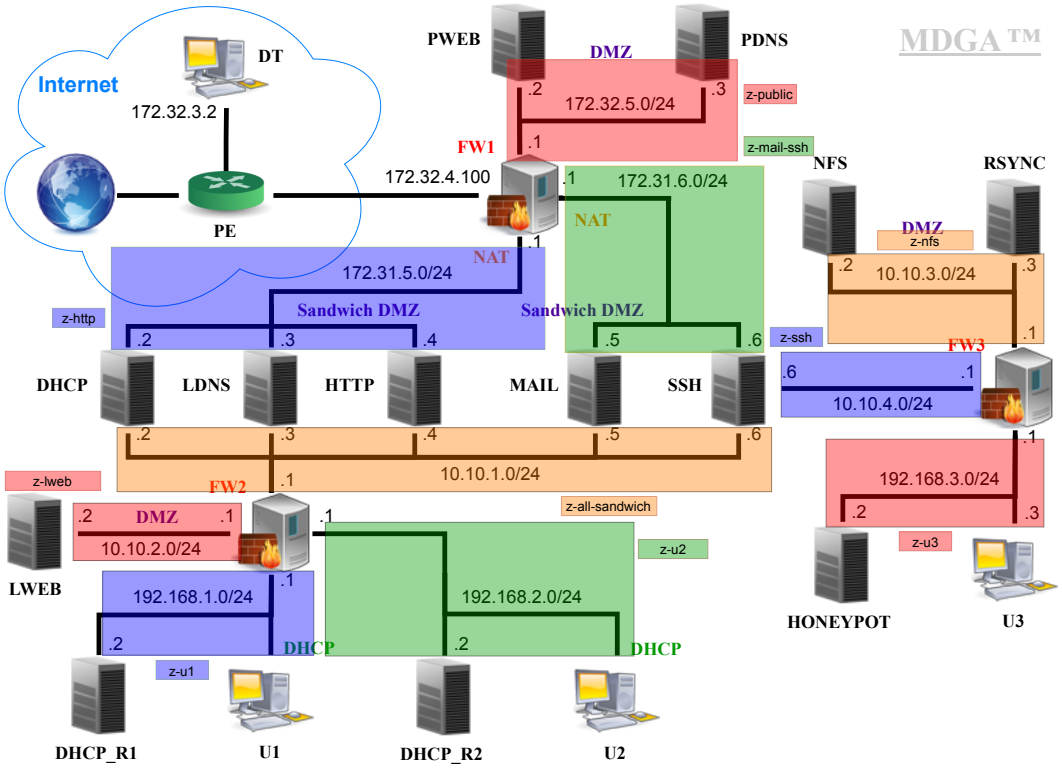
Introduction To Computer Security Assignment

1 Zones & Firewalls

Here is the order of zones, per firewall, from most important to less important.

- FW1: z-mail-ssh > z-http > z-public (> z-Internet)
- FW2: z-lweb > z-u1 > z-u2 > z-all-sandwich
- FW3: z-nfs > z-u3 > z-ssh



2 NAT

2.1 FW1

Translation table of the firewall								
extern				intern				comment
source	port	destination	port	source	port	destination	port	
-	-	172.32.4.100	22	-	-	172.31.6.6	22	SSH
-	-	172.32.4.100	25	-	-	172.31.6.5	25	SMTP(S)
-	-	172.32.4.100	993	-	-	172.31.6.5	993	IMAPS

3 Firewalls

Firewall 1							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-mail-ssh							
1	*	*	172.31.6.5	993	TCP	allow	Internet to MAIL (IMAPS)
2	*	*	172.31.6.5	25	TCP	allow	Internet to MAIL (SMTP)
3	*	*	172.31.6.6	22	TCP	allow	Internet to SSH
4	*	*	172.31.6.0/24	*	*	deny	input deny
Outgoing traffic z-mail-ssh							
5	172.31.6.6	*	*	22	TCP	allow	SSH to Internet
6	172.31.6.5	*	*	25	TCP	allow	MAIL (SMTP) to Internet
7	172.31.6.0/24	*	*	*	*	deny	output deny
Incoming traffic z-http							
8	*	*	172.31.5.0/24	*	*	deny	input deny
Outgoing traffic z-http							
9	172.31.5.3	*	*	53	TCP	allow	LDNS to Internet
10	172.31.5.3	*	*	53	UDP	allow	LDNS to Internet
11	172.31.5.4	*	*	80	TCP	allow	HTTP to Internet
12	172.31.5.4	*	*	443	TCP	allow	HTTPS to Internet
13	172.31.5.0/24	*	*	*	*	deny	output deny

Firewall 1 (cont.)							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-public							
14	*	*	172.32.5.2	80	TCP	allow	Internet to PWEB
15	*	*	172.32.5.2	443	TCP	allow	Internet to PWEB
16	172.31.6.6	*	172.32.5.2	22	TCP	allow	SSH to PWEB
17	*	*	172.32.5.3	53	TCP	allow	Internet to PDNS
18	*	*	172.32.5.3	53	UDP	allow	Internet to PDNS
19	*	*	172.32.5.0/24	*	*	deny	input deny
Outgoing traffic z-public							
20	172.32.5.3	*	*	53	TCP	allow	PDNS to Internet
21	172.32.5.3	*	*	53	UDP	allow	PDNS to Internet
22	172.32.5.0/24	*	*	*	*	deny	output deny
Other							
23	*	*	*	*	*	deny, log	Should not happen. Log to be sure.

Firewall 2							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-lweb							
1	192.168.1.0/24	*	10.10.2.2	21	TCP	allow	U1 to LWEB (ftp)
2	192.168.1.0/24	*	10.10.2.2	80	TCP	allow	U1 to LWEB (http)
3	192.168.2.0/24	*	10.10.2.2	80	TCP	allow	U2 to LWEB (http)
4	*	*	10.10.2.0/24	*	*	deny	input deny
Outgoing traffic z-lweb							
5	10.10.2.0/24	*	*	*	*	deny	output deny
Incoming traffic z-u1							
6	10.10.1.6	*	192.168.1.0/24	22	TCP	allow	SSH to U1
7	*	*	192.168.1.0/24	*	*	deny	input deny
Outgoing traffic z-u1							
8	192.168.1.0/24	*	10.10.1.4	3128	TCP	allow	U1 to HTTP
9	192.168.1.0/24	*	10.10.1.3	53	TCP	allow	U1 to LDNS
10	192.168.1.0/24	*	10.10.1.3	53	UDP	allow	U1 to LDNS
11	192.168.1.0/24	*	10.10.1.5	25	TCP	allow	U1 to MAIL (SMTP)
12	192.168.1.0/24	*	10.10.1.5	143	TCP	allow	U1 to MAIL (IMAP)
13	192.168.1.0/24	*	10.10.1.5	993	TCP	allow	U1 to MAIL (IMAPS)
14	192.168.1.0/24	*	10.10.1.6	22	TCP	allow	U1 to SSH
15	192.168.1.2	*	10.10.1.2	67	UDP	allow	DHCP_R1 to DHCP
16	192.168.1.0/24	*	*	*	*	deny	output deny

Firewall 2 (cont.)							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-u2							
17	10.10.1.6	*	192.168.2.0/24	22	TCP	allow	SSH to U2
18	*	*	192.168.2.0/24	*	*	deny	input deny
Outgoing traffic z-u2							
19	192.168.2.0/24	*	10.10.1.4	3128	TCP	allow	U2 to HTTP
20	192.168.2.0/24	*	10.10.1.3	53	TCP	allow	U2 to LDNS
21	192.168.2.0/24	*	10.10.1.3	53	UDP	allow	U2 to LDNS
22	192.168.2.0/24	*	10.10.1.5	25	TCP	allow	U2 to MAIL (SMTP)
23	192.168.2.0/24	*	10.10.1.5	143	TCP	allow	U2 to MAIL (IMAP)
24	192.168.2.0/24	*	10.10.1.5	993	TCP	allow	U2 to MAIL (IMAPS)
25	192.168.2.2	*	10.10.1.2	67	UDP	allow	DHCP_R2 to DHCP
26	192.168.2.0/24	*	*	*	*	deny	output deny
Incoming traffic z-all-sandwich							
27	*	*	10.10.1.0/24	*	*	deny	input deny
Outgoing traffic z-all-sandwich							
28	10.10.1.0/24	*	*	*	*	deny	output deny
Other							
29	*	*	*	*	*	deny, log	Should not happen. Log to be sure.

Firewall 3							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-nfs							
1	192.168.3.2	*	10.10.3.2	111	TCP	allow	HONEYPOT to NFS (portmapper)
2	192.168.3.2	*	10.10.3.2	111	UDP	allow	HONEYPOT to NFS (portmapper)
3	192.168.3.2	*	10.10.3.2	2046	TCP	allow	HONEYPOT to NFS (status)
4	192.168.3.2	*	10.10.3.2	2046	UDP	allow	HONEYPOT to NFS (status)
5	192.168.3.2	*	10.10.3.2	2047	TCP	allow	HONEYPOT to NFS (nlockmgr)
6	192.168.3.2	*	10.10.3.2	2047	UDP	allow	HONEYPOT to NFS (nlockmgr)
7	192.168.3.2	*	10.10.3.2	2048	TCP	allow	HONEYPOT to NFS (mountd)
8	192.168.3.2	*	10.10.3.2	2048	UDP	allow	HONEYPOT to NFS (mountd)
9	192.168.3.2	*	10.10.3.2	2049	TCP	allow	HONEYPOT to NFS
10	192.168.3.2	*	10.10.3.2	2049	UDP	allow	HONEYPOT to NFS
11	192.168.3.3	*	10.10.3.3	873	TCP	allow	U3 to RSYNC
12	192.168.3.3	*	10.10.3.3	22	TCP	allow	U3 to RSYNC (secured)
13	10.10.4.6	*	10.10.3.3	22	TCP	allow	SSH to RSYNC
14	*	*	10.10.3.0/24	*	*	deny	input deny
Outgoing traffic z-nfs							
15	10.10.3.0/24	*	*	*	*	deny	output deny

Firewall 3 (cont.)							
Number	Source	Source port	Destination	Destination Port	Protocol	Action	Comments
Incoming traffic z-u3							
16	10.10.4.6	*	192.168.3.2	22	TCP	allow	SSH to HONEYPOT
17	*	*	192.168.3.0/24	*	*	deny	input deny
Outgoing traffic z-u3							
18	192.168.3.3	*	10.10.4.6	22	TCP	allow	U3 to SSH
19	192.168.3.0/24	*	*	*	*	deny	output deny
Incoming traffic z-ssh							
20	*	*	10.10.4.0/24	*	*	deny	input deny
Outgoing traffic z-ssh							
21	10.10.4.0/24	*	*	*	*	deny	output deny
Other							
22	*	*	*	*	*	deny, log	Should not happen. Log to be sure.