Exercise 7 Report

Θεολογίτης Μιχαήλ , AM: 2017030043

The definition of stateful filtering seems to vary greatly among various product vendors. Stateful filtering can mean anything, from the ability to track and filter traffic based on the most minute of connection details to the ability to track and inspect session information at the application level. I will quote our book of the semester "Computer Security Principles and Practice, Third Edition" (page 312):

"A stateful packet inspection firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections (called "Connection State Table"). There is an entry for each currently established connection. ... A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections."

Additionally, the Stateful Firewall rules include a column, "check connection", in the access control list, as shown in Table 1, that indicates whether the packet should be checked (in "Connection State Table"), because it could potentially be malicious if no corresponding connection entry exists.

Table 1: Stateful Firewall Access Control List

Action	Source Address	Dest address	Protocol	Source Port	Dest Port	Flag Bit	Check Connection	Description
allow	147.27/16	outside of 147.27/16	ICMP	-	-	-		1.
allow	147.27/16	outside of 147.27/16	UDP	> 1023	53	-		2. DNS over UDP
allow	outside of 147.27/16	147.27/16	UDP	53	> 1023	-		3. DNS over UDP
allow	147.27/16	outside of 147.27/16	TCP	> 1023	*	any		4.
allow	outside of 147.27/16	147.27/16	TCP	*	> 1023	SYNACK	X	5. 3-Way Handshake
allow	outside of 147.27/16	147.27/16	TCP	*	> 1023	ACK	X	6. Data Transmission
allow	outside of 147.27/16	147.27/16	TCP	*	> 1023	FIN	X	7. Graceful Termination
allow	outside of 147.27/16	147.27/16	TCP	*	> 1023	RST	X	8. Immediate Termination
allow	147.27.15.134	not 147.27.15.134	TCP	**	> 1023	any		9.
allow	not 147.27.15.134	147.27.15.134	TCP	> 1023	**	SYN		10. 3-Way Handshake
allow	not 147.27.15.134	147.27.15.134	TCP	> 1023	**	ACK	X	11. Data Transmission
allow	not 147.27.15.134	147.27.15.134	TCP	> 1023	**	FIN	X	12. Graceful Termination
allow	not 147.27.15.134	147.27.15.134	TCP	> 1023	**	RST	X	13. Immediate Termination
deny	**all**	**all**	**all**	**all**	**all**	**all**		14. Default Rule

The *, and ** are placeholders for various ports that will be listed bellow. For example, * could be 443 (HTTP over SSL), or 22 (SSH, scp, sftp), or etc... This means that all the listed ports (bellow), EACH, have these 5 rules.

147.27.15.134 is `https://www.tuc.gr`'s IP and specific rules about the Web Server are implemented (as described in the assignment).

Ports

* Ports: 53 (DNS), 22 (SSH, sftp), 80 (HTTP), 443 (HTTPS), 8080 (HTTP Alternate)
** Ports: 80 (HTTP), 443 (HTTPS), 8080 (HTTP Alternate)

Descriptions

1. This rule allows ICMP packets to leave TUC's network.
2. 3. These rules allow all DNS packets to enter and leave TUC's network (DNS-over-UDP/53).
4. This rule allows all TCP packets from Internal Network Users to the Internet.
5. This rule allows SYNACK replies (considering 3-Way Handshake) to pass the firewall AFTER checking that the packet is part of a "Connection State Table" entry (which must have "SYN-SENT" state).
6. This rule allows normal Data Transmission, which always has ACK set, to pass the firewall AFTER checking that the packet is part of a "Connection State Table" entry (which must have "ESTABLISHED" state).
7. This rule allows to packets from a, for example, Web Server, to ask for a graceful close of the TCP connection (FIN set). These packets pass the firewall AFTER checking that the corresponding connection exists in the "Connection State Table".
8. This rule allows for an immediate termination of a connection (RST set) which happens mostly because of a fatal error. These packets pass the firewall

AFTER checking that the corresponding connection exists in the "Connection State Table".
9. This rule allows all TCP packets from `https://www.tuc.gr` (147.27.15.134) to pass the firewall (going to External Users).
10. This rule allows packets from External Users to ask for connection establishment with `https://www.tuc.gr` (147.27.15.134). There is no corresponding "Connection State Table" entry yet, since this is when it will be created with state "SYN-RCVD" so we should not check "Connection State Table".
11. This rule allows External Users to transmit data to `https://www.tuc.gr` (147.27.15.134) in normal Data Transmission (ACK set). The packet passes the firewall AFTER checking that the packet is part of a "Connection State Table" entry.
12. This rule allows External Users to ask for a graceful close of the TCP connection (FIN set). These packets pass the firewall AFTER checking that the corresponding connection exists in the "Connection State Table".
13. This rule allows packets from External Users to demand immediate termination of the connection (RST set) which happens mostly because of a fatal error. These packets pass the firewall AFTER checking that the corresponding connection exists in the "Connection State Table".
14. This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule. Packets that didn't match any of the rules above, will be DENIED according to the default policy. I believe in making it unpleasant for people who have no business connecting to our system, so the default rule uses DENY (and not REJECT).

Question 2 Answer

We would need 2 ethernet cards. One for the WAN NIC to connect to our ISP and one LAN NIC (using the firewall's LAN address as the gateway).