INFO-0045: Introduction to Computer Security

Project 1 - Firewalls
Part 2 - High-Level Rules

Maxime Goffart
180521

Olivier Joris
182113

Academic year 2021 - 2022

1 Firewall 1 (FW1)

For the first firewall, we have the following NAT table:

#	Intern				Exteren			
	Source IP	**Source port**	**Destination IP**	**Destination port**	**Source IP**	**Source port**	**Destination IP**	**Destination port**
1	172.31.5.3	*	*	53	172.32.4.100	5300	*	53
2	172.31.5.4	*	*	80	172.32.4.100	8000	*	80
3	172.31.5.4	*	*	443	172.32.4.100	4430	*	443
4	172.31.6.6	*	*	22	172.32.4.100	2200	*	22
5	172.32.4.100	25	172.31.6.5	25	*	*	172.32.4.100	25
6	172.32.4.100	993	172.31.6.5	993	*	*	172.32.4.100	993
7	172.32.4.100	22	172.31.6.6	22	*	*	172.32.4.100	22

Table 1: NAT table for FW1

For the first firewall, we have the following table of firewall rules:

#	**Source IP**	**Source port**	**Destination IP**	**Destination port**	**Protocol**	**Action**	**Comments**
z-mail-ssh in							
1	*	*	172.31.6.5	25	TCP	Accept	SMTP in
2	*	*	172.31.6.5	993	TCP	Accept	IMAPS in
3	*	*	172.31.6.6	22	TCP	Accept	SSH relay in
4	*	*	172.31.6.0/24	*	*	Log and drop	Block in
z-mail-ssh out							
5	172.31.6.5	*	*	25	TCP	Accept	SMTP out
6	172.31.6.6	*	172.32.5.2	22	TCP	Accept	SSH relay → PWEB
7	172.31.6.6	*	*	22	TCP	Accept	SSH relay → Internet
8	172.31.6.0/24	*	*	*	*	Log and drop	Block out
z-http in							
9	*	*	172.31.5.0/24	*	*	Log and drop	Block in
z-http out							
10	172.31.5.3	*	*	53	UDP	Accept	LDNS → remote DNS
11	172.31.5.3	*	*	53	TCP	Accept	LDNS → remote DNS
12	172.31.5.4	*	*	80	TCP	Accept	HTTP out
13	172.31.5.4	*	*	443	TCP	Accept	HTTPS out
14	172.31.5.0/24	*	*	*	*	Log and drop	Block out
z-public in							
15	*	*	172.32.5.2	80	TCP	Accept	LWEB HTTP in
16	*	*	172.32.5.2	443	TCP	Accept	LWEB HTTPS in
17	*	*	172.32.5.3	53	UDP	Accept	PDNS request in
18	*	*	172.32.5.3	53	TCP	Accept	PDNS request in
19	*	*	172.32.5.0/24	*	*	Log and drop	Block in
z-public out							
20	172.32.5.3	*	*	53	UDP	Accept	PDNS → remote DNS
21	172.32.5.3	*	*	53	TCP	Accept	PDNS → remote DNS
22	172.32.5.0/24	*	*	*	*	Log and drop	Block out
default							
23	*	*	*	*	*	Log and drop	Default rule

Table 2: High-level rules for FW1

2 Firewall 2 (FW2)

For the second firewall, we have the following table of firewall rules:

#	Source IP	Source port	Destination IP	Destination port	Protocol	Action	Comments
z-lweb in							
1	192.168.1.0/24	*	10.10.2.2	80	TCP	Accept	Web team → LWEB HTTP
2	192.168.2.0/24	*	10.10.2.2	80	TCP	Accept	Desk team → LWEB HTTP
3	192.168.1.0/24	*	10.10.2.2	21	TCP	Accept	Web team → LWEB FTP
4	*	*	10.10.2.0/24	*	*	Log and drop	Block in
z-lweb out							
5	10.10.2.0/24	*	*	*	*	Log and drop	Block out
z-u1 in							
6	10.10.1.6	*	192.168.1.0/24	22	TCP	Accept	In from SSH relay
7	*	*	192.168.1.0/24	*	*	Log and drop	Block in
z-u1 out							
8	192.168.1.2	*	10.10.1.2	67	UDP	Accept	DHCP_R1 → DHCP
9	192.168.1.2	*	10.10.1.2	68	UDP	Accept	DHCP_R1 → DHCP
10	192.168.1.0/24	*	10.10.1.3	53	UDP	Accept	LDNS requests out
11	192.168.1.0/24	*	10.10.1.3	53	TCP	Accept	LDNS requests out
12	192.168.1.0/24	*	10.10.1.4	3128	TCP	Accept	HTTP(S) out to proxy
13	192.168.1.0/24	*	10.10.1.6	22	TCP	Accept	Connections to SSH relay
14	192.168.1.0/24	*	10.10.1.5	25	TCP	Accept	Connections to SMTP
15	192.168.1.0/24	*	10.10.1.5	143	TCP	Accept	Connections to IMAP
16	192.168.1.0/24	*	*	*	*	Log and drop	Block out
z-u2 in							
17	10.10.1.6	*	192.168.2.0/24	22	TCP	Accept	In from SSH relay
18	*	*	192.168.2.0/24	*	*	Log and drop	Block in
z-u2 out							
19	192.168.2.2	*	10.10.1.2	67	UDP	Accept	DHCP_R2 → DHCP
20	192.168.2.2	*	10.10.1.2	68	UDP	Accept	DHCP_R2 → DHCP
21	192.168.2.0/24	*	10.10.1.3	53	UDP	Accept	LDNS requests out
22	192.168.2.0/24	*	10.10.1.3	53	TCP	Accept	LDNS requests out
23	192.168.2.0/24	*	10.10.1.4	3128	TCP	Accept	HTTP(S) out to proxy
24	192.168.2.0/24	*	10.10.1.15	25	TCP	Accept	Connections to SMTP
25	192.168.2.0/24	*	10.10.1.5	143	TCP	Accept	Connections to IMAP
26	192.168.2.0/24	*	*	*	*	Log and drop	Block out
z-all-sandwich in							
27	*	*	10.10.1.0/24	*	*	Log and drop	Block in
z-all-sandwich out							
28	10.10.1.0/24	*	*	*	*	Log and drop	Block out
default							
29	*	*	*	*	*	Log and drop	Default rule

Table 3: High-level rules for `FW2`

3 Firewall 3 (`FW3`)

For the third firewall, we have the following table of firewall rules:

#	Source IP	Source port	Destination IP	Destination port	Protocol	Action	Comments
z-nfs in							
1	192.168.3.2	*	10.10.3.2	111	TCP	Accept	HONEYPOT → NFS
2	192.168.3.2	*	10.10.3.2	111	UDP	Accept	HONEYPOT → NFS
3	192.168.3.2	*	10.10.3.2	2046	TCP	Accept	HONEYPOT → NFS
4	192.168.3.2	*	10.10.3.2	2046	UDP	Accept	HONEYPOT → NFS
5	192.168.3.2	*	10.10.3.2	2047	TCP	Accept	HONEYPOT → NFS
6	192.168.3.2	*	10.10.3.2	2047	UDP	Accept	HONEYPOT → NFS
7	192.168.3.2	*	10.10.3.2	2048	TCP	Accept	HONEYPOT → NFS
8	192.168.3.2	*	10.10.3.2	2048	UDP	Accept	HONEYPOT → NFS
9	192.168.3.2	*	10.10.3.2	2049	TCP	Accept	HONEYPOT → NFS
10	192.168.3.2	*	10.10.3.2	2049	UDP	Accept	HONEYPOT → NFS
11	192.168.3.3	*	10.10.3.3	873	TCP	Accept	U3 → RSYNC
12	10.10.4.6	*	10.10.3.3	22	TCP	Accept	SSH → RSYNC
13	*	*	10.10.3.0/24	*	*	Log and drop	Block in
z-nfs out							
14	10.10.3.0/24	*	*	*	*	Log and drop	Block out
z-u3 in							
15	10.10.4.6	*	192.168.3.2	22	TCP	Accept	SSH → HONEYPOT
16	*	*	192.168.3.0/24	*	*	Log and drop	Block in
z-u3 out							
17	192.168.3.3	*	10.10.4.6	22	TCP	Accept	U3 → SSH
18	192.168.3.0/24	*	*	*	*	Log and drop	Block out
z-ssh in							
19	*	*	10.10.4.0/24	*	*	Log and drop	Block in
z-ssh out							
20	10.10.4.0/24	*	*	*	*	Log and drop	Block out
default							
21	*	*	*	*	*	Log and drop	Default rule

Table 4: High-level rules for `FW3`