Project 2 - Firewalls

Introduction to Computer Security

Floriane Magera (S111295)
Fabrice Servais (S111093)

March 27, 2015

1 Zones

Zone	Elements
1	web
2	SMTP
3	I2
4	PDNS
5	DHCP_R2, U2
6	DHCP, SSH, HTTP, LDNS
7	RSYNC
8	DHCP_R1, I1, U1
9	Internet

Table 1: List of the zones and their components

2 Rules

Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments
Zone 4 : Incoming rules								
4		Any	Any	172.14.5.3	53	UDP/TCP	Allow	DNS requests from anywhere
4		Any	Any	172.14.5.3	Any	Any	Deny	Not a DNS request
Zone 4 : Outgoing rules								
4		172.14.5.3	Any	208.67.222.222	53	UDP/TCP	Allow	Ask other DNS
4		172.14.5.3	Any	Any	Any	Any	Deny	Not a DNS reply
Zone 1 : Incoming rules								
1		Any	Any	172.14.6.3	80	TCP	Allow	HTTP (web server)
1		Any	Any	172.14.6.3	443	TCP	Allow	HTTPS (web server)
1		172.14.5.2	Any	172.14.6.3	21	TCP	Allow	FTP from network (FW2)
1		172.14.6.2	Any	172.14.6.3	21	TCP	Allow	FTP from network (FW3)
1		Any	Any	172.14.6.3	Any	Any	Deny	Deny otherwise
Zone 1 : Outgoing rules								
1		172.14.6.3	20	Any	Any	TCP	Allow	FTP data
1		172.14.6.3	Any	Any	Any	Any	Deny	Deny otherwise
Zone 9 : Incoming rules								
9		172.14.5.3	Any	208.67.222.222	53	UDP/TCP	Allow	PDNS populate its cache (see zone 4, outgoing)
9		172.14.5.2	Any	Internet	Any	TCP	Allow	From FW2
9		172.14.7.2	Any	Internet	25, 587, 465	TCP	Allow	SMTP to internet
9		172.14.6.2	Any	Internet	Any	TCP	Allow	I2 (through FW3) to internet
9		Any	Any	Internet	Any	Any	Deny	Deny otherwise
Zone 9 : Outgoing rules								
9		Internet	Any	172.14.5.3	53	TCP/UDP	Allow	Internet searches in PDNS
9		Internet	Any	172.14.5.2	3003	TCP	Allow	Internet to SSH
9		Internet	Any	172.14.6.3	80	TCP	Allow	Visit website
9		Internet	Any	172.14.7.2	25, 587, 465	TCP	Allow	Internet to SMTP
9		Internet	Any	Any	Any	Deny	Deny otherwise	

Table 2: Firewall 1

At FW2 :

- Port 3000 : correspond to the requests from 172.16.6.4 (HTTP, other than :80 and :443)
- Port 3001 : correspond to the requests from 172.16.5.2 (DHCP_R2)
- Port 3002 : correspond to the requests from 172.16.6.2 (DHCP)
- Port 3003 : correspond to the requests from 172.16.6.3 (SSH)
- Port 3004 : correspond to the requests from 172.16.6.4:80 (HTTP)
- Port 3005 : correspond to the requests from 172.16.6.4:443 (HTTPS)
- Port 3006 : correspond to the requests from 172.16.6.5 (LDNS)
- Port 3007 : correspond to the requests from 172.16.9.2 (RSYNC)
- Port 3008 : correspond to the requests from 172.16.8.2 (DHCP_R1)
- Port 3009 : correspond to the requests from 172.16.8.3 (I1)
- Port 3010 to 3260: correspond to the requests from 172.16.8.4...254 (U1)
- Port 3261 to 3514: correspond to the requests from 172.16.5.3...254 (U2)

At FW3 :

- Port 3001 : correspond to the requests from 172.16.4.2:25 (I2)
- Port 3002 : correspond to the requests from 172.16.4.2:587 (I2)
- Port 3003 : correspond to the requests from 172.16.4.2:465 (I2)

Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments
Zone 3 : Incoming rules								
3		172.14.5.2	22	172.14.6.2	22	TCP	Allow	SSH
3		172.14.3.10	22	172.14.6.2	22	TCP	Allow	SSH from Internet
3		172.14.6.3	20	172.14.6.2	Any	TCP	Allow	FTP (data)
3		Any	Any	172.16.4.2	Any	Any	Deny	Deny otherwise
Zone 3 : Outgoing rules								
3		172.16.4.2	Any	172.14.5.2	22	TCP	Allow	SSH through FW2
3		172.16.4.2	Any	172.14.5.2	80	TCP	Allow	HTTP through FW2
3		172.16.4.2	Any	172.14.5.2	443	TCP	Allow	HTTPS through FW2
3		172.16.4.2	Any	172.14.5.2	3128	TCP	Allow	HTTP through FW2 (lynx)
3		172.16.4.2	Any	172.14.5.3	53	UDP/TCP	Allow	(P)DNS
3		172.16.4.2	Any	172.14.6.3	21/80	TCP	Allow	Web
3		172.16.4.2	Any	172.14.7.2	25/110/995	TCP	Allow	SMTP
3		172.16.4.2	Any	Any	Any	Any	Deny	Deny otherwise
Zone 2 : Incoming rules								
2		172.14.5.2	Any	172.14.7.2	25/110/995	TCP	Allow	SMTP from U2
2		172.14.3.10	Any	172.14.7.2	25/110/995	TCP	Allow	SMTP from Internet
2		172.14.6.2	Any	172.14.7.2	25/110/995	TCP	Allow	SMTP from I2
2		Any	Any	172.14.7.2	Any	Any	Deny	Deny otherwise
Zone 2 : Outgoing rules								
2		172.14.7.2	Any	172.14.5.2	25/110/995	TCP	Allow	SMTP can send to U2
2		172.14.7.2	Any	172.16.4.2	25/110/995	TCP	Allow	SMTP can send to I2
2		172.14.7.2	Any	172.14.5.3	53	UDP/TCP	Allow	SMTP can ask to PDNS
2		172.14.7.2	Any	Any	Any	Any	Deny	Deny requests from SMTP
Zone 1 : Incoming rules								
1		172.14.6.2	Any	172.14.6.3	80	TCP	Allow	HTTP (web server) from I2
1		172.14.6.2	Any	172.14.6.3	443	TCP	Allow	HTTPS (web server) from I2
1		172.14.6.2	Any	172.14.6.3	21	TCP	Allow	FTP from I2
1		Any	Any	172.14.6.3	Any	Any	Deny	Deny otherwise
Zone 1 : Outgoing rules								
1		172.14.6.3	20	Any	Any	TCP	Allow	FTP (data)
1		172.14.6.3	Any	Any	Any	Any	Deny	Deny otherwise
Default								
		Any	Any	Any	Any	Any	Deny	LOG and drop

Table 3: Firewall 3

Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments
Zone 7 : Incoming rules								
7	1	172.16.7.3	22	172.16.9.2	873	TCP	Allow	SSH
7	2	172.16.8.0	Any	172.16.9.2	873	TCP	Allow	
7	3	Any	Any	Any	Any	Any	Deny	
Zone 8 : Incoming rules								
8	1	172.16.7.3	22	172.16.8.0	22	TCP	Allow	SSH
8	2	172.16.6.1	3009	172.16.8.3...	Any	TCP	Allow	FTP
8	3	Any	Any	Any	Any	Any	Deny	
Zone 8 : Outgoing rules								
8	1	172.16.8.2	68	172.16.7.2	67	DHCP	Allow	
8	2	172.16.8.3...	80	172.16.7.4	Any	TCP	Allow	HTTP
8	3	172.16.8.3...	443	172.16.7.4	Any	TCP	Allow	HTTPS
8	4	172.16.8.3...	22	172.16.7.3	Any	TCP	Allow	SSH
8	5	172.16.8.3...	873	172.16.9.2	Any	TCP	Allow	RSYNC
8	6	172.16.8.3...	53	172.16.7.5	Any	TCP	Allow	DNS (local)
8	7	172.16.8.3...	80	172.14.6.3	Any	TCP	Allow	HTTP
8	8	172.16.8.3...	443	172.14.6.3	Any	TCP	Allow	HTTPS
8	9	172.16.8.3...	Any	172.14.6.3	20	TCP	Allow	FTP
8	10	Any	Any	Any	Any	Any	Deny	

Table 4: Firewall 4