Assignment

Assignment 1 – Egress filter - 10 Points

Write a one page tutorial on the reasons for or against egress filtering. Be certain to include the following:

Syntax of the filter
Description of each of the parts of the filter
Explain how to apply the filter
Explain how to test the filter

Firewall or filtering router acts as implementation of a company's security policy. It provides a mechanism for protecting important company data and processes. It communicates a consistent security standard to the technical staff, user community, and management. The reason why egress filtering should be apply is because it ensures that all packets leaving the network are using the legal IP address space that is allocated to us. Another reason is to ensure that our network is not used as a source for spoofed attacks. With the current popularity with distributed denial of service, spoofing is a major problem as it adds to the complexity of tracking down an attacker's exact location. Many attack tools and hijacking relay utilize the ability to spoof outbound traffic.

The best way to make sure that our internal network is not used to spoof outbound traffic is to ensure that only legal addresses are allowed out to the Internet. If only the legal addresses are allowed out, a potential attacker has a harder time hiding their tracks.

In order to help prevent our network from being used in denial of service (DOS) attacks, the following access list is in place on the routers. The access list is placed on the outbound of the interface that connects to the ISP.

Assuming our legal address is 192.160.100.0, a example of the egress filter rules on a Cisco router would be:

```
access-list 101 permit ip 192.160.100.0 0.0.0.255 any
access-list 101 deny ip any any log
```

The filter rules translate to this: "If the source IP is the 192.168.100.0 network, let the traffic through. Drop all packets using any other address as a source IP address." Once this filter has been applied, internal systems will no longer be able to generate packets that will appear to have originated from another network. Spoofing is no longer possible. In effect, this access list will prevent packets being sent from our network with any source IP address other than our legal network. If there is more than one connection to the Internet, this should be applied outbound on any interface connected to the Internet.

The "log" at the end of the deny statement in the access list, will log any packet that is sent with a source address other than the ones permitted by the previous statement. . All traffic that is not using this legal address space would be dropped by the router and promptly logged. Entries are logged to the console by default.

The following command from global configuration can also be added:

```
logging (IP address of syslogd server)
```

This will send all log entries to a syslogd server at the specified IP address which is listening on UDP/514.

Once the access-list is created, it needs be bind to the interface. To do that, we perform the following commands:

```
external-gw#interface ethernet0/0
external-gw#ip access-group 101 out
external-gw#^Z
external-gw#write
```

Once this filter has been applied, internal systems will no longer be able to generate packets that appear to have originated from another network. Spoofing is no longer possible.

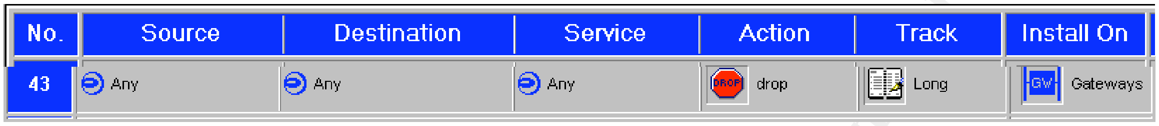
Once the egress filter in place, it needs to be tested. In order to test the filter, we need to send a few packets through the interface with spoofed source IP addresses. To accomplish this, we use a packet generator to create custom packets with an incorrect source address but a destination address that will be routed to the router with the egress filter. A second method is that, we can change the IP address of a machine on the network and send requests. We will not get a reply so we will need to check the logs on the router. The command "show ip access-list 101" will display counters for each access. This will result in a printout to the terminal of access list 101 showing the number of times each rule was used. If the filter is working we should see an increase in the number of times that the 'deny any' rule was used. This will confirm that the counter for the expression to pass the address block is incrementing.

If every network administrator were to employ an egress filter, denial of service attacks would be less likely to be successful. It would also be harder for an attacker to infiltrate our networks.

Assignment 2 – Firewall policy violations - 50 Points

List five violations of your site's firewall policy. For each log file detect:

Show the log entry with the violation, explain all fields in the detect with a key
Describe the rule that caught the violation including explaining the rule
Explain the potential damage if the firewall had not stopped the attack



No.	Source	Destination	Service	Action	Track	Install On
43	Any	Any	Any	drop	Long	Gateways

```
26May2000  3:50:24 drop   fw.acme.com >le0 proto tcp src 207.1.135.171 dst fw.acme.com
service 32776 s_port 46299 len 44 rule 43 xlatesrc 207.1.135.171 xlatedst fw.acme.com
xlatesport 46299 xlatedport smtp
```

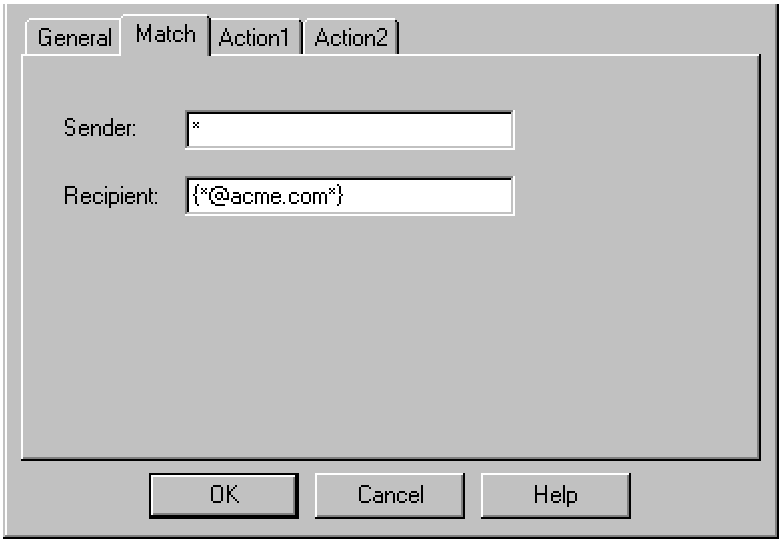
This log entry indicates that the firewall's (fw.acme.com) interface le0 detected a tcp connection from the source address 207.1.135.171. This host attempted to connect to the firewall port 32776 using the smtp protocol. The log shows that this connection attempt was dropped by rule 43. Rule 43 is the last rule in this firewall configuration. The last rule in the firewall shows that Any source trying to connect to any other source will be dropped.

```
26May2000  3:52:43 drop   fw.acme.com >le0 proto tcp src server.art-deco.co.jp dst
fw.acme.com service sunrpc s_port sunrpc len 40 rule 43
```

This log entry indicates that the firewall's (fw.acme.com) interface le0 detected a tcp connection from sarver.art-deco.co.jp (a server from Japan) trying to connect to r-services. The r-services are known to be potential security risk due to the nature of their programming. If the attacker were successful in connecting to the r-commands, then it is possible for them to gain access to the root id. Many company purchase firewall products, such as Check Point, but they fail to secure the underling operating system. This is a major risk a company takes when the system admin is not knowledgeable or does not place security as priority. This connection is also stopped by the rule above.

```
26May2000  8:42:47 drop   fw.acme.com >hme0 proto tcp src somepc01 dst fw_inside.acme.com
service Real-Audio-PNA s_port 56713 len 44 rule 43
```

This log entry indicates that the firewall's (fw.acme.com) interface le0 detected another tcp connection. However, a careful look reveals that the connection is made from the internal proxy to the inside interface of the firewall. The service requested is the Real-Audio service. It indicates that someone is trying use the Real-Audio application. Although there are minimum risk in using Real-Audio Player (as suppose to Real-Audio Server), it still take up lots of bandwidth. It is allow only as needed basis. The user



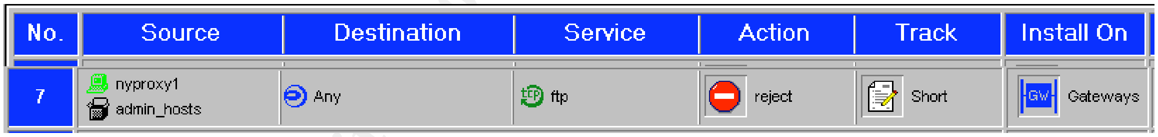
Sender: *

Recipient: {*@acme.com*}

needs to have the business justifications or it will not be allowed. The connection is also stopped by the rule above.

```
26May2000 6:06:43 reject fw.acme.com >daemon proto tcp src 203.238.91.79 dst fw.acme.com
service smtp s_port 3484 agent mail server from <advertiseonline@unbounded.com> to
<webmaster@fw.acme.com> rule 43 reason Content Security - access denied.
```

This log entry indicates that the firewall's (fw.acme.com) interface detected a tcp connection. Its source is from 203.238.91.79 with a source port of 3484. This connection was not DROPPING. Instead it was REJECTED due to the content check within Check Point SMTP definition. This would send the REJECTED message back to the initial requester. This also prevented unauthorized users to use our firewall to bounce or spam others.



No.	Source	Destination	Service	Action	Track	Install On
7	nyproxy1 admin_hosts	Any	ftp	reject	Short	Gateways

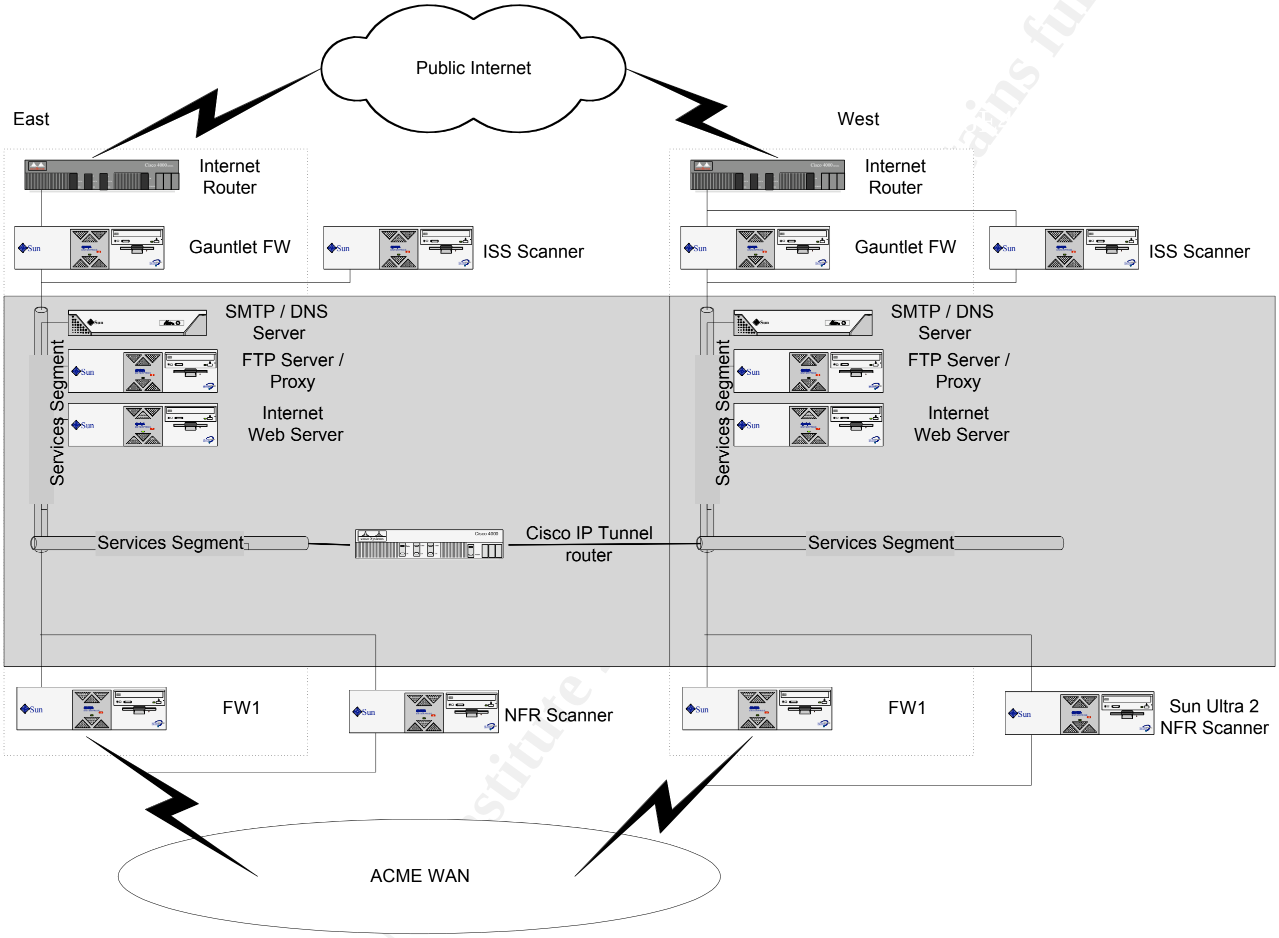
```
26May2000 9:17:08 reject fw_inside.acme.com >hme0 proto tcp src somepc02 dst ftp.abc.com
service ftp rule 7
```

This log entry indicates that the firewall's (fw.acme.com) interface hme0 detected a tcp connection. This time it is from somepc02 try to connect to abc.com using the ftp protocol. We could have left this rule out and let it default to the last rule of any - any - any - drop. As it turns out, this use to be a permitted function, but now the policy changed. We want to give the admins some time to adjust to the change. Therefore, the action is reject instead of drop. Eventually, this rule will be dropped and the last rule will be applied.

Assignment 3 – Defense in depth architecture - 10 Points each

Submit a detailed design for a site with dual connections to the Internet that is optimized to be resistant to DDOS attack. Include a description of the hardware and configuration. A drawing is a requirement for this assignment. Please keep in mind that the main goal of this assignment is to allow you to demonstrate what you have learned in the course, there may not be a "perfect" answer to this problem.

ASSIGNMENT #3 PART I



This design addresses the three main area that have been identified as limitations/weakness for any internet infrastructure.

Service delivery – The new architecture will provide controlled access to a wide range of Internet services. These services can be separated into two categories.

Internet services provided to ACME employees: - http access, real audio, real video, FTP access, Net News, etc.

Internet services ACME provides to the public Internet: - http sites, real audio / video presentations, Internet video conferencing, FTP sites, VPN termination points, etc.

Of this second set of services only a small subset will ever be public services. *Redundancy* – The designed architecture will provide the above services in a highly available manner. This redundancy will allow for 24x7 operation and will be capable of withstanding hardware/software failures. It will also prevent routine maintenance and upgrades from impacting service delivery. Where possible redundancy will be provided from different geographic locations, rather than multiple servers in a single location. This provides enhanced redundancy for disasters such as power failure, flood, fire, theft, etc, and reduces server count, cost and management overheads in each location.

Security – Security will form an integral part of the new Internet Services Architecture. Services will be ether managed out of band or via encrypted tunnels to prevent sniffing of administration passwords and data. This design will also address the distributed denial of service attackes. This will provide a secure and manageable DMZ from which our Internet and Intranet services can be hosted.

Internet Router

The internet connection consists of dual connections to different ISPs at two locations. The ISP connections are redundant via the BGP (border gateway protocol). The gateway routers employ ingress filters that allow established connections to the mail server, the ftp server, and the www server. Inbound new connections are allowed to the ftp, www, and dns servers. The following is the access list that is installed on the routers for incoming connections:

```
Access-list extended ingress permit tcp any www eq 80
Access-list extended ingress permit tcp any ftp eq 21, 20
Access-list extended ingress permit udp any dns eq 53
Access-list extended ingress permit tcp any smtp eq 25
Access-list extended ingress deny ip any any log
```

In addition to employing an ingress filter, we are employing an egress access list that allows only the gateway firewalls, the web proxy server, the mail server, and the ftp server from communicating out.

Finally, we have do not pass any ICMP packets on our outside routers. Also, we disable most services on the routers themselves.

Services segment

The services segment will provide a geographically independent area for the presentation of content to the public Internet and users within ACME. Using IP tunnelling the services segment is viewed as a single VLAN. This VLAN will accessible via two routes from the public Internet (East cost, West cost). These routes advertise the services segment as a single BGP autonomous system (AS). The design allows for the addition of further access points into the services segment to accommodate any expansion in ACME's branch network.

From within ACME there will also be two routes onto the services segment. These routes will advertise the services segment to the ACME WAN via EIGRP.

External Firewall

To provide maximum protection from the Internet the exterior Firewall will be the "Adaptive Proxy" based Firewall. An Adaptive proxies provide circuit level connections between each interface of the firewall at a protocol level. By its very nature a proxy must have a protocol level understanding of its data stream. It is this understanding that provides an extra layer of protection over state-full inspection. It is this added level of security that made a proxy Firewall our number one choice for the external Firewall.

Internal Firewall

Should the services segment become compromised in some way the Internal Network will be protected via a second Interior Firewall. This Firewall will be used to increase overall security and act as a point of audit and control between the Internal WAN and the DMZ.

ISS Scanner

ISS Scanner will be connected around the Exterior Firewall and will be used to provide detailed reports on the flow of data through it. These reports will be used to detect intrusion attempts and miss-configuration outside of ACME perimeter.

NFR Scanner

NFR Scanner will be connected to the DMZ and will be used to provide detailed reports on the flow of data in the DMZ. These reports will be used to detect intrusion attempts and miss-configuration within the DMZ. NFR was chosen instead of ISS because it provides: a) defence in depth, b) it could resolve data faster than ISS.

SMTP / DNS Server

DNS and SMTP Services will be provided on a separate box. This will increase service separation allowing maintenance to be performed with out impact to the security infrastructure.

Proxy Farm

A pair of servers will be used as general-purpose proxies for Internal access to the Internet. These servers will run a mixture of Netscape proxy server and FTP proxies. They will be used as a central point for Internet caching, content filtering and access reporting. The farm configuration allows for proxy redundancy and increased performance when experiencing heavy loads. It will also allow controlled maintenance to be performed with out impact to service delivery.

IP Tunnel server / VPN Router

This router will provide two main functions to the DMZ. Firstly it will provide the infrastructure with an IP tunnel back through the Interior Firewall to the other DMZ segments. This will allow DMZ hosts and services to be viewed as single entities regardless of location. Secondly it will provide IPSEC VPN tunnels out to the Internet for the connection of remote sites. Using this router the possibility of reducing WAN costs via the Internet can be investigated.

Load Balancers

Each geographic DMZ will incorporate a load-balancing device that will handle both the Internal and external traffic into the DMZ. Along with load balancing the device will be capable of providing redundancy to most IP services within the DMZ. Client connections will access services through the Load Balancer and be connected to the least loaded or currently available server.

ASSIGNMENT #3 PART II

A site has two critically important internal subnetworks, research and accounting, that require a high degree of protection. The site is connected to the Internet. An employee that has since left secured budget approval for one Cisco router, one proxy firewall and two appliance type firewalls with 2 10/100 NIC's, capable of performing in a bridging nature (similar to SunScreen), and this equipment has been ordered and has arrived and cannot be sent back. Submit a detailed design for the most effective protection. A drawing is a requirement for this assignment.

Assumptions:

1. Company has a class C legal address of (198.199.200.0)
2. Company has two critically import internal subnet (192.168.10.0 and 192.168.20.0) as the private IP addresses
3. Budgeted item has arrived:
   a) One Cisco router
   b) One proxy firewall with three interfaces address as follows:
      1) External 198.199.200.100
      2) Research 192.168.10.1
      3) Accounting 192.168.20.1
   c) Two appliance type firewall with two 10/100 NIC's
4. The only internet service allowed by the company is email and web browsing
5. Internal network is a 10/100 switch environment

Internet Router

The gateway routers employ ingress filters that allow established connections only to the proxy firewall. All other connection must be initiated from within the company or by the firewall. The following is the access list that is installed on the routers for incoming connections:

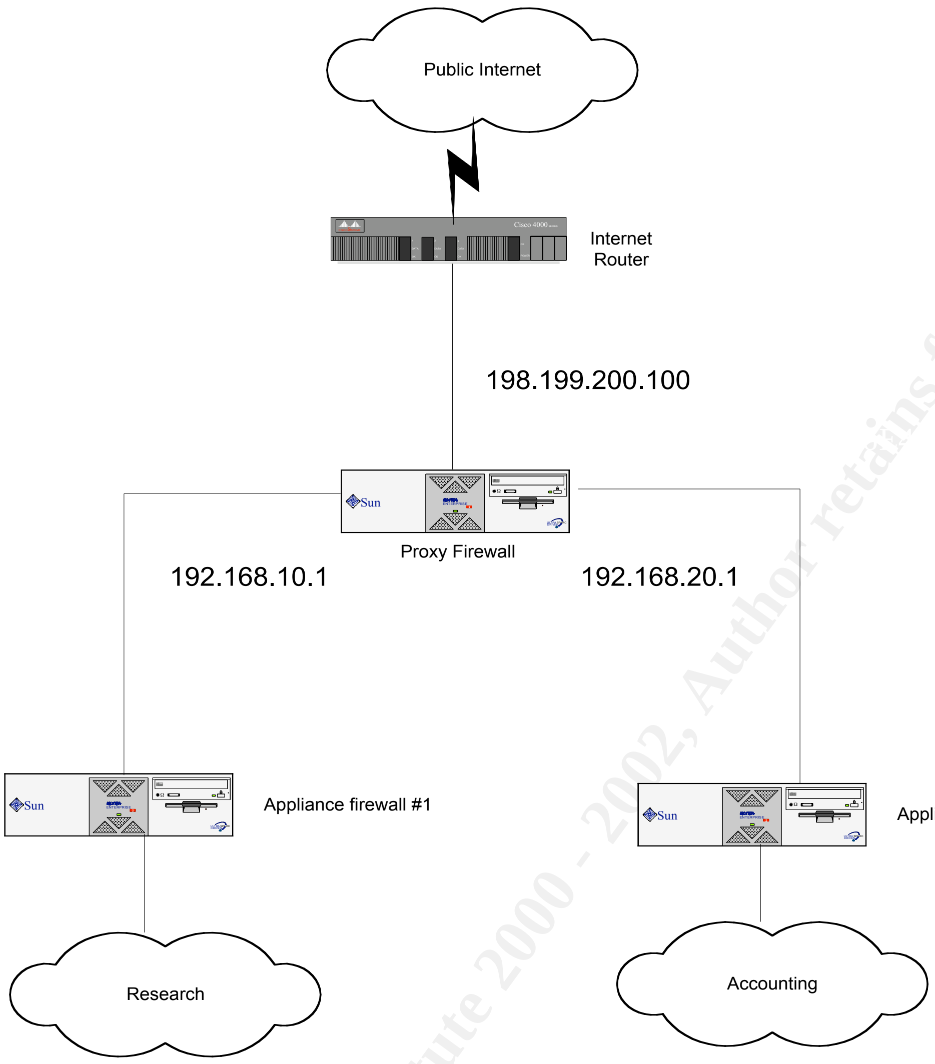
```
Access-list extended ingress permit tcp any smtp eq 25

Access-list extended ingress deny ip any any log
```

In addition to employing an ingress filter, we are employing an egress access list. The Internet router allows outbound connections only from the outside IP address of the proxy firewall. This helps with spoofing and other requests.

Proxy Firewall

To provide maximum protection from the Internet the exterior Firewall will be the "Adaptive Proxy" based Firewall. An Adaptive proxies provide circuit level connections between each interface of the firewall at a protocol level. By its very nature a proxy must have a protocol level understanding of its data stream. It is this understanding that provides an extra layer of protection over state-full inspection. The proxy firewall serves as the gateway for all Internet access.



Appliance Firewalls

Appliance firewall bridge data between the department subnet to the external network. All HTTP requests are send out through the proxy firewall. The Research users must point to 192.168.10.1 (the IP for the interface that connects the proxy to Research) and the Accounting users must point to 192.168.20.1, respectively. Since, no internal router was ordered this is a must to route the traffic to the Internet. The network appliance firewalls will allow only reply traffic to their own subnet. Any time requests are sent from within those segments that need to connect to the Internet, the traffic is passed through the firewalls.

Assignment 4 - Create a test that demonstrates your knowledge of the subject area - 20 Points

Develop a scenario that must be solved similar to the two above and submit both your question and your answer.

This assignment will be scored primarily on three factors:

Does the submission demonstrate the student's knowledge of the subject area, so pick a problem that

let's you flex your brain muscle!

Is the solution to the problem accurate

Is the solution well researched and list URLs, references and resources

A drawing is a requirement for this assignment.

Your company decided to open a branch office in Singapore. A T1 has been order from the local ISP and the connection is near completion. This will be your only link to the outside world. The remote office requires direct http connection to the Internet due to speed requirement. All other services such as email, and various corporate applications will be connect via this link and would require to be secured. The company has selected a VPN solution that is different from the proxy firewall. You give the following information:

1) Two routers
2) One State-full Inspection Firewall
3) One VPN Server. The VPN utilize UDP 500 and Protocol = 50
4) The external IP of the headquarters' firewall has the IP (200.200.200.10)
5) The VPN Server at headquarters is behind the firewall and is NATed.

Best of luck!

Sample Solution

Internet Router

Given these requirements, the only connection from the Internet should be the VPN from headquarter. Therefore, the Internet routers ingress filters should reflect the fact that the only allowed connections should be between headquarter and the VPN server. All other connection must be initiated from within the company or by the firewall. The following is the access list that is installed on the routers for incoming connections:

```
Access-list extended ingress permit udp 200.200.200.10 50 eq 500

Access-list extended ingress deny ip any any log
```

In addition to employing an ingress filter, we are employing an egress access list. The Internet router allows outbound connections only from the outside IP address of the proxy firewall. This helps with spoofing and other requests.

State-full Inspection Firewall

A state-full inspection firewall employing the technology to analyze data derived from various communication layers. This state is stored and updated dynamically for tracking connectionless protocols. The combination of data from the communication and application states, network configuration and security rules, are used to generate an appropriate action – accepting, rejecting the communication. The firewall is setup to allow http outbound and VPN (UDP = 500, protocol = 50) to pass through the firewall. ICMP should be turn off.

Rule #	Source	Destination	Service	Action	Log	comments
1	Any	firewall	Any	drop	long	Denied access to the firewall
2	Inside	Outside	Http	Allow		Web browsing
3	Headquarter	VPN	UDP/ESP	Allow	long	VPN from Headquarter
4	VPN	Headquarter	UDP/ESP	Allow	long	VPN to Headquarter
5	any	any	any	drop	long	All else drop and log

Virtual Private Network (VPN) Server

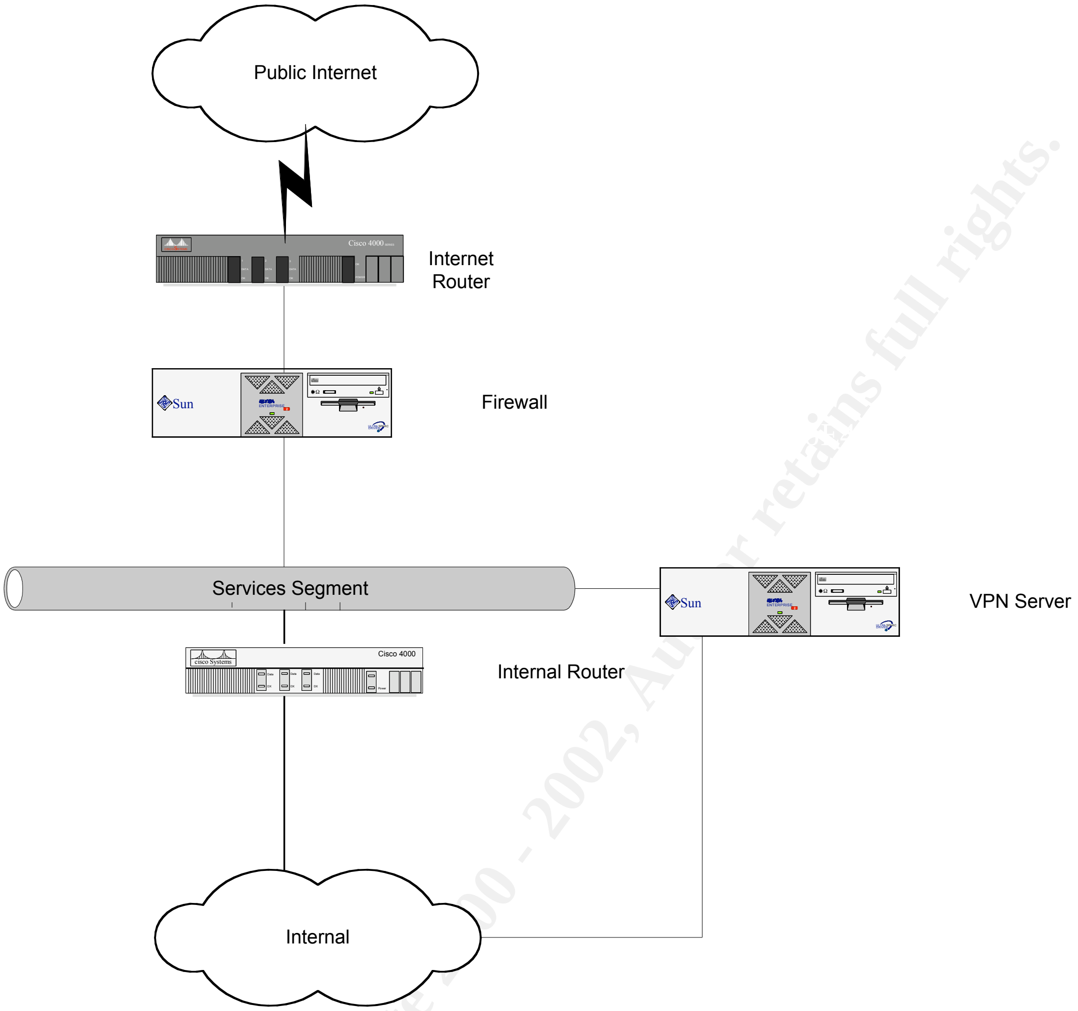
Advanced technology such as Secure Remote can be used to establish secure, encrypted sessions over the Internet to customer facilities. The VPN connection is allowed to be connected from the Internet by the firewall. Therefore, this server must be lock down. The server also by passes the internal router. It must be view with high sensitivity.

Internal Router

At this point, all VPN traffic is passed to the VPN server. There should only be outbound traffic. Therefore, the internal routers employ ingress filters that deny all inbound traffic. All other connection must be initiated from within the company. The following is the access list that is installed on the routers for incoming connections:

```
Access-list extended ingress deny ip any any log
```

In addition to employing an ingress filter, we are employing an egress access list. The Internal router allows outbound http connections only.



SECURITY IS PART OF THE INFRASTRUCTURE INTERNET SERVICES, NOT AN AFTER THOUGHT.