

Project 2 - Firewalls Introduction to Computer Security

Floriane Magera (S111295) Fabrice Servais (S111093)

 $March\ 27,\ 2015$

1 Zones

The list of the zones are presented in Table 1.

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

One can order the zones by security level. From the highest security: zone 7, zone 8, zone 6, zone 5, zone 3, zone 2, zone 4, zone 1, zone 9.

2 Rules

The rules for the firewalls are shown in Table's 2 to 5.

At FW2 we configured the NAT table as follow:

- For outgoing traffic, we used MASQUERADE in order to have dynamic mappings.
- For incoming traffic, we based ourselves on the destination port. For example, the port 22 meant that the destination had to be replaced by SSH address with DNAT. Only the servers are available.

At FW3, the traffic arriving directly addressed to the firewall is forwarded to I2 and the traffic that comes from I2 sees its ip address change thanks to MASQUERADE.

Zone	Number	Source	Port	Dest Port		Protocol	Action	Comments	
Zone 4: Incoming rules									
4	1	Any	Any	172.14.5.3 53		UDP/TCP	Allow	DNS requests	
4	2	Any	Any	172.14.5.3	Any	Any	Deny	Not a DNS request	
Zone 4: Outgoing rules									
4	3	172.14.5.3	Any	208.67.222.222	53	UDP/TCP	Allow	Ask prime DNS	
4	4	172.14.5.3	Any	Any	Any	Any	Deny	Not a DNS reply	
Zone	1: Incom	ning rules							
1	5	Any	Any	172.14.6.3	80	TCP	Allow	HTTP web server	
1	6	Any	Any	172.14.6.3	443	TCP	Allow	HTTPS web server	
1	7	172.14.5.2	Any	172.14.6.3	21	TCP	Allow	FTP	
1	8	172.14.6.2	Any	172.14.6.3	21	TCP	Allow	FTP	
1	9	Any	Any	172.14.6.3	Any	Any	Deny	Rejects other	
Zone	1 : Outgo	oing rules							
1	10	172.14.6.3	20	Any	Any	TCP	Allow	FTP data (reply)	
1	11	172.14.6.3	Any	Any	Any	Any	Deny	Rejects other	
Zone	9: Incon	ning rules				,			
9	12	172.14.5.3	Any	208.67.222.222	53	UDP/TCP	Allow	To prime DNS)	
9	13	172.14.5.2	Any	Internet	Any	TCP/UDP	Allow	From FW2	
9	14	172.14.7.2	Any	Internet	25, 110, 995	TCP	Allow	SMTP to internet	
9	15	172.14.6.2	Any	Internet	Any	TCP	Allow	I2 to internet	
9	16	Any	Any	Internet	Any	Any	Deny	Deny otherwise	
Zone	9: Outgo	oing rules							
9	17	Internet	Any	172.14.5.3	53	TCP/UDP	Allow	DNS on Internet	
9	18	Internet	Any	172.14.5.2	22	TCP	Allow	SSH (FW2)	
9	19	Internet	Any	172.14.6.2	22	TCP	Allow	SSH (FW3)	
9	20	Internet	Any	172.14.6.3	80	TCP	Allow	Visit website	
9	21	Internet	Any	172.14.7.2	25, 110, 995	TCP	Allow	Internet to SMTP	
9	22	Internet	Any	Any	Any	Any	Deny	Deny otherwise	
Deny	by defau	lt							
	23	Any	Any	Any	Any	Any	Deny	Deny by default	

Table 2: Firewall 1

Total	Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments	
Content										
Temperature Fig.	6	1	172.16.5.2	68	172.16.6.2	67	UDP	Allow	DHCP	
Temperature	6	2	Any	Any	172.16.6.3	22	TCP	Allow	SSH	
6 5 172.14.6.2 Any 172.16.6.4 443 TCP Allow HTTPS 6 6 172.14.6.2 Any 172.16.6.4 80 TCP Allow HTTP 6 7 172.14.6.2 Any 172.16.6.4 432 TCP Allow HTTPS 6 8 172.14.6.2 Any 172.16.6.5 53 UDP Allow HTTPS 6 9 172.16.5.0 Any 172.16.6.2 Any Any Deny 6 10 Any Any 172.16.6.3 Any Any Deny 6 11 Any Any 172.16.6.3 Any Deny Deny 6 12 Any Any 172.16.6.5 Any Any Deny Deny Zone 6: Outgoing rules TCP Allow SSH TCP Allow HTTP 6 15 172.16.6.3 Any Any Any Any<	6	3	172.16.5.0	Any	172.16.6.4	80	TCP	Allow	HTTP	
6 6 172.14.6.2 Any 172.16.6.4 80 TCP Allow HTTP 6 7 172.14.6.2 Any 172.16.6.4 3128 TCP Allow HTTP 6 8 172.16.5.0 Any 172.16.6.5 53 UDP Allow HTTPS 6 9 172.16.5.0 Any 172.16.6.2 Any Any Deny 6 10 Any Any 172.16.6.3 Any Any Deny 6 11 Any Any 172.16.6.3 Any Any Deny 6 12 Any Any 172.16.6.5 Any Any Deny 6 12 Any Any 172.16.6.5 Any Any Deny 6 14 172.16.6.3 Any 172.16.6.5 Any Any HTTPP 6 15 172.16.6.3 Any Any 443 TCP Allow HTTPP	6	4	172.16.5.0	Any	172.16.6.4	3128	TCP	Allow	HTTP redirection with lynx	
6 7 172.14.6.2 Any 172.16.6.4 3128 TCP Allow HTTP redirection with lynx 6 8 172.14.6.2 Any 172.16.6.4 443 TCP Allow HTTPS 6 9 172.16.5.0 Any Any Any Deny 6 10 Any Any 172.16.6.2 Any Any Deny 6 11 Any Any 172.16.6.3 Any Any Deny 6 12 Any Any 172.16.6.5 Any Any Deny 6 13 Any Any 172.16.6.5 Any Any Deny 6 14 172.16.6.4 Any Any Any Any HTTP 6 15 172.16.6.4 Any Any Any 443 TCP Allow HTTP 6 15 172.16.6.5 Any Any 443 TCP Allow HTTP <td>6</td> <td>5</td> <td>172.16.5.0</td> <td>Any</td> <td>172.16.6.4</td> <td>443</td> <td>TCP</td> <td>Allow</td> <td>HTTPS</td>	6	5	172.16.5.0	Any	172.16.6.4	443	TCP	Allow	HTTPS	
6 8 172.14.6.2 Any 172.16.6.4 443 TCP Allow HTTPS 6 9 172.16.5.0 Any 172.16.6.5 53 UDP Allow DNS 6 10 Any Any 172.16.6.2 Any Any Deny 6 11 Any Any 172.16.6.3 Any Any Deny 6 12 Any Any 172.16.6.4 Any Any Deny 6 13 Any Any 172.16.6.5 Any Any Deny 7 200 Coutgoing rules 7 TCP Allow SSH 6 14 172.16.6.3 Any Any 80 TCP Allow HTTP 6 15 172.16.6.4 Any Any 443 TCP Allow HTTP 6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow DNS	6	6	172.14.6.2	Any	172.16.6.4	80	TCP	Allow	HTTP	
6 9 172.16.5.0 Any 172.16.6.5 53 UDP Allow DNS 6 10 Any Any 172.16.6.2 Any Any Deny 6 11 Any Any 172.16.6.3 Any Any Deny 6 12 Any Any 172.16.6.5 Any Any Deny 6 13 Any Any 172.16.6.5 Any Any Deny 6 14 172.16.6.4 Any Any Any Any HTTP 6 15 172.16.6.4 Any Any 443 TCP Allow HTTP 6 16 172.16.6.4 Any Any 443 TCP Allow HTTP 6 17 172.16.6.5 Any 208.67.222.222 53 UDP Allow DHCP 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP	6	7	172.14.6.2	Any	172.16.6.4	3128	TCP	Allow	HTTP redirection with lynx	
6 10 Any Any 172.16.6.2 Any Any Deny 6 11 Any Any 172.16.6.3 Any Any Deny 6 12 Any Any 172.16.6.5 Any Any Deny 6 13 Any Any 172.16.6.5 Any Any Deny 6 14 172.16.6.3 Any Any Any Any SSH 6 15 172.16.6.4 Any Any Any 40 HTTP 6 16 172.16.6.5 Any Any Any 41 TCP Allow HTTPS 6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow DNS 6 19 172.16.6.5 Any 172.16.5.3 40 HTCP Allow DHCP 6 20 172.16.6.2 Any Any Any Any Any Deny D	6	8	172.14.6.2	Any	172.16.6.4	443	TCP	Allow	HTTPS	
6	6	9	172.16.5.0	Any	172.16.6.5	53	UDP	Allow	DNS	
Concord Conc	6	10	Any	Any	172.16.6.2	Any	Any	Deny		
Tope Continue Co	6	11	Any	Any	172.16.6.3	Any	Any	Deny		
Cone 6 : Outgoing rules	6	12	Any	Any	172.16.6.4	Any	Any	Deny		
6 14 172.16.6.3 Any Any 22 TCP Allow SSH 6 15 172.16.6.4 Any Any 80 TCP Allow HTTP 6 16 172.16.6.4 Any Any 443 TCP Allow HTTPS 6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow DNS 6 18 172.16.6.5 Any 208.67.222.222 53 UDP Allow DRS 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.3 Any Any Any Any Deny 6 21 172.16.6.4 Any Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any DHCP Allow HTTP 5 <td>6</td> <td>13</td> <td>Any</td> <td>Any</td> <td>172.16.6.5</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td></td>	6	13	Any	Any	172.16.6.5	Any	Any	Deny		
6 15 172.16.6.4 Any Any Any 443 TCP Allow HTTP 6 16 172.16.6.4 Any Any Any 443 TCP Allow HTTPS 6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow DNS 6 18 172.16.6.5 Any 208.67.222.222 53 UDP Allow DNS 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.5 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any DHCP 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow HTTP 5	Zone	6 : Outgo	oing rules							
6 16 172.16.6.4 Any Any 443 TCP Allow DNS 6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow DNS 6 18 172.16.6.5 Any 208.67.222.222 53 UDP Allow Prime DNS 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.2 Any Any Any Any Deny 6 22 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.3 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Deny Zone 5: Outgoing rules 5 24 172.16.5.3 68 172.16.6.2 67 DHCP Allow DHCP 5 24 172.16.5.3 Any 172.16.6.4 <td< td=""><td>6</td><td>14</td><td>172.16.6.3</td><td>Any</td><td>Any</td><td>22</td><td>TCP</td><td>Allow</td><td>SSH</td></td<>	6	14	172.16.6.3	Any	Any	22	TCP	Allow	SSH	
6 17 172.16.6.5 Any 172.14.5.3 53 UDP Allow prime DNS 6 18 172.16.6.5 Any 208.67.222.222 53 UDP Allow prime DNS 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.4 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5: Outgoing rules 5 24 172.16.5.3 Any 172.16.6.2 67 DHCP Allow DHCP 5 24 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 1	6	15	172.16.6.4	Any	Any	80	TCP	Allow	HTTP	
6 18 172.16.6.5 Any 208.67.222.222 53 UDP Allow prime DNS 6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.3 Any Any Any Any Deny 6 21 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.5 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any DHCP 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow HTTP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.3 22 TCP Allow HTTPS 5 27 172.16.5.3	6	16	172.16.6.4	Any	Any	443	TCP	Allow	HTTPS	
6 19 172.16.6.2 68 172.16.5.2 67 UDP Allow DHCP 6 20 172.16.6.2 Any Any Any Any Deny 6 21 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.4 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any DHCP 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.3 22 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow RSYNC 5 28 172.16.5.3	6	17	172.16.6.5	Any	172.14.5.3	53	UDP	Allow	DNS	
6 20 172.16.6.2 Any Any Any Any Deny 6 21 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.4 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5: Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.3 22 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.14.6.2 Any Any Allow DNS (local) <tr< td=""><td>6</td><td>18</td><td>172.16.6.5</td><td>Any</td><td>208.67.222.222</td><td>53</td><td>UDP</td><td>Allow</td><td>prime DNS</td></tr<>	6	18	172.16.6.5	Any	208.67.222.222	53	UDP	Allow	prime DNS	
6 21 172.16.6.3 Any Any Any Any Deny 6 22 172.16.6.4 Any Any Any Any Deny 6 23 172.16.6.5 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5: Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow RSYNC 5 28 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5	6	19	172.16.6.2	68	172.16.5.2	67	UDP	Allow	DHCP	
6 22 172.16.6.4 Any Any Any Any Deny Zone 5: Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5: Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow RSYNC 5 28 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HT	6	20	172.16.6.2	Any	Any	Any	Any	Deny		
6 23 172.16.6.5 Any Any Any Any Deny Zone 5 : Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5 : Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow RSYNC 5 28 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443	6	21	172.16.6.3	Any	Any	Any	Any	Deny		
Zone 5 : Incoming rules 5 1 Any Any 172.16.5.0 Any Any Deny Zone 5 : Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow HTTPS 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 21 TCP <	6	22	172.16.6.4	Any	Any	Any	Any	Deny		
5 1 Any Any 172.16.5.0 Any Any Deny Zone 5 : Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 26 172.16.5.3 Any 172.16.6.3 22 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 28 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow HTTP web server 5 31 172.16.5.3 Any 172.14.6.3 443 TCP Allow<	6	23	172.16.6.5	Any	Any	Any	Any	Deny		
Zone 5 : Outgoing rules 5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow SSH 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 21	Zone	5: Incon	ning rules							
5 24 172.16.5.2 68 172.16.6.2 67 DHCP Allow DHCP 5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow RSYNC 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTPS web server 5 32 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server<	5	1	Any	Any	172.16.5.0	Any	Any	Deny		
5 25 172.16.5.3 Any 172.16.6.4 80 TCP Allow HTTP 5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow SSH 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2	Zone	5 : Outgo	oing rules							
5 26 172.16.5.3 Any 172.16.6.4 443 TCP Allow HTTPS 5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow SSH 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny	5	24	172.16.5.2	68	172.16.6.2	67				
5 27 172.16.5.3 Any 172.16.6.3 22 TCP Allow SSH 5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny	5	25	172.16.5.3	Any	172.16.6.4	80	TCP	Allow	HTTP	
5 28 172.16.5.3 Any 172.16.9.2 873 TCP Allow RSYNC 5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny	5	26	172.16.5.3	Any	172.16.6.4	443			HTTPS	
5 29 172.16.5.3 Any 172.16.6.5 53 UDP/TCP Allow DNS (local) 5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny	5	27	172.16.5.3	Any	172.16.6.3	22		Allow	SSH	
5 30 172.16.5.3 Any 172.14.6.2 Any Any Allow Link to FW2 5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny by default	5	28	172.16.5.3	Any	172.16.9.2	873	TCP	Allow	RSYNC	
5 31 172.16.5.3 Any 172.14.6.3 80 TCP Allow HTTP web server 5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny by default	5	29	172.16.5.3	Any	172.16.6.5	53	UDP/TCP	Allow	DNS (local)	
5 32 172.16.5.3 Any 172.14.6.3 443 TCP Allow HTTPS web server 5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny by default	5	30	172.16.5.3	Any	172.14.6.2	Any	Any	Allow	Link to FW2	
5 33 172.16.5.3 Any 172.14.6.3 21 TCP Allow FTP web server 5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny by default	5	31		Any		80		Allow		
5 34 172.16.5.3 Any 172.14.7.2 Any TCP Allow SMTP 5 35 Any Any Any Any Deny Deny by default	5		172.16.5.3							
5 35 Any Any Any Any Deny Deny by default	5					21				
Deny by default			172.16.5.3		172.14.7.2	Any	TCP	Allow	SMTP	
				Any	Any	Any	Any	Deny		
36 Any Any Any Any Deny Deny by default	Deny	. •	lt							
		36	Any	Any	Any	Any	Any	Deny	Deny by default	

Table 3: Firewall 2

Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments	
Zone 3: Incoming rules									
3	1	172.14.5.2	Any	172.16.4.2	22	TCP	Allow	SSH (FW2)	
3	2	172.14.3.10	Any	172.16.4.2	22	TCP	Allow	SSH (Tom)	
3	3	172.14.6.3	20	172.14.6.2	Any	TCP	Allow	FTP (data)	
3	4	Any	Any	172.16.4.2	Any	Any	Deny	Deny otherwise	
Zone	Zone 3: Outgoing rules								
3	5	172.16.4.2	Any	172.14.5.2	22	TCP	Allow	SSH through FW2	
3	6	172.16.4.2	Any	172.14.5.2	80	TCP	Allow	HTTP through FW2	
3	7	172.16.4.2	Any	172.14.5.2	443	TCP	Allow	HTTPS through FW2	
3	8	172.16.4.2	Any	172.14.5.2	3128	TCP	Allow	HTTP through FW2 (lynx)	
3	9	172.16.4.2	Any	172.14.5.3	53	UDP/TCP	Allow	(P)DNS	
3	10	172.16.4.2	Any	172.14.6.3	21, 80	TCP	Allow	Web	
3	11	172.16.4.2	Any	172.14.7.2	25	TCP	Allow	SMTP	
3	12	172.16.4.2	Any	Any	Any	Any	Deny	Deny otherwise	
Zone	2 : Incom	ing rules				1			
2	13	172.14.5.2	Any	172.14.7.2	25, 110, 995	TCP	Allow	SMTP from FW2	
2	14	172.14.6.2	Any	172.14.7.2	25, 110, 995	TCP	Allow	SMTP from FW3	
2	15	172.14.3.10	Any	172.14.7.2	25, 110, 995	TCP	Allow	SMTP from Tim	
2	16	Any	Any	172.14.6.2	Any	Any	Deny	Deny otherwise	
Zone	2 : Outgo	ing rules							
2	17	172.14.7.2	Any	172.14.5.2	25, 110, 995	TCP	Allow	SMTP to FW2	
2	18	172.14.7.2	Any	172.14.6.2	25, 110, 995	TCP	Allow	SMTP to FW3	
2	19	172.14.7.2	Any	172.14.5.3	53	UDP/TCP	Allow	SMTP asks to PDNS	
2	20	172.14.7.2	Any	Any	Any	Any	Deny	Deny requests from SMTP	
Zone	1: Incom	ing rules							
1	21	172.14.6.2	Any	172.14.6.3	80	TCP	Allow	HTTP (web server)	
1	22	172.14.6.2	Any	172.14.6.3	443	TCP	Allow	HTTPS (web server)	
1	23	172.14.6.2	Any	172.14.6.3	21	TCP	Allow	FTP	
1	24	Any	Any	172.14.6.3	Any	Any	Deny	Deny otherwise	
Zone	1 : Outgo	ing rules							
1	25	172.14.6.3	20	Any	Any	TCP	Allow	FTP (data)	
1	26	172.14.6.3	Any	Any	Any	Any	Deny	Deny otherwise	
Deny	by defaul	t							
	27	Any	Any	Any	Any	Any	Deny	Deny by default	

Table 4: Firewall 3

Zone	Number	Source	Port	Dest	Port	Protocol	Action	Comments			
Zone 7: Incoming rules											
7	1	172.16.7.3	Any	172.16.9.2	22	TCP	Allow	RSYNC via SSH			
7	2	172.16.8.0	Any	172.16.9.2	873	TCP	Allow	RSYNC			
7	3	Any	Any	172.16.9.2	Any	Any	Deny				
Zone	Zone 7: Outgoing rules										
7	4	172.16.9.2	Any	Any	Any	Any	Deny				
Zone	8: Incon	ning rules									
8	5	172.16.7.2	68	172.16.8.2	67	UDP	Allow	DHCP			
8	6	172.16.7.3	Any	172.16.8.0	22	TCP	Allow	SSH			
8	7	Any	Any	172.16.8.0	Any	Any	Deny				
Zone	8 : Outgo	oing rules									
8	8	172.16.8.2	68	172.16.7.2	67	UDP	Allow	DHCP			
8	9	172.16.8.3	Any	172.16.7.4	80	TCP	Allow	HTTP			
8	10	172.16.8.3	Any	172.16.7.4	3128	TCP	Allow	HTTP for lynx			
8	11	172.16.8.3	Any	172.16.7.4	443	TCP	Allow	HTTPS			
8	12	172.16.8.3	Any	172.16.7.3	22	TCP	Allow	SSH			
8	13	172.16.8.3	Any	172.16.9.2	873	TCP	Allow	RSYNC			
8	14	172.16.8.3	Any	172.16.7.5	53	UDP	Allow	DNS (local)			
8	15	172.16.8.2	Any	Any	Any	Any	Deny				
8	16	172.16.8.3	Any	Any	Any	Any	Deny				
8	17	172.16.8.0	Any	Any	Any	Any	Deny				
8	18	Any	Any	Any	Any	Any	Deny				
Deny	by defau	lt									
	19	Any	Any	Any	Any	Any	Deny	Deny by default			

Table 5: Firewall 4