Global Information Assurance Certification Paper

SANS GIAC Firewalls, Perimeter Protection, and VPNs GCFW Practical Assignment

Version 1.5e

GIAC Enterprises Security Architecture, Security Policy and Audit

Carl Fortune
November 13, 2001

Table of Contents

Introduction

GEP is a growing Internet startup company that specializes in the sales of fortune cookie sayings to businesses that produce fortune cookies. The company is concerned about the security of their network. GIAC solicited bids from network security design firms and awarded the project to Secure Network Consulting a small highly skilled computer and network security firm.

Scope of Work

This project will be presented in four phases.

Assignment 1 - Proposed network architecture:
The proposed network architecture will define how each requirement set forth in the request for proposal (RFP) is to be met along with each assumption used.

Assignment 2 – Security Policies:
Security Policies will be thoroughly defined for the three primary components that are put in place to secure the network, the border router, the primary firewall and the virtual private network (VPN) solution.

Assignment 3 – Audit of the proposed network architecture:
This audit will consist of three phases. The first phase is the plan for the perimeter assessment. The second phase will be to implement the assessment plan and the third phase will be to analyze the data gained during the assessment to either reinforce the proposed security architecture or recommend changes to the proposal.

Assignment 4 – Design under fire:

Phase One (Assignment 1) - Security Architecture for GEP

The company:

GEP (GEP) is a growing Internet based startup company whose business is to sell fortune cookie sayings online. The projected gross income for the coming year is $200 million.

GEP Corporate

GEP's corporate location employees will need access to several servers such as login servers, file servers, FTP servers, DNS servers, mail server, WWW server and a database server. These servers must be protected from both internal and external threats to the extent possible.

Remote Workforce

GEP also has a traveling workforce. These employees will need a secure remote access solution to provide them with the same level of access that they would have if they were on-site at the GEP headquarters. The client laptops will be loaded with a VPN Secure Connectivity PGPvpn client. On the firewall, a trusted vpn link will be configured for the road warriors. This will give them access to everything they would have if they were sitting in GEP's corporate offices.

Merged Partners

GEP has recently completed a merger/acquisition with an international partner that will need the same access to the network as the internal employees. This fully merged partner will operate under the same security policy as the corporate headquarters location. This location will need secure, trusted access to the GEP internal network. The function of this business unit is to translate the fortune cookie sayings.

Suppliers

GEP also will provide a secure access solution for their suppliers. The Suppliers will need to upload new fortune cookie sayings to a FTP server within GEP's service network without the risk their product being stolen by eavesdropping on the Internet.

Customers

GEP's customers will be able to purchase fortune cookie sayings on-line via the web server in the Service network. The web server will query the SQL database, which will also be located in the Service network but will not be accessible by the world.

IP Address Space: (Assume that the 192.168.xxx.xxx addresses are legal and routable)

Interface	External	Internal
Border Router	192.168.50.71	192.168.25.97
Primary Firewall	192.168.25.98	10.0.2.129
Firewall Service Interface	10.0.7.1	
Firewall IDS Interface	10.0.6.1	
Mail Service Network	10.0.7.2	
DNS Service Network	10.0.7.3	
FTP Service Network	10.0.7.4	
Data Base Service Network	10.0.7.5	
WWW Service Network	10.0.7.6	
Internal Router	10.0.2.130	
Client Workstations	10.0.5.2-254	
Management Workstations	10.0.4.2-254	
Internal Servers	10.0.3.2-254	

Network Architecture

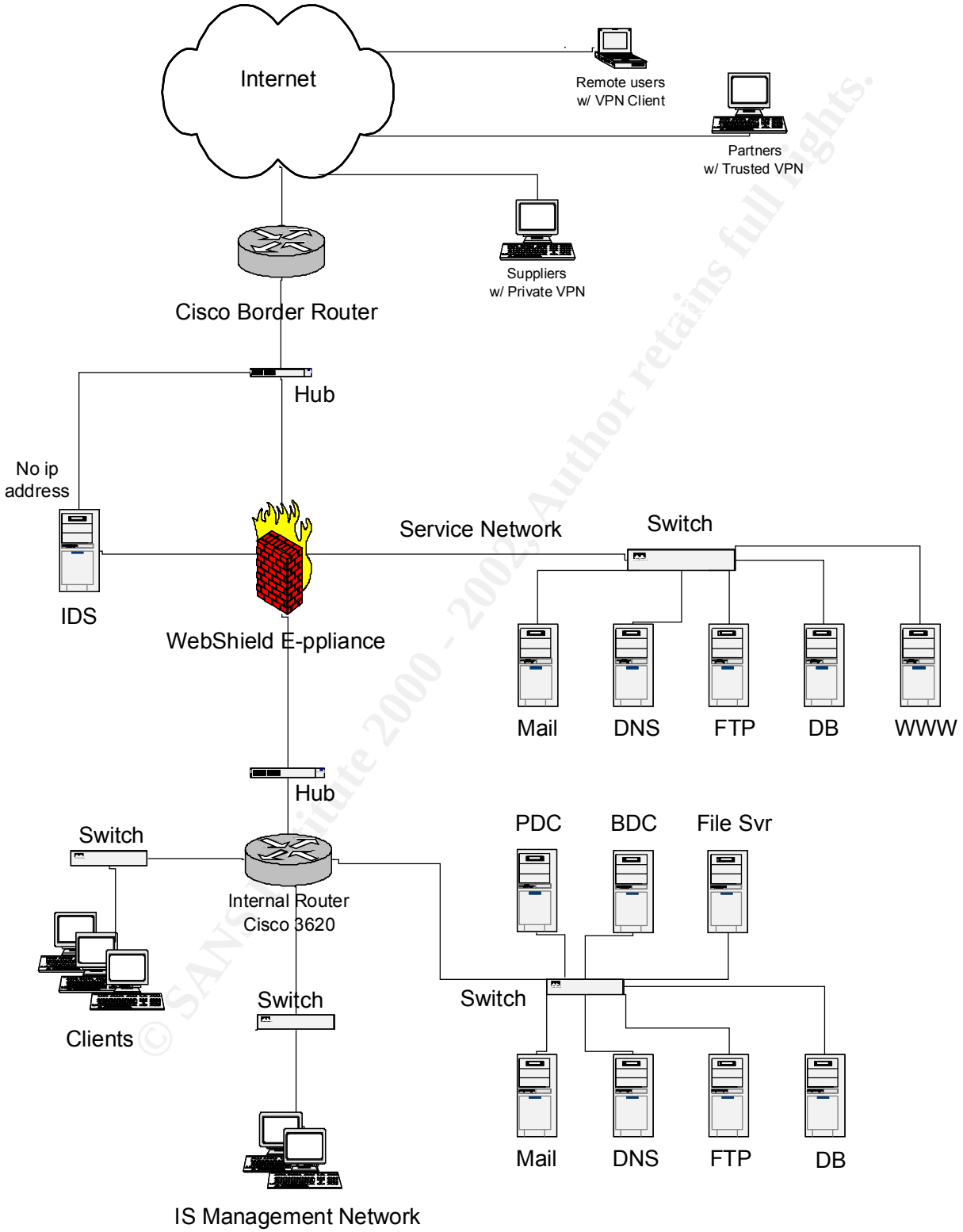


Figure 1

Border Router

In an effort to implement defense-in-depth, the GEP network will utilize a border router with several security features including access control lists as a filtering first defense against intrusion.

We will use a Cisco 3640 router for our border router. The Cisco 3640 was chosen to ensure that the size of the router does not create a bottleneck to or from the network. The 3640 comes with 8 MB of Flash SIMM memory and is expandable to 32 MB. Flash memory is non-volatile and is used to store copies of the Cisco Internetwork Operating System (Cisco IOS). The 3640 comes with 32 MB of DRAM and is expandable to 128 MB. This router will have a fairly heavy processing load due to the fact that this is an e-commerce site. The router, in addition to routing, will be used as the first line of defense and therefore will filter traffic based on access control lists. Using Access Controls lists place additional load on the router.

A Cisco router was chosen for the reliability and since there are a large number of Cisco routers in operation, finding IT staff that can maintain the routers will be easier. The Cisco IOS is capable of implementing several security features such as basic packet filtering, reflexive access lists, remote authentication servers, neighbor router authentication and tcp intercept.

Monitoring Hub/IDS

Downstream of the border router there will be a Cisco 12 port FastHub 400 where an intrusion detection sensor will sit. The intrusion detection system will consist of a box running Windows NT 4.0 and RealSecure version 6.0 Intrusion Detection software. The box will have two network interfaces. One will be connected to the primary firewall while the other with have all protocol bindings disabled with no ip address assigned and will be the sensor plugged into the hub in the DMZ. The Windows NT operating system will be hardened according to the SANS Securing Windows NT document.

Primary Firewall

The primary firewall chosen is a Network Associates WebShield 300 E-ppliance version 1.5 which is essentially a Sun Netra T1, running Solaris 2.5.6 with Gauntlet 5.5 running on top of it. The WebShield E-ppliance is an application level proxing firewall that also does packet filtering.

VPN Solution

The WebShield firewall will also be used to implement the VPN solution. Trusted VPN links will be provided for the merged Partners and the employees of GEP that need to access the internal network remotely. A Private VPN Link will be provided for the Suppliers.

Service Network Switch

As part of a defense-in-depth strategy, services to the external clients (suppliers, partners, customers) will be provided from a service network through a switch off one interface of the primary firewall. This configuration provides an extra layer of protection for the servers that will be accessed by the world. This Service network will include a web server for customer e-commerce, a FTP server for supplier and partner upload and download, a mail server for mail transfer, a database server that will be accessed by the web server and a DNS server that is participating in a split DNS solution.

The switch will be a Cisco Catalyst® 2950 Series, twelve port switch. This is an auto-sensing 10/100 Fast Ethernet switch. The initial network design will only place five devices on the switch. The extra ports will be turned off.

Service Network Services

The Service network DNS server will advertise only the addresses in the DMZ and Service network. The DNS server is a Sun Netra T1 running RedHat Linux 6.2 and Bind version 8.1.2.

The FTP server is a Dell 2400 running RedHat Linux 6.2 and WU-FTP version 2.6.0. This FTP server will allow the Suppliers to upload new fortunes to the server, while the Partners will use the FTP server to download fortunes for translation and then upload when complete. The WebShield FTP Proxy will be configured to control access to the FTP server.

The Web server will host the corporate web site, which will be used for e-commerce transactions. The Web server is a Dell 4400 running RedHat Linux 6.2 and Apache version 1.3. For the online sales of fortunes, the web server will utilize the database server, which will maintain a database of fortunes.

The mail server is a Dell 2400 running Windows 2000 server and Exchange 2000. This mail server will provide a drop point for incoming mail and will transfer mail between the internal mail server and the Internet. All of the servers in the service network will be hardened bastion hosts.

Internal Network

On the Internal network, the first network component downstream from the firewall will be another Cisco 12 port FastHub 400 that will be used for network monitoring. The internal router will be plugged into this hub. The internal router is a Cisco 3620 running IOS 12.1.

Internal Services

The following servers will be set up on the internal network:

PDC	Windows 2000 Server
BDC	Windows 2000 Server
File Server	Novell Netware 5.1
Mail	Exchange 2000 running on Windows 2000 Server
DNS	Linux 6.2 running Bind version 8.1.2
FTP	Linux 6.2 running wu-FTP
Database	Windows 2000 Professional running SQL

Split DNS

On the internal network, the DNS server will contain the database files for the internal networks and a database file for the service network. All other queries will be forwarded to the DNS server in the Service network. The Service network DNS will reply if information is cached other wise it will send the query to the Internet. The service network DNS will only contain a database file for the service network and a database for the root servers. All DNS resolver files on internal machines, including the primary firewall will be set to the internal DNS server.

Assignment 2 – Security Policies

General Security Policy for GEP

This policy is in-place to protect the "network" from sabotage and from inappropriate access, both intentional and accidental. The "network" is defined as all personal computers, workstations, servers, hubs, switches, cabling, data and routers. All data that traverses the corporate network is the property of the GEP. This includes all e-mail sent or received. All network traffic is subject to being monitored at any time.

This security policy is to be read and signed by all employees. An IS department person will explain the all parts of this security policy to employees before they sign.

Only IS department staff are allowed to configure personal computers, servers, routers switches and remote access solutions. New computer equipment and software will be purchased by or approved through the IS department.

The use of modems are not allowed on any personal computers on company premises. All remote access to the network will be through the remote access solution configured by the IS department. Personnel must request to be set up for remote access privileges through their department head who will forward the request to the IS department.

The operating system on all PCs will be Microsoft Windows NT 4.0, unless approved through the IS department.

The password policy is as follows:

Password History:	10 passwords
Maximum Password Age:	30 days
Minimum Password Age:	5 days
Minimum Password Length:	8 characters
Complexity Requirements:	Combination of upper and lower case use at least one special character and at least one number.
Account Lockout:	After 3 invalid sign-on attempts and until IS admin unlocks account.

Passwords should never be exchanged over the telephone or via e-mail.

All servers, hubs, switches and routers will be kept behind locked doors.

Department heads should review this policy every six months and any time a major business system change is planned. This policy is not meant to remain static. It needs to fit the business at hand and if any part of it inhibits the mission of this corporation it must be reevaluated.

Primary Firewall

The Sun WebShield 300 E-ppliance version 1.5 will be used for the primary firewall. The operating system is a hardened version of Solaris 2.5.6. The operating system hardening disables NFS, NIS, RPC several other services by renaming the startup scripts in /etc/rc2.d and /etc/rc3.d. It also disables IP packet forwarding, source routed packets and ICMP redirects. Since the OS hardening was done prior to purchase of the box, the white paper by Lance Spitzner "Armoring Solaris" was used as a reference to ensure that the hardening was appropriate.

The WebShield E-ppliance is managed via a secured Windows NT 4.0 workstation using the WebShield GUI interface.

The WebShield firewall uses several different methods to control which packets make it to the destination address.

The primary operation of this firewall is as an application level proxy. This means that each packet that comes from and is going to an application that WebShield has a proxy

for, goes all the way up the OSI model to the application level. The actual payload of each packet can be analyzed rather than just filtering on the packet headers. The proxy for the application understands the data in the payload. One of advantages of a proxy is that a packet cannot claim to be for a particular application and then do something else entirely. The packet is unwrapped by a small program that only understands the application that it is proxying for. If for example the packet claims to be for http on port 80, it will go to the http proxy and if it is actually something else the proxy will not know what to do with it and it will land in the bit bucket. Another example, which will be used by GEP, is the FTP Proxy. Using the Proxy firewall's FTP proxy, different instances of the proxy can be set up for different clients. And the rules will be customized depending on the client. Our Suppliers will go through the FTP proxy on their way to the FTP server. The proxy rules for the Suppliers will on allow requests coming from their source address to put or STOR files on the FTP server. The Customers of GEP, through another instance of the FTP proxy will only be able to download files.

Another advantage to using a Proxy firewall is virus scanning. Without bringing a packet up to the application layer, the payload cannot be scanned for viruses. The WebShield product can be set to perform content scanning to catch viruses. In addition, the WebShield firewall can log many different scenarios. Where as a packet filter can log each packet that matches a rule, the WebShield firewall can log source-routed packets, ICMP redirects, packets that contain malformed IP options and it will summarize the logs daily. The summarized reports can then be e-mailed to the administrator.

As mentioned above, not all applications have a proxy written for them. This could be the case if the application is a proprietary protocol or custom application. To avoid not being able to use an application, a Plug Proxy can be created for TCP based transport through the firewall. This is accomplished by setting up a different instance of a plug proxy for each application that does not have a Proxy. The Plug will listen on a specified port for that application. It will then check to see if there is a source or destination rule set to determine where the packet is allowed to go. The danger in the Plug Proxy is that the payload is not being analyzed since the application itself is not understood.

A third type of Proxy that WebShield offers is a Circuit Proxy. The Circuit Proxy works in the same way as the Plug Proxy except that authentication is supported.

Initial Configuration

The E-ppliance does not have a monitor or keyboard. The initial configuration is done through console connection to the Lights Out Management (LOM) port. Connection for this firewall was done using a Windows NT box running Terraterm. On the initial boot you are forced into the WebShield configuration. You can choose to then connect via web interface or through what they call the TUI interface. In either case the initial configuration takes care of defining the interfaces, the trusted and untrusted networks,

the ip address(s) of the management workstation(s) you will use, username and password for the management station login and DNS setup.

Once this initial configuration is completed and the firewall has been rebooted, connection from the management workstation can be made. The WebShield GUI is a JAVA application that can run on either Windows NT or Solaris. All of the following screen shot for the firewall and vpn setup are from the management GUI.

Packet filtering

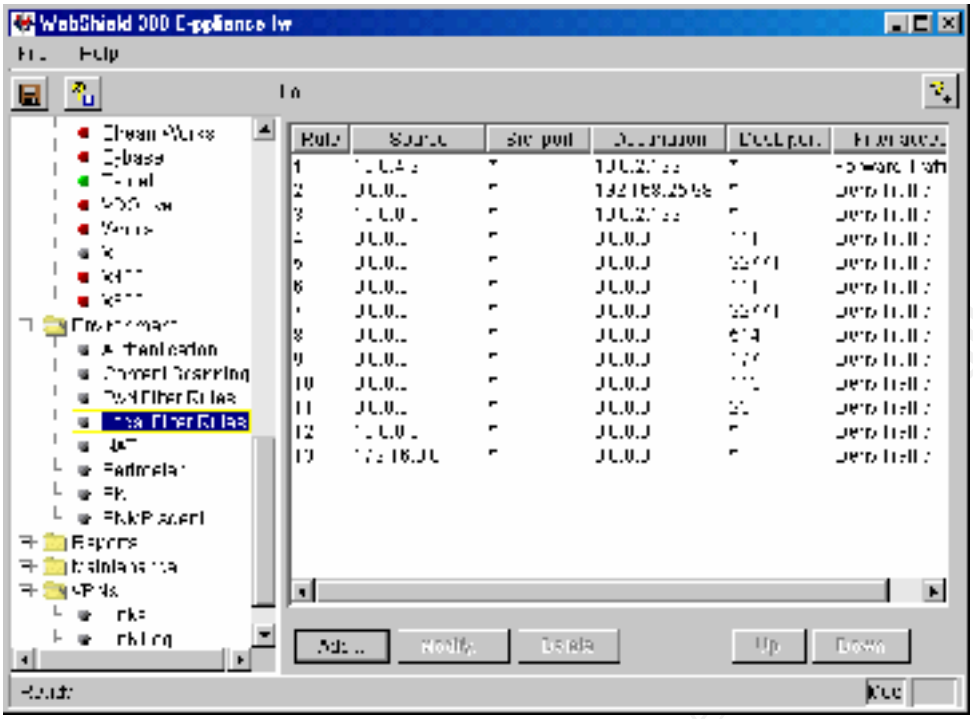
The WebShield supports Packet filtering and Network Address Translation. WebShield separates the packet filtering rules into Forward rules and Local rules. The forward filtering rules apply to packets with a destination other than the firewall itself. Whereas the local filtering rules apply to packets destined for the firewall itself. By default WebShield creates local filter rules set to block UDP and TCP traffic destined to the firewall for port 111 and port 32771 which are rpc related and port 514 syslog and 177 X display manger.

Since the incoming packets will have to pass through the packet filter rules first, the packet filter rules will be described first.

First of all, to protect the firewall itself, there will be a local filter rule restricting access to the firewall's ip address from all ip addresses. This is called the firewall lockdown rule.

Since this rule will block all access, we need to put a rule ahead of this rule that says that access to the firewalls ip address is allowed from the administrator's ip address.

The WebShield E-ppliance guards against spoofing attacks by default. For each packet it receives it compares the source address to the interface that it came in on, compares this to configuration tables created during initial configuration, and if for example a 10 dot address is trying to enter on the hme0 external interface the packet is dropped. Therefore, no rules will be written for anti-spoofing.



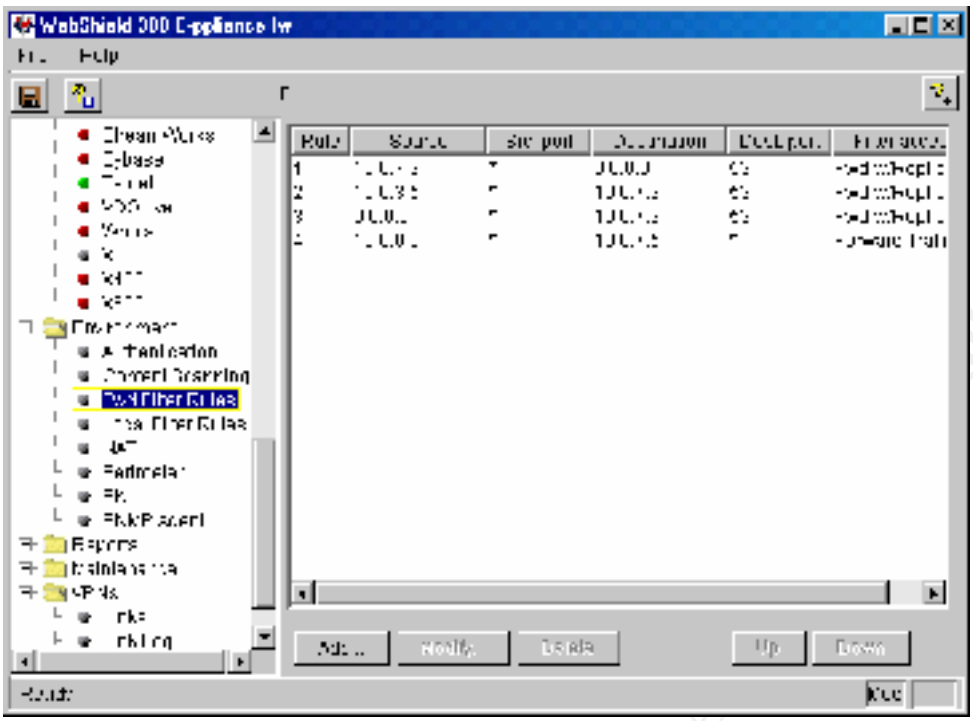
The screen shot above shows the list of local filter rules as seen from the management GUI. Local filter rules control packets that are destined for the firewall itself. I will explain the rules by number:

1. This rule permits access to the firewall from the management workstation.
2. Firewall lockdown rule for the external interface.
3. Firewall lockdown rule for the internal interfaces
4. Portmapper tcp deny rule.
5. RPC tcp deny rule.
6. Portmapper udp deny rule.
7. RPC udp deny rule.
8. Syslog deny rule, we don't want to log directly to the firewall.
9. X display manager protocol, no X window should run on firewall.
10. Ident deny rule, you don't want to identify the firewall to connection attempts.
11. Telnet deny rule on the external interface.

Each one of these rules will be set up to log.

Forward Packet Filter Rules

Forward packet filter rules are used for allowing packets through the firewall that 1. Are destined for something other than the firewall and 2. There is no proxy to handle the packet. The screen shot below shows the facility for creating forward filtering rules.



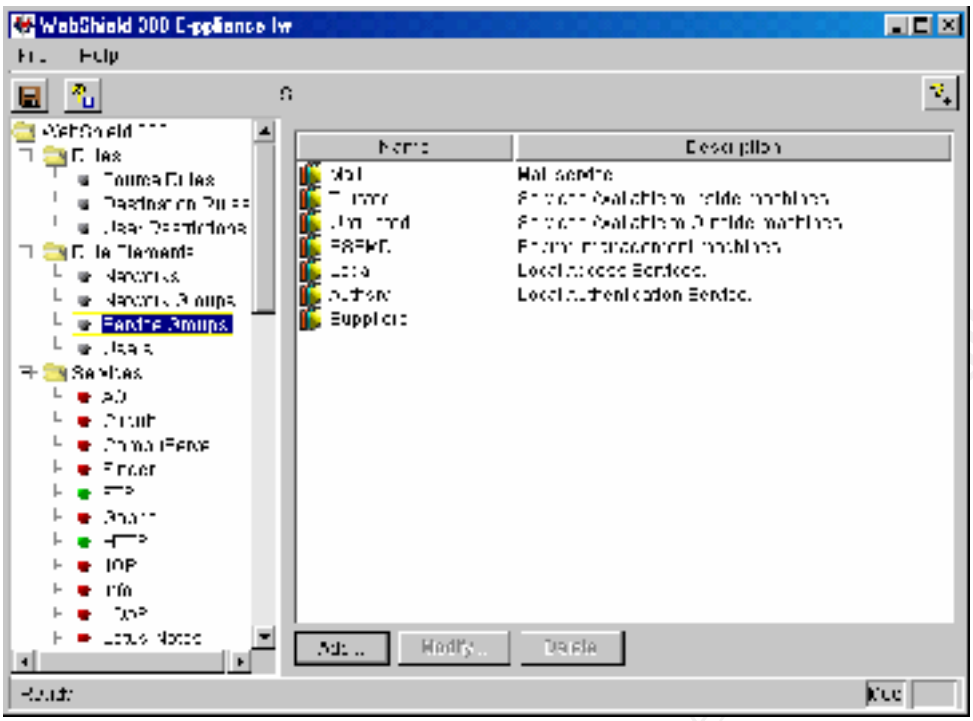
The only forward filtering rules created are for DNS and to access the database server from the internal network. This firewall does not include a proxy for handling DNS. Therefore, three rules where created.

1. From the external DNS server to the world.
2. From the internal DNS server to the external DNS server.
3. From the world to the external DNS server.
4. The fourth rule is to allow traffic from the internal network to the database server.

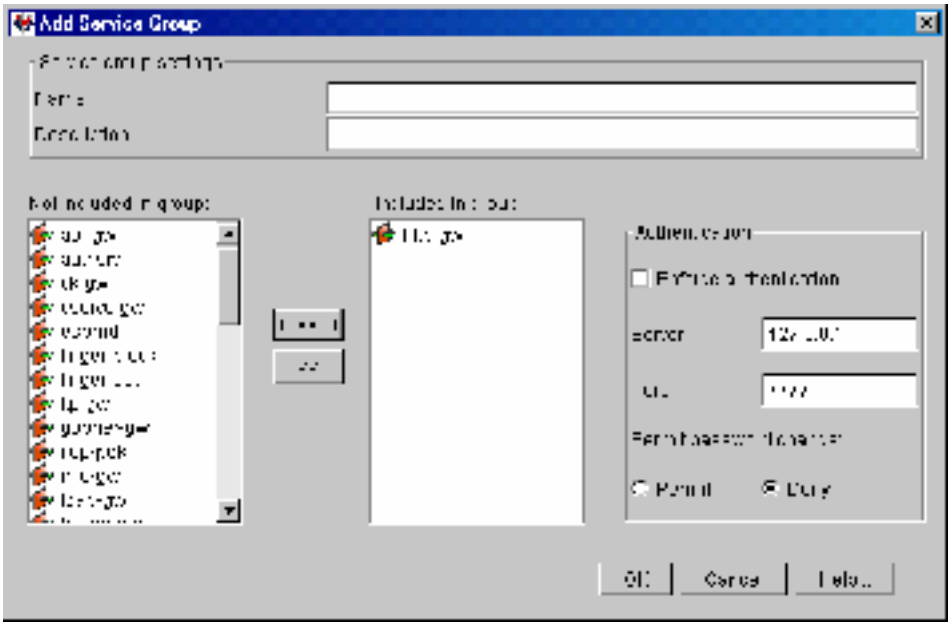
The respective proxies will handle all other traffic through the firewall.

Proxy Rules

To set up a proxy rule on the WebShield you must start by configuring a Service Group. Most likely you will want to permit or deny more than one service with a single rule. Therefore, determine what these services are and create a service group. Once this is done this same service group can be used for other rules if needed. As shown in the screen shot below, to create a Service Group, expand the Rule Elements folder, select Service Group and click Add.



Then as shown below, name the group, select the services from the window on the left and add them to the window on the right. Authentication can be set here and whether or not the user can change their own password. Click OK and the group is created.

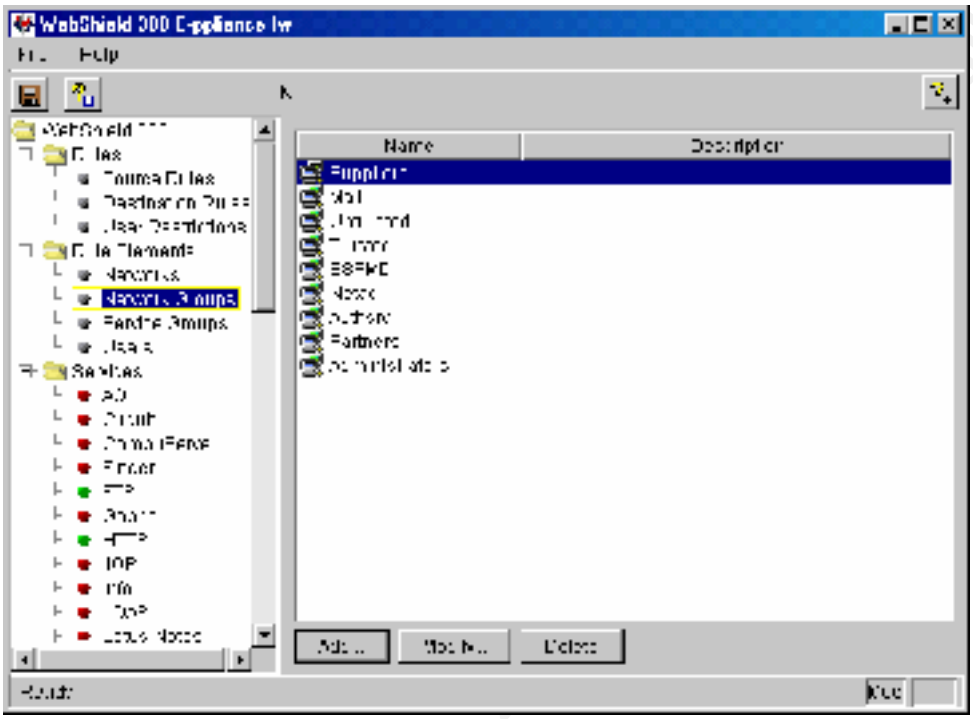


The Untrusted service group should be edited to ensure that only the services that you want are in the group.

Next you would create network groups. These are ip addresses that will be permitted or denied access to the Service groups.

Default Rules

During the configuration of the firewall there are several default rules and groups created.

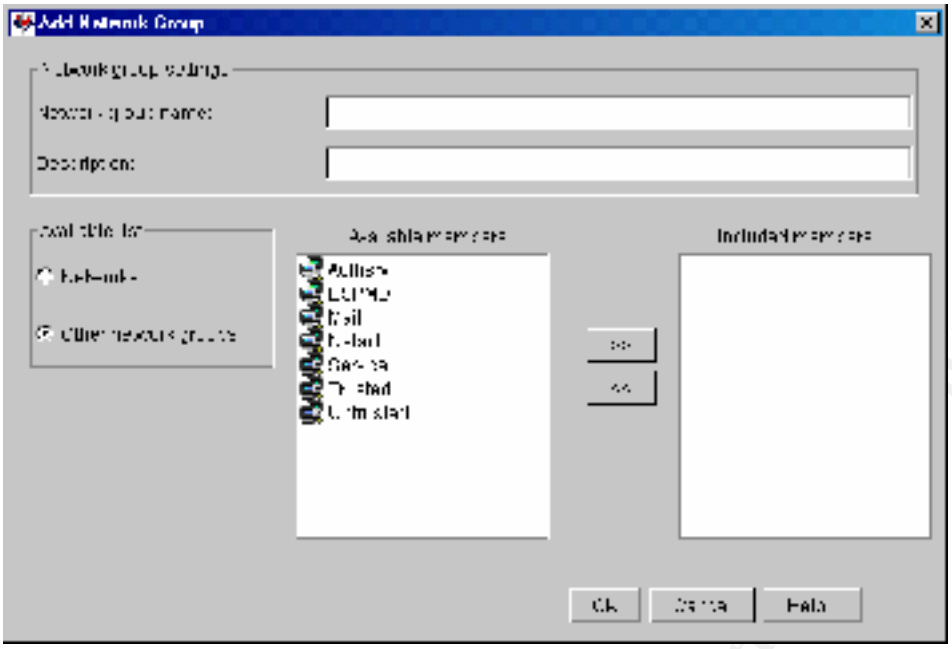


As you see in the above screen shot there are several Network Groups. The Untrusted, Trusted, ESPMD, Netacl and Authsrv were created by default using the initial configuration information. Members of the ESPMD group are those that can configure the firewall through the management GUI. You will not be able to connect to the firewall through the GUI interface unless your ip address is in the ESPMD group.

The Untrusted and Trusted groups are created from the initial configuration information when you are asked to provide ip addresses for the Trusted and Untrusted networks.

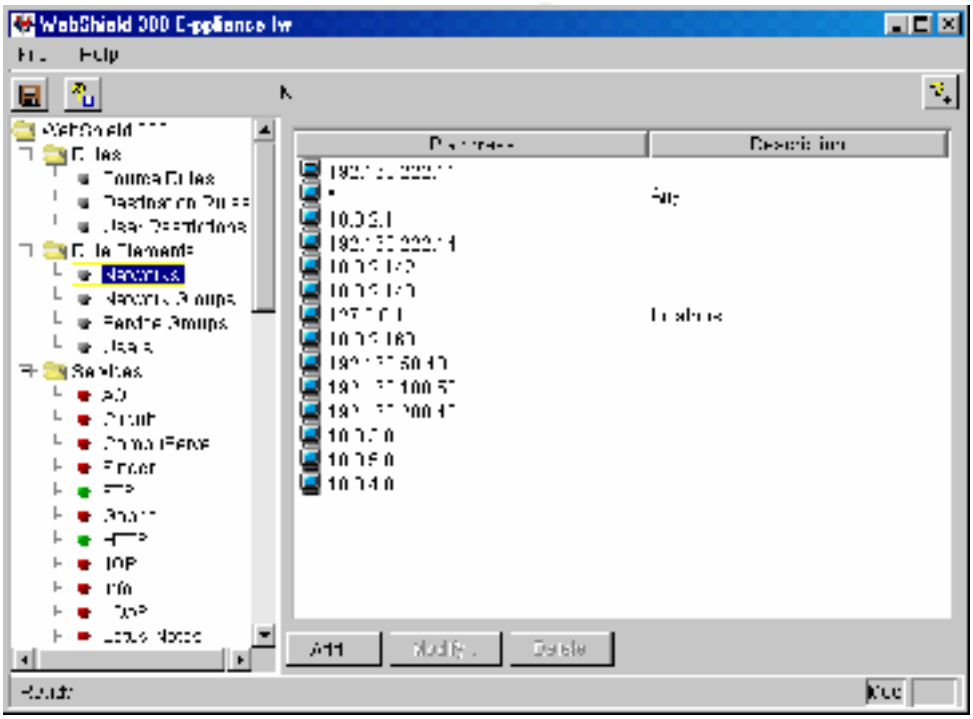
The only member of the Netacl and Authsrv groups is the loop back address 127.0.0.1.

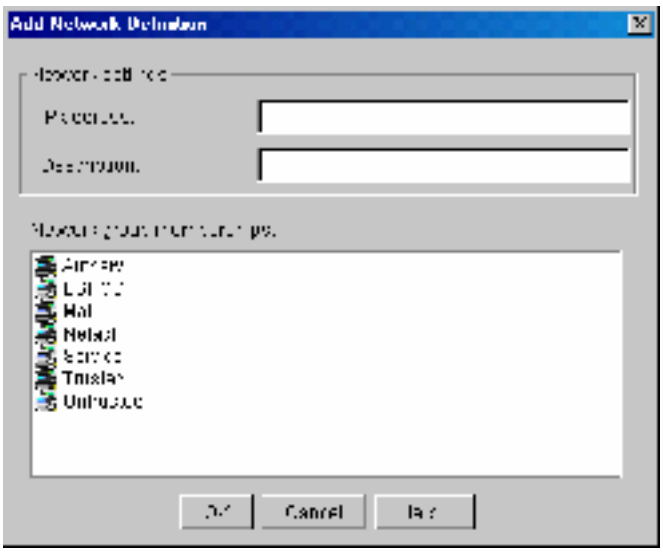
To add a Network Group click on add and use the screen shown below:



Give the Network Group a name. You can then add existing Networks, existing Network Groups or leave it empty until you add other individual ip addresses or networks, which you will do next. Click OK.

Now click on Networks and click Add.





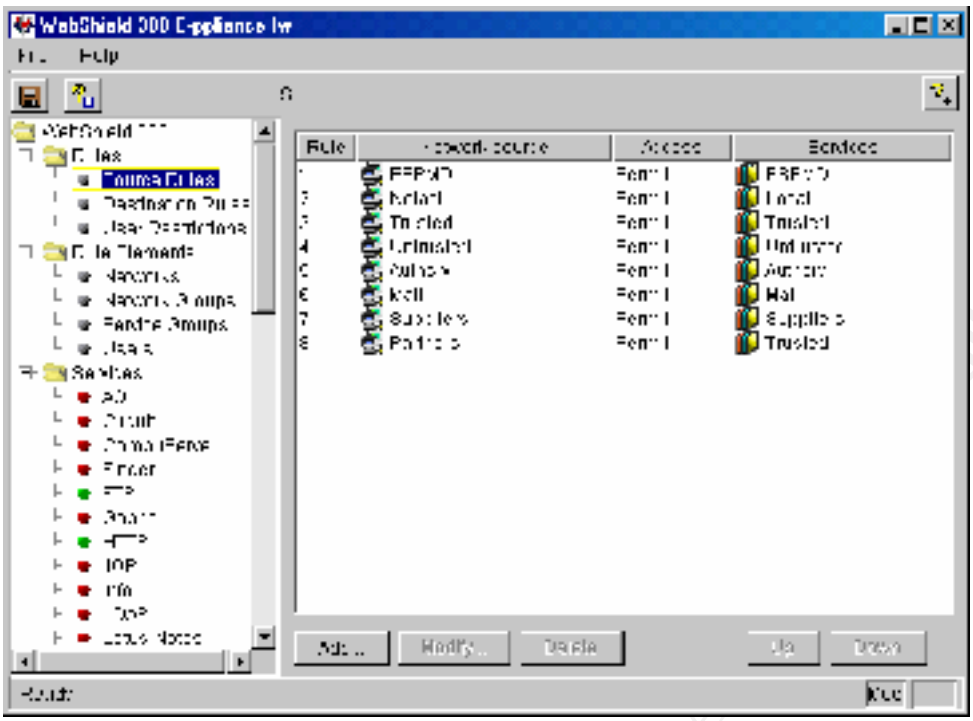
Here you give the network address or individual address and select the group that you created above to populate the Network Group. Click OK.

For example, the trusted group would consist of all ip addresses on the internal network. This illustrates why you want to have rules in place that deny ip addresses coming into your network if they have addresses that are from your internal network.

Now that you have defined network groups and/or ip addresses that you will use in your rules and you have defined some service groups, you are ready to start writing your rule set in accordance with your firewall security policy.

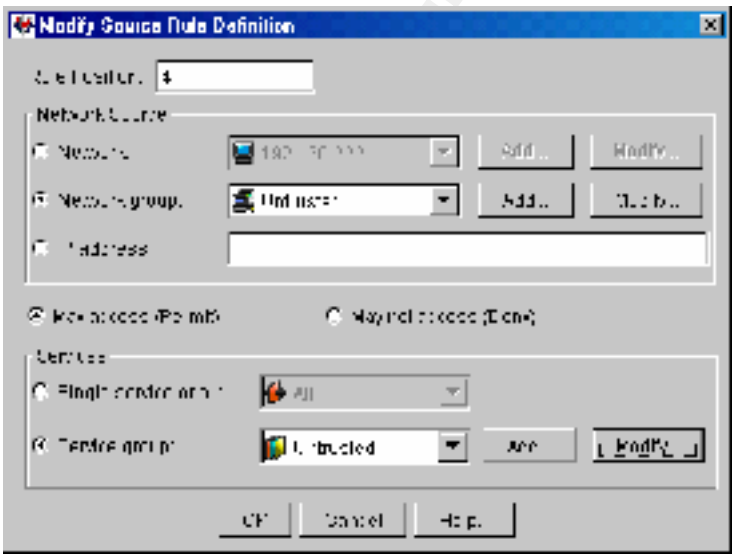
This is accomplished with two source rules. During the initial configuration of the firewall, from the console, you set which ip addresses can use the WebShield GUI to manage the firewall. From that, a configuration a rule named ESPMS is created which stands for Enterprise Security Product Manager. During the initial configuration you also setup a username and password to use when logging into the management GUI.

In WebShield, the rules are in two pieces, the source rule and the destination rule. The source rule includes which users or groups can access which services. Once a source rule is configures the user or group will not be able to use the service without a destination rule. The destination rule allows or denies a service group access to particular destinations. Therefore, a group must be granted access to a service first and then that service must be granted access to a destination.

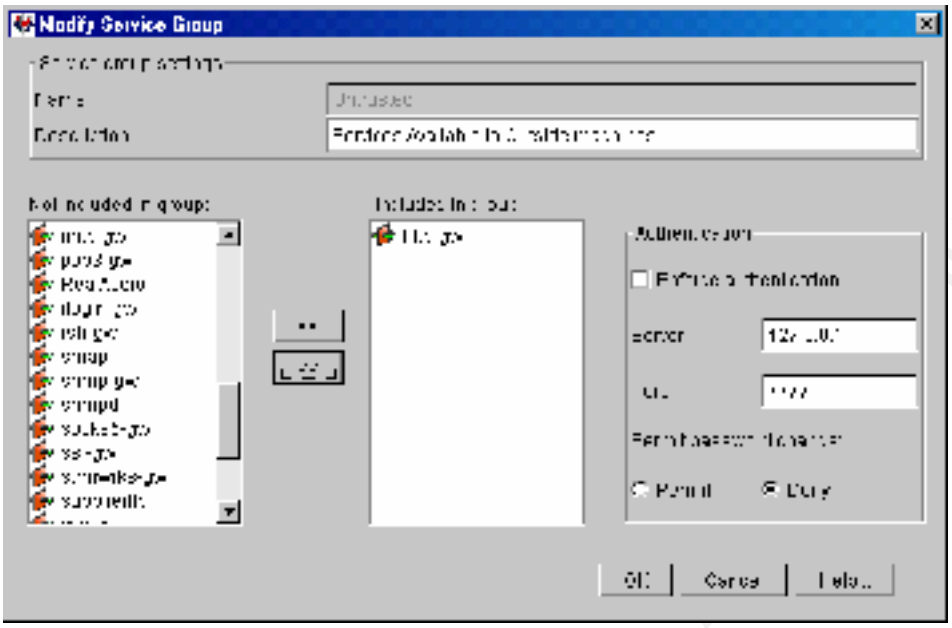


Several other rules are set up by default on the WebShield as you can see in the above graphic. From the information input during the initial configuration of the firewall from the console, you input the trusted network and the interface it is connected to. The same goes for the Untrusted side. From this WebShield creates the default groups and rules for the Trusted and Untrusted networks. These groups and rules can be changed from the administrative GUI at any time after the initial configuration.

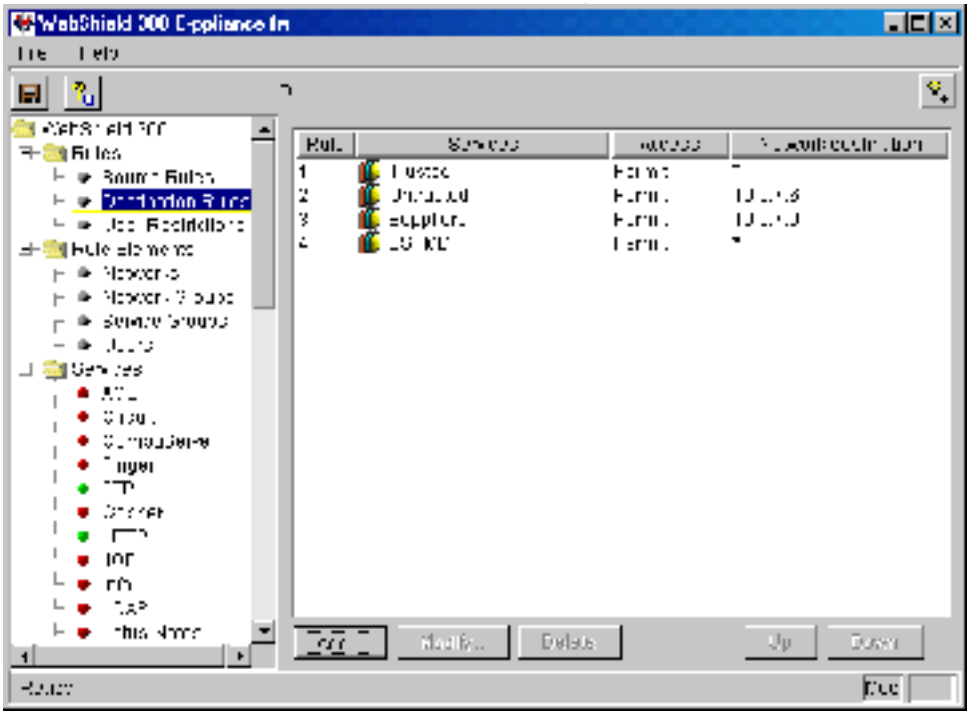
To add or modify a source rule select Add or Modify:



By clicking on modify in the Services box you can see below which services the Untrusted group has access to:



They are only allowed access to the http proxy and therefore will only be able to access the Web site. Next you will see the Destination Rule set:



Here you see that there is only four rules. The Trusted service group is available to internal users, the road warriors and the Partners. The Suppliers group gives them

access to the FTP server. The ESPMD gives the administrator privileges to the management workstation.

Patches

The system can not be as secure as possible without keeping the patches up to date. To determine which patches have been installed, This information is kept in the patchlog file. This file is located in the /usr/local/etc/mgmt directory.

Download the patches to the FTP server from the Solaris and PGP web sites.
Telnet to the firewall, login and su to root.
Connect to the FTP server and get the patches.
Exit from FTP and type ./xxx.patch in the directory where the patch is located.
This will create a directory named from the patch.dir.
Change to that directory and type sh ./apply.

Logging

A server within the management zone will be configured as the syslog server. The border router, the IDS, the primary firewall and the other servers in the service network will all log to the syslog server.

Border Router Security Policy:

The operating system on the router currently is 12.1. The feature set is the IP Plus feature pack. The firewall feature set was not installed because of the added processing load and since firewalling is not the primary task of this piece of equipment. The border router will be physically secured in a locked room using a punch combination lock. Physical access to the router will be permitted by network administrative personnel only. The passwords will be kept in an envelope in a locked cabinet in the CIO's office.

The enable secret password will be used. The enable secret password utilizes a stronger encryption algorithm than the enable password. Next we will enable service password-encryption command so that the password is encrypted. When you display the running or startup configuration the password will be shown encrypted rather than in plain text.

TCP intercept is a feature that will guard against DDOS attacks by intercepting incoming tcp connection attempts and verifying that the requesting host can be contacted.

There are five vty lines used for telneting to the router (0 through 4). One password will be set for all five vty lines. To telnet to the router, first use secure shell (ssh) to connect to the primary firewall. Then telnet to the inside interface of the router. This ensures that when connecting to the router from the world, the traffic is encrypted until it passes

through the firewall. If you were to telnet directly to the router from the internet, all traffic during a telnet session is sent in clear text and is vulnerable to sniffing.

A telnet banner will be set stating that only authorized access is permitted. At this time privilege levels that control which commands a user can execute depending on their authentication will not be used. No modem will be attached to the router for remote configuration.

Since this router will only have two interfaces, one connected to the ISP and one connected to the DMZ, no dynamic routing protocols will be configured. Static routes will be used. One danger in using dynamic routing protocols is that your router could receive a route update that points the router to a network where you do not want your traffic to go. In a large network where you would need to use dynamic routing, you would configure neighbor router authentication so that you control which routers your routers receive routing updates from.

The basic packet filtering capability will be used on two routers. On the Border router and on the internal router. Creating packet filters on the Border router will serve two purposes. It will filter out packets that do not need to enter the network, which will reduce the load placed on the Proxy firewall. Secondly, putting packet filtering on the border router makes it the first line of defense. Another set of packet filtering rules will be placed on an internal router that will separate the internal networks.

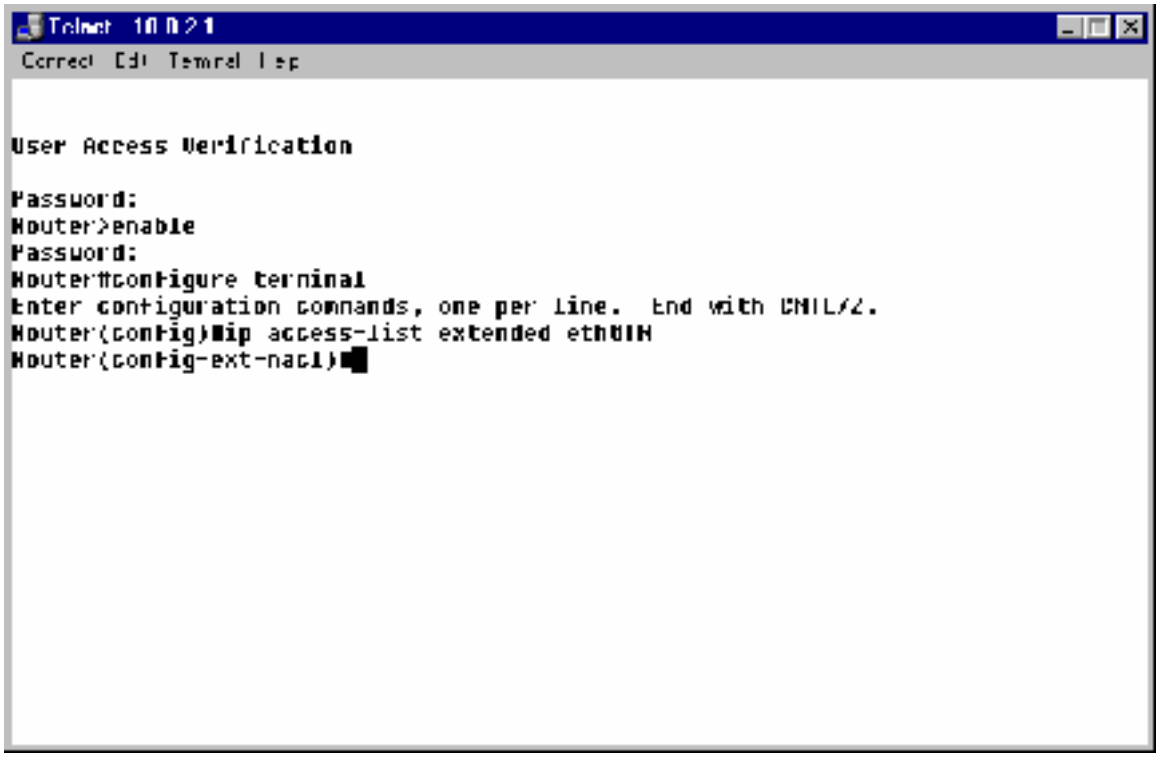
The following settings will be used on the router:

Enable secret password	Better encryption for the password
No ip finger	No finger service to id users
No ip http server	No web interface access
Service password encryption	Password will not display in plain text
No source ip route	The packet cannot determine route
No cdp run	No Cisco discovery protocol
No ntp server	No network time protocol
No service udp-small-server	The router should not provide services
No service tcp-small-server	

The external interface will have an access list configured IN and the internal interface will have an access list configured OUT. Setting up the access control lists in this way filters packets before they are forwarded to the interface on the other side of the router cutting down on the number of packets that actually enter the router and use up processor cycles.

To configure the access-lists on the router, as shown below, you enter privileged mode by using the enable command. Once in the privileged mode you enter global configuration mode by entering the configure terminal command. You then create the

access-list by entering “ip access-list extended eth0IN”. This command creates an ip extended access-list named eth0IN.



Once the access-list is created, the rules that will make up the list can be pasted in from a text editor such as notepad. It is recommended that the access-list rules be typed up in a text editor to allow quick editing and replacement of the access-list on the router. Once the access-list is applied to the interface it cannot be edited in place. It must be deleted and reapplied. The access-lists shown below can be pasted in and then the access-list must be grouped to the correct interface either IN or OUT.

ip access-list extended atmingress	**ip access-list extended egress**
permit tcp any host xxx.xxx.xxx.4 eq www log deny ip any host xxx.xxx.xxx.4 log deny tcp 10.0.0.0 0.255.255.255 any log deny udp 10.0.0.0 0.255.255.255 any log deny icmp 10.0.0.0 0.255.255.255 any log deny tcp 172.16.0.0 0.15.255.255 any log deny udp 172.16.0.0 0.15.255.255 any log deny icmp 172.16.0.0 0.15.255.255 any log deny tcp 192.168.0.0 0.0.255.255 any log deny udp 192.168.0.0 0.0.255.255 any log deny icmp 192.168.0.0 0.0.255.255 any log deny tcp xxx.xxx.xxx.0 0.0.0.31 any log deny udp xxx.xxx.xxx.0 0.0.0.31 any log	permit ip host xxx.xxx.xxx.2 any permit ip host xxx.xxx.xxx.4 any permit icmp host xxx.xxx.xxx.xxx any permit icmp host xxx.xxx.xxx.2 any deny ip any any log

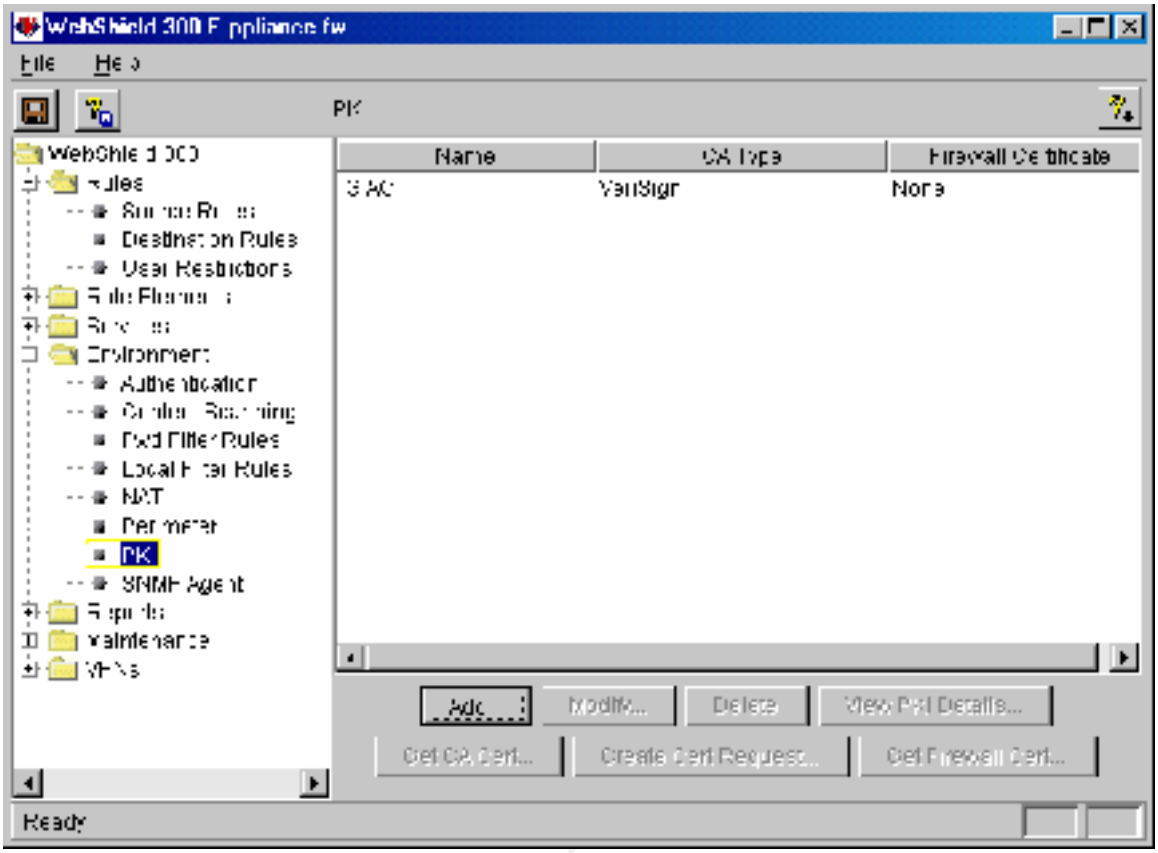
deny icmp xxx.xxx.xxx.0 0.0.0.31 any log deny ip host 0.0.0.0 any log deny ip 127.0.0.0 0.255.255.255 any log deny udp any any eq sunrpc deny tcp any any eq sunrpc deny tcp any any range 137 139 deny udp any any range netbios-ns netbios-ss deny tcp any any range exec cmd deny udp any any eq 2049 deny tcp any any eq 2049 deny udp any any eq 4045 deny tcp any any range 6000 6100 deny udp any any eq 389 deny tcp any any eq 389 deny udp any any eq tftp deny tcp any any eq finger deny udp any any eq syslog deny tcp any any eq lpd permit ip any host xxx.xxx.xxx.2	

Virtual Private Network

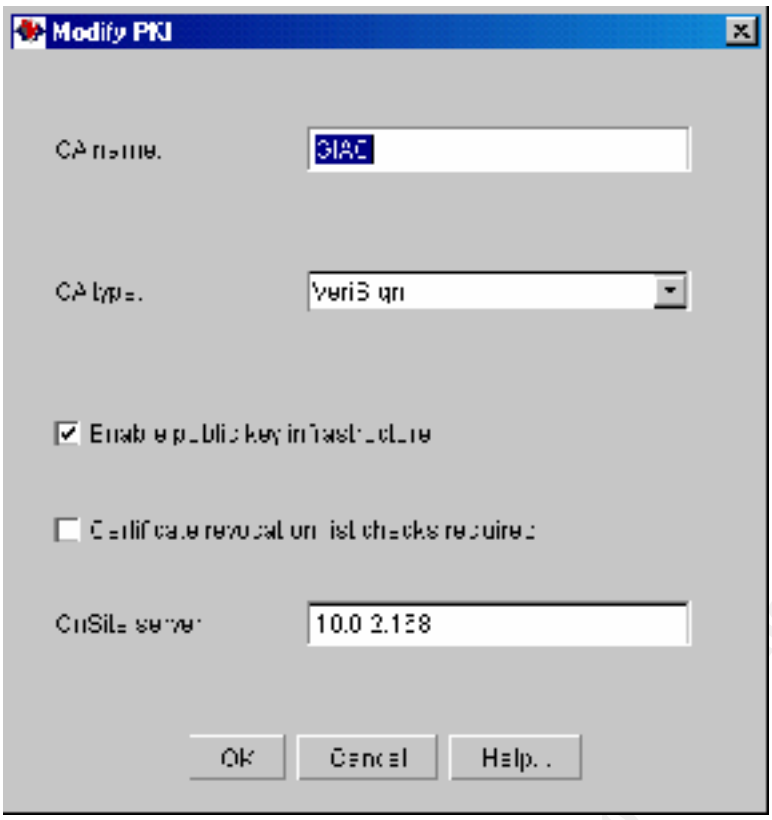
The E-appliance will also used to provide the VPN solution. Two different types of VPN are required. For the Suppliers, because they need access but are not operating with the same security policy, will use a Private Link. The Private Link provides privacy without trust. The data is encrypted during transit until is enters the GEP' firewall. The firewall will decrypt the data and submit the packets to the packet filtering and proxy rules without trust.

The second VPN will be set up for the Partners. Since the Partners have merged with GEP, both entities are operating under the same security policy. Therefore, a Trusted Link will be used. In a Trusted Link the data is encrypted and treated as though it is the same network as the internal network. It essentially extends the LAN by combining two LANs across a WAN. The data coming in through the Trusted VPN is not submitted to the incoming packet filter rules or the incoming proxy rules. The mobile GEP employees (road warriors) will also utilize a trusted VPN connection.

To create the VPN links you must first decide whether to use certificate based or pre-shared secret authentication. GEP will use certificates based authentication using VeriSign as the certificate authority (CA). To set up the CA click on expand the Environment folder as shown below and click on PKI.

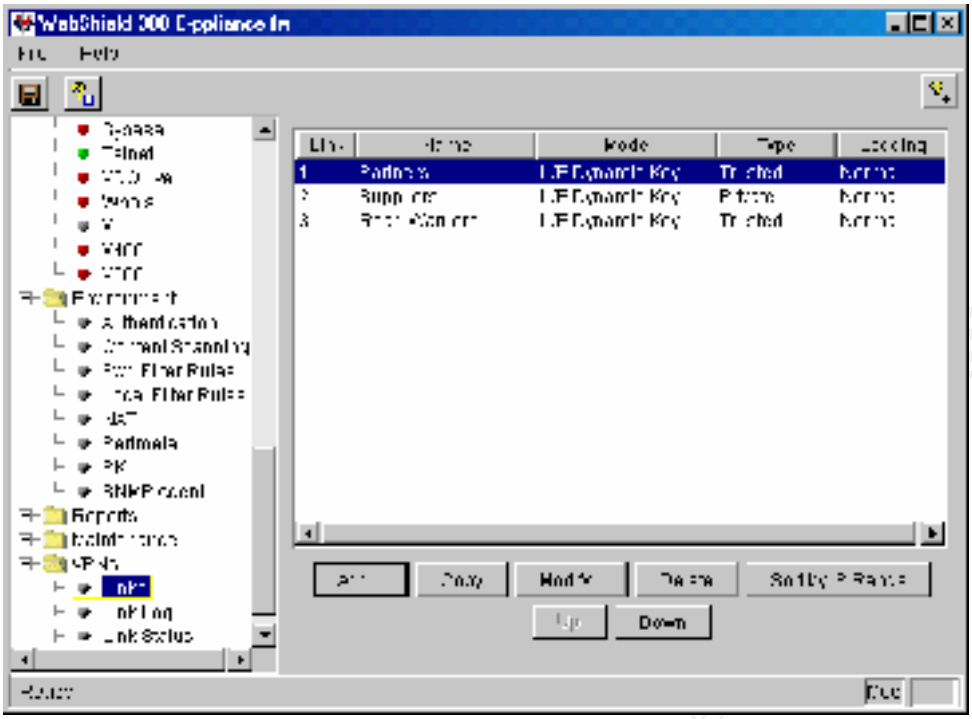


Click add to set up the CA

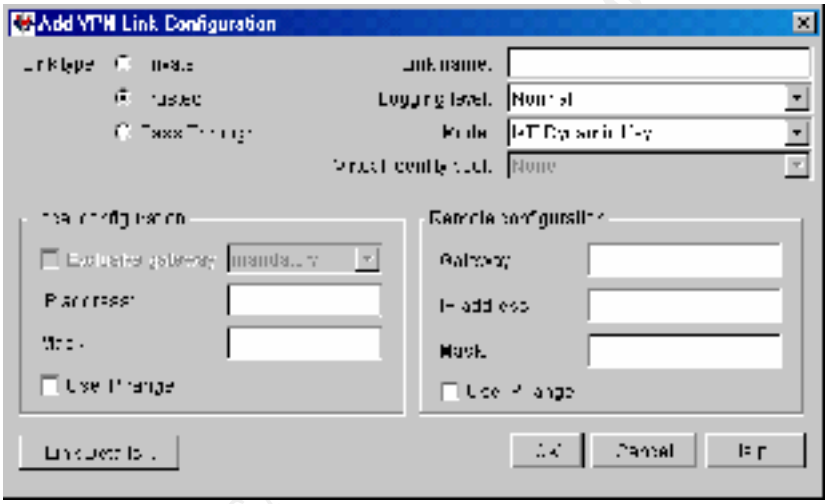


You will add an original name, select the CA type and tell the application where you will be loading the certificates from.

Next expand the VPN folder and click on Links as shown below.



Click on Add to create a VPN link.



Select the Link type, give the a descriptive name, set the logging level and choose IKE Dynamic Key.

Under local configuration, input the ip address of your firewall. In the Remote configuration box you input the ip address of the other end of the VPN link. Now click OK.

VPN links need to be created on the other end of the VPN link before the link can be used.

Assignment 3 – Audit Your Security Architecture

Planning:

The first step in auditing the security architecture would be to gather information about the network. Auditing the primary firewall and pointing out vulnerabilities when there is some other easier route around the firewall, such as remote dial-in access to an internal system, is a waste of time. All routes to the internal network should go through the firewall.

Once sufficient data has been gathered about the network, an auditing plan can be developed. The auditing plan must have the approval of key management personnel.

The plan should include a time/cost budget and detail what is going to be done and when. A thorough audit should include the review of the following three main areas:

1. The documentation and procedures that bear on network security.
2. The physical security of key network components.
3. The system's security related configurations.

Documentation

Review of documentation is important in trying to determine if there are sufficient procedures in place to maintain a reasonably secure network. Areas that need consideration include password policies, adding and deleting users, who is granted access to what (both logical and physical areas), and backup procedures including storage of back-up media.

The time of the assessment will be important. The assessment should take place under realistic loads on the network. Monitoring the network during normal working hours can sometimes reveal that data is flowing across the network that should not be.

Going into the assessment with realistic expectations is important. There is no such thing as a secure network. A network should be made as secure as possible considering cost, manpower, usability of the system etc. It will be hard to define an endpoint if there is no idea what the customer is shooting for.

Cost Estimate:

Personnel	**Task**	**Hourly Rate ($/hr)**	**# of Hours**	**Total ($)**
Senior security engineer	Review of network and documentation.	225	8	1800.00
Security engineer	Review and documentation of	150	8	1200.00

	physical location of key network equipment.			
Senior security engineer	Scanning of perimeter systems.	225	4	900.00
Security engineer	Documentation of OS versions, configuration and patch levels.	150	2	300.00
Senior security engineer	Compilation of data and report writing,	225	4	900.00
Security engineer	Compilation of data and report writing.	150	4	600.00
Total				5700.00

Physical Security:

The physical security of the router, primary firewall, hubs, switches and servers is of great importance. The physical location of each of these components will be noted and recommendations made if each is not in a secure location. The term "secure location" needs to be defined. In most cases this would mean that the systems are behind locked doors that only IS department personnel and upper management can access. Access to these areas should be logged.

OS Hardened, Patches installed

Verify that the operating system has been hardened to an acceptable level. The E-ppliance comes with a "hardened" version of Solaris 2.5.6. This will be verified by referencing the white paper by Lance Spitzner http://WWW.enteract.com/~lspitz/armoring.html and the Sun site http://WWW.sun.com/security/blueprints for guidance on appropriate Sun operating system hardening. Next verify that Solaris and WebShield patches are up-to-date.

Tools Used:

The tools used for this audit include Nessus, Nmap, Hping, and Ethereal. Each of these tools are freely available on the internet, are well documented and used commonly in the computer security environment. Commands such as netstat will be run to gain information on the individual system and compared to the results of Nessus and Nmap output.

If the assessment is taking place on a new system before the firewall is put into production it will first be scanned before it is connected to the production network. First, the netstat –tan command will be done each interface of the firewall. These results will be saved and compared with port scans. A scan will be done on the system using nmap to determine what services are being advertised. This baseline scan of the system will show the system at a point when you know no other systems have had an

effect on it. It will also reveal to you any typical traffic generated by the firewall itself. After the baseline scans the system would be put in-place and scanned again.

Scans will be done from locations outside of each interface on the firewall. This way we will see which ports and services are open from each connected network. The scans will encompass icmp and all ports both tcp and udp and the scan results will be compared to the results of the netstat command. If the results differ we will conduct research to determine the cause.

Next we will analyze the rule sets on the firewall. Testing will be conducted to determine if the rule sets are blocking and allowing according the firewall policy. For example, icmp should not be allowed to the internal network. Pings will be sent to each network behind the firewall and using ethereal we will determine what happens to these packets. Another example would be to attempt a connection to the internal FTP server, this should not be successful. Testing will not only take place from the outside in, the rule sets must be tested from the internal network out also. For example, packets with a source address other than the GEP addresses should not be allowed to pass through the router. Hping will be used to craft packets to test the packet filtering rules.

As stated above, Nessus and Nmap scans were conducted on each interface of the border router and the primary firewall. However, for brevity, only the Nessus and Nmap scans of the external interface of the primary firewall are included here.

Results of the Nmap scan on the external interface:

```
Starting nmap V. 2.54BETA30 ( WWW.insecure.org/nmap/ )

Host (10.0.2.126) appears to be up ... good.
Initiating Connect() Scan against (10.0.2.126)
Adding open port 8004/tcp
Adding open port 25/tcp
Adding open port 443/tcp
Adding open port 110/tcp
Adding open port 80/tcp
Adding open port 21/tcp
The Connect() Scan took 18 seconds to scan 65535 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Interesting ports on (10.0.2.126):
(The 65525 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open FTP
23/tcp filtered telnet

25/tcp open smtp
80/tcp open http
```

110/tcp open pop-3
111/tcp filtered sunrpc
113/tcp filtered auth
443/tcp open https
8004/tcp open unknown
32771/tcp filtered sometimes-rpc5
No exact OS matches for host (If you know what OS is running on it, see http://WWW.insecure.org/cgi-bin/nmap-submit.cgi).
Uptime 17.392 days (since Fri Oct 26 08:16:40 2001)
TCP Sequence Prediction: Class=random positive increments
Difficulty=32250 (Worthy challenge)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds

Analysis of Nmap Results

The results of this nmap scan on the external interface of the primary firewall show that the following ports/services are accessible:

Port 21, FTP - This port/service combination is open on all three interfaces of the firewall. We will allow this port to remain open to serve the users that require FTP services to and from the FTP server in the service network. FTP is proxied on the firewall and each entity (internal employees, suppliers, partners) have access only to the commands they require to do their job. These restrictions are set in the FTP proxy settings.

Port 23, Telnet - This port/service combination is filtered by both packet filtering rules and the telnet proxy. The only allowed telnet is from the management workstation located behind the internal router with an access list blocking all ip addresses from connecting to it (i.e. blocking any SYNs destined for the management workstations).

Port 80, HTTP - This port/service combination is a proxied service on the firewall and remain open. Proxy rules control who can connect to port 80 and determines the allowed destinations. For example, anyone connecting from an untrusted network will be allowed to connect to port 80 but a destination rule will only allow connection to the web server in the service network.

Port 110, POP3 - This port/service combination, found open on the external interface will be left open so that internal users on the trusted network can connect out to their POP3 mail accounts. POP3 will is a proxied service and is not allowed for untrusted networks in the proxy rules.

Port 111, RPC – This port/service combination is blocked by default packet filtering rules. This port is commonly referred to in Unix as portmapper and can give up juicy information on ports and services available if an attacker can connect to it.

Port 113, Ident – This port/service combination is blocked by a default packet filtering rule. The Ident service is the Identification protocol and was used for identifying a client when a connection attempt was made. The client can spoof this information and therefore ident is a vulnerability and should not be allowed.

Port 443, HTTPS – This port/service combination is open and will remain so for connection to the secure web server.

Port 8004, - This port is used by the WebShield GUI interface. The WebShield GUI application is installed on the management workstations and is used to configure and maintain the firewall after the initial configuration which is done through connection via a console cable. This port will remain open to the internal management workstations but will be blocked from the untrusted networks. The access to this port is controlled through a proxy rule called ESPMD which stands for Enterprise Security Product Manager.

Port 32771, RPC – This port/service combination listens for remote procedure calls and on this version of Solaris has a buffer overflow vulnerability. This port is blocked by default packet filtering rules.

There are a couple of other points of interest from this Nmap output. The operating system could not be determined. This is a good thing. The less information an attacker can glean from your systems the better. It will by a little time and hopefully by keeping an eye on the logs, potential attackers will be noticed. The second point is the TCP sequence number prediction difficulty was 32250. The lower the number, the easier it is to guess the next TCP sequence number which is needed for hijacking attacks. This results show that this type of attack would be fairly difficult to pull off.

Results of the Nessus scan on the external interface:
Nessus Scan ReportNessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 2
Number of security warnings found : 8
Number of security notes found : 4
List of the tested hosts :
10.0.2.126(Security holes found)

10.0.2.126 :
List of open ports :
FTP (21/tcp) (Security hole found)
smtp (25/tcp) (Security warnings found)
http (80/tcp) (Security hole found)
pop3 (110/tcp)
https (443/tcp)

unknown (8004/tcp)
general/udp (Security notes found)
general/tcp (Security notes found)
general/icmp (Security warnings found)

Vulnerability found on port FTP (21/tcp)
The remote FTP server closes the connection when one of the commands USER, PASS or HELP is given with a too long argument. This probably due to a buffer overflow, which allows anyone to execute arbitrary code on the remote host. This problem is threatening, because the attackers don't need an account to exploit this flaw.

Solution : Upgrade your FTP server or change it
Risk factor : High
Information found on port FTP (21/tcp)
Remote FTP server banner :
fw.l2.vtio.org FTP proxy (version v1.5) ready.

Warning found on port smtp (25/tcp)
The remote SMTP server answers to the EXPN and/or VRFY commands. The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.

Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

Solution : if you are using sendmail, add the option
O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

Warning found on port smtp (25/tcp)
The remote STMP server seems to allow remote users to send mail anonymously by providing a too long argument to the HELO command (more than 1024 chars).

This problem may allow bad guys to send hate mail, or threatening mail using your server and keep their anonymity.

Risk factor : Low.

Solution : If you are using sendmail, upgrade to version 8.9.x. If you do not run sendmail, contact your vendor.
CVE : CAN-1999-0098

Warning found on port smtp (25/tcp)
The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to : user@hostname1@victim

Then the remote SMTP server (victim) will happily send the mail to : user@hostname1

Using this flaw, an attacker may route a message through your firewall, in order to exploit other SMTP servers that can not be reached from the outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
SOME SMTP SERVERS LIKE POSTFIX WILL NOT
COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert : R$*@$*@$* $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor : Low

Warning found on port smtp (25/tcp)
The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay any more.
CVE : CAN-1999-0512

Information found on port smtp (25/tcp)
Remote SMTP server banner :
fw.l2.vtio.org SMTP/smap Ready.
214-Commands214-HELO MAIL RCPT DATA RSET

214 NOOP QUIT HELP VRFY EXPN

Vulnerability found on port http (80/tcp)
The Sambar web server is running. It provides a web interface for configuration purposes. The admin user has no password and there are some other default users without passwords. Everyone could set the HTTP-Root to c:\ and delete your files!

*** this may be a false positive - go to http://the_server/sysadmin/ and
have a look at it by yourself.
Solution : Change the passwords via the web interface or use a real web server
like Apache.

Risk factor : High

Warning found on port http (80/tcp)
It seems that the PUT method is enabled on your web server. Although we could not exploit this, you'd better disable it.
Solution : disable this method
Risk factor : Serious

Warning found on port http (80/tcp)
It seems that the DELETE method is enabled on your web server. Although we could not exploit this, you'd better disable it Solution : disable this method
Risk factor : Medium

Information found on port general/udp
For your information, here is the traceroute to 10.0.2.126 :
192.168.222.1
10.1.1.6
10.0.2.126

Information found on port general/tcp
QueSO has found out that the remote host OS is
* Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

CVE : CAN-1999-0454

Warning found on port general/icmp
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentications protocols.
Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

Warning found on port general/icmp
The remote host answered to an ICMP_MASKREQ query and sent us its netmask.

An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters.

Solution : reconfigure the remote host so that it does not answer to those requests.
Set up filters that deny ICMP packets of type 17.

Risk factor : Low
CVE : CAN-1999-0524

This file was generated by Nessus, the open-sourced security scanner.

As you can see Nessus does a little more than Nmap. It actually does run Nmap to determine which ports are open and determines which services are listening. Nessus then attempts to exploit vulnerabilities based on the open ports, services and operating systems found. It then suggests solutions and quotes the Common Vulnerabilities and Exposures (CVE) number for reference.

Recommendations:

Telnet will be blocked and OpenSSH for Solaris will be installed for connection to the firewall.

Look into upgrading the FTP server on the firewall.

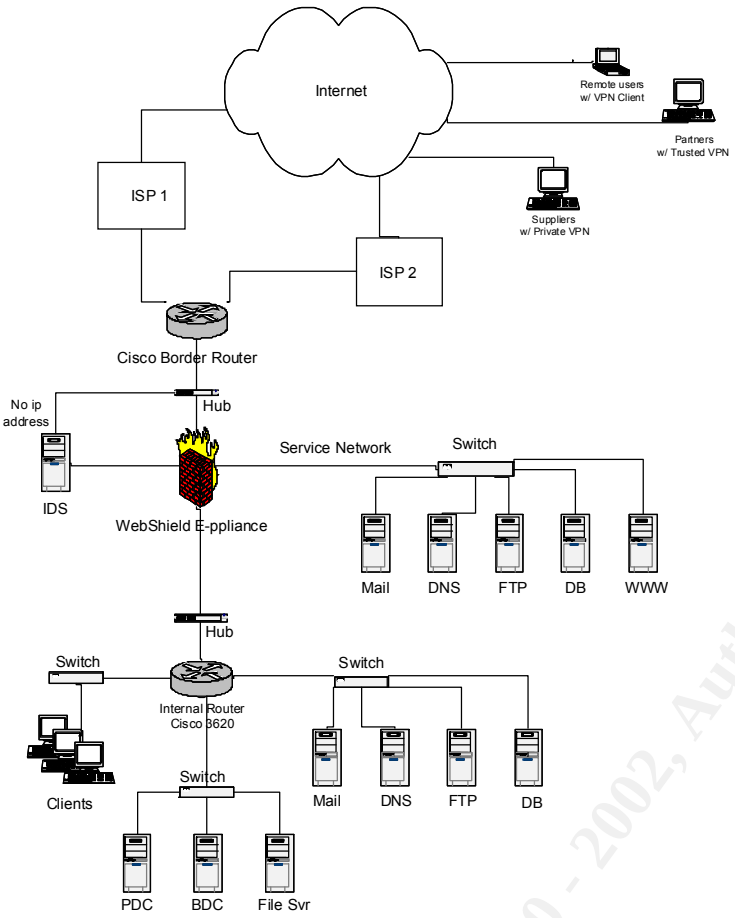
Since we are using sendmail, we will upgrade it to the newest stable version 8.12.1.

Disable PUT on the web proxy.

Filter icmp on the firewall to only allow echoreply.

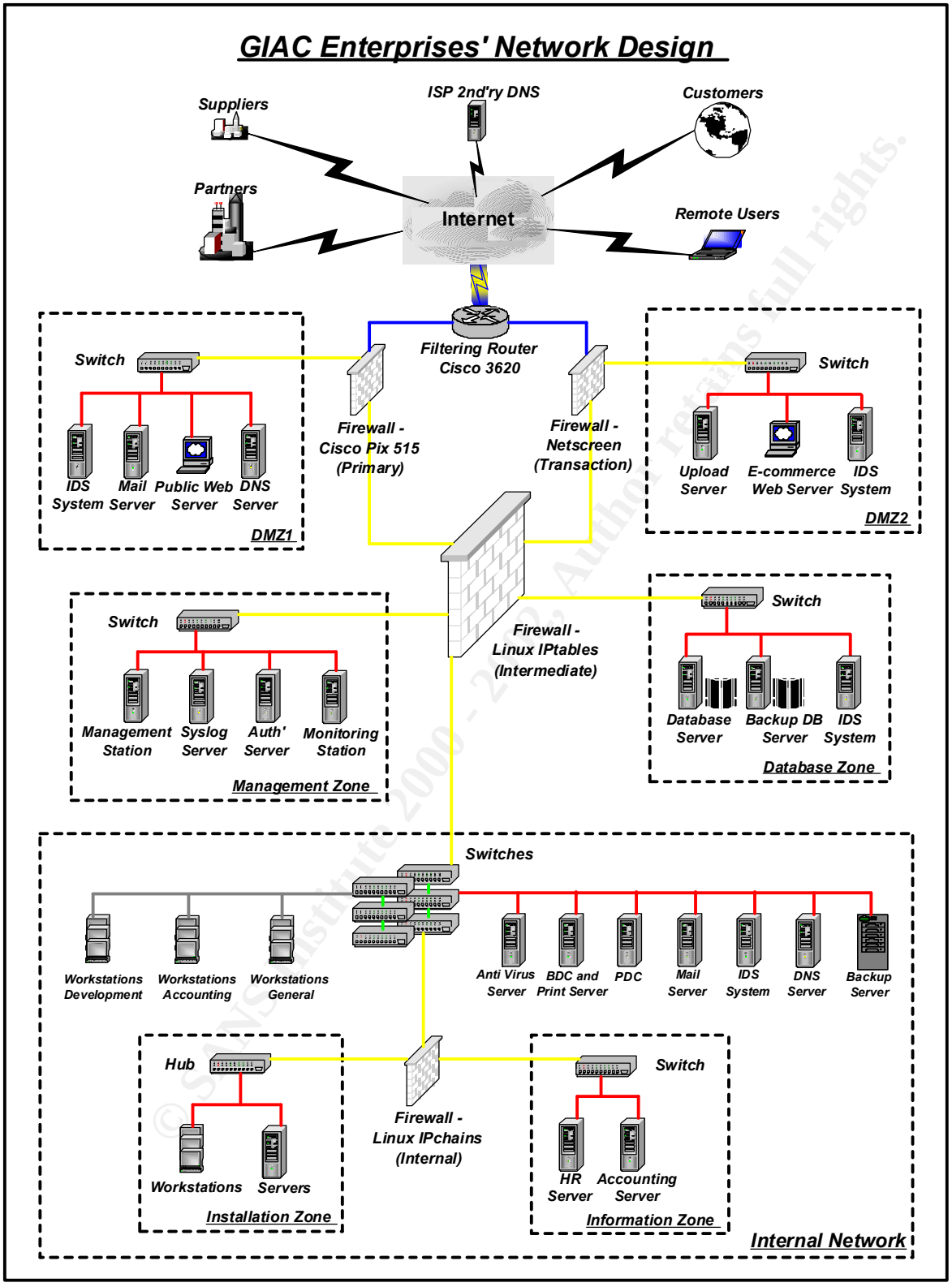
Both tools agree on which ports and services are open which serves as a good check on the results.

Change the architecture to provide a secondary route to an ISP. Considering that this is an e-commerce site, providing a secondary route to the world would provide redundancy to protect against problems at the ISP and denial of service attacks as shown below.



Assignment 4 – Design Under Fire

For this portion of the practical I have chosen the practical submitted by Mark Johnston. His network design is shown below.



Attack against the firewall using a vulnerability specific to the product.

The task for the first part of Assignment 4 is to design an attack against the primary firewall using a known vulnerability. Mark Johnston's network design for GEP utilizes a Cisco Pix 515 firewall running version 6.0. Very few holes have been found in this version to date. The vulnerability that I have chosen to exploit is the Firewall Manager Plaintext Password Vulnerability bugtraq ID # 3419 http://WWW.securityfocus.com/bid/3419 .

Cisco PIX Firewall Manager (PFM) is software that can be used to configure and manage a Cisco PIX Firewall. After the PFM software makes an initial connection to the PIX Firewall, the administrative password is stored on the local management workstation. A malicious user could use this password to connect to the PIX Firewall and make configuration changes. The Firewall Manager stores the 'enable' password (the password used to gain access to the firewall) in plaintext on the Windows NT workstation running the PFM software. Additionally, the password is stored in a location that is accessible to all users on the workstation. If the workstation is compromised, it is trivial to retrieve the password and gain access to the Pix Firewall.

Yes, the attacker would have to obtain access to the local workstation in order to exploit this vulnerability. However, most information security breaches are not external ones. They are internal ones caused by sabotage, accidents or incompetence. Therefore, I do not think it is unrealistic that someone within GEP could gain physical access to the firewall management workstation.

The only posted solution to this vulnerability is to use the PIX Device Manager instead of the PIX Firewall Manager (PFM).

Denial of service attack.

50 compromised cable modem/DSL systems are set to attack the external interface of Mark's Cisco border router. The theoretical attack we will use is simply port scanning of the Router. Mark's border router is running IOS version 12.1. For this exercise I have assumed that it is either 12.1(3)T or 12.1(2)T and will attack the router to exploit the IOS Reload after Scanning Vulnerability, VU#178024 http://WWW.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml .The following three paragraphs are taken from the Cisco Security Advisory for this vulnerability.

Security Scanning software can cause a memory error in Cisco IOS® Software that will cause a reload to occur. This vulnerability affects only Cisco IOS software version 12.1(2)T and 12.1(3)T, and limited deployment releases based on those versions.

An attempt to make a TCP connection to ports 3100-3999, 5100-5999, 7100-7999, and 10100-10999 will cause the router to unexpectedly reload at the next show running-config, or write memory, or any command that causes the configuration file to be accessed. Cisco IOS software cannot be configured to support any services that might

listen at those port addresses, and cannot be configured to accept connections on those ports, however, connection attempts to these ports in the affected version will cause memory corruption, later leading to an unexpected reload.

The described defect can be used to mount a denial of service (DoS) attack on any vulnerable Cisco product, which may result in violations of the availability aspects of a customer's security policy. This defect by itself does not cause the disclosure of confidential information nor allow unauthorized access.

The countermeasure to combat this denial of service attack is to upgrade the IOS to IOS 12.2 when it is available. Additionally, looking at the ports that Cisco says will cause the reload when a connection attempt is made, it would seem that by blocking those ports with an access list on the external interface the reload would not occur.

Attack on an internal system through the perimeter system.

Mark's primary firewall is the Cisco Pix 515 version 6.0. An old vulnerability that has been reintroduced is the SMTP Content Filtering Evasion Vulnerability with bugtraq ID 1698.

I have chosen to attempt the compromise of the mail server using the above vulnerability. My reasons for doing so would be to obtain a list of users. This list of users could then be utilized in further attacks where brute force password cracking would be necessary. Obtaining the user names would greatly increase the chances of cracking passwords

The following information on this vulnerability was taken from the Vulnerabilities section of the SecurityFocus web site.

Like other firewalls, the Cisco PIX Firewall implements technology that reads the contents of packets passing through it for application-level filtering. In the case of SMTP, it can be configured so only certain smtp commands can be allowed through (for example, dropping extra functionality, such as HELP or commands that could be a security concern, like EXPN or VRFY). When receiving messages, it allows all text through between "data" and "<CR><LF><CR><LF>.<CR><LF>", as this is where the body of the message would normally go and there could be words in it that are smtp commands which shouldn't be filtered. Due to the nature of SMTP and flaws in exceptional condition handling of PIX, it is reportedly possible to evade the smtp command restrictions by tricking the firewall into thinking the body of the message is being sent when it isn't.

During communication with an smtp server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the smtp server will return error 503, saying that rcpt was required. The firewall, however, thinks everything is alright and will let everything through until receiving "<CR><LF><CR><LF>.<CR><LF>". It is then possible for the attacker to do whatever he wishes on the email server.

If the mail server itself is not properly secured, an attacker may be able to collect information about existing e-mail accounts and aliases, or may be able to execute arbitrary code on the mail server. Cisco has released a firmware upgrade to fix this vulnerability. The Pix should be upgraded to version 6.1(1).

References

Stevens, W. Richard, TCP/IP Illustrated, Volume 1. USA: Addison Wesley February 2000.

Albitz, Paul, Liu, Cricket, DNS and BIND USA: O'Reilly September 1998.

Cisco Press, Cisco IOS Network Security USA: Macmillan Publishing Company 1998.

Network Associates, Webshield 300 E-ppliance Administrator's Guide USA: Network Associates, 2000.

Cisco website http://www.cisco.com/

Dr. Philip Enslow, a professor in the College of Computing – Ga Tech http://gtresearchnews.gatech.edu/reshor/rh-win99/info.html

WWW.pgp.com knowledgebase

SANS Track 2 – Firewalls and Intrusion Detection Course Materials.

D. Brent Chapman and Elizabeth D. Zwicky Building Internet Firewalls, USA O'Reilly June 2000.

CertCC www.cert.org

Security Focus www.securityfocus.com

Snort port database www.snort.org

Lance Spitzners white papers http://WWW.enteract.com/~lspitz/armoring.html