ISEC 325 Homework 05

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [2 points] Name and describe the two basic functions of a firewall?
   The two basic security functions of a firewall are packet filtering and implementing proxy access for specific services.
2. [2 points] When does packet filtering offer an advantage over other security methods, such as proxy services?
   Packet filtering firewalls can be easily be reconfigured for specific protocols whereas proxy firewalls are designed to work on the application level alone. Packet filtering protects networks from port scanning and other types of attacks. Stateful packet filtering firewalls can also detect connectionless packet traffic such as UDP and RPC.
3. [2 points] Compare and contrast stateful and stateless firewalls.
   Stateless firewalls just look at the packet header information the IP address and port number the advantage of stateless is that processing is faster. Stateful check the header but also check the state of the connection between internal and external computers. A stateful firewall uses connection state to determine how to allow traffic. The disadvantage of stateful firewalls is that they take extra processing time which can leave them vulnerable to denial of service and distributed denial of service attacks.
4. [4 points] Compare and contrast the four architectural implementations for firewalls.
   The four architectural implementations for firewalls are Packet-filtering routers, Screened host firewalls, Dual-homed firewalls and Screened subnet firewalls. Packet-filtering routers sit on the perimeter between the network and the isp.
   Packet-filtering routers are configured to reject packets that the organization does not want to allow in their network and lowers the organizations risk of attack. The drawbacks of packet-filtering routers are lack of auditing and lack of strong authentication. The complexity of the access control lists for them also slows the network down.
   Screened Host Firewalls combine packet filtering with a separate dedicated firewall like a proxy server. The packet filtering firewall prescreens the packets to minimize traffic to the proxy server. The proxy firewall examines an application layer protocol like HTTP and performs the proxy services. The proxy firewall is a desirable attack target because it can give out information on the configuration of your network and provide internal information. This setup is often used solely on the perimeter and is often referred to as the sacrificial host.
   Dual-Homed Host Firewalls are when the bastion host has two network interface cards so that all traffic must go through the firewall, the setup often uses network address translation to map real valid external IP addresses. It also can translate several protocols at their layers. The downside is that if it is compromised you lose your connection and that it can be become overloaded with traffic.

Screened Subnet Firewalls provide the demilitarized zone which can be a port on the firewall linking to a single bastion host or can be connected to a screened subnet. It can consist of one or two packet filtering monitors and two bastions hosts. The connections from outside are filtered through the external filtering router, connections from the outside are routed through the DMZ, the only connections into the internal network are trusted connections. It can be expensive to implement. It can also provide you with an extranet where additional authentication and authorization controls may be put in place.

5. [3 points] List the benefits of locating a firewall on the perimeter of a network.

The benefits of placing a firewall on the perimeter of a network are that when a firewall is on the perimeter it is the first place the data and connection to your internal network takes place. This is an advantage because you can inspect packets, check connections, and filter traffic through proxy servers and the DMZ before it gets to your internal network.

6. [2 points] How do firewalls affect network penetration testing? Why?

Network firewalls cause problems with penetration testing because when a port scan is done it does not come up with the true ports open in the network but rather the ports the firewall is allowing access to.

7. [6 points] Consider the network diagram of Figure 1, and the IP addresses of specific hosts in Table 1.

Out of the necessity of completing this early enough to ensure I am correct for the midterm I don't think I will be able to ask the questions of you I would like to ask. I don't understand why these firewalls don't have internal and external ip addresses and I don't understand the policy column and can't seem to find examples in the book. I listened to the meet twice, but we do not cover the policy part of the rule in the meet, so I was unable to fill it out.

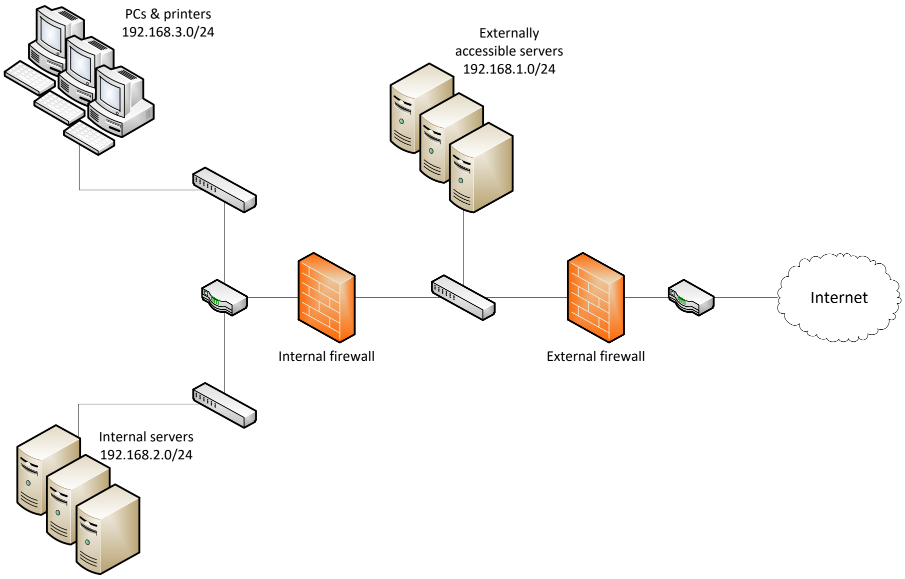

Figure 1: Network diagram

Table 1: Host IP addreses

Host	IP address
DMZ web server	192.168.1.2
DMZ email server	192.168.1.3
DMZ DNS server	192.168.1.4
Internal MySQL server	192.168.2.2
Internal WSUS server	192.168.2.3

Implement policies on the internal and external firewalls such that:

a. The PCs and printers can reach the DMZ for web (standard and https), email, and DNS services.
b. The PCs and printers can reach the Internet.
c. The internal servers can reach the DMZ for DNS services.
d. The externally accessible web server can reach the internal MySQL server
e. Hosts on the internet can reach the DMZ for web, email, and DNS services
f. Of the internal servers, only the WSUS internal server can reach the internet.
g. None of the DMZ servers should be able to reach the Internet.
h. Nothing else should be permitted

In the policy field, reference one of the policies (a-h) that you are addressing. You may need more or less rows to create the rules. You will need to look up what ports are used by services (i.e. HTTP, HTTPS, DNS, POP, IMAP, SMTP, MySQL, etc.)

Table 2: Internal Firewall rules, internal-facing port

Source IP	Source port	Dest. IP	Dest. Port	Action	Policy
192.168.3.0/24	*	192.168.1.2/4	25,80,443,53	allow	
192.168.3.0/24	*	*	80,443	allow	
192.168.2.0/24	*	192.168.1.4	53	allow	
192.168.2.3	*	*	*	allow	
*	*	*	*	deny	

Table 3: Internal Firewall rules, DMZ-facing port.

Source IP	Source port	Dest. IP	Dest. Port	Action	Policy
192.168.3.0/24	*	*	80,443	allow	
192.168.2.3	*	*	*	allow	
192.168.1.2/4	*	*	*	deny	
*	*	*	*	deny	

Table 4: External Firewall rules, DMZ-facing port

Source IP	Source port	Dest. IP	Dest. Port	Action	Policy
*	80	192.168.2.2	3306	allow	
*	*	*	*	deny	

Table 5: External Firewall rules, external-facing port

Source IP	Source port	Dest. IP	Dest. Port	Action	Policy
*	80	192.168.2.2	3306	allow	
*	*	192.168.1.2/4	80,443,25,53	allow	
*	*	*	*	deny	

8. [1 point] Imagine that the situation of question 7 had changed, and the system administrators wanted to protect the internal servers from malicious internal traffic. How could the design be altered so that internal hosts could only access CIFS, and DHCP on the internal servers?
   You would have to change your topology and move the internal firewall back behind the router so that you could write the rules from internal pcs to the internal servers only allowing connections from the internal pc to connect to ports 67 and 445.
   192.168.3.0/24 * 192.168.2.0/24 67,443 allow
   * * 192.168.2.0/24 * deny
9. [1 point] Imagine again the situation of question 7 had changed, and the system administrators wanted their own internal network on 192.168.4.0/24 that had full access to the DMZ machines (for remote login, remote desktop, etc). What firewall and port would need new rules? What would that rule look like?
   The internal firewall with the internal port would need the rule.
   192.168.4.0/24 * 192.168.1.2/4 * allow
10. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This was a great week in class in the reading, the meet session and the homework. We never went into depth about firewalls when I attended ITT only that they were perimeter devices that had to use redundancy. I found it very interesting to know how they worked and the different types. I always wanted to know more about proxy servers and how they worked, in the other course that I am taking this semester we are discussing them as well and how network administrators use AD LT to configure proxy servers on the perimeter as well. I didn't know that firewalls did basically the same thing. We are studying Windows Server 2008 so I realize it may be out of date and firewalls are the primary perimeter solution for the DMZ. I had heard people talk about working with firewalls and reviewing logs. I also never understood how an organization could employ a few people to manage firewalls, I didn't understand how complex and important they could be. I feel like I have a good understanding of what they are, what they do and common ways they are set up. I am very happy with what I have learned this week.

I am a bit rusty on setting up the firewall rules. I didn't see them cover it in the book, so I watched our meet session a few times. I didn't see anything about the policy in the MEET, so I left it out. I thought you would follow the bit stream so if you are going out you hit the internal firewall internal port first, if you aren't using the DMZ you would hit the external internal port next. I could be wrong on that because I found it a bit confusing and took awhile to work with it and understand it. I don't think it would be as difficult if there were examples like the questions asked in the book although I don't think it is terrible to take a try at it. It would be nice to go over something like this at the end of class on Thursday? I know you can't give away how to do the homework in class but perhaps something similar especially if something like this is on the midterm.