

University of Liège Faculty of Applied Science

Securing network with firewalls and NATs

Step 2: high-level rules

Maxime Meurisse Valentin Vermeylen

Master in Civil Engineering Academic year 2020-2021

1 High-level rules

The rules for each firewall are defined in Tables 1, 2, 3 and 4. For each zone, from more secured to less secured, we define first the rules for incoming traffic and then the rules for outgoing traffic. We end with a rule that deny all and log. Each rule is described by a small comment.

Firewall 1 acts as a NAT. The rules of this NAT are listed in the Table 5.

1.1 Firewall 1

Coutgoing traffic z-ssh-top	#	Source	Port	Destination	Port	Protocol	Action	Comments		
Telephone Tele										
Course Cour		*	*	172.16.31.3	22	TCP	allow	SSH from Internet		
Outgoing traffic z-ssh-top	2	*	*	172.16.31.0/24	*	*	deny			
Topic										
Incoming traffic z-u1	3	172.16.31.3	*			-	allow	SSH to Internet		
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	4	172.16.31.0/24	*	*	*	*	deny	deny everything		
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$				Inaomi	na troffi	0 ~ 0.1		else out of z-ssn-top		
Outgoing traffic z-u1	E	*	*				dones	doner orrowething		
6 192.168.1.2 * 172.16.32.3 67 TCP allow server DHCP relay to server 7 192.168.1.0/24 * 172.15.30.2 80 TCP allow U1 to PWEH (HTTP) 8 192.168.1.0/24 * 172.15.30.2 443 TCP allow U1 to PWEH (HTTPS) 9 192.168.1.0/24 * 172.16.32.2 3128 TCP allow U1 to HTTP prox. (HTTPS) 10 192.168.1.0/24 * 172.16.32.4 53 TCP allow U1 to LDNS (UDP) 11 192.168.1.0/24 * 172.16.32.5 25 TCP allow U1 to LDNS (UDP) 13 192.168.1.0/24 * 172.16.32.5 25 TCP allow U1 to MAII (IMAP) 14 192.168.1.0/24 * * * deny deny everthing els out of z-u1 Incoming traffic z-mail-top 15 * 172.16.32.5 25 TCP allow MAIL from Internet (SMTP) 16 * 172.16.32.5 993 TCP allow MAIL from Internet (IMAPS) <	Э	'	·	192.108.1.0/24	,	·	deny			
Server Total Tot										
Teach Teac	6	192.168.1.2	*	172.16.32.3	67	TCP	allow	· ·		
Section		,								
Second	7	192.168.1.0/24	*	172.15.30.2	80	TCP	allow			
10 192.168.1.0/24 * 172.16.32.4 53 TCP allow U1 to LDNS (TCP 11 192.168.1.0/24 * 172.16.32.4 53 UDP allow U1 to LDNS (UDP 12 192.168.1.0/24 * 172.16.32.5 25 TCP allow U1 to MAII (SMTP)	8	192.168.1.0/24	*	172.15.30.2	443	TCP	allow			
11 192.168.1.0/24 * 172.16.32.4 53 UDP allow U1 to LDNS (UDP allow (SMTP) 12 192.168.1.0/24 * 172.16.32.5 25 TCP allow U1 to MAII (SMTP) 13 192.168.1.0/24 * 172.16.32.5 143 TCP allow U1 to MAII (IMAP) 14 192.168.1.0/24 * * * deny deny everthing elso out of z-u1 Incoming traffic z-mail-top 15 * 172.16.32.5 25 TCP allow MAIL from Internet (SMTP) 16 * 172.16.32.5 993 TCP allow MAIL from Internet (IMAPS) 17 * 172.16.32.0/24 * * deny deny everything else to z-mail-top	9	192.168.1.0/24	*	172.16.32.2	3128	TCP	allow	U1 to HTTP proxy		
12 192.168.1.0/24 * 172.16.32.5 25 TCP allow U1 to MAII (SMTP) 13 192.168.1.0/24 * 172.16.32.5 143 TCP allow U1 to MAII (IMAP) 14 192.168.1.0/24 * * * deny deny everthing els out of z-u1 Incoming traffic z-mail-top 15 * 172.16.32.5 25 TCP allow MAIL from Internet (SMTP) 16 * 172.16.32.5 993 TCP allow MAIL from Internet (IMAPS) 17 * 172.16.32.0/24 * * deny deny everything else to z-mail-top	10	192.168.1.0/24	*	172.16.32.4	53	TCP	allow	U1 to LDNS (TCP)		
13 192.168.1.0/24 * 172.16.32.5 143 TCP allow U1 to MAII (IMAP) 14 192.168.1.0/24 * * * * deny deny everthing elso out of z-u1	11	192.168.1.0/24	*	172.16.32.4	53	UDP	allow	U1 to LDNS (UDP)		
13 192.108.1.0/24 172.10.32.5 143 1CF allow (IMAP)	12	192.168.1.0/24	*	172.16.32.5	25	TCP	allow			
14 192.168.1.0/24 * * * deny deny everthing elso out of z-u1 Incoming traffic z-mail-top 15 * 172.16.32.5 25 TCP allow MAIL from Internet (SMTP) 16 * 172.16.32.5 993 TCP allow MAIL from Internet (IMAPS) 17 * 172.16.32.0/24 * * deny deny everything else to z-mail-top	13	192.168.1.0/24	*	172.16.32.5	143	TCP	allow			
	14	192.168.1.0/24	*	*	*	*	deny	deny everthing else		
15				Incoming	$\frac{1}{\text{traffic } z}$	-mail-top				
16 * * 172.16.32.5 993 TCP allow MAIL from Internet (IMAPS) 17 * 172.16.32.0/24 * * deny deny everything else to z-mail-top	15	*	*	172.16.32.5	25	TCP	allow	MAIL from Internet (SMTP)		
else to z-mail-top	16	*	*	172.16.32.5	993	TCP	allow	MAIL from Inter-		
	17	*	*	172.16.32.0/24	*	*	deny			
Outgoing traffic z-mail-top				Outgoing	$\frac{1}{\text{traffic } z}$	-mail-top				
	18	172.16.32.2	*				allow	HTTP out (HTTP)		
19 172.16.32.2 * * 443 TCP allow HTTP ou (HTTPS)	19	172.16.32.2	*	*	443	TCP	allow			
20 172.16.32.4 * * 53 TCP allow DNS out (TCP)	20	172.16.32.4	*	*	53	TCP	allow	, ,		
21 172.16.32.4 * * 53 UDP allow DNS out (UDP)			*	*				. ,		
,			*	*	25			MAIL out (SMTP)		

23	172.16.32.5	*	*	993	TCP	allow	MAIL out (IMAPS)				
24	172.16.32.0/24	*	*	*	*	deny	deny everything else out of z-mail-top				
Incoming traffic z -pweb											
25 *											
26	*	*	172.15.30.2	443	TCP	allow	HTTPS in (to allow from Internet)				
27	*	*	172.15.30.3	53	TCP	allow	PDNS from Internet (TCP)				
28	*	*	172.15.30.3	53	UDP	allow	PDNS from Internet (UDP)				
29	*	*	172.15.30.0/24	*	*	deny	$\begin{array}{ccc} \text{deny} & \text{everything} \\ \text{else to } z\text{-}pweb \end{array}$				
			Outgoin	g traffic	z- $pweb$						
30	172.15.30.3	*	*	53	TCP	allow	DNS out (TCP)				
31	172.15.30.3	*	*	53	UDP	allow	DNS out (UDP)				
32	172.15.30.0/24	*	*	*	*	deny	deny everything else out of z - $pweb$				
	Other										
33	*	*	*	*	*	deny, log	Should not happen. Log to be sure.				

Table 1: Rules for firewall FW1.

1.2 Firewall 2

#	Source	Port	Destination	Port	Protocol	Action	Comments				
	Incoming traffic z-lweb										
1	10.10.3.2	*	10.10.4.2	80	TCP	allow	LWEB from HTTP				
2	192.168.2.0/24	*	10.10.4.2	80	TCP	allow	LWEB from U2				
3	192.168.2.0/24	*	10.10.4.2	20	TCP	allow	FTP from U2				
4	192.168.2.0/24	*	10.10.4.2	21	TCP	allow	FTP from U2				
5	*	*	10.10.4.0/24	*	*	deny	deny everything				
							else to z-lweb				
	Outgoing traffic z-lweb										
6	10.10.4.0/24	*	*	*	*	deny	deny everything				
							else out of z-lweb				
	Incoming traffic z-u2										
7	*	*	192.168.2.0/24	*	*	deny	deny everything				
							else to z - u 2				
			Outgoi	ng traffi	c z-u2						
8	192.168.2.2	*	10.10.3.3	67	TCP	allow	DHCP relay to				
							server				
9	192.168.2.0/24	*	10.10.3.2	3128	TCP	allow	U2 to HTTP proxy				
10	192.168.2.0/24	*	10.10.3.4	53	TCP	allow	U2 to LDNS (TCP)				
11	192.168.2.0/24	*	10.10.3.4	53	UDP	allow	U2 to LDNS (UDP)				
12	192.168.2.0/24	*	10.10.3.5	25	TCP	allow	U2 to MAIL				
							(SMTP)				

13	192.168.2.0/24	*	10.10.3.5	143	TCP	allow	U2 to MAIL			
							(IMAP)			
14	192.168.2.0/24	*	*	*	*	deny	deny everything			
							else out of z - u 2			
	Incoming traffic z-mail-bottom									
15	*	*	10.10.3.0/24	*	*	deny	deny everything			
							else to z - $mail$ -			
							bottom			
	Outgoing traffic z-mail-bottom									
16	10.10.3.0/24	*	*	*	*	deny	deny everything			
							else out of z-mail-			
							bottom			
	Other									
17	*	*	*	*	*	deny, log	Should not happen.			
							Log to be sure.			

Table 2: Rules for firewall FW2.

1.3 Firewall 3

#	Source	Port	Destination	Port	Protocol	Action	Comments					
			Incomi	ng traffi	c <i>z-u3</i>							
1	10.10.1.3	*	192.168.3.2	22	TCP	allow	SSH to U3					
2	*	*	192.168.3.0/24	*	*	deny	deny everything					
else to z-u3												
	Outgoing traffic z-u3											
3	192.168.3.2	*	10.10.1.3	22	TCP	allow	U3 to SSH					
4	192.168.3.2	*	10.10.1.4	873	TCP	allow	U3 to RSYNC					
5	192.168.3.2	*	10.10.2.2	2046	TCP	allow	U3 to NFS (TCP) -					
							status					
6	192.168.3.2	*	10.10.2.2	2046	UDP	allow	U3 to NFS (UDP) -					
	1001000	*	101000	20.45			status					
7	192.168.3.2	*	10.10.2.2	2047	TCP	allow	U3 to NFS (TCP) -					
0	100 100 2 0	*	10 10 0 0	20.47	IIDD	11	nlockmgr					
8	192.168.3.2	7	10.10.2.2	2047	UDP	allow	U3 to NFS (UDP) - nlockmgr					
9	192.168.3.2	*	10.10.2.2	2048	TCP	allow	U3 to NFS (TCP) -					
9	192.100.3.2		10.10.2.2	2046	101	anow	mountd					
10	192.168.3.2	*	10.10.2.2	2048	UDP	allow	U3 to NFS (UDP) -					
10	102.100.0.2		10.10.2.2	2010	CDI	anow	mountd					
11	192.168.3.2	*	10.10.2.2	2049	TCP	allow	U3 to NFS (TCP)					
12	192.168.3.2	*	10.10.2.2	2049	UDP	allow	U3 to NFS (UDP)					
13	192.168.3.0/24	*	*	*	*	deny	deny everything					
							else out of z - u 3					
Incoming traffic z-nfs												
14	*	*	10.10.2.0/24	*	*	deny	deny everything					
else to z-nfs												
			Outgoir	ng traffi	c z-nfs							
15	10.10.2.0/24	*	*	*	*	deny	deny everything					
							else out of z-nfs					
			Incoming t	raffic z -s	ssh-bottom							

16	*	*	10.10.1.0/24	*	*	deny	deny everything		
							else to z - ssh - $bottom$		
Outgoing traffic z-ssh-bottom									
17	10.10.1.0/24	*	*	*	*	deny	deny everything		
							else out of z-ssh-		
							bottom		
				Other					
18	*	*	*	*	*	deny, log	Should not happen.		
							Log to be sure.		

Table 3: Rules for firewall FW3.

1.4 Firewall 4

#	Source	Port	Destination	Port	Protocol	Action	Comments					
	Incoming traffic z-ssh-top											
1	192.168.1.0/24	*	172.16.31.3	22	TCP	allow	SSH from U1					
2	192.168.1.0/24	*	172.16.31.4	873	TCP	allow	RSYNC from U1					
3	*	*	172.16.31.0/24	*	*	deny	deny everything					
else to z-ssh-top												
	Outgoing traffic z-ssh-top											
			T .				else out of z-ssh-top					
	Incoming traffic <i>z-u1</i> 5											
5	Ψ	T	192.168.1.0/24	T	Ψ	deny	deny everything else to z-u1					
			Outmai	 ng traffi			else to z-u1					
6	192.168.1.2	*	172.16.32.3	67	TCP	allow	DHCP relay to					
0	192.108.1.2		172.10.32.3	07	TCP	anow	DHCP relay to server					
7	192.168.1.0/24	*	172.15.30.2	80	TCP	allow	U1 to PWEB					
'	192.100.1.0/24		172.10.50.2	80	101	anow	(HTTP)					
8	192.168.1.0/24	*	172.15.30.2	443	TCP	allow	U1 to PWEB					
	102.1100.11.0/21		1,2,10,00,2	110	101		(HTTPS)					
9	192.168.1.0/24	*	172.16.32.2	3128	TCP	allow	U1 to HTTP proxy					
10	192.168.1.0/24	*	172.16.32.4	53	TCP	allow	U1 to LDNS (TCP)					
11	192.168.1.0/24	*	172.16.32.4	53	UDP	allow	U1 to LDNS (UDP)					
12	192.168.1.0/24	*	172.16.32.5	25	TCP	allow	U1 to MAIL					
							(SMTP)					
13	192.168.1.0/24	*	172.16.32.5	143	TCP	allow	U1 to MAIL					
	,					_	(IMAP)					
14	192.168.1.0/24	*	*	*	*	deny	deny everything					
			T .	, m	•7 ,		else out of z-u1					
	, it	-1-	Incoming		-	,						
15	*	*	172.16.32.0/24	*	*	deny	deny everything					
else to z-mail-top												
Outgoing traffic <i>z-mail-top</i> 16 172 16 22 0/24 *							1 ,1.					
16	172.16.32.0/24	T	T	, T	7	deny	deny everything else out of z-mail-					
							top					
			Incomin	g traffic	z-nweh		,					
17	*	*	172.15.30.0/24	*	*	deny	deny everything					
''			1.2.10.00.0/24			delly	else to z-pweb					
		l			l .		T					

	Outgoing traffic z-pweb											
18	172.15.30.0/24	*	*	*	*	deny	deny everything					
							else out of z-pweb					
	Other											
19	*	*	*	*	*	deny, log	Should not happen.					
							Log to be sure.					

Table 4: Rules for firewall FW4.

1.5 NAT (firewall 1)

#		In	itern		Extern				
//-	Source	Port	Destination	Port	Source	Port	Destination	Port	
1	172.16.32.2	*	*	80	172.15.29.130	3001	*	80	
2	172.16.32.2	*	*	443	172.15.29.130	3002	*	443	
3	172.16.32.3	*	*	53	172.15.29.130	3003	*	53	
4	172.16.32.5	*	*	25	172.15.29.130	3004	*	25	
5	172.16.32.5	*	*	993	172.15.29.130	3005	*	993	
6	172.16.31.3	*	*	22	172.15.29.130	3006	*	22	

Table 5: Rules for NAT (firewall FW1).

The first two rules translate the address of the HTTP proxy when it makes requests to the Internet.

The third rule translates the address of the local DNS server to allow requests to outside DNS servers, if needed.

The fourth and fifth rules translate the address of the MAIL server to allow the sending and receiving of mails outside the company's network.

Finally, the last rule translates the SSH relay when it makes SSH requests to the Internet.