Test 2 Answers

1. Directional Firewall Rules answer

Firewall #1 should be placed between The internet and R1.

Outbound Rules:

1. Allow apps that are CRUCIAL for the operation of the company to access the internet
2. Block all other traffic from seeing the internet.

Inbound Rules:

1. Block all instructions that are not first requested from the user. (This means the packet should be a reply to the original request with a source port within the network).
2. Allow instructions that are required for website and email.
3. Allow all other traffic.

Firewall #2 should be placed between R2 and Sales.

Outbound Rules:

1. Allow apps that are CRUCIAL for the operation of the company to access R1
2. Allow access to the server IF it involves Sales.
   1. This includes ports such as 80 (HTTP), 443 (HTTPS), 110 (POP3), and 25 (SMTP).
3. Allow access to the other parallel networks IF and ONLY IF it involves Sales.
4. Block all other traffic.

Inbound Rules:

1. Block traffic that does not include information about sales. (This is so that Sales network cannot access critical information meant for Administrators, or access accounting information meant for Accounting network).
2. Allow all other traffic.

Firewall #3 should be placed between R2 and Accounting.

Outbound Rules:

1. Allow apps that are CRUCIAL for the operation of the company to access R1
2. Allow access to the server IF it involves accounting
   1. This includes ports such as 80 (HTTP), 443 (HTTPS), 110 (POP3), and 25 (SMTP).
3. Allow access to the other parallel networks IF and ONLY IF it involves Accounting.
4. Block all other traffic.

Inbound Rules:

1. Block traffic that does not include information about Accounting. (This is so that Accounting network cannot access critical information meant for Administrators, or access sales information meant for Sales network).
2. Allow all other traffic.
3. An attack is possible since we were only allowed 3 firewalls, it is crucial to note that the Administration network has access to all information coming in and out after Firewall 1. This means using an XSS attack (possibly a reflection or something similar to project 3) and getting into the administration network, would give access to practically everything in the network since Administration has access to it all. This is possible since in our implementation we were only allowed three firewalls, and chose to cover up other areas of the company network.
4. This is because if the user was to try to add anonymity on their side, the server would think the SYN is coming from somewhere (for example call it ‘area 1’) and then it would try to SYN-ACK, but the SYN-ACK would not work because it is not the real IP of the user. In order to receive the data when in anonymous TLS, the user would have to spoof their own IP (which isn’t spoofing at all is it!?). What would happen is the server either would not send the data to the right place (if spoofing another IP) or the data would go to the right place, but there is actually no anonymity at all since the spoofed IP is the actual IP of the user.
5. Because having 3 nodes is what makes Tor so strong. If we were to change that number to have just one node, it is much easier to traverse and/or guess which node was used as opposed to traversing/guessing a 3 node combination to trace back to the source.
6. Attackers could choose any node in the circuit and try to flood that one particular node. If the node is random, then eventually tor will make that node the entry node and this will cause a DoS attack, since it was previously flooded to the point of crashing (or slowing down so much its effectively crashing). However, with the safety of checking to ensure a node works for a minimum month, we ensure the node we are picking currently works at least long enough to gather the data requested and leave before any slowing down or flooding can occur.
7. This domain could be used to trick users into going to this domain and entering their log in information which could then be saved by the domain and used maliciously. This information could be used to access the accounts of all those who tried to log in on the malicious domain. A domain that looks very similar to a real domain would work since most people do not look that closely to the specifics of the website page they are on (For example, main.google.com in small context looks a lot like main..google.com or maingoogle.com). All the attacker needs to do is get users to get to this page and display a similar page to the actual site before asking for log in information. It is also important to notice similarities in letters with certain fonts. This is why I,l, and 1 all look similar in small context.
8. If an attacker records all messages for a time, and then later manages to break in and steal the private key, they would then be able to decrypt all private messages that were previously recorded. The private key used is a long-lived private key which is why it remains on the server after it is closed. These are found in RSA and standard Diffie-Hellman key exchanges. This could be fixed by using a KEX that has an ephemeral private key such as the Elliptic curve Diffie-Hellman.