CSC474 - Homework 4*

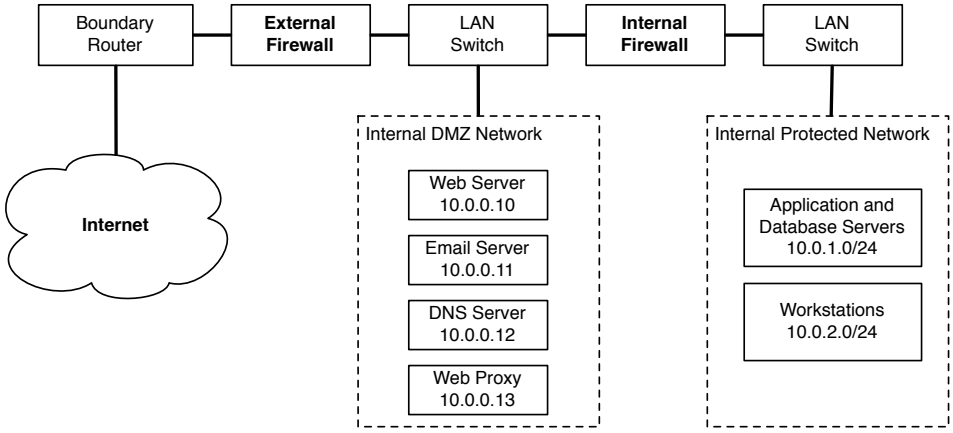
Assigned October 18th, 2022; Due 11:59pm on Sunday October 30th, 2021

50 points

Prof. William Enck

1 Firewalls {30 points}

You are given the following "informal firewall policy" details to be implemented using a firewall setup for the following network.



1. E-mail may be sent using SMTP in both directions through the firewall, but it must be relayed via the DMZ mail gateway that provides header sanitization and content filtering. External e-mail must be destined for the DMZ mail server.

2. Users inside may retrieve their e-mail from the DMZ mail gateway, using either IMAP or IMAPS, and authenticate themselves.

3. Users outside may retrieve their e-mail from the DMZ mail gateway, but only if they use the secure IMAP protocol, and authenticate themselves

4. Web requests (both insecure and secure) are allowed from any internal user out through the firewall but must be relayed via the DMZ Web proxy, which provides content filtering (noting this is not possible for secure requests), and users must authenticate with the proxy for logging. The DMZ Web proxy must be allowed to make Web requests to anywhere on the Internet.

*Last revised on October 14, 2022.

5. Web requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server

6. DNS lookup requests by internal users allowed via the DMZ DNS server, which queries to the Internet.

7. External DNS requests are provided by the DMZ DNS server.

8. Management and update of information on the DMZ servers is allowed using secure shell connections from relevant authorized internal users (may have different sets of users on each system as appropriate), but only from the internal network and the DMZ.

Design suitable packet filter rulesets to be implemented on the "External Firewall" and the "Internal Firewall" to satisfy the aforementioned policy requirements.

For this question, you should assume a **stateless** firewall. Recall that this means that you need to define rules for both directions, as discussed in class. Note that this question requires you to define the firewall policy for two different firewalls ("External Firewall" and "Internal Firewall"). Use the following table as an example of how define your rules. This example assumes a single firewall that is protecting hosts in the 10.0.0.0/24 subnet. It defines a stateless ruleset that allows the hosts in the subnet to access HTTP on the Internet.

Action	Src IP	Src Port	Dest IP	Dest Port	Protocol	Flags	Comment
allow	10.0.0.0/24	*	*	80	TCP		allow hosts to access the web (outbound)
allow	*	80	10.0.0.0/24	*	TCP	ACK	allow hosts to access the web (reply traffic)
deny	*	*	*	*	*		Default deny

2 Routing {20 points}

(a) {7 points} BGP hijack attacks can be classified into two types: *prefix* and *subprefix*. Which is more dangerous and why?

(b) {7 points} AS relationships can be classified as *customer-provider* and *peer-peer*. A customer AS pays the provider AS to both send and receive traffic. In contrast, peer ASes commonly have a settlement-free peering arrangement, meaning they transit each others traffic for free. ASes typically avoid forwarding traffic from one neighbor to another if it cannot generate revenue for doing so.

BGP prefix filtering rules are a allowlisting technique used to filter out bogus BGP announcements. Rules are commonly based on an economically motivated rule of thumb: AS a will typically announce a route to a neighboring AS n only if: (1) n is a customer of a; (2) the route for a prefix originated by a; or (3) the route is through a customer of a.

For what type of sources (e.g., customer, provider, peer) does prefix filtering work well? For what type of sources does it not work well? For both cases, explain why.

(c) {6 points} Briefly describe BGPsec and give two reasons why the Internet has been slow to adopt it (and similar protocols).