permit | Yes |
| 9) any | External DNS | UDP port 53 | permit | Yes |
| 10) External DNS | any | UDP port 53 | permit | Yes |
| 11) any | Web servers | http, https | permit | Yes |
| 12) any | any | any | deny | Yes |

**Explanation of ACL of external firewall**

The implementation of ACL of external firewall also follows the general guideline of implementing of ACL, from most specific to most general.

For rule 1, suppliers/partners can access the public Web server through specific port 543 with SSL enabled to supply or retrieve the information.

For rule 2, as suppliers/partners need to authenticate with SecureID token, this rule allows the Web server to communicate with the ACE authentication server to check whether the authentication is success.

For rule 3, as all the data supplied by suppliers or required by the partners is stored in the external database. Also when the customer purchase the

product through Internet, the payment information will be stored in the external database server. This rule allows the Web server communicating with the database server using SQLPLUS and FTP.
For rule 4, it allows the management console of firewall to sync the time with the NTP server.
For rule 5, it allows the QMAIL relaying all incoming SMTP mail to Webshield for virus scanning.
For rule 7, it allows the outgoing Internet access services i.e. HTTP & FTP and outgoing SMTP mail to Internet. As stated before, Webshield acts as the proxy layer, that is why the source IP address of outgoing traffic has been translated to the IP of Webshield external interface.
For rule 6, it is to deny the SMTP and FTP traffic from Webshield entering the public zone and management console that is permitted in the rule 7(as the destination is any).
For rule 8, it allows the incoming SMTP mail from anywhere in Internet to reach the Qmail SMTP relay.
For rule 9, this is the DNS service that allows any IP (including the internal DNS, Webshield and Internet) to query the external DNS server.
For rule 10, it allows the external DNS to query the others DNS servers in Internet for host to IP resolve.
For rule 11, it allows the Public in anywhere to access Web servers using HTTP and HTTPS services.
For line 12, actually it can be omitted if the traffic dropped by the firewall is not necessary to be logged as the ACL of external firewall is " Everything is denied but which specially is permitted" . Setting this rule is for the logging purpose.

**Ordering**

For rule 1 to 6, they can be placed in a different order as they are for different services and there is no conflict between them. But they must be placed before rule 7 to 12 as they are much specific than rule 7 to 12.
For rule 6, it must be placed before rule 7 as it is used to block the traffic, which is permitted to pass through the firewall in rule 7.
For rule 7 to 11, they can also be placed in a different order as they are for different services and there is no conflict between them. But they must be placed after rule 1 to 6 as they are less specific and before rule 12 as it is the explicitly deny rule.
The rule 12 must be placed at the last. If it is placed before any permitted traffic rules, permitted packet will be dropped by this denied rule anyway.

**Internal Firewall**

| Source | Destination | Service | Action | Log |
|---|---|---|---|---|
| 1) ACE clients | ACE server | UDP port 5500 | permit | Yes |
| 2) Internal mail server | Webshield | smtp | permit | Yes |
| 3) Webshield | Internal mail server | smtp | permit | Yes |
| 4) Internal DNS | External DNS | UDP port 53 | permit | Yes |
| 5) Internal DB & Public Web server | External DB | sqlplus,ftp | permit | Yes |

| | Source | Destination | Service | Action | Log |
|---|---|---|---|---|---|
| 6) | Internal DB | ftp server | ftp | permit | Yes |
| 7) | Mgt console of External firewall, Firewall/VPN Gateway | syslog server | UDP port 514 | permit | Yes |
| 8) | Mgt console of External firewall, Firewall/VPN Gateway | NTP server | ntp | permit | Yes |
| 9) | Proxy server | External DB, Public zone & Mgt Console | ftp | deny | Yes |
| 10) | Proxy server | External DB, Mgt Console | http, https | deny | Yes |
| 11) | Proxy server | any | ftp,http,https | permit | Yes |
| 12) | any | any | any | deny | Yes |

**Explanation of ACL of internal firewall**

For rule 1, it allows the two-factor authentication agents including the ftp server for the suppliers/partners using VPN, the Web server agent for the suppliers/partners through Internet, the VPN gateway to query the ACE authentication server.

For rule 2, the outgoing SMTP mail is sent from internal mail server to Webshield for virus scanning then sent to Internet.

For rule 3, the incoming SMTP mail is sent from Webshield to Internal mail server after the Internet SMTP mail has been virus scanned.

For rule 4, the internal DNS query the external DNS server for Internet host name to IP resolve.

For rule 5, as all the data supplied by suppliers or required by the partners is stored in the external database. When the customer purchase the product through Internet, the payment information will be stored in the external database server. Moreover, the internal database server will sync the data with the internal database periodically. This rule allows the Web server and internal data server to communicate with database server using SQLPLUS and FTP.

For rule 6, the information required by the partners and provided by the suppliers are stored in the FTP server when using VPN as a communication channel. This rule allows the internal database server to put and get the information to FTP server.

For rule 7, the traffic log of three firewalls will be logged in the central log server. This rule allows the firewall put the traffic log to the central log server through SYSLOG service.

For rule 8, to correlate the traffic events of three firewalls and carry out the log analysis, it is important that the time stamp of each firewall should be the same. This rule allows three firewalls to sync time with the NTP server using NTP service.

For rule 11, the internal staff will access the Internet through the proxy server. This rule allows the proxy server to access the Internet using FTP, HTTP and HTTPS.

For rule 9 and 10, they are used to deny the traffic from proxy server entering the public zone and management console that is permitted in the rule 11(as the destination is any).
For line 12, actually it can be omitted if the traffic dropped by the firewall is not necessary to be logged as the ACL of external firewall is " Everything is denied but which specially is permitted" . Setting this rule is for the logging purpose.

**Ordering**

For rule 1 to 10, they can be placed in a different order as they are for different services and there is no conflict between them.
For rule 9 & 10 , it must be placed before rule 11 as it is used to block the traffic, which is permitted to pass through the firewall in rule 11.
For rule 12 it must be placed at the last. If it is placed before any permitted traffic rules, permitted packet will be dropped by this denied rule anyway.

**Firewall/VPN Gateway**

| | Source | Destination | Service | Action | Log |
|---|---|---|---|---|---|
| 1) | ftp server | ACE server | UDP port 5500 | permit | Yes |
| 2) | Firewall/VPN Gateway | syslog server | UDP port 514 | permit | Yes |
| 3) | Firewall/VPN Gateway | NTP server | ntp | permit | Yes |
| 4) | Internal DB | ftp server | ftp | permit | Yes |
| 5) | Supplier/Partner Group | ftp server | ftp | VPN tunnel | Yes |
| 6) | Sales Group | Internal mail server | pop3 | VPN tunnel | Yes |
| 7) | Sales Group | Internal DB server | sqlplus | VPN tunnel | Yes |
| 8) | teleworker Group | Internal servers | telnet,ftp | VPN tunnel | Yes |
| 9) | any | any | any | deny | Yes |

**Explanation of ACL of firewall/VPN Gateway**

For rule 1, it allows the two-factor authentication agents including the ftp server for the suppliers/partners using VPN, the Web server agent for the suppliers/partners through Internet, the VPN gateway to query the ACE authentication server.
For rule 2, the traffic log of three firewalls will be logged in the central log server. This rule allows the firewall/VPN gateway put the traffic log to the central log server through SYSLOG service.
For rule 3, to correlate the traffic events of three firewalls and carry out the log analysis, it is important that the time stamp of each firewall should be the same. This rule allows firewall/VPN gateway to sync time with the NTP server using NTP service.
For rule 4, the information required by the partners and provided by the suppliers is stored in the FTP server when using VPN as a communication channel. This rule allows the internal database server to put and get the

information to FTP server.
For rule 5, the suppliers and partners can put and get the information of the FTP server when using the VPN tunneling.
For rule 6, the sales force needs to access the internal mail server from Internet. This rule allows it to do so using POP3 through VPN.
For rule 7, it allows the sales force to access the internal database server using SQLPLUS through VPN
For rule 8, teleworker needs to access the internal system. This rule allows to do so using TELNET through VPN.
For line 9, actually it can be omitted if the traffic dropped by the firewall is not necessary to be logged as the ACL of external firewall is "Everything is denied but which specially is permitted". Setting this rule is for the logging purpose

**Ordering**

For rule 1 to 8, they can be placed in a different order as they are for different services and there is no conflict between them.
For rule 9 it must be placed at the last. If it is placed before any permitted traffic rules, permitted packet will be dropped by this denied rule anyway.

**Tutorial- External Firewall**

**Introduction**

A zone ruleset is a set of security rule that is assigned to individual interface. It will control all the incoming and outgoing traffic which flows through the interface. So the number of active zone rulesets is equal to the number of active interfaces.
The firewall will intercept the packet according to the zone ruleset defined. If no rule is found that matches the information in the packet, such packet will be dropped by the last rule "drop all packets rule". This drop all packets rule is default last rule in the ruleset.

**Rule numbering**

A zone ruleset can contain up to 65,535 rules. The number of the "drop all packets" rule is 65,535. The range of number of firewall administrator defined rules is from 1000 to 64,999. Other ranges (1-199, 500-999, 65,000-65,534) are reserved for future use. 200-299 is used for firewall, administration and proxy rule, whereas 300-399 is user authentication rule.

**Elements of the rule**

1) Rule no. The first field is the rule no. The number of first rule created by the administrator in the zone ruleset is 1,000.
2) Direction. Three options are available: "In to zone", "Out of zone" & "Both". "In to zone" is the direction that packets leave the firewall and flow into the zone. "Out of zone" is the direction that packets flow out of the zone and enter the firewall.
3) Source IP. It is the address from which the packets are sent. This field can be a single IP address or host group. How to define the host group will be described later.
4) Destination IP. It is the address to which the packets are sent. This field

can be a single IP address or host group.

5) Service. It can be a single service such as http, ftp, smtp or dns or a group of services. How to define the service group will be described later.
6) Action. It is the action that will be applied to the packet when the above field information (except the rule no) matches with the packet. It can be drop, pass and proxy. If the "proxy" action is selected, the firewall will reflect the session to the server running the Lucent Proxy Agent application. The agent will then determine whether it is dropped or passed. Please note that only smtp and http service can be proxied.
7) Drop Action. Two options: None or Notify. If notification is required to send to the source when the packet is dropped, choose Notify. Otherwise, choose None.
8) Audit. Two options: Yes or No. It is used to determine whether the traffic will be logged by the firewall.

**How to Create Host Group**

1) Login in the Lucent security management server LSMS. (Figure 2. LSMS Navigator – Login)

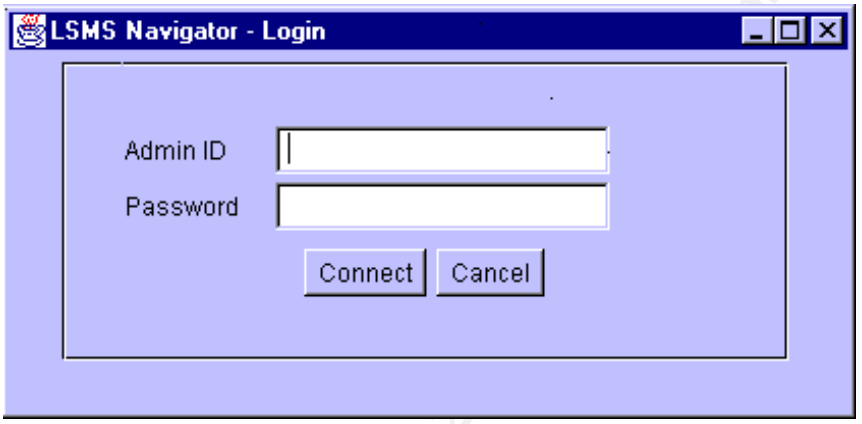



Figure 2. LSMS Navigator Login

2) Select the host group folder in the Navigator Window. (Figure 3. Navigator Window)

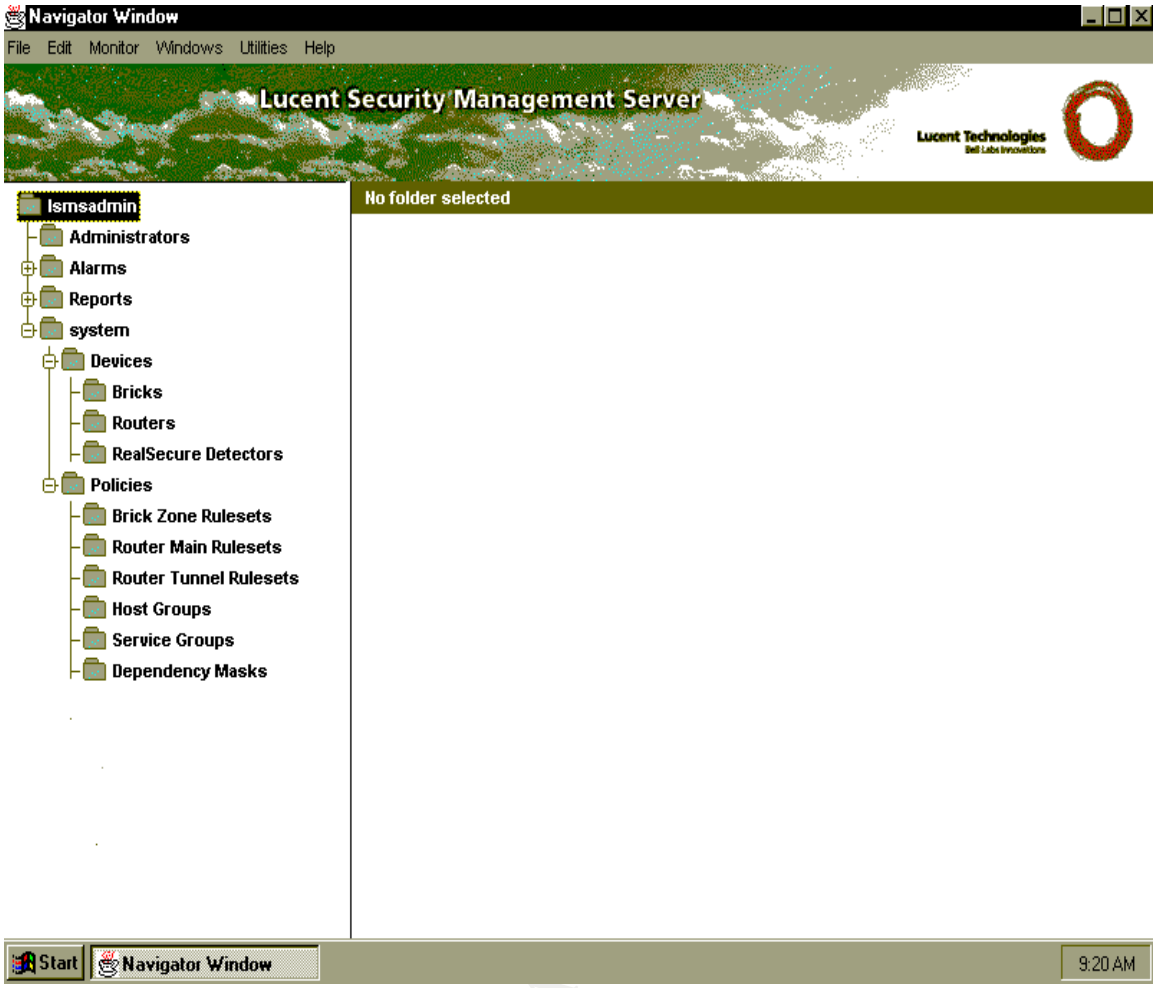



Figure 3. Navigator Window

3) Right click the host group folder and select the New Hosts Group from the menu. Host group editor will be showed. (Figure 4. Host Group Editor)
4) In the name field, enter the name of the host group. The name must be unique. The name can be up to 44 characters in maximum. It is case sensitive, i.e. Web and web are two different groups. It is a mandatory field.
5) For the description field, it is optional. It can be up to 80 characters in maximum. It is also case sensitive.
6) Host addresses field. It is the mandatory field. Four formats can be entered.
   a) Single IP address (for example, 172.16.1.1)
   b) Network IP with subnet mask (for example, 172.16.0.0/16)
   c) IP address range (for example, 172.16.1.1 - 172.16.1.200)
   d) An asterisk (all host)
6) Click the "File" item in the menu bar and select save option to save the host group.

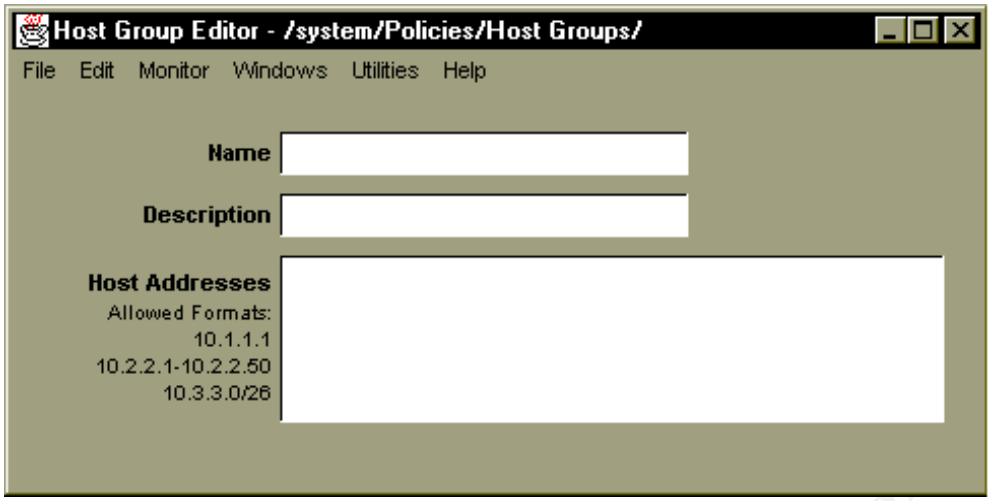



Figure 4. Host Group Editor

**How to create Service Group**

1) Select the service group folder in the Navigator Window.
2) Right-click the service group folder and select New Service Group. Service group editor will be showed. (Figure 5. Service Group Editor)

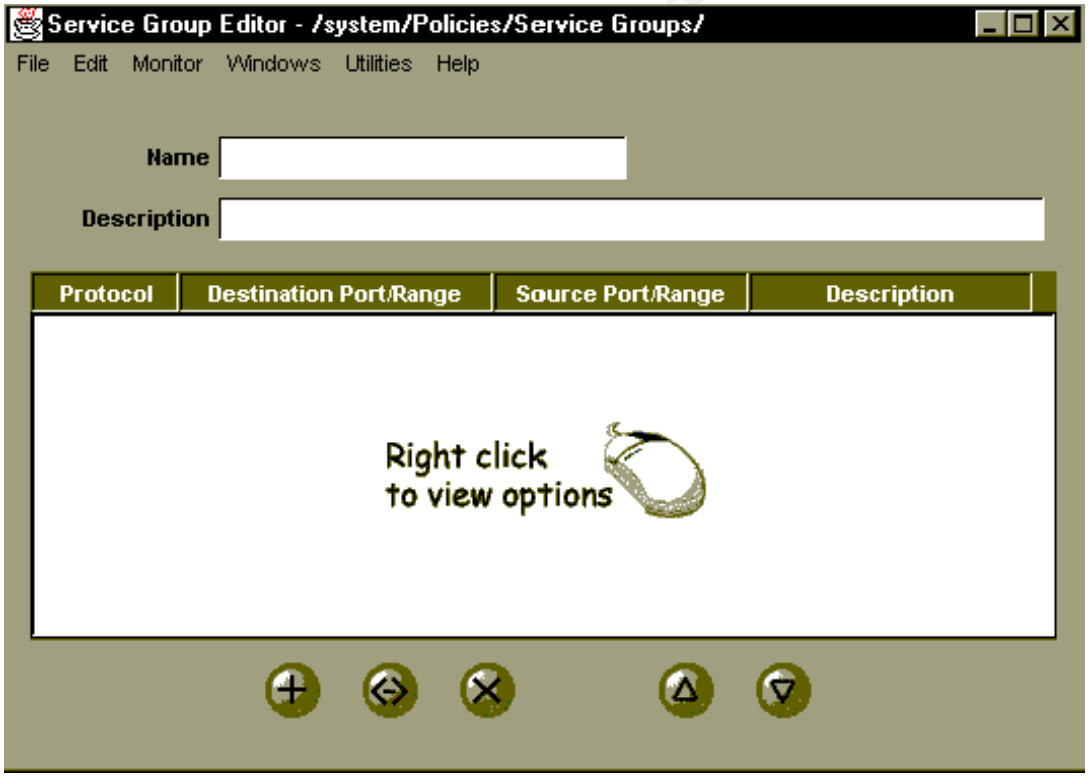



Figure 5. Service Group Editor

3) In the name field, enter the name of the service group. The name must be unique. The name can be up to 44 characters in maximum. It is case sensitive, i.e. Web and web are two different groups. It is a mandatory field.

4) For the description field, it is optional. It can be up to 80 characters in maximum. It is also case sensitive.
5) Click the "+" button to add the new service in the group. The "Service Editor" window will be displayed. (Figure 6. Service Editor)

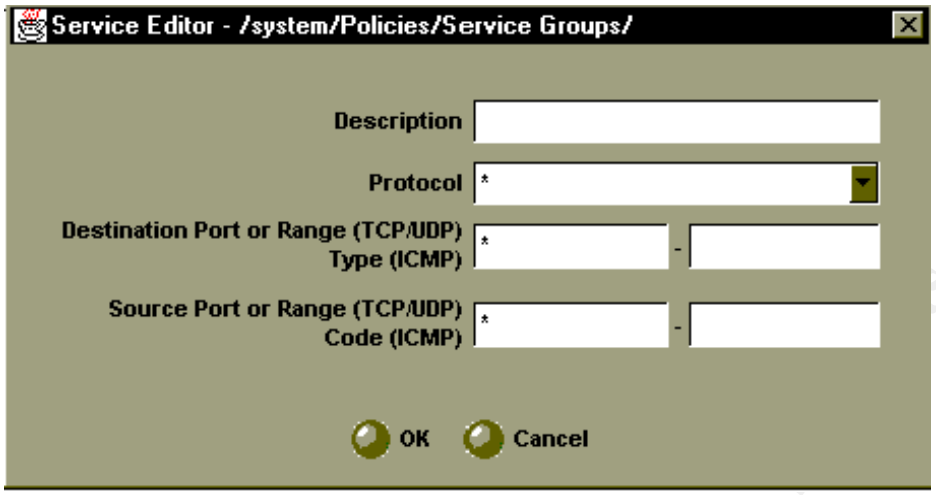



Figure 6. Service Editor

6) In the description field, enter the description of the service. It is optional.
7) Select the protocol from the drop-down list in the protocol field. Four options can be chosen:
   a) An asterisk (any protocol)
   b) TCP
   c) UDP
   d) ICMP
8) In the Destination Port or range field, enter the port number or a range of port number of the destination port. The default value is asterisk.
9) In the Source Port or range field, enter the port number or a range of port number of the source port. The default value is asterisk.
10) Click "OK" button to save the setting. The service created will be shown in the Service Group Editor.
11) Repeat the step 5 to 10 if another services are needed to add in the service group.

**How to create zone ruleset**

1) Select the zone ruleset folder in the Navigator Window.
2) Right click the zone ruleset and select the New Zone Ruleset. Zone ruleset editor will be shown.(Figure 7. Brick Zone Ruleset Editor)

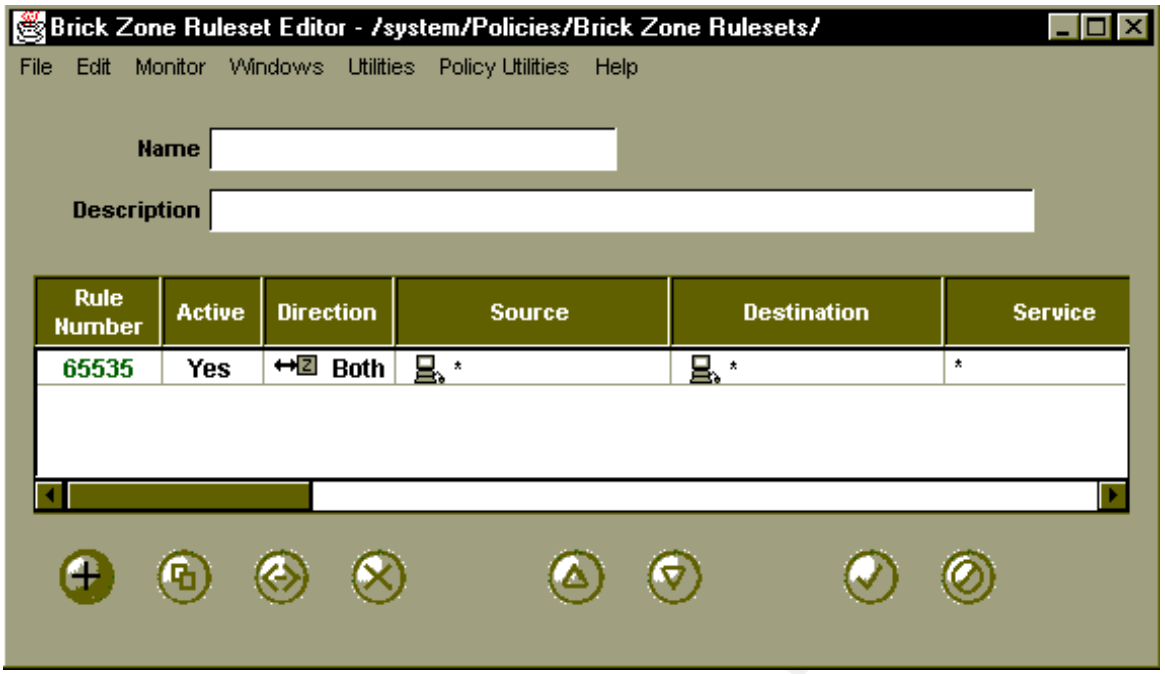



Figure 7. Brick Zone Ruleset Editor

3) In the name field, enter the name of the zone ruleset. The name must be unique. The name can be up to 44 characters in maximum. It is case sensitive, i.e. Web and web are two different groups. It is a mandatory field.
4) For the description field, it is optional. It can be up to 80 characters in maximum. It is also case sensitive.
5) The rule "drop all packet" rule with rule number 65535 is created automatically.
6) To create a new rule, click the "+" button. Zone Rule Editor will be displayed.(Figure 8.Brick Zone Rule Editor)
7) By defuault, the rule is active. If you would to like to disable it, choose "NO" in the Rule Active field.
8) In the Direction field, "Both" is the default. Two other options "In to Zone" and "Out of Zone" can be selected.
9) In the Source field, you can enter IP address or choose the host group by clicking the drop-down list.
10) In the Destination field, you can etner IP address or choose the host group by clicking the drop-down list.
11) There are three ways to enter the service in the Service Field
a) By default, it is an asterisk. This means all protocols are allowed.
b) Click the drop-down list. Three protocols TCP, UDP and ICMP can be selected.
c) Click the drop-down list and selected the "Browse" option. A window with all service groups will appear. You can select one of the service groups from the list.
12) In the Action field, the default action is "Drop". "Pass" and "Proxy" are the other options. If "Drop" action is selected, Drop Action can also be selected.
13) The default value of the Audit Session field is "Yes". If traffic logging of this rule is not necessary, select the option "No".
14) Click OK to save the rule.

15) Repeat 6 to 14 to create another rule.
16) Click the "UP Arrow" and "DOWN Arrow" button in the Ruleset Editor to change the order of rules if necessary.
15) Select the file in the menu bar in the Ruleset Editor and select Save to save the zone ruleset.

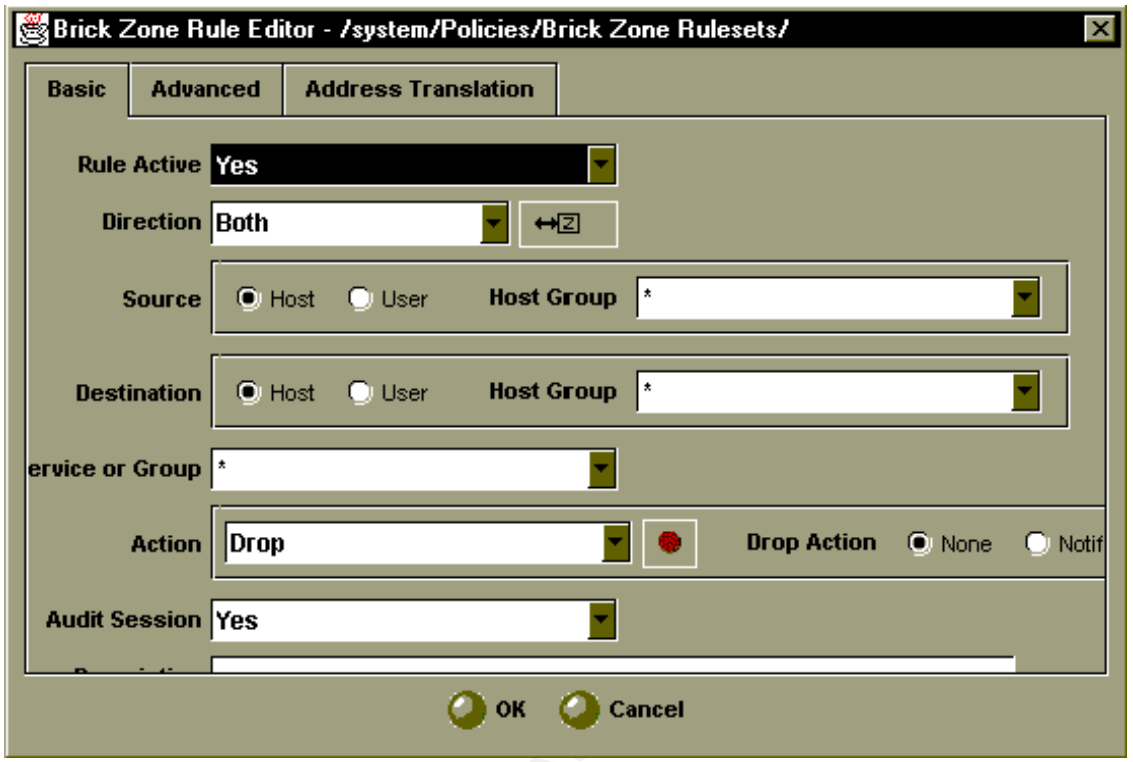



Figure 8.Brick Zone Rule Editor

**How to assign the zone ruleset to Interface**

1) Select the brick sub-folder under the device folder in Navigator Window.
2) Double-click the firewall name that containing the interface (Since the management console can manage serval firewalls).The Firewall Editor will be displayed.(Figure 9. Brick Editor)

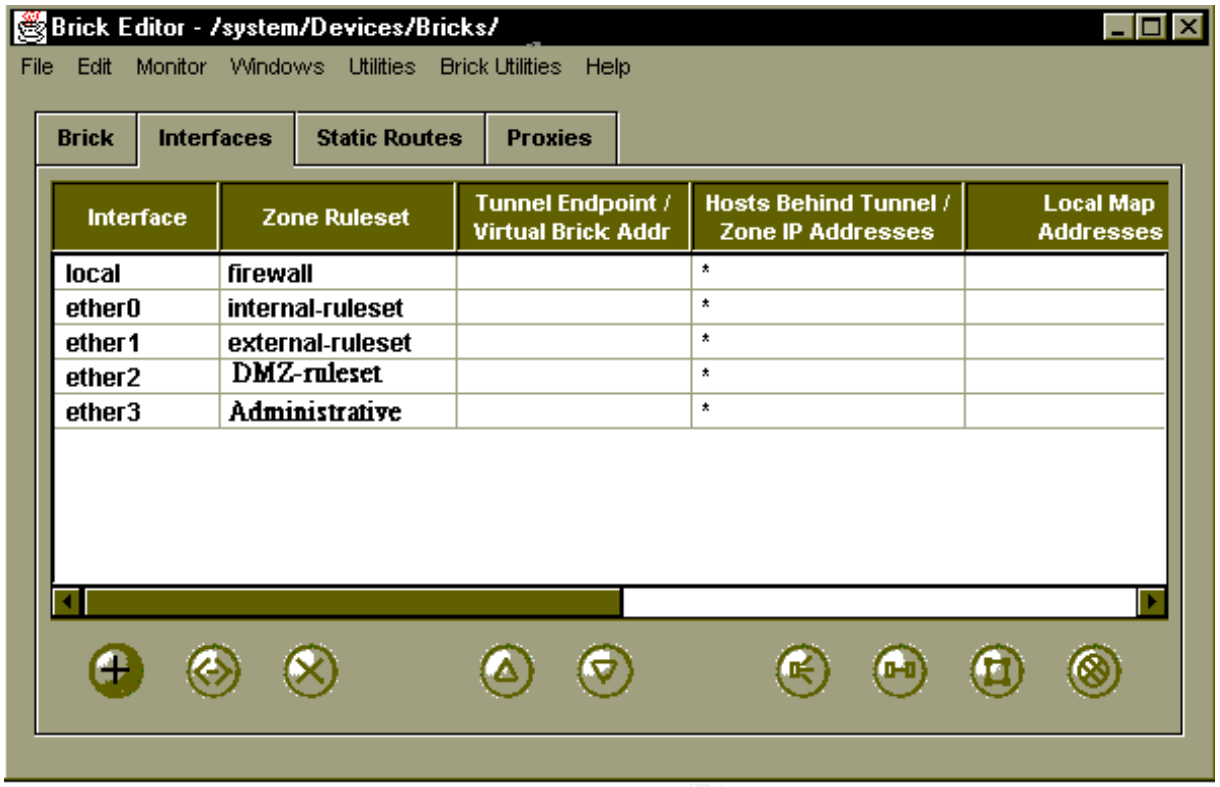



Figure 9. Brick Editor

3) Click the Interface to display the Interface tab.
4) Double-click the interface to which the zone ruleset will be assigned. The Interface Editor (Figure 10. Interface Editor) will appear.

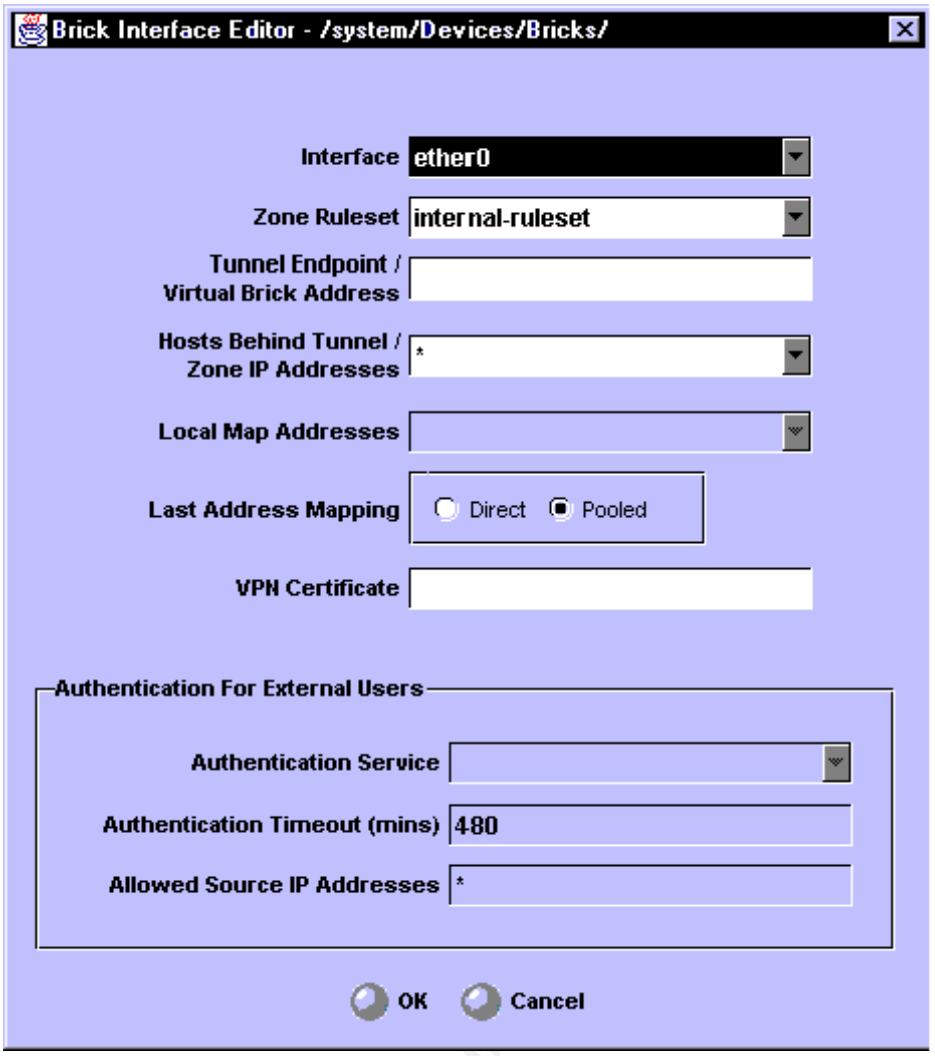



Figure 10 Interface Editor

5) In the Zone Ruleset field, click the drop-down list and select "Browse". All zone rulesets will be shown . Select the zone ruleset that will be assigned to the Interface.
6) Click OK button to save the setting and return to the Firewall Editor.
7) Repeat the step 3 to 6 to assign the other zone rulesets to Interfaces.
8) Select the file in the menu bar in the Firewall Editor and select Save to save the assignment of the zone rulesets to Interfaces.

## How to active the zone ruleset to firewall

After defining the host group and serivce group, creating the different zone rulesets, assigning the zone ruleset to the interface, the rulesets have to be applied to the firewall. To do so, you must follow the procedure below.
1) Select the Utilities from menu bar in the Navigator Window. An "Apply Brick" window will be dislayed. (Figure 11. "Apply Brick" Window)
2) Click OK button to apply the rulesets to the firewall.

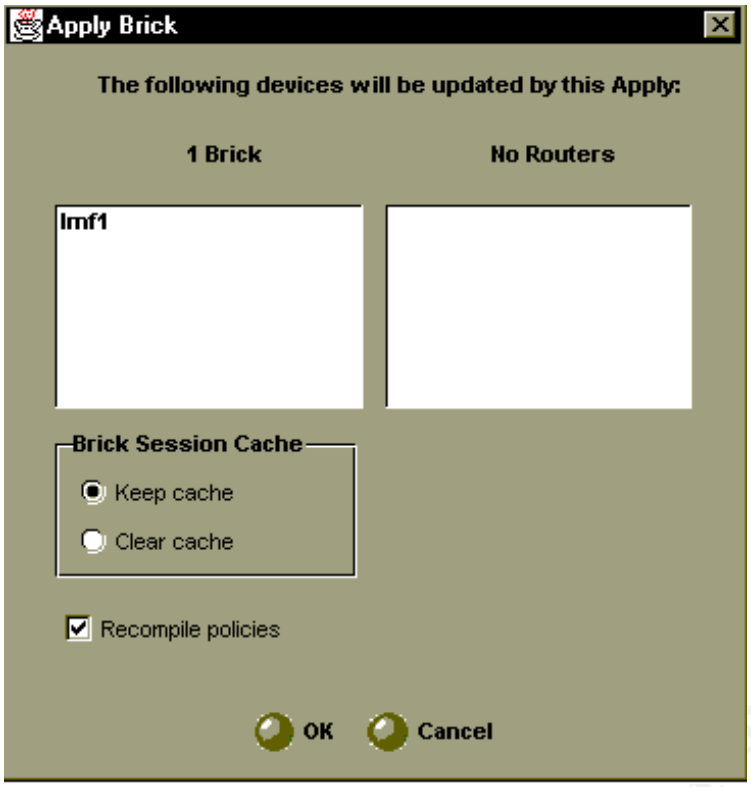



Figure 11. "Apply Brick" Window

**Rulesets of the external firewall**

Internal ruleset(Figure 11), DMZ ruleset(Figrue 12) and external ruleset(Figure 13) have been created according to the ACL of the external firewall listed above. The Internal ruleset will be assigned to the interface which is connected to the Webshield. The public zone ruelset will be assigned to the interface that is connected to the public access servers network.(ie. the network with Public Web server, external DNS and SMTP relay). The external ruleset will be assigned to the interface that is connected to Internet.


Figure 11 Internal Ruleset


Figure 12 DMZ Ruleset


Figure 13 External Ruleset

## Ruleset Creation/Implementation Tips

1) You must pay the attention to the rule number when creating rules. Click the NEW button without first selecting the existing rule, the rule number will be 1000. If you click the NEW button after selecting the rule, the rule number of the new rule will be the number of the existing rule being selected. The rule number of the existing rule will move up one number. Rules below the selected rule will also be renumbered accordingly.

2) There is a field "Session Cache" in the Save Policy Window.Two options can be selected."Keep cache" & "Clear cache". "Keep cache" is the default value. This means that the session information will be kept when applying the zone ruleset to the firewall. So if you do not want to disrupt any sessions that are already established, keep the defualt value.

3) General speaking, it should be a deny rule(rule 7) to block the traffic, which is permitted to pass through the firewall in rule 8. Actually this rule can be omitted. Although the traffic can be passed according to the internal zone ruleset, it will be dropped by the public zone ruleset due to no permit rule to such traffic in the public zone ruleset.

4) You may notice that the audit session field is "No" when the direction of the

permit rule is out of zone, "Yes" when the direction of the permit rule is in to zone in both internal and public zone ruleset. It is to eliminate the duplicate entry in the firewall session log. Let's take the rule 1,001 of both internal ruleset and pulbic zone ruleset as an example. Both rules decribe the same thing: traffic from Web servers to external database server with destination port 21 & 1521. If the audit of both rules is turned on, such traffic will be logged twice.

## Assignment 3: Verify the Firewall Policy

### Methodology

It includes three main parts: 1) checking OS and software of firewall, 2) function of the firewall & 3) auditing rulesets.
Basically, the methodology is based on "Testing the firewall system" from Cert.org. Details please refer to the following URL
http://www.cert.org/security-improvement/practices/p060.html

OS and software of firewall checking
1) To check whether the latest security patch of software version of firewall is applied.
2) To check what services are "opened" on the firewall and check whether they should be opened.
3) to fin out vulnerabilities on the firewall and check whether countermeasures are applied.
4) To check whether the latest security patch installed in the OS where firewall run on. Also check whether it is "harden". More information can be found at

For Solaris, Linux, HP-UX, Cisco, Window 2000 & Window NT hardening guide.
http://www.cisecurity.org/ The Centre for Internet Security

For security best practice and implementation,
http://www.cert.org/security-improvement/

For Sun Solaris system security
http://www.sun.com/solutions/blueprints/browsesubject.html#security

### Functionality

1) Routing function to check whether packets will be routed correctly
2) Filtering function to check whether the traffic is allowed or denied to pass
3) Logging function to check whether the traffic events will be logged correctly

### Audit the policy ruleset

The following rulesets are being scanned using nmap

| | Source | Destination | Service | Action | Log |
|---|---|---|---|---|---|
| 1) | supplier/partner Group | Web servers | TCP port 543 | permit | Yes |
| 2) | Web server | ACE server | UDP port 5500 | permit | Yes |
| 3) | Web server | DB server in internal firewall | sqlplus,ftp | permit | Yes |
| 4) | Mgt console | NTP server | ntp | permit | Yes |
| 5) | SMTP mail relay | Webshield external interface | smtp | permit | Yes |
| 6) | Webshield | Public zone | ftp,smtp | deny | Yes |

| | | | | |
|---|---|---|---|---|
| external interface | & Mgt console | | | |
| 7) Webshield external interface | any | ftp,http, ,https,smtp | permit | Yes |
| 8) any | SMTP mail relay | smtp | permit | Yes |
| 9) any | External DNS | UDP port 53 | permit | Yes |
| 10) External DNS | any | UDP port 53 | permit | Yes |
| 11) any | Web servers | http, https | permit | Yes |
| 12) any | any | any | deny | Yes |

**Tools used for auditing**

Ruleset will be tested by using nmap scanning tools run on WinXP. The Window based version of nmap can be downloaded from www.insecure.org/nmap

The logging of the firewall will be used to check whether the denied traffic is really denied to pass through the firewall.

Additionally,when the destination is LINUX, tcpdump command will be used to capture the events.

When the destination is UNIX, built-in command snoop will be used to capture the events.

Sniffer will also be used when the destination is in Internet.

**Consideration**

1) To test the routing function, the packet filtering need to be disabled. It means that the access control function is disabled and the protection of the network is also turned off.
2) There may be an impact to the users if the firewall is in production as downtime may be required.
3) It is not possible to test all cases of packet filter configuration because of too many combinations. Let' s the case that only port number is variable and source and destination are fixed. The full range is 1-65535. If the full range is being scanned, it will take several hours even a day to test one rule only depending on which scanning mode is used.
4) Sniffer will be used. Not only the expected traffic will be captured, another traffic including some confidential information such as plaint-text password flowing through the segment where the sniffer is "listening" on will also be captured.
5) Although the tool nmap used for auditing is freeware, the policies of the corporate may be not allowed to use such software without approval from management.
6) Some systems will not follow the RFC of responding the incoming packet with different flag bits up. Even though the design of OS is followed the RFC, the response packet may not be allowed to pass the firewall.
7) The scanning mechai for UDP of nmap is sent A UDP packet with zero byte data. If an ICMP port unreachable message is received, the port is closed. Otherwise, it is assumed that the port is opened. Such ICMP message may be dropped by firewall
8) Some firewalls will drop the "abnormal packet" (such as all six flag bits have been turned on/off) even through all information in TCP/IP header are matched with the rule. Pay attention to the scan method when using nmap.

9) Pay attention to any hidden system rules of firewall.
10) Pay attention to the PORT mode FTP (active mode). It is an inbound traffic from ftp server to ftp client with TCP source port 20 (ftp-data) and any destination port >1023 are used. Check whether such inbound traffic is permitted but no ftp control connection is established before.
11) Pay attention to the DNS query. The UDP source and destination port 53 are used. Check whether the traffic only with UDP source port 53 is denied.
12) Pay attention to DNS zone transfer, which TCP destination port 53 is used.

**Countermeasure of above points**

1) The firewall must be totally isolated from the Internet. It is preferable to isolate from the internal network too. If it is not feasible to do so, It is recommended to add a temporary rule to allow the ping request and reply from any to any to test the routing function.
2)If the firewall is in production, the audit test should be carried out after office hour in order to minimize the impact to users as it need to be disconnected from internal network and Internet.
The test of routing function of firewall is required to disconnect the firewall from internal network and Internet. For auditing ruleset, although it is not necessary to suspend the service for auditing them (as nmap is allowed to set the source IP address explicitly), it is recommended to do so if possible as the scanning will cause the performance degrade of the server and even crash the server.
The on-line purchasing service for customer will also be suspended. One-week notice posted on the Web site is recommended.
3) Not full range will be scanned. As all OS of the machines are UNIX or LINUX, port numbers 1- 1023 are required user root privilege to start. So 1 - 1023 ports will be scanned. If port number of application is within this range, (port number minus 500) to (port number add 500) range will be scanned.
If the source or destination is any, 4 IP addresses will be used for scanning.
4) Time slot for suspension of the service should be arranged in order to prevent the leakage of confidential and personal information.
5) Seek the management' s approval if necessary.
6) Do not rely on the scanning result of the nmap. View the log data from the output of snoop, sniffer and the firewall logs.
7) Same as point 6.
8) The purpose of this auditing exercise is to test the firewall rule sets, so TCP Connect & TCP SYN scan option of nmap will be used for scanning to prevent the firewall dropping the "abnormal" packet and get the wrong result. If the source and destination are machines in the GIAC enterprise network, TCP connect scan method of nmap will be used. But if the destination is Internet, TCP three-way handshake cannot be performed as the host cannot be reached when the firewall is isolated. TCP SYN scan of nmap will be used.
9) Check with manufacturer of firewall and manual to check whether any hidden system rules.
10) Add one more test case to scan the DNS server with source TCP port is 20 and destination TCP port 1024-2024.
11)Add one more test case to scan the DNS server with source UDP port 53 and destination TCP port 1-1023.
12) Add one more test case to scan the DNS server with destination TCP port

53.

**Test plan**
**Audit the firewall itself**

Routing Function
1) Disconnect the Security Infrasturcture from internal network and Internet
2) Disable the packet filter function
3) Generate traffic using nmap from four different directions:
   a) From internal to external
   b) From internal to public zone
   c) From external to public zone
   d) From public zone to internal
4) Check whether the traffic is routed correctly.

Filtering Function
1) Enable the packet filter function that no traffic is permitted to pass through the firewall.
2) Generate traffic from four different directions.
3) Check whether the traffic will be denied.

Logging Function
1) Check the log of the firewall whether the event logging of above two tests is correct.

**Auditing firewall rulesets**
The commands for testing rulesets are listed below.

Command for rule 1
case 1 : nmap -sT -P0 172.16.1.10-11 (with source IP in supplier/partner Group by changing the IP setting of WinXP)
case 2 : nmap -sT -P0 -p 543 172.16.10-11 (with source IP NOT in supplier/partner Group and destination port with 543)

Command for rule 2
case 1 : nmap -sU -P0 -p 5000-6000 172.16.3.11 (with source IP is Web server IP)
case 2 : nmap -sU -P0 -p 5500 172.16.3.11 (with source IP NOT Web server and destination port with port 5500)

Command for rule 3
case 1: nmap -sT -P0 172.16.4.10 (with source IP is Web server IP)
case 2 nmap -sT -P0 -p 1021 - 2021 172.16.4.10 (with source IP is Web server IP)
case 3: nmap -sT -P0 -p 1521 172.16.4.10 (with source IP NOT Web server IP and destination port with 1521)
case 4: nmap -sT -P0 -p 21 172.16.4.10 (with source IP NOT Web server IP and destination port with 21)

Command for rule 4

case 1: nmap -sU -P0 172.16.3.10 (with source IP is firewall management console IP)
case 2 : nmap -sU -P0 -p 123 172.16.3.10 (with source IP NOT firewall management console IP and destination port with UDP port 123)

Command for rule 5
case 1: nmap -sT -P0 172.16.1.2 (with source IP is SMTP mail relay)
case 2 : nmap -sT -P0 -p 25 172.16.1.2 (with source IP NOT SMTP mail relay and destination port with 25)

Command for rule 6
case 1: nmap -sT -P0 -p 21,25 172.16.1.11-20 (with source IP is webshield external interface and destination is Public zone)
case 2: nmap -sT -P0 -p 21,25 172.16.1.5 (with source IP is webshield external interface and destination is management console)

Command for rule 7
nmap -sS -P0 202.30.245.161-4 (with source IP is webshield external interface)

Command for rule 8
nmap -sT -P0 172.16.1.12 (with destination IP is SMTP mail relay)

Command for rule 9
nmap -sU -P0 172.16.1.13 (with destination IP is DNS server)

Command for rule 10
nmap -sU -P0 202.30.245.161-4 (with source IP is DNS server)

Command for rule 11
nmap -sT -P0 172.16.1.10-11 (with destination IP is Public Web server)

Command for scanning with source TCP port 20 and destination port >1023
nmap -sS -P0 -p 1023-2023 -g 20 172.16.1.11-20

Command for scanning with source UDP port 53
nmap -sU -P0 -g 53 172.16.1.13

Command for testing the DNS zone transfer
nmap -sT -P0 -p 53 172.16.1.13

Command of snoop for capturing event on UNIX
snoop -V -d le0 > trafficevent.log
where -V is log the detail information
-d is to specify which interface is used to receive packets &le0 is the device name of the network interface
The captured date will be redirected to the text file trafficevent.log

Command of tcpdump for capturing event of LINUX
tcpdump > trafficevent.log

## Cost and level of effort

The preparation work of auditing including preparation of test plan, meeting with user to gather information and installation of scanning tools is 2 man-days.
The estimated man-hour of scanning all rules and the functional test of firewall is about 10 man-hours. Suspension of service for scanning is recommended. The downtime will be scheduled from 8:00 p.m. to 6:00 a.m. During the downtime, no on-line purchasing service will be provided. The sale volume of this month may be affected slightly.
It takes 3 man-day to analysis the result and prepare the report.
One analyst/consultant will be dedicated to this assessment for 7 days.
So the cost for the auditing will be = US$1,000 * 7 = US$7,000.

## Result Analysis

Before analysing the result, let's have a look at the nmap command and its parameter. By default, port number 1-1023 will be scanned if not specify.

| | |
|---|---|
| -sT | scan using TCP connect scan |
| -sS | scan using TCP SYN scan |
| -sU | scan the UDP protocol |
| -g port number | scan using this source port number |
| -p port number | scan using this destination port number |
| -P0 | do not ping the host before scanning |

Detail about nmap please refer to www.insecure.org/nmap

Not all the captured results will be all showed. Five scanning results are showed below together with the explanations.
1) Rule 9.Traffic captured in DNS server. It is scanned using UDP scanning method. The direction of traffic is from outside to DNS server.
2) Rule 7.Traffic captured by sniffer. It is scanned using TCP SYN scanning method.The direction of traffic is from Webshield to outside.
3) Rule 8.Traffic captured in SMTP server. It is sacnned using TCP Connect method.The direction of traffic is from outside to SMTP mail relay.
4) Rule 3.Traffic captured in external database server. It is also scanned using TCP Connect method. The direction of traffic is from Web server to external database server.
5) Rule 11.Traffic captured in Web server. It is also scanned using TCP Connect method.The direction of traffic is from outside to Web server.

### Rule 9 Traffic captured in DNS server

The result below is the traffic generated by the nmap in order to scan the UDP port 53, DNS service. The length of the UDP packet is 8 bytes. It is because the scanning method of nmap for UDP is sending a UDP packet with 0 byte UDP data. The size of UDP header is 8 bytes.
From the result, only the packet with destination UDP port 53 can pass through the firewall to the DNS server.

```
201.70.246.168 ->172.16.1.13    ETHER Type=0800 (IP), size = 60 bytes
201.70.246.168 -> 172.16.1.13   IP   D=172.16.1.13 S=201.70.246.168 LEN=28,ID=12846
201.70.246.168 -> 172.16.1.13    UDP D=53 S=40781 LEN=8
201.70.246.168 -> 172.16.1.13    DNS C port=40781
```

**Rule 7 Traffic captured by sniffer**

The sniffer captures packets with TCP port 80, 443 and 25 & 21 the Syn flag up. It indicates that the TCP packet with port 80, 443 and 25 from Webshield to Internet can pass through the firewall. Normally, if the destination can be reached, "Acknowledgement" packet from destination host and packet with Reset flag up from nmap will be captured. But the firewall is isolated, no such packet can be captured. Also, the data of ether header is omitted as it does not provide any relevant information.

From the result, only the packet with destination TCP port 21,25,80 and 433 from Webshield can pass through the firewall to outside.

```
----------------------------------------------------------------------------------------------------
IP:     ----- IP Header -----
IP:
IP:    Version = 4
IP:    Header length = 20 bytes
IP:    Type of service = 0x00
IP:              xxx. .... = 0 (precedence)
IP:              ...0 .... = normal delay
IP:              .... 0... = normal throughput
IP:              .... .0.. = normal reliability
IP:    Total length = 40 bytes
IP:    Identification = 2587
IP:    Flags = 0x0
IP:              .0.. .... = may fragment
IP:              ..0. .... = last fragment
IP:    Fragment offset = 0 bytes
IP:    Time to live = 50 seconds/hops
IP:    Protocol = 6 (TCP)
IP:    Header checksum = 66db
IP:    Source address = 172.16.1.2, 172.16.1.2
IP:    Destination address = 202.30.245.161, 202.30.245.161
IP:    No options
IP:
TCP:    ----- TCP Header -----
TCP:
TCP:   Source port = 20
TCP:   Destination port = 80
TCP:   Sequence number = 680862004
TCP:   Acknowledgement number = 0
TCP:   Data offset = 20 bytes
TCP:   Flags = 0x02
TCP:             ..0. .... = No urgent pointer
TCP:             ...0 .... = No acknowledgement
TCP:             .... 0... = No push
TCP:             .... .0.. = No reset
TCP:              .... ..1. = Syn
TCP:             .... ...0 = No Fin
TCP:   Window = 1024
TCP:   Checksum = 0x6b8d
TCP:   Urgent pointer = 0
```

```
TCP:   No options
TCP:

----------------------------------------------------------------------------------------------------
IP:     ----- IP Header -----
IP:
IP:    Version = 4
IP:    Header length = 20 bytes
IP:    Type of service = 0x00
IP:           xxx. .... = 0 (precedence)
IP:           ...0 .... = normal delay
IP:           .... 0... = normal throughput
IP:           .... .0.. = normal reliability
IP:    Total length = 40 bytes
IP:    Identification = 2587
IP:    Flags = 0x0
IP:           .0.. .... = may fragment
IP:           ..0. .... = last fragment
IP:    Fragment offset = 0 bytes
IP:    Time to live = 50 seconds/hops
IP:    Protocol = 6 (TCP)
IP:    Header checksum = 66db
IP:    Source address = 172.16.1.2, 172.16.1.2
IP:    Destination address = 202.30.245.161, 202.30.245.161
IP:    No options
IP:
TCP:    ----- TCP Header -----
TCP:
TCP:   Source port = 20
TCP:   Destination port = 443
TCP:   Sequence number = 680862004
TCP:   Acknowledgement number = 0
TCP:   Data offset = 20 bytes
TCP:   Flags = 0x02
TCP:           ..0. .... = No urgent pointer
TCP:           ...0 .... = No acknowledgement
TCP:           .... 0... = No push
TCP:           .... .0.. = No reset
TCP:           .... ..1. = Syn
TCP:           .... ...0 = No Fin
TCP:   Window = 1024
TCP:   Checksum = 0x6b8d
TCP:    Urgent pointer = 0
TCP:   No options
TCP:

----------------------------------------------------------------------------------------------------
IP:     ----- IP Header -----
IP:
IP:    Version = 4
IP:    Header length = 20 bytes
IP:    Type of service = 0x00
IP:           xxx. .... = 0 (precedence)
IP:           ...0 .... = normal delay
IP:           .... 0... = normal throughput
IP:           .... .0.. = normal reliability
IP:    Total length = 40 bytes
IP:    Identification = 93
IP:    Flags = 0x0
IP:           .0.. .... = may fragment
```

```
IP:           ..0. .... = last fragment
IP:    Fragment offset = 0 bytes
IP:    Time to live = 50 seconds/hops
IP:    Protocol = 6 (TCP)
IP:    Header checksum = 7099
IP:    Source address = 172.16.1.2, 172.16.1.2
IP:    Destination address = 202.30.245.161, 202.30.245.161
IP:    No options
IP:
TCP:   ----- TCP Header -----
TCP:
TCP:   Source port = 20
TCP:   Destination port = 25
TCP:   Sequence number = 680862004
TCP:   Acknowledgement number = 0
TCP:   Data offset = 20 bytes
TCP:   Flags = 0x02
TCP:          ..0. .... = No urgent pointer
TCP:          ...0 .... = No acknowledgement
TCP:          .... 0... = No push
TCP:          .... .0.. = No reset
TCP:          .... ..1. = Syn
TCP:          .... ...0 = No Fin
TCP:   Window = 1024
TCP:   Checksum = 0x6fd9
TCP:   Urgent pointer = 0
TCP:   No options
TCP:

IP:    ----- IP Header -----
IP:
IP:    Version = 4
IP:    Header length = 20 bytes
IP:    Type of service = 0x00
IP:          xxx. .... = 0 (precedence)
IP:          ...0 .... = normal delay
IP:          .... 0... = normal throughput
IP:          .... .0.. = normal reliability
IP:    Total length = 40 bytes
IP:    Identification = 93
IP:    Flags = 0x0
IP:          .0.. .... = may fragment
IP:          ..0. .... = last fragment
IP:    Fragment offset = 0 bytes
IP:    Time to live = 50 seconds/hops
IP:    Protocol = 6 (TCP)
IP:    Header checksum = 7099
IP:    Source address = 172.16.1.2, 172.16.1.2
IP:    Destination address = 202.30.245.161, 202.30.245.161
IP:    No options
IP:
TCP:   ----- TCP Header -----
TCP:
TCP:   Source port = 20
TCP:   Destination port = 21
TCP:   Sequence number = 680862004
TCP:   Acknowledgement number = 0
TCP:   Data offset = 20 bytes
TCP:   Flags = 0x02
TCP:          ..0. .... = No urgent pointer
```

```
TCP:          ...0 .... = No acknowledgement
TCP:          .... 0... = No push
TCP:          .... .0.. = No reset
TCP:          .... ..1. = Syn
TCP:          .... ...0 = No Fin
TCP:  Window = 1024
TCP:  Checksum = 0x6fd9
TCP:  Urgent pointer = 0
TCP:  No options
TCP:
```

### Rule 8 Traffic capture in SMTP mail relay

The following is the logged event scanning by nmap using TCP connect method. The QUIT command is issued from nmap after the three-way handshake is completed to close the connection. The SMTP mail relay sends "FIN flag bit up" packet to close the connection. The nmap also sends "RST flag bit up" packet to close the connection.

From the result, only the packet with destination TCP port 25 can pass through the firewall to SMTP mail relay.

```
  202.70.246.168 -> 172.16.1.12    ETHER Type=0800 (IP), size = 62 bytes
  202.70.246.168 -> 172.16.1.12    IP  D=172.16.1.12 S=202.70.246.168 LEN=48, ID=685
  202.70.246.168 -> 172.16.1.12    TCP D=25 S=1056 Syn Seq=17022137 Len=0
Win=8760
  202.70.246.168 -> 172.16.1.12    SMTP C port=1056
_____
  172.16.1.12 -> 202.70.246.168    ETHER Type=0800 (IP), size = 58 bytes
  172.16.1.12 -> 202.70.246.168    IP  D=202.70.246.168 S=172.16.1.12 LEN=44,
ID=47925
  172.16.1.12 -> 202.70.246.168    TCP D=1056 S=25 Syn Ack=17022138
Seq=2186417350 Len=0 Win=8760
  172.16.1.12 -> 202.70.246.168    SMTP R port=1056
_____
  202.70.246.168 -> 172.16.1.12    ETHER Type=0800 (IP), size = 60 bytes
  202.70.246.168 -> 172.16.1.12    IP  D=172.16.1.12 S=202.70.246.168  LEN=40,
ID=692
  202.70.246.168 -> 172.16.1.12    TCP D=25 S=1056 Ack=2186417351 Seq=17022138
Len=0 Win=8760
  202.70.246.168 -> 172.16.1.12    SMTP C port=1056
_____
  172.16.1.12 -> 202.70.246.168    ETHER Type=0800 (IP), size = 134 bytes
  172.16.1.12 -> 202.70.246.168    IP  D=202.70.246.168 S=172.16.1.12 LEN=120,
ID=47931
  172.16.1.12 -> 202.70.246.168    TCP D=1056 S=25 Ack=17022138 Seq=2186417351
Len=80 Win=8760
  172.16.1.12 -> 202.70.246.168    SMTP R port=1056 220 exsmtp ESMTP Sendm
_____
```

Three-way handshake completed.

```
  202.70.246.168 -> 172.16.1.12    ETHER Type=0800 (IP), size = 60 bytes
  202.70.246.168 -> 172.16.1.12    IP  D=172.16.1.12 S=202.70.246.168 LEN=40,
ID=696
  202.70.246.168 -> 172.16.1.12    TCP D=25 S=1056 Fin Ack=2186417431
Seq=17022144 Len=0 Win=8680
  202.70.246.168 -> 172.16.1.12    SMTP C port=1056
_____
 202.70.246.168 -> 172.16.1.12     ETHER Type=0800 (IP), size = 60 bytes
```

202.70.246.168 -> 172.16.1.12 IP D=172.16.1.12 S=202.70.246.168 LEN=46, ID=695
202.70.246.168 -> 172.16.1.12 TCP D=25 S=1056 Ack=2186417431 Seq=17022138 Len=6 Win=8680
202.70.246.168 -> 172.16.1.12 SMTP C port=1056 **QUIT\r\n**

---

172.16.1.12 -> 202.70.246.168 ETHER Type=0800 (IP), size = 54 bytes
172.16.1.12 -> 202.70.246.168 IP D=202.70.246.168 S=172.16.1.12 LEN=40, ID=47932
172.16.1.12 -> 202.70.246.168 TCP D=1056 S=25 Ack=17022144 Seq=2186417431 Len=0 Win=8760
172.16.1.12 -> 202.70.246.168 SMTP R port=1056

---

172.16.1.12 -> 202.70.246.168 ETHER Type=0800 (IP), size = 83 bytes
172.16.1.12 -> 202.70.246.168 IP D=202.70.246.168 S=172.16.1.12 LEN=69, ID=47933
172.16.1.12 -> 202.70.246.168 TCP D=1056 S=25 Ack=17022144 Seq=2186417431 Len=29 Win=8760
172.16.1.12 -> 202.70.246.168 SMTP R port=1056 221 exsmtp closing con

---

172.16.1.12 -> 202.70.246.168 ETHER Type=0800 (IP), size = 54 bytes
172.16.1.12 -> 202.70.246.168 IP D=202.70.246.168 S=172.16.1.12 LEN=40, ID=47934
172.16.1.12 -> 202.70.246.168 TCP D=1056 S=25 **Fin** Ack=17022144 Seq=2186417460 Len=0 Win=8760
172.16.1.12 -> 202.70.246.168 SMTP R port=1056

---

202.70.246.168 -> 172.16.1.12 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 -> 172.16.1.12 IP D=172.16.1.12 S=202.70.246.168 LEN=40, ID=704
202.70.246.168 -> 172.16.1.12 TCP D=25 S=1056 **Rst** Seq=17022145 Len=0 Win=0
202.70.246.168 -> 172.16.1.12 SMTP C port=1056

---

202.70.246.168 -> 172.16.1.12 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 -> 172.16.1.12 IP D=172.16.1.12 S=202.70.246.168 LEN=40, ID=705
202.70.246.168 -> 172.16.1.12 TCP D=25 S=1056 Rst Seq=17022144 Len=0 Win=0
202.70.246.168 -> 172.16.1.12 SMTP C port=1056

---

### Rule 3 Traffic captured in external database server

The following is the logged event scanning by nmap using TCP connect method. A "FIN flag bit up" is issued from nmap after the three-way handshake is completed to close the connection.
From the result, only the packet with source IP of Web server and destination TCP port 21 can pass through the firewall to external database server.

172.16.1.10 -> 172.16.4.10 ETHER Type=0800 (IP), size = 62 bytes
172.16.1.10 ->172.16.4.10 IP D=172.16.4.10 S=172.16.1.10 LEN=48, ID=1599
172.16.1.10 ->172.16.4.10 TCP D=**21** S=1084 **Syn** Seq=1111666277 Len=0 Win=8760
172.16.1.10 -> 172.16.4.10 FTP C port=1084

---

172.16.4.10 -> 172.16.1.10 ETHER Type=0800 (IP), size = 58 bytes
172.16.4.10 ->172.16.1.10 IP D=172.16.1.10 S=172.16.4.10 LEN=44, ID=17620
172.16.4.10 -> 172.16.1.10 TCP D=1084 S=21 Syn Ack=1111666278 Seq=2770785657 Len=0 Win=8760
172.16.4.10 -> 172.16.1.10 FTP R port=1084

---

172.16.1.10 -> 172.16.4.10 ETHER Type=0800 (IP), size = 60 bytes
172.16.1.10 -> 172.16.4.10 IP D=172.16.4.10 S=172.16.1.10 LEN=40, ID=1600
172.16.1.10->172.16.4.10 TCP D=21 S=1084 Ack=2770785658 Seq=1111666278 Len=0 Win=8760
172.16.1.10 -> 172.16.4.10 FTP C port=1084

---

172.16.4.10 -> 172.16.1.10 ETHER Type=0800 (IP), size = 94 bytes
172.16.4.10 ->172.16.1.10 IP D=172.16.1.10 S=172.16.4.10 LEN=80, ID=17621
172.16.4.10-> 172.16.1.10 TCP D=1084 S=21 Ack=1111666278 Seq=2770785658 Len=40 Win=8760
172.16.4.10 -> 172.16.1.10 FTP R port=1084 220 exdb FTP server

---

Three-way handshake completed.

172.16.1.10 -> 172.16.4.10 ETHER Type=0800 (IP), size = 60 bytes
172.16.1.10->172.16.4.10 IP D=172.16.4.10 S=172.16.1.10 LEN=40, ID=1601
172.16.1.10 -> 172.16.4.10 TCP D=21 S=1084 **Rst** Seq=1111666278 Len=0 Win=0
172.16.1.10 -> 172.16.4.10 FTP C port=1084

---

172.16.1.10 -> 172.16.4.10 ETHER Type=0800 (IP), size = 60 bytes
172.16.1.10 -> 172.16.4.10 IP D=172.16.4.10 S=172.16.1.10 LEN=40, ID=1602
172.16.1.10 -> 172.16.4.10 TCP D=21 S=1084 Rst Seq=1111666278 Len=0 Win=0
172.16.1.10 -> 172.16.4.10 FTP C port=1084

---

**Rule 11 Traffic captured in Web server**

The following is the logged event scanning by nmap using TCP connect method. The Web server detects that the HTTP connection is bad request after the three-way handshake is completed. So it sends a "FIN flag bit up" packet to close the connection. The nmap also sends "RST flag bit up" packet to close the connection.

From the result, only the packet with destination TCP port 80 can pass through the firewall to Web server.

202.70.246.168 -> 172.16.1.10 ETHER Type=0800 (IP), size = 62 bytes
202.70.246.168 -> 172.16.1.10 IP D=172.16.1.10 S=202.70.246.168 LEN=48, ID=676
202.70.246.168 -> 172.16.1.10 TCP D=**80** S=1054 **Syn** Seq=16845584 Len=0 Win=8760
202.70.246.168 -> 172.16.1.10 HTTP C port=1054

---

172.16.1.10 -> 202.70.246.168 ETHER Type=0800 (IP), size = 58 bytes
172.16.1.10-> 202.70.246.168 IP D=202.70.246.168 S=172.16.1.10 LEN=44, ID=47923
172.16.1.10 -> 202.70.246.168 TCP D=1054 S=80 Syn Ack=16845585 Seq=2186216788 Len=0 Win=8760
172.16.1.10 -> 202.70.246.168 HTTP R port=1054

---

202.70.246.168 -> 172.16.1.10 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168->172.16.1.10 IP D=172.16.1.10 S=202.70.246.168 LEN=40, ID=688
202.70.246.168->172.16.1.10 TCP D=80 S=1054 Ack=2186216789 Seq=16845585 Len=0 Win=8760
202.70.246.168 -> 172.16.1.10 HTTP C port=1054

---

172.16.1.10 -> 202.70.246.168 ETHER Type=0800 (IP), size = 54 bytes
172.16.1.10->202.70.246.168 IP D=202.70.246.168 S=172.16.1.10 LEN=40, ID=47928
172.16.1.10->202.70.246.168 TCP D=1054 S=80 Ack=16845586 Seq=2186216789 Len=0 Win=8760

172.16.1.10 -> 202.70.246.168 HTTP R port=1054

---

172.16.1.10 -> 202.70.246.168 ETHER Type=0800 (IP), size = 176 bytes
172.16.1.10 ->202.70.246.168 IP D=202.70.246.168 S=172.16.1.10 LEN=162, ID=47929
172.16.1.10 -> 202.70.246.168 TCP D=1054 S=80 Ack=16845586 Seq=2186216789 Len=122 Win=8760
172.16.1.10 -> 202.70.246.168 HTTP **HTTP/1.0 400 Bad Request**

---

172.16.1.10 -> 202.70.246.168 ETHER Type=0800 (IP), size = 54 bytes
172.16.1.10 -> 202.70.246.168 IP D=202.70.246.168 S=172.16.1.10 LEN=40, ID=47930
172.16.1.10 -> 202.70.246.168 TCP D=1054 S=80 **Fin** Ack=16845586 Seq=2186216911 Len=0 Win=8760
172.16.1.10 -> 202.70.246.168 HTTP R port=1054

---

202.70.246.168 -> 172.16.1.10 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 ->172.16.1.10 IP D=172.16.1.10 S=202.70.246.168 LEN=40, ID=693
202.70.246.168 -> 172.16.1.10 TCP D=80 S=1054 **Rst** Seq=16845586 Len=0 Win=0
202.70.246.168 -> 172.16.1.10 HTTP C port=1054

---

202.70.246.168 -> 172.16.1.10 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 ->172.16.1.10 IP D=172.16.1.10 S=202.70.246.168 LEN=40, ID=694
202.70.246.168 ->172.16.1.10 TCP D=80 S=1054 **Rst** Seq=16845586 Len=0 Win=0
202.70.246.168 -> 172.16.1.10 HTTP C port=1054

---

## Assessment conclusion and recommendation

From all the scanning results, the firewall is actually implementing GIAC Enterprise's security policy but the DNS zone transfer. From scanning results the pakect with destination TCP port 53 can pass through the firewall to the DNS server, which should be denied.The result is listed below.

202.70.246.168 -> 172.16.1.13 ETHER Type=0800 (IP), size = 62 bytes
202.70.246.168 -> 172.16.1.13 IP D=172.16.1.13 S=202.70.246.168 LEN=48, ID=810
202.70.246.168 -> 172.16.1.13 **TCP D=53** S=1055 **Syn** Seq=2646779711 Len=0 Win=8760
202.70.246.168 -> 172.16.1.13 DNS C port=1055

---

172.16.1.13 -> 202.70.246.168 ETHER Type=0800 (IP), size = 58 bytes
172.16.1.13 ->202.70.246.168 IP D=202.70.246.168 S=172.16.1.13 LEN=44, ID=24193
172.16.1.13 -> 202.70.246.168 TCP D=1055 S=53 Syn Ack=2646779712 Seq=437581773 Len=0 Win=8760
172.16.1.13 -> 202.70.246.168 DNS R port=1055

---

202.70.246.168 -> 172.16.1.13 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 -> 172.16.1.13 IP D=172.16.1.13 S=202.70.246.168 LEN=40, ID=811
202.70.246.168 -> 172.16.1.13 TCP D=53 S=1055 Ack=437581774 Seq=2646779712 Len=0 Win=8760
202.70.246.168 -> 172.16.1.13 DNS C port=1055

---

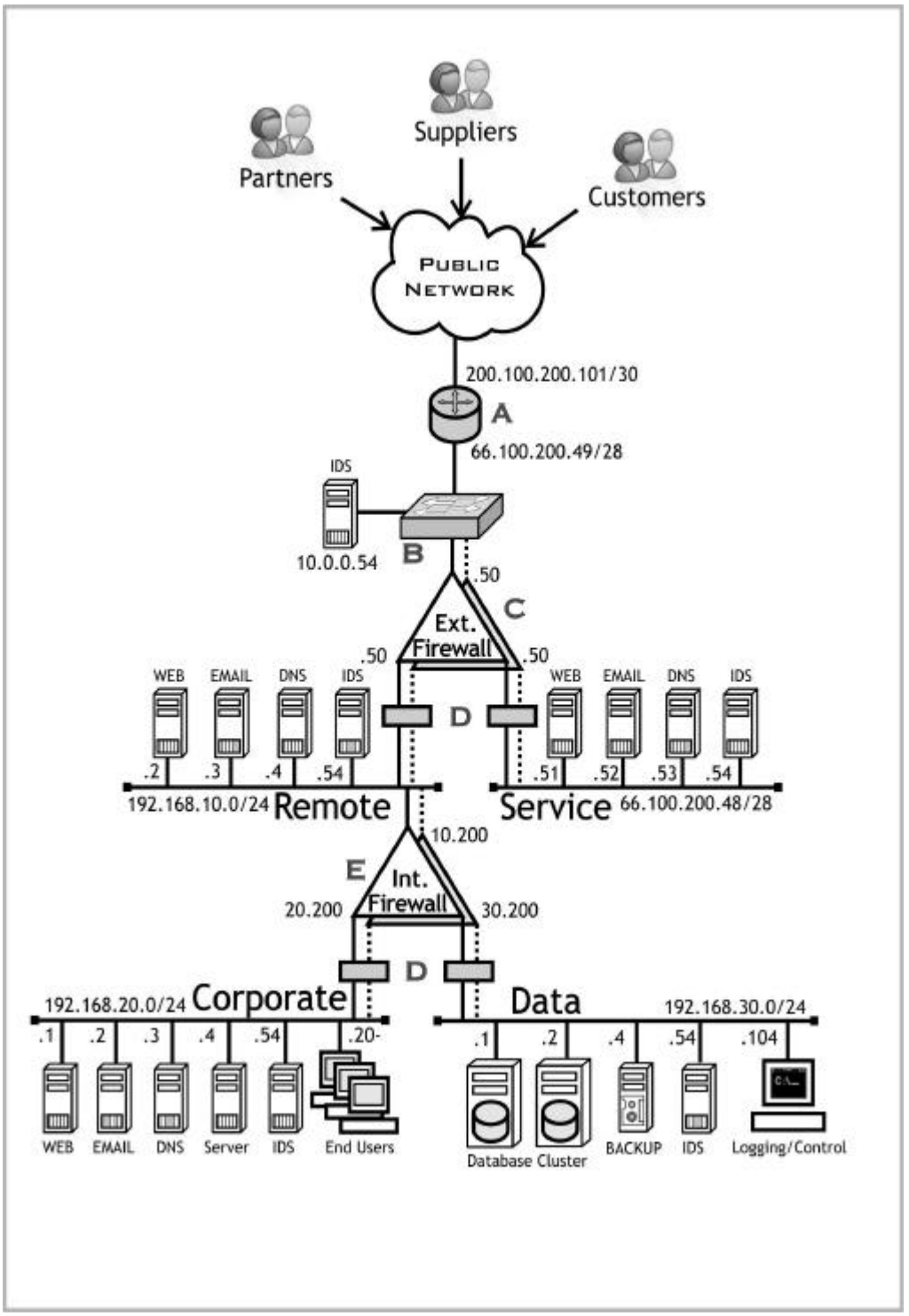
202.70.246.168 -> 172.16.1.13 ETHER Type=0800 (IP), size = 60 bytes
202.70.246.168 -> 172.16.1.13 IP D=172.16.1.13 S=202.70.246.168 LEN=40, ID=812
202.70.246.168 -> 172.16.1.13 TCP D=53 S=1055 Rst Seq=2646779712 Len=0 Win=0
202.70.246.168 -> 172.16.1.13 DNS C port=1055

---

After the invetigation, the DNS service pre-defined in firewall includes two services :UDP port 53 & TCP port 53. It is recommended to remove the service TCP port 53 manually from the DNS service.

## Assignment 4 Design Under Fire

http://www.giac.org/practical/KELLY_FULLER_GCFWpdf.zip




### 1) Vulnerability found on Watchguard Firebox 4500

Description
Dynamic VPN Configuration Protocol service (DVCP) in Watchguard Firebox

firmware 5.x.x allows remote attackers to cause a denial of service (crash) via a malformed packet containing tab characters to TCP port 4110. (Refer to URLhttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1046)

Impact

Rebooting the firewall is necessary for the DVCP service to function again.

References
CAN-2002-1046 (under review)
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1046
BID:5186
URL:http://www.securityfocus.com/bid/5186
XF:firebox-dvcp-dos(9509)
URL:http://www.iss.net/security_center/static/9509.php
VULNWATCH:20020709 [VulnWatch] KPMG2002030: Watchguard Firebox Dynamic VPN Configuration Protocol DoS
URL:http://archives.neohapsis.com/archives/vulnwatch/2002-q3/0012.html

## Tools used to carry out the attack

The Nessus tools will be used to carry out the attack. The reason why Nessus tools are chosen is that it provides a full rich subroutines. Although no exploit tools or script is available on the Internet, user can utilize such subroutines to develop the plug-in by themselves. The following codes are developed based on the vulnerability described above. Details on how to use and develop the plug-in of Nessus, please refer to www.nessus.org.

```
ip = forge_ip_packet(    ip_v : 4,
                         ip_hl : 5,
                          ip_tos : 0,
                         ip_len : 20,
                          ip_id : 0xF1C,
                         ip_p : IPPROTO_TCP,
                         ip_ttl : 255,
                          ip_off : 0,
                          ip_src : addr);

tcpip = forge_tcp_packet(     ip          : ip,
                              th_sport : 14000,
                              th_dport : 4110,
                               th_flags : TH_ACK,
                               th_seq     : 0xF1C,
                               th_ack     : 0,
                               th_x2      : 0,
                               th_off     : 5,
                               th_win     : 2048,
                              th_urp     : 0
                               data       :                          );
```

send_packet(tcpip, pcap_active:FALSE) x 20; (The 'x' operator will repeat the send_packet 20 times)

**Result**

As the TCP flag in the TCP packet is configured to ACK, it can bypass the access list of the router and reach the firewall. The attack will be successful and the DVCP service will be crashed if the firmware have not been upgraded from 5.0 to 6.0.

**2) A denial of service attack**

DDOS attack will be designed as 50 systems are compromised. DDOS can launch attacks from many sources to the target. The intruder controls a list of masters.

Then masters will send the command to a large number of lists of daemons in order to carry out the attack to the target. The masters and daemons are installed in the system by intruder through the exploitation of vulnerability found on the compromised systems. Tribe FloodNet 2K (TFN2K) is used to carry out the DDOS attack. Master program will be installed in 5 compromised systems and daemons are installed in 45 compromised systems. One master controls nine daemons.

TFN2K can conduct different kinds of DOS attacks (TCP SYN flood, UDP flood, Teardrop etc) to the victim machine. It also can spoof the source IP address. And it is designed to work on UNIX based and Window NT systems.

**Countermeasure**

Honor speaking, there is no single solution to prevent against DDOS attack and no solution to stop the DDOS attack. Here are the suggestions to minimize the impact under the DDOS attack.

1) Implement network based intrusion detection system to detect the DOS attack.

2) Implement bandwidth management tools to control or limit the bandwidth consumed by traffic. For example, if the system is under UDP flood attack, the flooding traffic will be limited to the setting of the management tools for the UDP services.

3) Choose a firewall with detecting and dropping DOS attack features.

4) Harden the system in the DMZ and apply the latest security patch in order to prevent the intruder planting the DDOS master or daemon in the system.

5) Apply the anti IP spoofing rule in the access-list of the boundary router.

6)Coordinate with the ISP to monitor the traffic and alert the company when DDOS is occurred.

7) Develop contingency response plan when under DDOS attacks and seek the top management's approval and support.

8) Follow the CERT/CC and SANS recommendation. More details can be found in "Results of the Distributed-Systems Intruder Tools Workshop". (URL-http://www.cert.org/repots/dsit_workshop-final.html) "Consensus Roadmap for Defeating Distributed Denial of Service Attacks" (URL http://www.sans.org/ddos_roadmap.htm)

## 3) Attacking plan to compromise an internal system through the perimeter system

### General steps to compromise the system

1) Reconnaissance
It should include finding out the layout and network design of the perimeter and internal system, the brand name and version of the perimeter system and internal system.
2) Choose which system is the target to compromise.
3) Research the vulnerabilities of the perimeter system and internal target.
4) Design a process to compromise the internal target through the perimeter system based on the vulnerabilities found.

### Step 1: Reconnaissance

a) To find out the brand name of the internal mail system. A mail with a wrong recipient name can be sent to the mail system. An undeliverable message will be sent from the postmaster to alert sender. Normally the information of the brand name and even the version can be found in the return mail. The wrong mail address can be found in the Web site easily. Normally, some e-mail accounts are posted on the Web site for enquiry. For example, enquiry@giac.com is the enquiry account of GIAC.COM. The wrong mail address just omits one character, i.e. **enquir@giac.com**
The following is the return message from GIAC.COM. It shows that the internal mail system is Mircosoft Exchange server.

From: System Administrator <POSTMASTER@GIAC.COM>
To: benjaminlam@abc.com
Subject: Undeliverable:
Date: Thu, 24 Oct 2002 22:50:22 +0800
Your message
To: enquir@giac.com
Sent: Thu, 24 Oct 2002 22:40:45 +0800
did not reach the following recipient(s):
ENQUIR@GIAC.COM on Thu, 24 Oct 2002 22:50:19 +0800
The recipient name is not recognized
The MTS-ID of the original message is: c=us;a=
p=iss;l=VENUS0210241450VQVQV311
**MSEXCH:**IMS:iss:WATER:VENUS 0 (000C05A6) Unknown Recipient

b) To discover the brand name of SMTP mail relay
Use the command nslookup in LIUNX or UNIX platform to find out the public IP address of the mail server. Then use the telnet "IP address" 25 to connect to the server. A banner will show the brand name and even the version normally.
As the SMTP proxy of firewall responds to the telnet command but not the SMTP mail relay, only the brand name of firewall will be found. It is a Watchguard firewall.

c) To discover the brand name of public Web server

Normally, we can use the following steps to find out the brand name of Web server.
1) Telnet www.giac.com 80
2) GET /index.html HTTP /1.0

The returned result is something like that.

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 19 Nov 2002 01:17:27 GMT
Connection: close
Content-Length: 407
Content-Type: text/html
<html><head><title>Error 400</title>

The Web server should return a "bad request" message together with the HTTP header information. The brand name and version will be included in the HTTP header.

But as the firewall is proxy type, the telnet to port 80 request will be handled by the firewall not directly by the Web server. The following steps cannot discover the brand name and version of Web server. The only way to get the information of Web server is using the browser to view the Web page and get the HTTP header by the sniffer. Usually, brand name and version will be found out in the HTTP headers.

**Step 2: Choose which system is the target to compromise**

Mail system will be chosen. Reasons for choosing a mail system are listed as below.
a) Which internal systems and how they can communicate to Internet depend on the security policies of company. It will spend a lot of time to research or find out the details of policies. But one policy is almost the same for all companies. if they want to send and receive Internet emails. The internal mail system must be allowed to communicate to Internet or SMTP mail relay in the DMZ. It can save a lot of time to find out the details of policies.
b) The brand name and version of internal mail system and/or SMTP mail relay are easier to detect when comparing to other internal systems.

**Step 3: Vulnerability Research**

Vulnerabilities of mail server, firewall, web server and Window 2000 server (the OS of the mail server) will be searched.

a) Vulnerability found on SMTP proxy of Watchguard firewall
Description
SMTP proxy in WatchGuard Firebox (2500 and 4500) 4.5 and 4.6 allows a remote attacker to bypass firewall filtering via a base64 MIME encoded email attachment whose boundary name ends in two dashes.
(Refer to URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0692)

Impact
This makes it possible for a remote user to send attachments such as functional vbscripts in email, and bypass filtering of the firewall.
(Refer to URL http://www.securityfocus.com/bid/2855)

References
CVE-2001-0692
URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0692
XF:firebox-smtp-bypass-filter(6682)
URL:http://www.iss.net/security_center/static/6682.php
BID:2855
URL:http://www.securityfocus.com/bid/2855

b) Vulnerabilities (two) found on IIS Web server

Description:
Buffer overflow in the chunked encoding transfer mechanism in Internet Information Server (IIS) 4.0 and 5.0 Active Server Pages allows attackers to cause denial of service or execute arbitrary code. (Refer to URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0079)

Impact
An intruder can interrupt the ordinary operation of a vulnerable IIS server or execute arbitrary code with the privileges of ASP ISAPI extension, ASP.DLL. On IIS 4.0, intruder will take full administrative control as ASP.DLL runs as part of the operating system. On IIS 5.0, ASP.DLL runs with the privileges of the IWAM_computername account. (Refer to URL http://www.kb.cert.org/vuls/id/610291)

References
CAN-2002-0079 (under review)
URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0079
BUGTRAQ:20020410 Windows 2000 and NT4 IIS .ASP Remote Buffer Overflow
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=101846993304518&w=2
MS:MS02-018
URL:http://www.microsoft.com/technet/security/bulletin/ms02-018.asp
CERT:CA-2002-09
URL:http://www.cert.org/advisories/CA-2002-09.html
CISCO:20020415 Microsoft IIS Vulnerabilities in Cisco Products - MS02-018
URL:http://www.cisco.com/warp/public/707/Microsoft-IIS-vulnerabilities-MS02-018.shtml

The following exploit code is copied from the SecurityFocus Web site.(URL http://www.securityfocus.com/bid/4485)
Using a utility such as telnet or netcat:

**********Begin Session**********
POST /iisstart.asp HTTP/1.1

Accept: */*
Host: eeye.com
Content-Type: application/x-www-form-urlencoded
Transfer-Encoding: chunked

10
PADPADPADPADPADP
4
DATA
4
DEST
0
[enter]
[enter]
**********End Session**********
Description
Buffer overflow in the ism.dll ISAPI extension that implements HTR scripting in Internet Information Server (IIS) 4.0 and 5.0 allows attackers to cause a denial of service or execute arbitrary code via HTR requests with long variable names. (Refer to URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0071)

Impact
An intruder can interrupt the normal operation of the IIS server. In addition, an intruder may be able to use this vulnerability to execute arbitrary code with the privileges of the HTR ISAPI extension.
On IIS4.0, this permits administrative control of the operating system. On IIS 5.0 and 5.1, this permits access with the privileges of the IWAM_comptuernamed account. (Refer to URL http://www.kb.cert.org/vuls/id/363715)

References
CAN-2002-0071 (under review)
URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0071
ATSTAKE:A041002-1
URL:http://www.atstake.com/research/advisories/2002/a041002-1.txt
BUGTRAQ:20020411 KPMG-2002010: Microsoft IIS .htr ISAPI buffer overrun
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=101854087828265&w=2
VULNWATCH:20020411 [VulnWatch] KPMG2002010: Microsoft IIS .htr ISAPI buffer overrun
MS:MS02-018
URL:http://www.microsoft.com/technet/security/bulletin/ms02-018.asp
CERT:CA-2002-09
URL:http://www.cert.org/advisories/CA-2002-09.html
CISCO:20020415 Microsoft IIS Vulnerabilities in Cisco Products - MS02-018
URL:http://www.cisco.com/warp/public/707/Microsoft-IIS-vulnerabilities-MS02-018.shtml

c) Vulnerability found on Microsoft Windows 2000 server

Description
Buffer overflow in SMB protocol in Microsoft Windows NT, Windows 2000, and Windows XP allows attackers to cause denial of service via a SMB_COM_TRANSACTION packet with a request for the (1) NetShareEnum, (2) NetServerEnum2, or (3)NetServerEnum3, "Unchecked Buffer in Network Share Provider Can Lead to Denial of Service".
(Refer to URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0724)

Impact
It will cause denial of service to the server. It may also be possible to execute arbitrary code and gain local access to the vulnerable system.

References
CAN-2002-0724 (under review)
URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0724
BUGTRAQ:20020822 CORE-20020618: Vulnerabilities in Windows SMB (DoS)
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=103011556323184&w=2
BID:5556
http://online.securityfocus.com/bid/5556
MS:MS02-045
URL:http://www.microsoft.com/technet/security/bulletin/ms02-045.asp
CERT-VN:VU#311619
URL:http://www.kb.cert.org/vuls/id/311619
CERT-VN:VU#342243
URL:http://www.kb.cert.org/vuls/id/342243
CERT-VN:VU#250635
URL:http://www.kb.cert.org/vuls/id/250635

## Step 4: The attacking process and result

Firstly, I will try to do is to find out whether any SMTP mail relay has been implemented and the brand name and version of SMTP mail relay if it exists. But due to the proxy type of firewall, no information can be found.
Then, vulnerability of firewall will be researched and I will try to exploit such vulnerability, if any, to compromise the perimeter system or even the internal system.
Two vulnerabilities are found. One is about SMTP proxy service, the other is Dynamic VPN Configuration Protocol (DVCP) service. But such vulnerabilities cannot be used to compromise the system protected by firewall. It is because vulnerability on DVCP only cause the denial of service and vulnerability on SMTP relay only can bypass the checking on attachment.
The next step is to trying to use the public access Web server as "stepping stone" to compromise the internal mail server. It is found that Internet mail can be sent to GIAC.COM through the Web page interface. So the Web server should be allowed at least to "talk" with the SMTP mail relay or even "talk"

with internal mail system directly.
Two vulnerabilities are found. But it should also be failed since the latest service patch (SP3 of Mircosoft server 2000) should be installed in the Web server. Vulnerabilities found can be fixed by the SP3.
In conclusion, it is failed to compromise the internal mail system.

## Reference


Solaris, Linux, HP-UX, Cisco, Window 2000 & Window NT hardening guide.
URL http://www.cisecurity.org/

Security best practice and implementation
URL http://www.cert.org/security-improvement/

Sun Solaris system security
URL http://www.sun.com/solutions/blueprints/browsesubject.html#security

Test the firewall system
URL http://www.cert.org/security-improvement/practices/p060.html

NMAP scanning tool
URL http://www.insecure.org/nmap/

NESSUS security assessment tool
URL http://www.neessus.org/

Results of the Distributed-Systems Intruder Tools Workshop
URL http://www.cert.org/repots/dsit_workshop-final.html

Consensus Roadmap for Defeating Distributed Denial of Service Attacks
URL http://www.sans.org/ddos_roadmap.htm

Vulnerability research Web site
URL http://www.securityfocus.com/
URL http://cve.mitre.org/
URL http://www.iss.net/security_center/

Lucent Security Management Server Administration Guide

Netscreen Concept & Examples ScreenOS Reference Guide