The University of Sydney
School of Information Technologies

THE UNIVERSITY OF SYDNEY

INFO2222—Usability and Security S1 2018
Week 11 Assignment

This assignment covers firewalls and TLS.

1 Task Firewalls

You want to configure a firewall for your home network. Figure 1 shows the configuration you want to achieve. In Zone 2, you've got one Web server (`131.159.20.1`) on TCP ports 80 and 443, and one mail server (`131.159.20.2`) on TCP port 25. Your home users reside in Zone 1.
Your security policy is as follows:

1. Your home users may freely access any Web service, anywhere, on ports 80 and 443, but only if they initiate the connection themselves (i.e. they are allowed to browse the Web). No one outside Zone 1 can initiate connections to Zone 1, on any port.

2. Everyone, including the Evil Internet, can access the web server (both ports) and mail server in Zone 2. However, no host in Zone 2 can initiate connections anywhere else.

3. Your web server should only be reachable on TCP ports 80 and 443 and your mail server should only be reachable on port 25.

4. Home users can access the servers in Zone 2 via SSH, too. They can also use SSH to hosts on the Evil Internet. However, for port 22, hosts in Zone 2 can only be contacted by hosts in Zone 1.

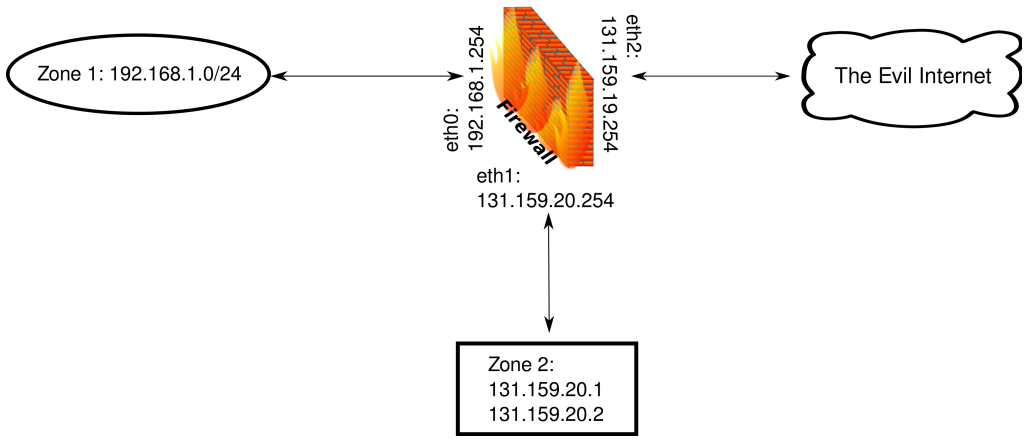

Figure 1: The network topology, with a firewall in the middle.

a)
The policy has some ambiguities and conflicts. Find them and resolve them with common sense by deciding which rule should take precedence.

You can use zone names instead of IP ranges. Use 'Ext' if you want to refer to the Evil Internet, 'Zone 1' if you want to refer to Zone 1 etc. Use * to indicate 'all'. You may match on multiple ports in one rule.
Make sure you drop spoofed packets.

b)
Draw and complete a table to define a stateful firewall configuration for the given scenario (as in the lecture). Hint: we needed 8 rules.

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action

Table 1: Template for stateful filtering.

2 Task TLS

We return to TLS. Load the file *tls.pcap* into your Wireshark and answer the following questions:

- Can you identify the protocol inside the TLS? How?
- Can you identify the destination host? How?
- Why would TLS carry plaintext information that identifies the destination host? (Hint: google for Virtual Hosts)
- Let's have a look at that certificate: for which entity is it issued? And by whom?
- How many certificates are there in the connection?
- What kind of key exchange algorithm is used?
- Are the Diffie-Hellman values (called *parameters*) signed? Why?