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		EXTERN				
Source	Source Port	Destination	Destination Port	Source	Source Port	Destination	Destination Port	
*	*	172.31.5.3	53	*	*	172.32.4.100	53	
*	*	172.31.5.4	80	*	*	172.32.4.100	80	
*	*	172.31.5.4	443	*	*	172.32.4.100	443	
*	*	172.31.6.5	25	*	*	172.32.4.100	25	
*	*	172.31.6.5	993	*	*	172.32.4.100	993	
*	*	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	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 o	ut			
5	172.31.6.5	*	*	25	TCP	Accept	SMTP out	
6	172.31.6.6	*	172.32.5.2	22	TCP	Accept	$SSH \text{ relay} \rightarrow PWEB$	
7	172.31.6.6	*	*	22	TCP	Accept	$SSH \text{ relay} \rightarrow Internet$	
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	;	1		
10	172.31.5.3	*	*	53	UDP	Accept	$LDNS \rightarrow remote\ DNS$	
11	172.31.5.3	*	*	53	TCP	Accept	$LDNS \rightarrow remote\ DNS$	
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 ir				
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	$PDNS \rightarrow remote\ DNS$	
21	172.32.5.3	*	*	53	TCP	Accept	$PDNS \rightarrow remote\ DNS$	
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:

1 192.168.1.0/24 * 10.10.2.2 80 TCP Accept Web team → LWEB HTT 3 192.168.1.0/24 * 10.10.2.2 21 TCP Accept Web team → LWEB HTT 3 192.168.1.0/24 * 10.10.2.2 21 TCP Accept Web team → LWEB FTP 4 * * Log and drop Block in School Scho	#	Source IP	Source	Destination IP	Destination port	Protocol	Action	Comments			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		F F									
2	1	192.168.1.0/24	*	10.10.2.2	80	TCP	Accept	Web team \rightarrow LWEB HTTP			
3 192.168.1.0/24 * 10.10.2.2 21 TCP Accept Web team → LWEB FTP 4 * * Log and drop Block in	2	192.168.2.0/24	*	10.10.2.2	80	TCP		Desk team \rightarrow LWEB HTTP			
Solution Solution	3	192.168.1.0/24	*	10.10.2.2	21	TCP		Web team \rightarrow LWEB FTP			
Total Tot	4	*	*	10.10.2.0/24	*	*	Log and drop	Block in			
Solution Solution											
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 z-u1 out 8 192.168.1.2 * 10.10.1.2 68 UDP Accept DHCP_R1 → DHCP 9 192.168.1.0/24 * 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 LDNS requests out 12 192.168.1.0/24 * 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 17 Accept Accept Connections to IMAP	5	10.10.2.0/24	*	*	*	*	Log and drop	Block out			
The first content of the fi		<u> </u>			z-u1 ii	n					
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	6	10.10.1.6	*	192.168.1.0/24	22	TCP	Accept	In from SSH relay			
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 * 10.10.1.6 22 TCP Accept LDNS requests out 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 * 19.2.168.2.0/24 * * Log and drop Block out z-u2 in 17 10.10.1.6 * 192.168.2.0/24 * * Accept In fr	7	*	*	192.168.1.0/24	*	*	Log and drop	Block in			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$,	z-u1 ou	ıt					
10	8	192.168.1.2	*	10.10.1.2	67	UDP	Accept	DHCP $R1 \rightarrow DHCP$			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	9	192.168.1.2	*	10.10.1.2	68	UDP	Accept	$\overline{\text{DHCP}}$ R1 \rightarrow DHCP			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	10	192.168.1.0/24	*	10.10.1.3	53	UDP	Accept	LDNS requests out			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	11	192.168.1.0/24	*	10.10.1.3	53	TCP	Accept	LDNS requests out			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	12	192.168.1.0/24	*	10.10.1.4	3128	TCP	Accept	HTTP(S) out to proxy			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	13	192.168.1.0/24	*	10.10.1.6	22	TCP	Accept	Connections to SSH relay			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	14	192.168.1.0/24	*	10.10.1.5	25	TCP	Accept				
$ \begin{array}{ c c c c c c c c c }\hline 17 & 10.10.1.6 & * & 192.168.2.0/24 & 22 & TCP & Accept & In from SSH relay \\\hline 18 & * & 192.168.2.0/24 & * & Log and drop & Block in \\\hline \hline & & & & & & & & & & & & & & & & & $	15	192.168.1.0/24	*	10.10.1.5	143	TCP	Accept	Connections to IMAP			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	16	192.168.1.0/24	*	*	*	*	Log and drop	Block out			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$,			z-u2 ii	1					
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	17	10.10.1.6	*	192.168.2.0/24	22	TCP	Accept	In from SSH relay			
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	18	*	*	192.168.2.0/24	*	*	Log and drop	Block in			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$,	z-u2 ou	ıt					
21 192.168.2.0/24 * 10.10.1.3 53 UDP Accept LDNS requests out	19	192.168.2.2	*	10.10.1.2	67	UDP	Accept				
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	20	192.168.2.2	*	10.10.1.2	68	UDP	Accept				
23 192.168.2.0/24 * 10.10.1.4 3128 TCP Accept HTTP(S) out to proxy	21	192.168.2.0/24	*	10.10.1.3	53	UDP	Accept	LDNS requests out			
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	22	192.168.2.0/24	*	10.10.1.3	53		Accept				
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 27 * * 10.10.1.0/24 * * Log and drop Block in 28 10.10.1.0/24 * * * Log and drop Block out 28 10.10.1.0/24 * * * Log and drop Block out 29 10.10.1.0/24 * * * Log and drop Block out 20 10.10.1.0/24 * * * Log and drop Block out 21 10.10.1.0/24 * * * Log and drop Block out 22 10.10.1.0/24 * * * Log and drop Block out 23 10.10.1.0/24 * * * Log and drop Block out 3 10.10.1.0/24 * * * Log and drop Block out 3 10.10.1.0/24 * * * Log and drop Block out	23	192.168.2.0/24	*	10.10.1.4	3128		Accept	HTTP(S) out to proxy			
26 192.168.2.0/24 * * * Log and drop Block out	24	192.168.2.0/24	*	10.10.1.15	25	TCP	Accept	Connections to SMTP			
Z-all-sandwich in Eog and drop Block out	25	192.168.2.0/24	*				Accept	Connections to IMAP			
27 * * 10.10.1.0/24 * * Log and drop Block in	26	192.168.2.0/24	*	*	*	*	Log and drop	Block out			
27 10.10.1.0/24 Log and drop Block in	z-all-sandwich in										
28 10.10.1.0/24 * * * Log and drop Block out default	27	*	*	10.10.1.0/24	*	*	Log and drop	Block in			
28 10.10.1.0/24 Log and drop Block out default											
	28	10.10.1.0/24	*	*	*	*	Log and drop	Block out			
90 * * * * * * Log and drop Default mile		*	•		defaul	t					
29 Log and drop Default rule	29	*	*	*	*	*	Log and drop	Default rule			

Table 3: High-level rules for ${\tt FW2}$

3 Firewall 3 (FW3)

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

	Source	Source	Destination	Destination	Protocol	Action	Comments		
#	IP	port	IP	port	Frotocoi	Action	Comments		
z-nfs in									
1	192.168.3.2	*	10.10.3.2	111	TCP	Accept	$HONEYPOT \rightarrow NFS$		
2	192.168.3.2	*	10.10.3.2	111	UDP	Accept	$HONEYPOT \rightarrow NFS$		
3	192.168.3.2	*	10.10.3.2	2046	TCP	Accept	$HONEYPOT \rightarrow NFS$		
4	192.168.3.2	*	10.10.3.2	2046	UDP	Accept	$HONEYPOT \rightarrow NFS$		
5	192.168.3.2	*	10.10.3.2	2047	TCP	Accept	$HONEYPOT \rightarrow NFS$		
6	192.168.3.2	*	10.10.3.2	2047	UDP	Accept	$HONEYPOT \rightarrow NFS$		
7	192.168.3.2	*	10.10.3.2	2048	TCP	Accept	$HONEYPOT \rightarrow NFS$		
8	192.168.3.2	*	10.10.3.2	2048	UDP	Accept	$HONEYPOT \rightarrow NFS$		
9	192.168.3.2	*	10.10.3.2	2049	TCP	Accept	$HONEYPOT \rightarrow NFS$		
10	192.168.3.2	*	10.10.3.2	2049	UDP	Accept	$HONEYPOT \rightarrow NFS$		
11	192.168.3.3	*	10.10.3.3	873	TCP	Accept	$U3 \rightarrow RSYNC$		
12	10.10.4.6	*	10.10.3.3	22	TCP	Accept	$SSH \rightarrow RSYNC$		
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	$SSH \rightarrow HONEYPOT$		
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	$U3 \rightarrow SSH$		
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