GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Robert V. McMillen Jr.
GIAC Firewall & Perimeter Protection Assignment

Assignment 1 - Egress filter (10 Points):

The main mission of an egress filter is to only allow legitimate network addresses from leaving the network. This will prevent hackers from using the network as an attack launching area (spoofing source ip addresses).

The easiest way to accomplish this task is to implement such a filter at the border router. Assuming the border router is made by Cisco, the following filter will accomplish the mission:

```
access-list 110 permit ip 222.222.222.0 0.0.0.255 any
access-list 110 deny any log
```

Assuming we have a class C (222.222.222.0) network, the first line of the Extended Access List (access-list 110) will permit our entire class C network to access the Internet. The 0.0.0.255 declares address comparison will stop after the first three octets. The second line is for logging purposes only. The access-list will deny by default, but it will not log the dropped packets which can alert a system administrator of a possible intruder using the network for illegitimate purposes.

The access-group should be applied as follows (assuming eth1 is the network side interface):

```
int eth1
    ip address 222.222.222.1 255.255.255.0
    ip access-group 110 in
```

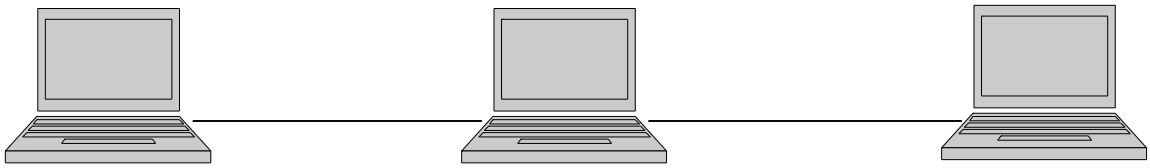
The first two lines establish interface configuration. The last line applies the filter to input traffic on the network side interface. This implementation will prevent the router from routing the packet from network interface to external interface just to drop it (wasting CPU time).

Finally, the filter needs to be tested in order to ensure it is working properly. First, ensure the legitimate network address space can access the Internet by accessing resources on the Internet. Next, use a tool which allows changes in source ip address. Nmap (by Fyodor) will allow you to perform port scans with decoy source ip addresses. By using the decoy flag and several ip addresses not belonging to the legitimate network space, the filter can be tested, and the logs should reflect the dropped packets.

Robert V. McMillen Jr.
GIAC Firewall & Perimeter Protection Assignment

Assignment 2 – Firewall policy violations (50 points):

Background: Three laptops in two networks (depicted below).



LAN	firewall	attacker
WinNT 4.0	Linux 2.2.12-20	Linux 2.2.12-20
10.0.0.2	eth0: 10.0.0.1	131.120.103.20
	eth1: 131.120.103.5	

The firewall rules were generated with ipchains. The policy violations were accomplished by the use of nmap (network mapper) and spak (packet generator).

First Violation (UDP Scan)

Log (see Log Key at end of assignment):

```
    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
1. May 29 18:16:52 firewall kernel: Packet log: input REJECT eth1 PROTO=17
       (8)      (9)       (10)    (11) (12)  (13)   (14)     (15)   (16) (17)
131.120.103.20:36536 131.120.103.5:892 L=28 S=0x00 I=11053 F=0x0000 T=47 (#81)

(1)     (2)      (3)                        (4)   (5)   (6)   (7)
2. May 29 18:16:52 firewall kernel: Packet log: output DENY eth1 PROTO=1
    (8)      (9)     (10)    (11)(12)  (13)   (14)    (15)   (16)  (17)
131.120.103.5:3 131.120.103.20:3 L=76 S=0xC0 I=1782 F=0x0000 T=255 (#15)
```

Line 1 rejects an incoming UDP packet to port 892, and line 2 denies a destination unreachable icmp message from reaching the attacker.

Rule:

chain	#	target	prot	opt	source	dest	ports
input	81	Reject	all	log	anywhere	anywhere	n/a
output	15	Deny	icmp	log	firewall	anywhere	type 3

Input rule 81 rejects and logs all input traffic not specifically allowed into the network by previous rules. While output rule 15 Denies icmp type 3 traffic (destination unreachable) from leaving the network.

Possible Damage:

These rules will not prevent reconnaissance of the firewall, but it will prevent the attacker from gathering information (UDP ports) on LAN machines. It will also alert the firewall administrator of the port scan.

Second Violation (TCP Scan)

Log (see Log Key at end of assignment):

```
    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
1. May 29 17:16:58 firewall kernel: Packet log: input REJECT eth1 PROTO=1
        (8)      (9)    (10)    (11)(12)  (13)   (14)     (15)   (16)  (17)
   131.120.103.20:8 131.120.103.5:0 L=28 S=0x00 I=18271 F=0x0000 T=42 (#81)

    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
2. May 29 17:16:58 firewall kernel: Packet log: output DENY eth1 PROTO=1

        (8)      (9)    (10)    (11)(12)  (13) (14)   (15)   (16)  (17)
   131.120.103.5:3 131.120.103.20:3 L=76 S=0xC0 I=0 F=0x0000 T=255 (#15)

    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
3. May 29 17:16:58 firewall kernel: Packet log: input REJECT eth1 PROTO=6
         (8)      (9)     (10)    (11)  (12)  (13)   (14)   (15)   (16)  (17)
   131.120.103.20:36455 131.120.103.5:80 L=40 S=0x00 I=7207 F=0x0000 T=37 (#81)


    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
4. May 29 17:16:58 firewall kernel: Packet log: output DENY eth1 PROTO=1
        (8)      (9)    (10)    (11)(12)  (13)   (14)  (15)   (16)  (17)
   131.120.103.5:3 131.120.103.20:3 L=88 S=0xC0 I=1 F=0x0000 T=255 (#15)
```

The log shows the rejection of a ping request (line 1) and the denial of a destination unreachable icmp message (line 2) from reaching the attacker. Line 3 shows the rejection of an incoming tcp packet destined for port 80, and line 4 denies the destination unreachable icmp message from reaching the attacker.

Rule:

chain	#	target	prot	opt	source	dest	ports
input	81	Reject	all	log	anywhere	anywhere	n/a
output	15	Deny	icmp	log	firewall	anywhere	type 3

Input rule 81 rejects and logs all input traffic not specifically allowed into the network by previous rules. While output rule 15 Denies icmp type 3 traffic (destination unreachable) from leaving the network.

Possible Damage:

Again, these rules will not prevent reconnaissance of the firewall, but it will prevent the attacker from gathering information (TCP ports) on LAN machines and alert the firewall administrator of the port scan.

Third Violation (SYN Scan)

Log (see Log Key at end of assignment):

```
    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
1. May 29 18:59:32 firewall kernel: Packet log: input REJECT eth1 PROTO=6

       (8)      (9)         (10)   (11) (12)  (13)   (14)     (15)   (16) (18)
131.120.103.20:37774 131.120.103.5:1367 L=40 S=0x00 I=21186 F=0x0000 T=49 SYN
(17)
(#81)

    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
2. May 29 18:59:32 firewall kernel: Packet log: output DENY eth1 PROTO=1

       (8)   (9)     (10)    (11)(12)  (13)   (14)    (15)   (16)  (17)
131.120.103.5:3 131.120.103.20:3 L=88 S=0xC0 I=3616 F=0x0000 T=255 (#15)
```

Line 1 rejects an incoming tcp packet with the syn flag set destined for port 1367, while line 2, denies the destination unreachable message from reaching the attacker.

Rule:

chain	#	target	prot	opt	source	dest	ports
input	81	Reject	all	log	anywhere	anywhere	n/a
output	15	Deny	icmp	log	firewall	anywhere	type 3

Input rule 81 rejects and logs all input traffic not specifically allowed into the network by previous rules. While output rule 15 Denies icmp type 3 traffic (destination unreachable) from leaving the network.

Possible Damage:

Again, these rules will not prevent reconnaissance of the firewall, but it will prevent the attacker from gathering information (TCP ports) on LAN machines and alert the firewall administrator of the port scan.

Fourth Violation

Log:

```
    (1)     (2)      (3)                        (4)   (5)   (6)   (7)
1. Jun 1 20:57:22 firewall kernel: Packet log: input REJECT eth1 PROTO=17

      (8)      (9)        (10)   (11)(12)  (13)   (14)     (15)   (16)  (17)
131.120.103.20:137 131.120.103.5:137 L=96 S=0x00 I=15362 F=0x0000 T=128 (#81)
```

This log entry denies a UDP netbios packet from entering the network.

Rule:

chain	#	target	prot	opt	source	dest	ports
input	81	Reject	all	log	anywhere	anywhere	n/a

Input rule 81 rejects and logs all input traffic not specifically allowed into the network by previous rules.

Possible Damage:

By preventing netbios from entering the network via the external interface, the firewall prevents Windows enumeration via netbios. It also prevents external exploitation of the file and print sharing services.

Fifth Violation (outsider spoofing)

Log:

```
   (1)     (2)      (3)                        (4)   (5)   (6)   (7)
1. May 29 22:37:07 firewall kernel: Packet log: input DENY eth1 PROTO=1

       (8)   (9)     (10)   (11)(12)  (13)   (14)     (15)   (16) (17)
131.120.103.5:8 131.120.103.5:0 L=28 S=0x00 I=33514 F=0x0000 T=42 (#3)
```

This log shows the denial of an incoming ping request with a source address corresponding to the firewall.

Rule:

chain	#	target	prot	opt	source	dest	ports
input	3	DENY	all	log	firewall	anywhere	n/a

This rule denies and logs all incoming traffic with a source address corresponding to the firewall.

Robert V. McMillen Jr.

Possible Damage:

By ensuring LAN addresses are not allowed to enter as a source address via the external interface, the firewall prevents several denial of service attacks from entering the network.

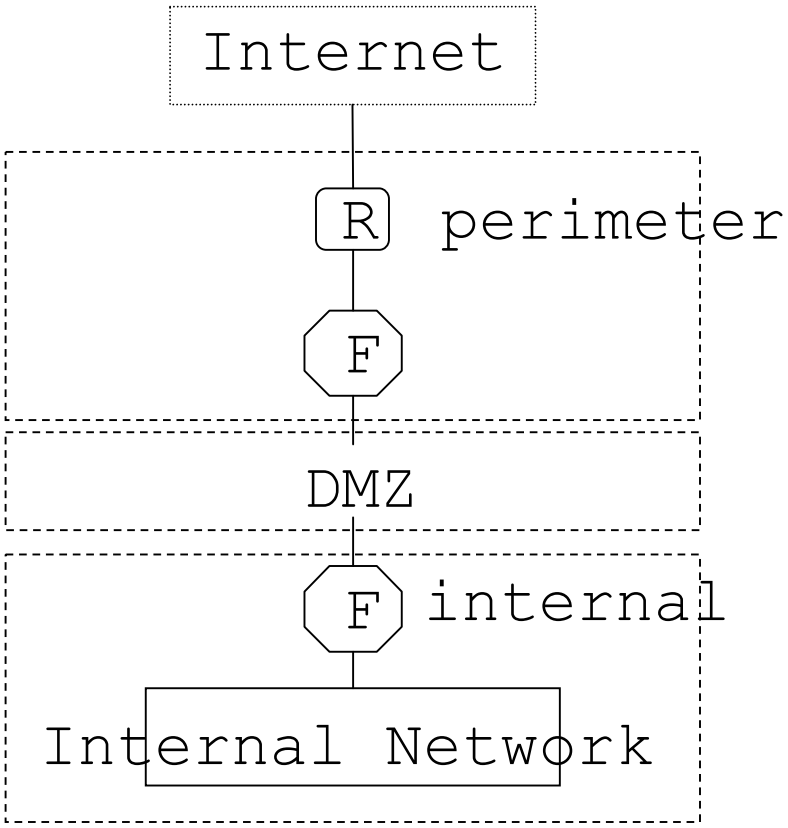
Log Key:

Field 1 is the date.
Field 2 is the time the log was written.
Field 3 is the computer's hostname.
Field 4 is the firewall chain the rule is attached to.
Field 5 is the action taken with regard to this packet.
Field 6 is the pertinent network interface.
Field 7 is the message protocol in the packet. 6(tcp), 17(udp), 1(icmp/<code>)
Field 8 is the packet's source address.
Field 9 is the packet's source port.
Field 10 is the packet's destination address.
Field 11 is the packet's destination port.
Field 12 is the packet's total length in bytes.
Field 13 is the type of service (TOS) field.
Field 14 is the packets datagram ID.
Field 15 is the fragment offset.
Field 16 is the packet's time-to-live (TTL) field.
Field 17 is the rule number which generator the log.
Field 18 is the TCP flag.

Robert V. McMillen Jr.
GIAC Firewall & Perimeter Protection Assignment

Assignment 3 - Defense in depth architecture (10 Pts each)

a.



Since the security policy was not provided, I will have to make some assumptions and speak in general terms about the system design. The diagram only shows one external connection in order to keep it simple.

I will break the design into three sections: Perimeter, DMZ, and Internal security.

The perimeter will consist of our border routers and firewalls. The routers will be hardened (disabling unnecessary services) and configured to do some basic packet filtering. We will prevent spoofing by permitting only legitimate outgoing traffic and denying incoming traffic imitating our internal network. The border routers will also block source routing and ICMP broadcasts. The firewall will deny everything by default and only permit necessary services(mail, web, dns, etc) established by the security policy.

The DMZ will contain all, if any, public servers (DNS, Web, Mail, etc). These machines will be hardened (only provide required services) and monitored with an Intrusion Detection System (IDS) which will send a copy of its log to

a central logging machine within the internal network. The IDS will be configured to detect compromised public servers in the DMZ.

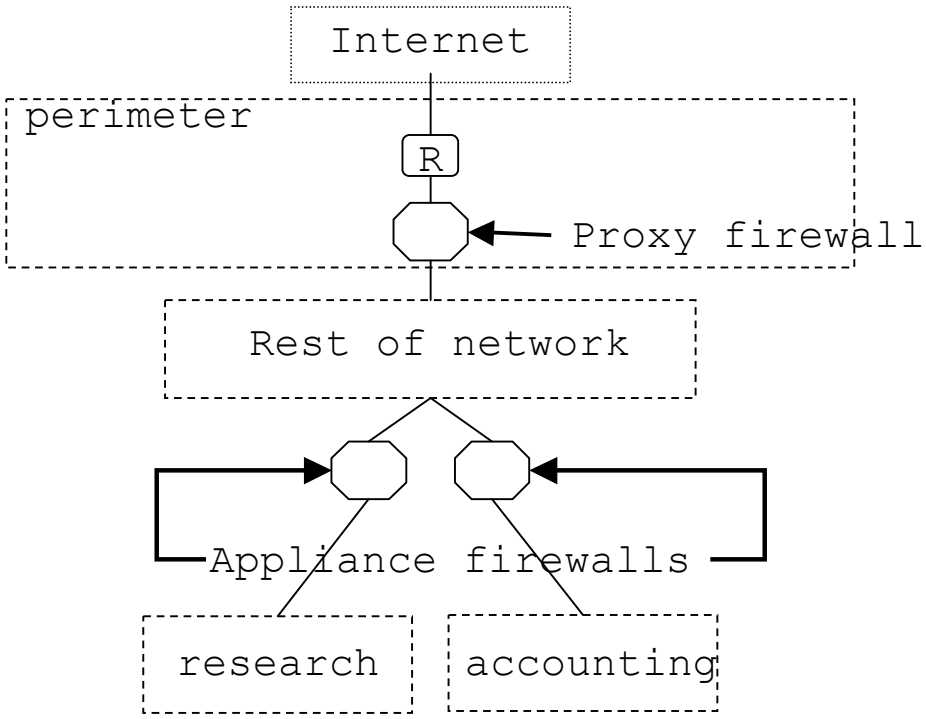
The internal network will be protected by a choke firewall. If any of the public servers are compromised, the choke firewall will prevent access to our internal network. Again, this firewall is configured to deny everything by default and permit only required services. The choke firewall will also perform network address translation in order to hide our interior network.

A combination of network based and host based IDS will be configured throughout the interior network. The mission of the IDS will be to keep our internal users straight, and detect compromised machines that could possibly be used for denial of service.

Finally, the network will use two DNS server: one inside the choke firewall and one within the DMZ. The DMZ DNS server will only have our public machines listed in its database. It will conduct recursive queries for the internal DNS server, but it will not be allowed to query the interior DNS server.

This design uses a defense in depth approach. It should minimize denial of service to our network because we have two connections to the internet. If one is denied, our network can use the other (built in redundancy). The design will ensure our system is not used for denial of service.

b.



This design is similar to the previous problem with the exception of equipment limitation. I still have the border router configured to perform basic packet filtering in order to drop spoofed traffic, source routing, and ICMP broadcast. The proxy firewall will deny everything by default and only permit necessary services(mail, web, dns, etc) established by the security policy. Due to budget constraints, the perimeter security will be the only protection available to the majority of the network.

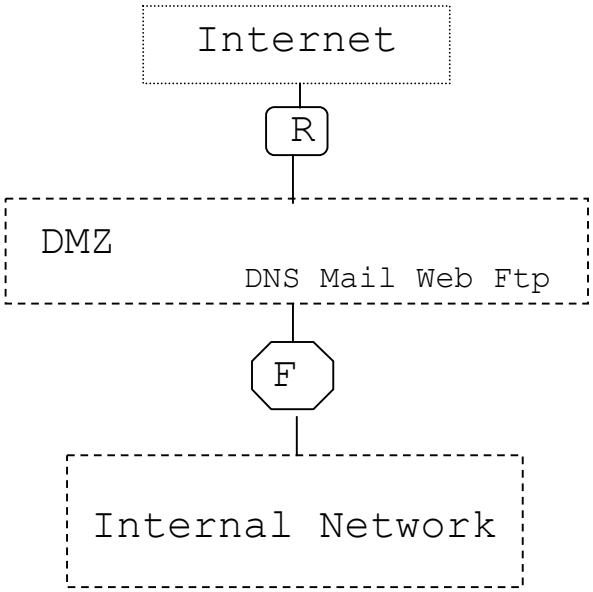
The two appliance firewalls will be used to protect the sensitive departments within the organization. Each will be configured to comply with each department's specific security policy, and will ensure only authorized personnel have access to the sensitive information within each department. Basically, the research and accounting departments will be isolated from each other and from the remainder of the network.

Robert V. McMillen Jr.
GIAC Firewall & Perimeter Protection Assignment

Assignment 4 – Create a test that demonstrates your knowledge of the subject area (20 Points)

Question:

You have inherited a network from a system administrator who built the network in a hurry. All devices have a basic/default configuration. The network consists of an internet connection, a router, a DMZ with public servers (DNS, Mail, Web, Ftp), and a firewall (see figure below). The previous system administrator had firewall and intrusion detection software, and several extra computers in the office, but not attached to the network. Is the current configuration adequate to safeguard the network? If so, support your answer. If not, using the additional resources found in the office, how would you increase the network's security posture?



Answer:

I do not think the security is adequate. Security devices and public servers should not be configured with default settings. Everything that is exposed to the internet should be hardened (only providing required services and updating patches).

The first thing I would do is harden all public servers, the firewall, and the router. I would configure the router to perform basic packet filtering (drop spoofed traffic, source routing, and ICMP broadcast). I would add

a firewall between the border router and the DMZ. This way, I can restrict access to the public servers by only allowing incoming traffic to the specific services the public servers offer. The existing firewall will become a choke firewall. This firewall will prevent compromised public servers from accessing the internal network.

The next thing I would do is add an intrusion detection system (IDS) in the DMZ and the internal network. The IDS in the DMZ will alert the system administrator of possible compromised public servers that may be attacking the choke firewall. The internal IDS will serve dual purpose. It will keep the insiders straight, while at the same time, alert the firewall administrator of a possible firewall breach.

After everything is hardened and configured properly, I will add a central logging machine. Everything (router, firewalls, and IDS) will send their logs to a central location for proper log analysis. This way, if one security device detects an attack in one area of the network, I can compare it with other security devices in order to keep track and/or eradicate the infiltrator.

References:

Firewall 101: Perimeter Protection with Firewalls by SANS/GIAC

Advanced Perimeter Protection and Defense In-Depth by SANS/GIAC

Linux Firewalls by Robert L. Ziegler: New Riders Publishing, 2000