Global Information Assurance Certification Paper

L. Christopher Paul
SANS GIAC Firewall and Perimeter Protection Curriculum
Practical Assignment for SNAP San Jose
June 13, 2000

Assignments:

Assignment 1 – Egress Filtering

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

Assignment 2 – Firewall Policy Violations

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

Assignment 3 – Defense in Depth

A. 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.

B. 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.

Assignment 4 – Question Creation

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.

Assignment 1 - Egress Filter

Egress filtering, or the application of a ruleset to traffic leaving a network, has come to prominence because of the recent Distributed Denial of Service (DDOS) attacks against some prominent WWW portal and e-Commerce sites.

Until recently little or no attention was paid to the traffic leaving a network and firewalls were put into place primarily to prevent attackers from compromising hosts on the internal network. With the preponderance of email viruses that do not need to be opened in order to infect, mobile laptop users with dial-up connections, insecure web browsers and other security issues, it can no longer be assumed that 'bad guys' are on the outside.

There appears to be little doubt that the Internet is rapidly becoming a business-critical application not only for corporate America, but for the world as well. If this progression is going to continue it will be necessary for the Internet community to undergo a considerable change in the way that it perceives what is proper 'nettiquite'.

In its early days, the Internet was much like a rural farmer in mid-America. Freedom was something that he took for grated much as the fresh air that he breathed and the scenic view that he enjoyed from the back porch. He minded his own business and, by and large, everyone else kept to themselves. His nearest neighbor was several miles down the road and he permitted the family dog the freedom to run on the homestead.

But seemingly overnight the city began encroaching upon his home and what had been woods and corn fields were quickly replaced with office buildings and mini-marts. As much as he may disagree with what is happening around him, there is little that he can do about; And while the temptation to continue to let 'Spot' run free remains it is time to realize that this policy is not safe for the neighbors. Nor is it safe for the dog -- it's time to put a fence up.

Egress filtering is that fence. It can keep an infected server or workstation from 'attacking the neighbor' in much the same way that a physical fence can keep a rabid dog from taking a chunk out of the seat of neighbor Jimmy's pants.

Egress Filtering for Linux & IPChains:

As with most packet-filtering firewalls and routers, there is a simple and effective way to prevent spoofed traffic from leaving your network. With IPChains, it's simply a matter of not forwarding outbound traffic whose source IP address differs from the address space that the router or firewall is serving.

For example, if you have a firewall that is serving the 10.0.2.0/24 (eth1) subnet, you simply need to insert a rule into the ruleset that prevents any non-local traffic from leaving that network.

Example:

```
/sbin/ipchains -I input -i eth1 -s ! 10.0.2.0/24 -j REJECT -l
```

This command inserts a rule at the top of the input chain (-I input) for the second ethernet interface (-i eth1) that tells it to reject and log (-j REJECT -l) all packets whose source port are not on the local subnet. (-s ! 10.0.2.0/24)

Testing the Rule:

To test the rule, you can use ipchains' –C option to see what the firewall will do with a particular packet. First make sure that the forwarding is working for an address that is legal on that subnet:

```
/sbin/ipchains -C forward -i eth1 -s 10.0.2.1 1025 -d 10.0.1.2 80 –p icmp
```

If that works, change the source IP to one that is not legal for that subnet and see what happens to that traffic:

```
/sbin/ipchains -C forward -i eth1 -s 192.168.1.1 1025 -d 10.0.1.2 80 –p icmp
```

If the first command reports that the traffic is forwarded or masqueraded and the second one states that the packet would be rejected, then the egress filter is in place and working properly.

Be sure and repeat the testing for the TCP and UDP protocols (-p tcp & -p udp) just to make sure.

Assignment 2 – Firewall Policy Violations

All of the policy violations in this section have the same format, namely:

```
Jun  1 11:11:49 mail kernel: Packet log: input REJECT eth0 PROTO=17
10.100.1.228:57048 192.168.1.211:137 L=78 S=0x00 I=53412 F=0x0000  T=108 (#3)
```

Field	Example	Description
Date & Time	Jun 1 11:11:49	Date and time that the packet was logged.
Hostname	mail	The hostname of the computer.
Syslog Facility	kernel: Packet log:	The syslog level at which the syslog event occurred. Should always be 'kernel'. 'Packet log:' is appended for clarity's sake and can be used in searching the logs.
Chain Name	input	The chain to which the rule is attached to. Possible values are: input, output and forward.
Action Taken	REJECT	How the packet was handled. Possible values are: ACCEPT, REJECT, DENY, MASQ, REDIRECT and RETURN.
Interface	eth0	The network interface on which the packet was detected.
Protocol #	PROTO=17	The protocol of the packet. Common values are: 1 (ICMP), 6 (TCP), and 17 (UDP). ICMP traffic is also displayed with the ICMP code.
Source	10.100.1.228:57048	The source IP address and port number of the packet.
Destination	192.168.1.211:137	The destination IP address and port number of the packet.
Length	L=78	The total length of the packet.
TOS	S=0x00	The 'Type of Service' values from the packet.
ID	I=53412	Either the Packet ID or the segment that the TCP fragment belongs to.
Fragment Offset	F=0x0000	If the packet is part of a fragment, this field contains the fragment offset.
TTL	T=108	The time-to-live values from the packet.
Rule #	(#3)	The rule number that logged this entry.

1 – Netbios-ns Traffic

Detect:

```
Jun  1 11:11:49 firewall kernel: Packet log: input REJECT eth0 PROTO=17
10.100.1.228:57048 192.168.1.211:137 L=78 S=0x00 I=53412 F=0x0000  T=108
(#3)
```

This detect shows that remote host 10.100.1.228 tried to connect from port 57048 to UDP port 137 on the firewall via the external interface (eth0). This packet was REJECTed by the firewall filters.

Rule:

```
/sbin/ipchains -A input -i eth0 -s 0/0 -d 192.168.1.211/24 137:139 -p udp
-j REJECT -l
```

This rules rejects all netbios traffic (-p udp & 137:139) directed at this network (-s 0/0 –d 192.168.1.211) as there is no reason legitimate for this traffic to be traversing the Internet. It applies as an inbound rule (-A input) on the first ethernet interface (-i eth0). All traffic will be rejected and logged (-j REJECT –l).

Potential:
Netbios Name Service is a protocol designed to permit hosts to exchange information about themselves and other hosts without the necessity of having a centralized server. Had this traffic been allowed into the network, the 10.100.1.228 host would have obtained name and (potentially OS) information about targeted Windows hosts.

This information gathering could then have been he prelude to surfing for open or exploitable Windows shares.

2 – Telnet

Detect:
```
May 4 19:24:31 firewall kernel: Packet log: input DENY eth0 PROTO=6
10.100.1.41:3633 192.168.1.211:23 L=44 S=0x00 I=3981 F=0x4000 T=126 (#11)
```

Rule:
```
/sbin/ipchains -A input -i eth0 -s 0/0 -d 192.168.1.211/24 0:1023 -p tcp -
j DENY -l
```

This rule also applies to the inbound (-A input) chain on the 1st ethernet interface (-i eth0). It denies and logs (-j DENY -l) all TCP traffic to low-numbered ports (-p tcp & 0:1023) unless specifically permitted by a previous rule.

Potential:
Telnet is an insecure remote access tool available on UNIX and other platforms. By having this service accessible from outside the network, yet another pathway into the host is provided. In addition to possible buffer overflow and other exploits, this is yet another method by which an attacker could validate and test usernames and passwords.

3 - DNS Zone Transfer

Detect:
```
May 16 16:50:14 firewall kernel: Packet log: input DENY eth0 PROTO=6
10.100.1.218:4008 192.168.1.211:53 L=60 S=0x00 I=32792 F=0x4000 T=54 SYN
(#11)
```

Rule:
```
/sbin/ipchains -A input -i eth0 -s 0/0 -d 192.168.1.211/24 0:1023 -p tcp -
j DENY -l
```

This rule also applies to the inbound (-A input) chain on the 1st ethernet interface (-i eth0). It denies and logs (-j DENY -l) all TCP traffic to low-numbered ports (-p tcp 0:1023) unless specifically permitted by a previous rule.

Potential:
This site configured to use a split DNS with information about publicly accessible servers being outsourced.

Had this traffic not been stopped at the firewall, a complete map of the internal network would have been available to anyone. With that information, individual hosts could have been targeted for further exploration or exploitation.

In addition to having a map of the network, there have in the past been a number of security issues with various name servers and with the information of which internal hosts were running which versions of the service, further exploitation may have been possible.

4 - VPN Traffic

Detect:

```
May 16 14:42:37 firewall kernel: Packet log: input DENY eth0 PROTO=17
10.0.0.160:1025 192.168.1.211:500 L=84 S=0x00 I=11566 F=0x0000 T=122 (#5)
```

Rule:

```
/sbin/ipchains -A input -i eth0 -s 0/0 -d 192.168.1.211/24 0:1023 -p udp -
j DENY -l
```

This rule also applies to the inbound (-A input) chain on the 1st ethernet interface (-i eth0). It denies and logs (-j DENY -l) all UDP traffic to low-numbered ports (-p tcp & 0:1023) unless specifically permitted by a previous rule.

Potential:
Port UDP/500 is used by IPSEC for ISAKMP key negotiations as the initial part of a VPN connection.

A Virtual Private Network (VPN) is a network designed to carry traffic in encrypted form across a public network. Due to encapsulation, the exact nature of the traffic can not be determined. The computer inside of the firewall would then re-broadcast the traffic back into the local network, thereby bypassing any and all policy management done at the firewall.

If inside users are permitted to set-up and access VPN servers from outside the network, then it effectively defeats in-bound policy management. It is essentially the same as permitting network users to have unregulated dial-in access.

5 - Trojan Scan

Detect:

```
Jun  3 06:52:14 firewall kernel: Packet log: input DENY eth0 PROTO=6
10.100.1.215:1443 192.168.1.211:27374 L=48 S=0x00 I=14045 F=0x4000 T=115
SYN (#14)
```

Rule:

```
/sbin/ipchains -A input -i eth0 -s 0/0 -d 192.168.1.211/24 0:65535 -y -p
tcp -j DENY -l
```

This rule also applies to the inbound (-A input) chain on the 1st ethernet interface (-i eth0). It denies and logs (-j DENY -l) all TCP traffic (-p tcp & 0:65535) with the SYN flag set
(-y), unless specifically permitted by a previous rule.

Potential:
Most likely this is a search for the SubSeven (v. 2.1) trojan. SubSeven is a 'remote management tool' for Windows and can be used to do everything from grab screen captures and sniffing passwords from the keybard to turning on a camera or microphone connected to the infected PC.

By blocking these packets, it elminates the ability for the controlling program to communicate with the trojan should one of the protected machines become infected.

If the firewall had not blocked these packets, any infected machines could have been used to gather corporate or private information, been used in a DDOS attack against another site or in just about any other manner in which the controlling agent wished.

Assignment 3 – Defense in Depth Architecture

A. DDOS Resistant Site

The diagram shown (Figure 1) shows an example network capable of making an effort of resisting a Distributed Denial of Service (DDoS) attack. While it is, at present, impossible to stop these attacks from occurring, it is possible to provide some bit of redundancy and fail-over should an attack take place. Please note that design, nor any other design can guarantee that such an attack will fail – it simply attempts to absorb as much of the damage as possible while maintaining some sort of service.

While this network is designed around protecting a WWW server, it could easily be modified to protect any type of mission-critical server from this type of attack.

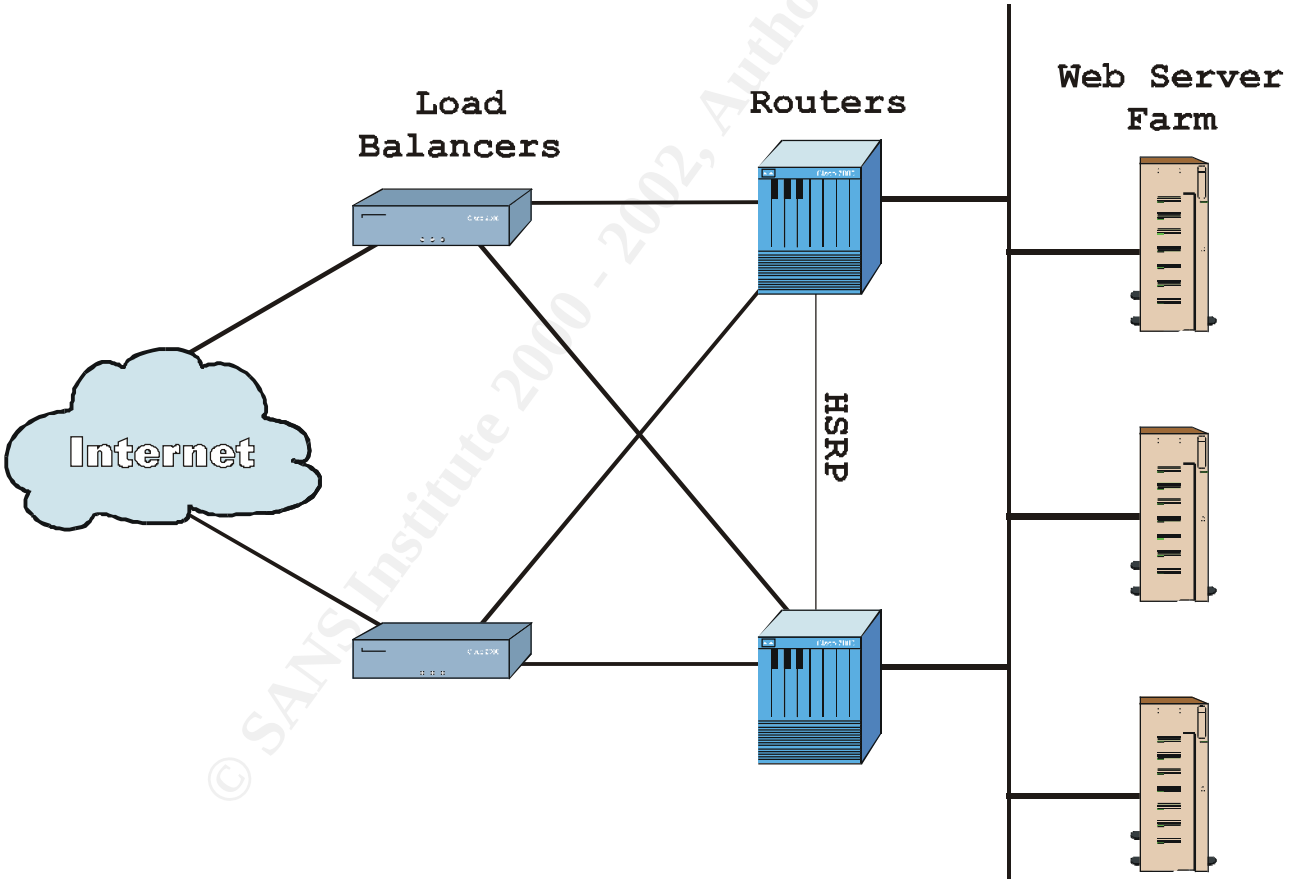

Figure 1

This first line of defense in this network is in providing dual connectivity to the Internet, preferably via two separate ISPs. By employing some form of load-balancing device (such as LocalDirector or Big-IP) the incoming Web traffic can be divided among the various servers in the server farm preventing one of them from becoming overwhelmed as easily. Beyond that, by employing the Hot-Spare Route Protocol (or something similar) between the routers, should one

of them become bogged down with the traffic, the other one would try to take over its functionality until such time that it could recover.

B. Multiple Firewalls

With the equipment given, I would design a plan formed around the diagram in Figure 2. This three-tiered approach would provide considerable security with the equipment available.

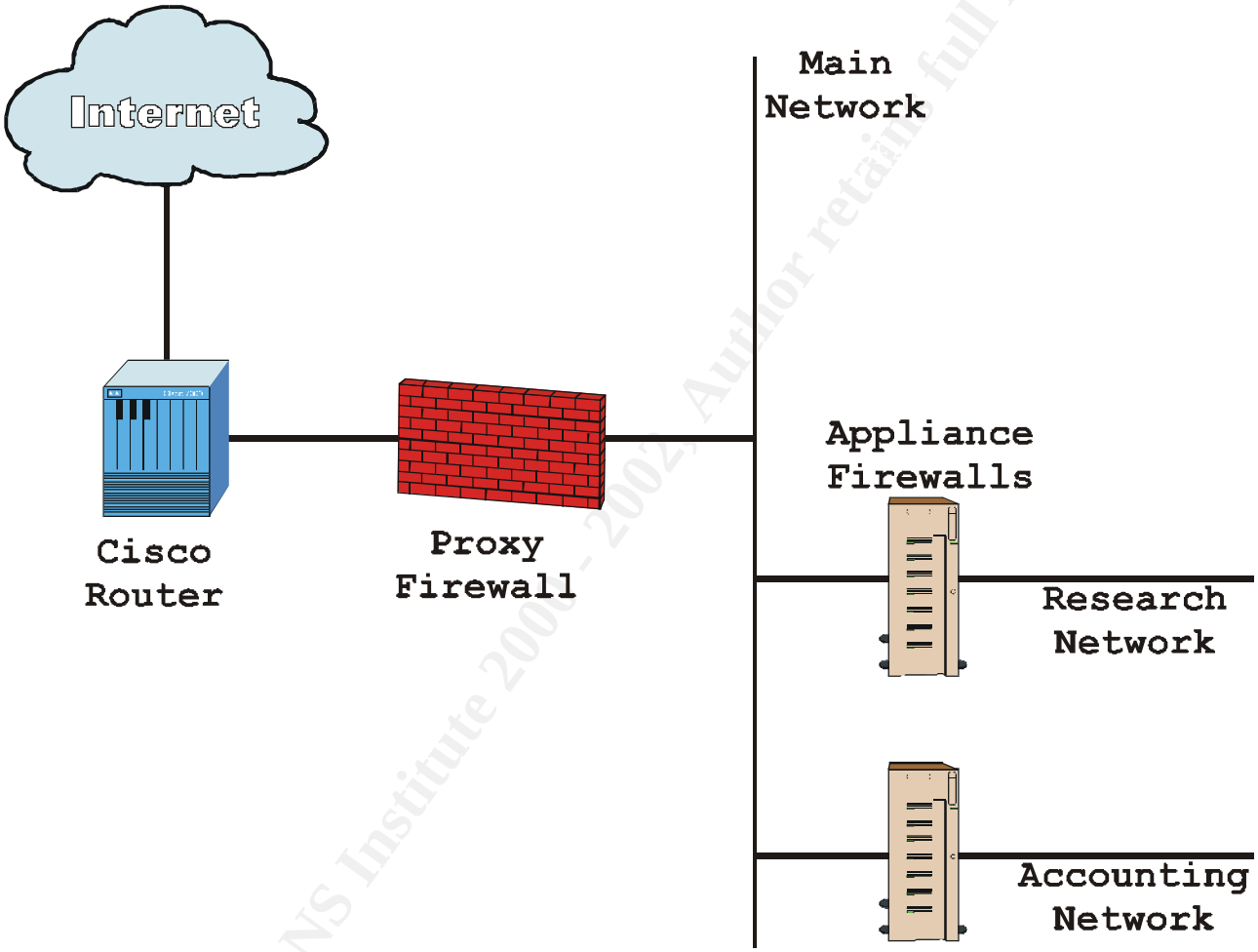

Figure 2

The Cisco router provides the first layer of defense by applying some generalized filtering rules to alleviate the stress on the Proxy Firewall. The router can take care of denying inappropriate traffic such as IANA restricted and private address space, denying source routed packets, some ICMP messages and TCP/UDP traffic not specifically permitted by policy.

Behind this the proxy firewall provides the main source of protection for the majority of the network. This firewall denies all traffic not in response to sessions originating from within the internal network and provides a further layer of obfuscation for potential attackers trying to gain information about the network.

Behind the proxy firewall lies the main network and the Accounting and Research networks. The later two are further protected by appliance-type firewalls with only accepted network traffic permitted out and only responses to that traffic permitted back in.

This architecture further limits an intruder in that each layer of the defense is on a different vendor's platform. This means that the same exploit that an attacker can use to bypass one layer of the defense perimeter can not by used to gain further access to the network – especially Accounting and Research.

Assignment 4 – Test Question Creation

QUESTION:
Submit a detailed plan (with a diagram) for a site with the following requirements:

- A Proxy Firewall that permits employees Internet WWW and ftp access only.
- A split DNS configuration
- VPN connectivity for travelling sales staff and telecommuters
- Publicly accessible WWW and ftp services.

Include in the description a generalized ruleset for any filtering that would need to be done at the various stages of the network.

ANSWER:
The following diagram depicts one design for such a network of the many potential designs available given the stated requirements.

The equipment used is:

- A router capable of packet filtering
- A proxy firewall
- A WWW/FTP server
- A VPN server
- Two DNS servers

The network configuration would be as follows:

The proxy firewall would, of course provide services for internal users to go out to the web and the ftp sites; while denying all other traffic.

The router would block all traffic to the screened network except for:

- dst port 53/udp to the Ext. DNS Server
- dst port 53/tcp from the site's secondary DNS server (assumed to be on a different network)
- dst port 80/tcp to the WWW/FTP server
- dst port 20/tcp to the WWW/FTP server
- dst port 21/tcp to the WWW/FTP server
- the ports necessary for the vendor's implementation of the VPN server
- ICMP traffic may be permitted from the protected network for administrative testing

To all hosts on the screened and protected networks, the router would also block:

- source-routed traffic
- all private and reserved address space

To the Internet, the router would be configured to block:

- all traffic whose source IP is not local to either the screened or the protected network (egress filtering)

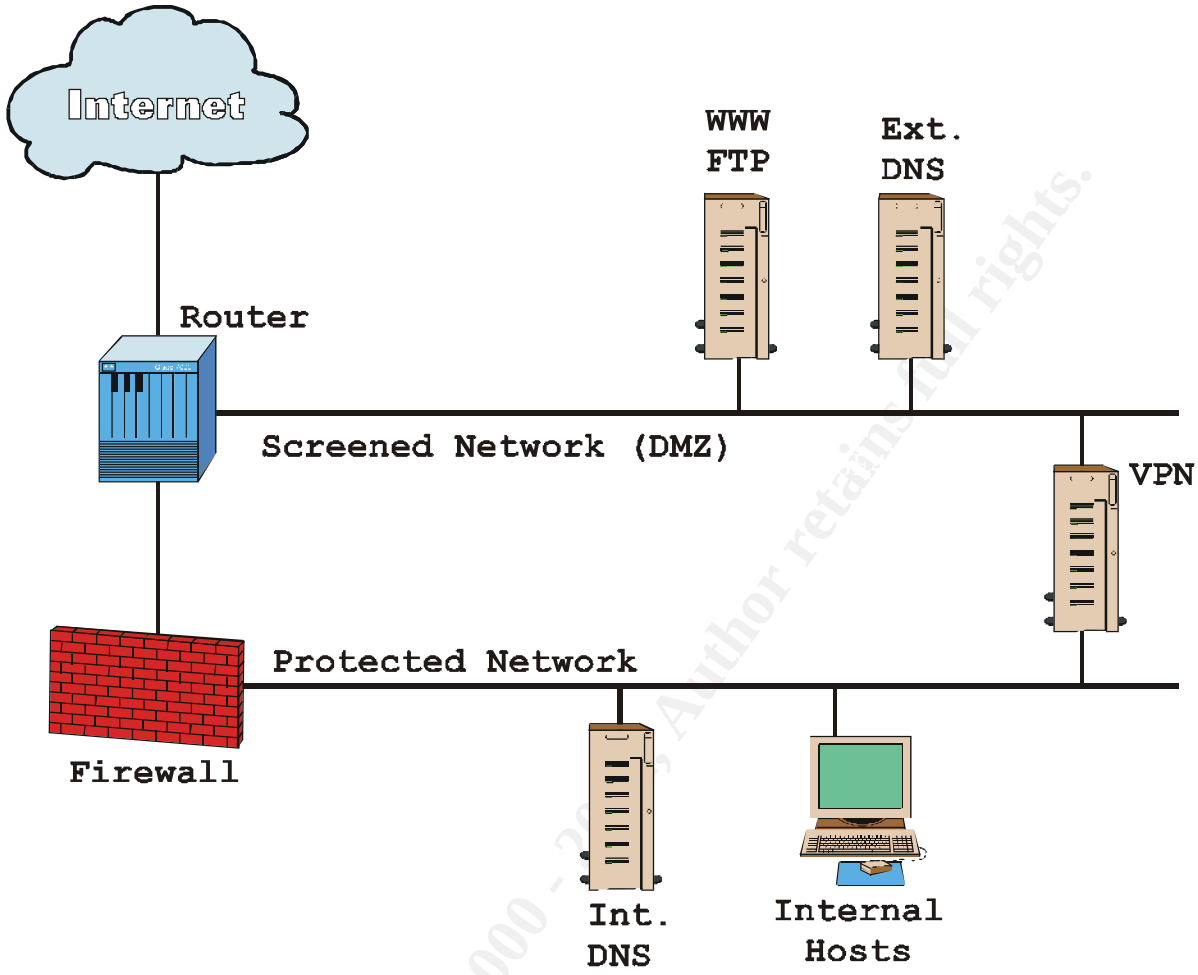

Figure 3

In addition to the servers shown and the services listed, it may be prudent to install some form of secondary authentication to the VPN server such as the RSA ACE/SecurID.