INFO0045: Firewalls Assignment
High-Level Rules - Answers

J. Iurman
University of Liège

1 Reminder

You are in a **stateful** context.

2 NAT

Only static NAT rules are listed here. Don't forget to also implement dynamic ones, if any.

2.1 Firewall 1

Translation table of the firewall								
extern				intern				comment
source	port	destination	port	source	port	destination	port	
-	-	172.15.29.130	22	-	-	172.16.31.3	22	SSH
-	-	172.15.29.130	25	-	-	172.16.32.5	25	SMTP
-	-	172.15.29.130	993	-	-	172.16.32.5	993	IMAPS

2.2 Firewall 2

None.

2.3 Firewall 3

None.

2.4 Firewall 4

None.

3 Rules

3.1 Firewall 1

#	Source	Sport	Destination	Dport	Proto	Action	Comments
Incoming traffic z-ssh-top							
1	*	*	172.16.31.3	22	TCP	allow	Internet -> SSH
2	*	*	172.16.31.0/24	*	*	deny	input deny
Outgoing traffic z-ssh-top							
3	172.16.31.3	*	*	22	TCP	allow	SSH -> Internet
4	172.16.31.3	*	172.16.32.4	53	TCP	allow	SSH -> LDNS
5	172.16.31.3	*	172.16.32.4	53	UDP	allow	SSH -> LDNS
6	172.16.31.0/24	*	*	*	*	deny	output deny
Incoming traffic z-u1							
7	*	*	192.168.1.0/24	*	*	deny	input deny
Outgoing traffic z-u1							
8	192.168.1.0/24	*	172.15.30.2	80	TCP	allow	U1 -> PWEB
9	192.168.1.0/24	*	172.15.30.2	443	TCP	allow	U1 -> PWEB
10	192.168.1.0/24	*	172.16.32.2	3128	TCP	allow	U1 -> HTTP
11	192.168.1.0/24	*	172.16.32.4	53	TCP	allow	U1 -> LDNS
12	192.168.1.0/24	*	172.16.32.4	53	UDP	allow	U1 -> LDNS
13	192.168.1.0/24	*	172.16.32.5	25	TCP	allow	U1 -> SMTP
14	192.168.1.0/24	*	172.16.32.5	143	TCP	allow	U1 -> IMAP
15	192.168.1.0/24	*	172.16.32.5	993	TCP	allow	U1 -> IMAPS
16	192.168.1.2	*	172.16.32.3	67	UDP	allow	DHCP_R1 -> DHCP
17	192.168.1.0/24	*	*	*	*	deny	output deny
Incoming traffic z-mail-top							
18	*	*	172.16.32.5	25	TCP	allow	Internet -> SMTP
19	*	*	172.16.32.5	993	TCP	allow	Internet -> IMAPS
20	*	*	172.16.32.0/24	*	*	deny	input deny
Outgoing traffic z-mail-top							
21	172.16.32.2	*	*	80	TCP	allow	HTTP -> Internet
22	172.16.32.2	*	*	443	TCP	allow	HTTP -> Internet
23	172.16.32.4	*	*	53	UDP	allow	LDNS -> Internet
24	172.16.32.4	*	*	53	TCP	allow	LDNS -> Internet
25	172.16.32.5	*	*	25	TCP	allow	SMTP -> Internet
26	172.16.32.0/24	*	*	*	*	deny	output deny

#	Source	Sport	Destination	Dport	Proto	Action	Comments
Incoming traffic z-pweb							
27	*	*	172.15.30.2	80	TCP	allow	Internet -> PWEB
28	*	*	172.15.30.2	443	TCP	allow	Internet -> PWEB
29	*	*	172.15.30.3	53	TCP	allow	Internet -> PDNS
30	*	*	172.15.30.3	53	UDP	allow	Internet -> PDNS
31	*	*	172.15.30.0/24	*	*	deny	input deny
Outgoing traffic z-pweb							
32	172.15.30.3	*	*	53	UDP	allow	PDNS -> Internet
33	172.15.30.3	*	*	53	TCP	allow	PDNS -> Internet
34	172.15.30.0/24	*	*	*	*	deny	output deny
Other							
35	*	*	*	*	*	log + deny	Should not happen

3.2 Firewall 2

#	Source	Sport	Destination	Dport	Proto	Action	Comments
Incoming traffic z-lweb							
1	10.10.3.2	*	10.10.4.2	80	TCP	allow	HTTP -> LWEB
2	192.168.2.0/24	*	10.10.4.2	80	TCP	allow	U2 -> LWEB
3	192.168.2.0/24	*	10.10.4.2	21	TCP	allow	U2 -> FTP
4	*	*	10.10.4.0/24	*	*	deny	input deny
Outgoing traffic z-lweb							
5	10.10.4.0/24	*	*	*	*	deny	output deny
Incoming traffic z-u2							
6	*	*	192.168.2.0/24	*	*	deny	input deny
Outgoing traffic z-u2							
7	192.168.2.0/24	*	10.10.3.2	3128	TCP	allow	U2 -> HTTP
8	192.168.2.2	*	10.10.3.3	67	UDP	allow	DHCP_R2 -> DHCP
9	192.168.2.0/24	*	10.10.3.4	53	UDP	allow	U2 -> LDNS
10	192.168.2.0/24	*	10.10.3.4	53	TCP	allow	U2 -> LDNS
11	192.168.2.0/24	*	10.10.3.5	25	TCP	allow	U2 -> SMTP
12	192.168.2.0/24	*	10.10.3.5	143	TCP	allow	U2 -> IMAP
13	192.168.2.0/24	*	10.10.3.5	993	TCP	allow	U2 -> IMAPS
14	192.168.2.0/24	*	*	*	*	deny	output deny
Incoming traffic z-mail-bottom							
15	*	*	10.10.3.0/24	*	*	deny	input deny
Outgoing traffic z-mail-bottom							
16	10.10.3.0/24	*	*	*	*	deny	output deny
Other							
17	*	*	*	*	*	log + deny	Should not happen

3.3 Firewall 3

#	Source	Sport	Destination	Dport	Proto	Action	Comments
Incoming traffic z-u3							
1	10.10.1.3	*	192.168.3.2	22	TCP	allow	SSH -> U3
2	*	*	192.168.3.0/24	*	*	deny	input deny
Outgoing traffic z-u3							
3	192.168.3.2	*	10.10.2.2	111	TCP	allow	U3 -> NFS
4	192.168.3.2	*	10.10.2.2	111	UDP	allow	U3 -> NFS
5	192.168.3.2	*	10.10.2.2	2046	TCP	allow	U3 -> NFS
6	192.168.3.2	*	10.10.2.2	2046	UDP	allow	U3 -> NFS
7	192.168.3.2	*	10.10.2.2	2047	TCP	allow	U3 -> NFS
8	192.168.3.2	*	10.10.2.2	2047	UDP	allow	U3 -> NFS
9	192.168.3.2	*	10.10.2.2	2048	TCP	allow	U3 -> NFS
10	192.168.3.2	*	10.10.2.2	2048	UDP	allow	U3 -> NFS
11	192.168.3.2	*	10.10.2.2	2049	TCP	allow	U3 -> NFS
12	192.168.3.2	*	10.10.2.2	2049	UDP	allow	U3 -> NFS
13	192.168.3.2	*	10.10.1.3	22	TCP	allow	U3 -> SSH
14	192.168.3.2	*	10.10.1.4	873	TCP	allow	U3 -> RSYNC
15	192.168.3.0/24	*	*	*	*	deny	output deny
Incoming traffic z-nfs							
16	*	*	10.10.2.0/24	*	*	deny	input deny
Outgoing traffic z-nfs							
17	10.10.2.0/24	*	*	*	*	deny	output deny
Incoming traffic z-ssh-bottom							
18	*	*	10.10.1.0/24	*	*	deny	input deny
Outgoing traffic z-ssh-bottom							
19	10.10.1.0/24	*	*	*	*	deny	output deny
Other							
20	*	*	*	*	*	log + deny	Should not happen

3.4 Firewall 4

#	Source	Sport	Destination	Dport	Proto	Action	Comments
Incoming traffic z-ssh-top							
1	192.168.1.0/24	*	172.16.31.4	873	TCP	allow	U1 -> RSYNC
2	192.168.1.0/24	*	172.16.31.3	22	TCP	allow	U1 -> SSH
3	*	*	172.16.31.0/24	*	*	deny	input deny
Outgoing traffic z-ssh-top							
4	172.16.31.0/24	*	*	*	*	deny	output deny
Incoming traffic z-u1							
5	*	*	192.168.1.0/24	*	*	deny	input deny
Outgoing traffic z-u1							
6	192.168.1.0/24	*	172.16.32.2	3128	TCP	allow	U1 -> HTTP
7	192.168.1.2	*	172.16.32.3	67	UDP	allow	DHCP_R1 -> DHCP
8	192.168.1.0/24	*	172.16.32.4	53	UDP	allow	U1 -> LDNS
9	192.168.1.0/24	*	172.16.32.4	53	TCP	allow	U1 -> LDNS
10	192.168.1.0/24	*	172.16.32.5	25	TCP	allow	U1 -> SMTP
11	192.168.1.0/24	*	172.16.32.5	143	TCP	allow	U1 -> IMAP
12	192.168.1.0/24	*	172.16.32.5	993	TCP	allow	U1 -> IMAPS
13	192.168.1.0/24	*	172.15.30.2	80	TCP	allow	U1 -> PWEB
14	192.168.1.0/24	*	172.15.30.2	443	TCP	allow	U1 -> PWEB
15	192.168.1.0/24	*	*	*	*	deny	output deny
Incoming traffic z-mail-top							
16	*	*	172.16.32.0/24	*	*	deny	input deny
outgoing traffic z-mail-top							
17	172.16.32.0/24	*	*	*	*	deny	output deny
Incoming traffic z-pweb							
18	*	*	172.15.30.0/24	*	*	deny	input deny
outgoing traffic z-pweb							
19	172.15.30.0/24	*	*	*	*	deny	output deny
Other							
20	*	*	*	*	*	log + deny	Should not happen