# 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 functions of a firewall are to block unauthorized traffic from passing and allow authorized traffic to pass through.

1. [2 points] When does packet filtering offer an advantage over other security methods, such as proxy services?

Packet filtering has an advantage over some other security as it can follow a set of rules determined by the firewall and use this to check incoming traffic and stopping many from getting through. It lets the other security focus on different parts with less traffic to hopefully decrease the number of threats that can slip through.

1. [2 points] Compare and contrast stateful and stateless firewalls.

Stateful and stateless firewalls are both packet- filtering firewalls that check incoming traffic and determining whether it can proceed. The stateless firewalls will use only the header information to pass or block packets and not look at the state of the computers’ connection. The stateful firewalls will look at the data that is contained within the packet and check the state of the connection between the internal and external computers before deciding on if the packet can be allowed or blocked.

1. [4 points] Compare and contrast the four architectural implementations for firewalls.

The first implementation is packet-filtering routers which are located between the internal and external connection on the perimeter so it can accept and deny packets before it gets to the internal network. The second is screened host firewalls which takes the packet-filtering router and adds a firewall that can look at the application layer protocol after they have been cleared through the packet-filtering. The dual-honed firewalls have two NICs with one connected to the internal and the other to the external network, it looks and maps the IP addresses using NATs. The final one is the screened subnet firewall which is made of three components which is the public interface that interacts with the internet, the demilitarized zone that is a buffer between the first and second component, and the system which connects to the local architectures and the intranet.

1. [3 points] List the benefits of locating a firewall on the perimeter of a network.

The benefits of locating a firewall on the perimeter of a network are that it can prevent malicious traffic from leaving the network, it provides a more precise control on the external resources, provides critical resources, gives an audit trail, and provides a means of authentication.

1. [2 points] How do firewalls affect network penetration testing? Why?

Firewalls makes network penetration testing harder as it will block incoming connections, log the connection attempts, and will even rewrite the packets.

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



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:

* 1. The PCs and printers can reach the DMZ for web (standard and https), email, and DNS services.
  2. The PCs and printers can reach the Internet.
  3. The internal servers can reach the DMZ for DNS services.
  4. The externally accessible web server can reach the internal MySQL server
  5. Hosts on the internet can reach the DMZ for web, email, and DNS services
  6. Of the internal servers, only the WSUS internal server can reach the internet.
  7. None of the DMZ servers should be able to reach the Internet.
  8. 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 | Any | Any | Any | Pass | Policy B |
| 192.168.3.0/24 | Any | 192.168.1.2 | 80 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.2 | 443 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.3 | 25 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.4 | 53 | Pass | Policy A |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source IP | Source port | Dest. IP | Dest. Port | Action | Policy |
| 192.168.2.0/24 | Any | 192.168.1.4 | 53 | Pass | Policy C |
| 192.168.3.0/24 | Any | 192.168.1.2 | 80 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.2 | 443 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.3 | 25 | Pass | Policy A |
| 192.168.3.0/24 | Any | 192.168.1.4 | 53 | Pass | Policy A |

Table 4: External Firewall rules, DMZ-facing port

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source IP | Source port | Dest. IP | Dest. Port | Action | Policy |
| 192.168.2.0/24 | Any | 192.168.2.2 | 80 | Pass | Policy D |
| 192.168.1.2 | 80 | Any | Any | Drop | Policy G |
| 192.168.1.2 | 443 | Any | Any | Drop | Policy G |
| 192.168.1.3 | 25 | Any | Any | Drop | Policy G |
| 192.168.1.4 | 53 | Any | Any | Drop | Policy G |
| 192.168.2.3 | 80 | Any | Any | Pass | Policy F |
| 192.168.2.3 | 443 | Any | Any | Pass | Policy F |

Table 4: External Firewall rules, external-facing port

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source IP | Source port | Dest. IP | Dest. Port | Action | Policy |
| Any | Any | 192.168.1.2 | 80 | Pass | Policy E |
| Any | Any | 192.168.1.2 | 443 | Pass | Policy E |
| Any | Any | 192.168.1.3 | 25 | Pass | Policy E |
| Any | Any | 192.168.1.4 | 53 | Pass | Policy E |
| Any | Any | Any | Any | Drop | Policy H |

1. [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?

The policies can be changed so that the internal servers do not reach each other without a firewall in between them for example, the internal servers is shown behind the internal firewall with the externally accessible servers between this wall and the external firewall, by circling through the externally accessible server, the packets will have to go through the firewall twice where it has a better chance to protect against malicious internal traffic.

1. [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?

By bringing in their own internal network, they would be run like the policy c and a where they would need access to the ports, 80,442,25, and 23. The policy would be something like, the internal network 192.168.4.0/24 can reach the DMZ for full access.

1. [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 week expanded on firewalls and how they are used to protect our networks and systems. Firewalls are something that we tend to all have but we do not spend as much time on the why we need it. Going into this week, I had a basic understanding of firewalls and how they protect against threats, but I do not remember going through the different types and more in-depth on their job. My other security classes have touched on firewalls, but I believe it was not a lot as the focus was more on the traffic and the ports. It is interesting to see the different types of firewalls and how their security differs from each other. I do enjoy this class and the information we are covering.