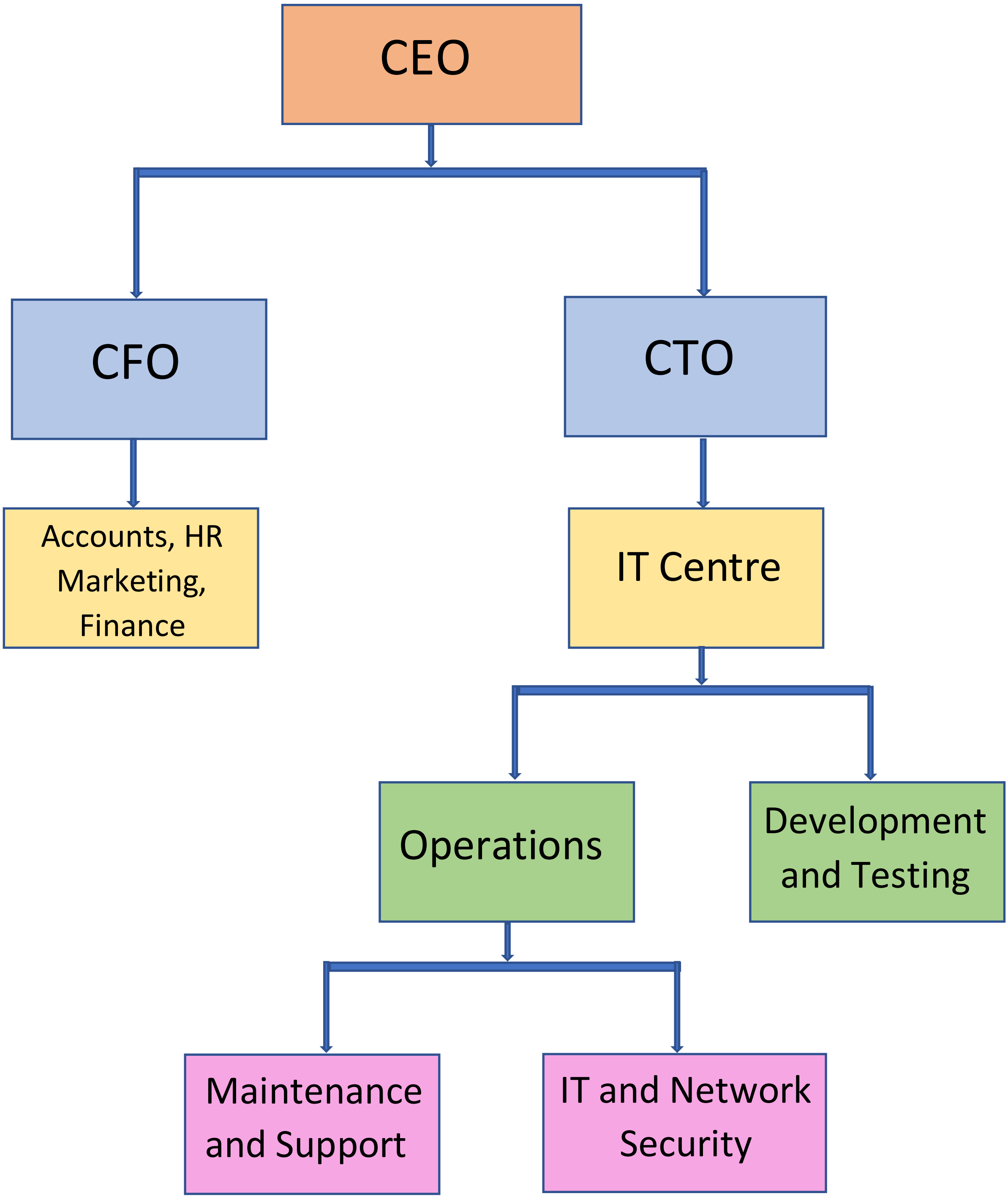
SECURED NETWORK ARCHITECTURE REPORT

EPITA

ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

Contents

1. Organisational Chart

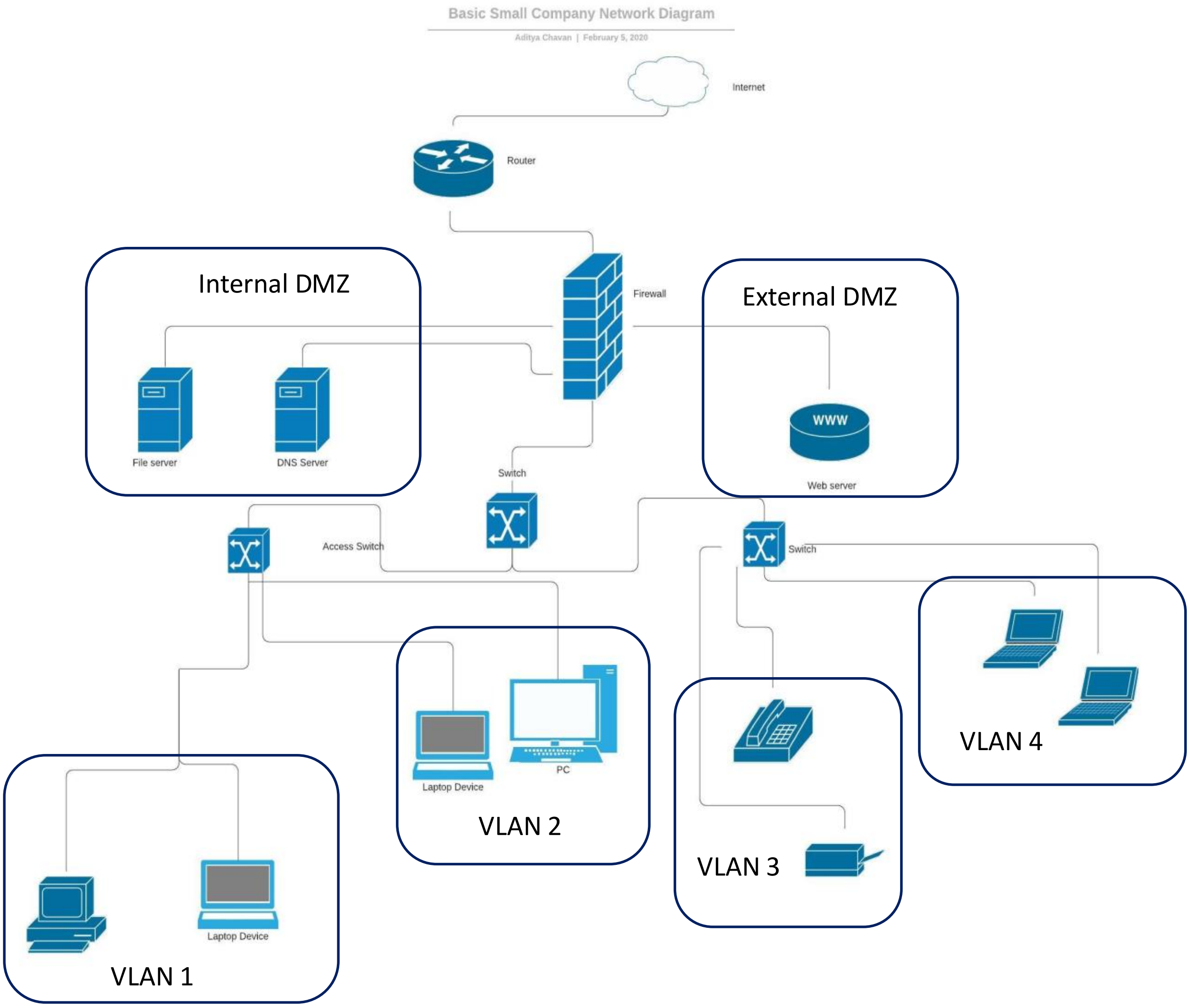


2. Shopping List

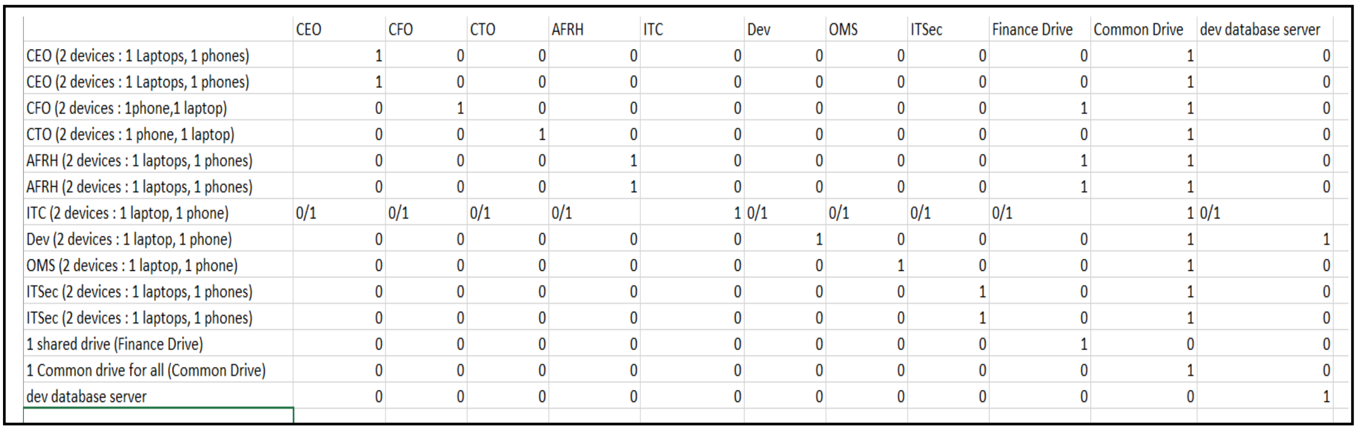
Device	Model	Units
Laptops	Lenovo	10
Router	D-link	2
Switch	Cisco c2960	3
Server	Dell PowerEdge T20	3
Printer	HP Colour LaserJet MFP M477fdw	2
Firewall	ASA1 5506-X	2
ISP	SFR	1
IP Cameras	Blink XT2	1
Antivirus	Kaspersky	1

- CEO (2 devices: 1 Laptop, 1 phone)
- CEO (2 devices: 1 Laptop, 1 phone)
- CFO (2 devices: 1phone,1 laptop)
- CTO (2 devices: 1 phone, 1 laptop)
- AFRH (2 devices: 1 laptop, 1 phone)
- AFRH (2 devices: 1 laptop, 1 phone)
- ITC (2 devices: 1 laptop, 1 phone)
- Dev (2 devices: 1 laptop, 1 phone)
- OMS (2 devices: 1 laptop, 1 phone)
- ITSec (2 devices: 1 laptop, 1 phone)
- ITSec (2 devices: 1 laptop, 1 phone)
- 1 shared drive (Finance Drive)
- 1 Common drive for all (Common Drive)
- Dev database server

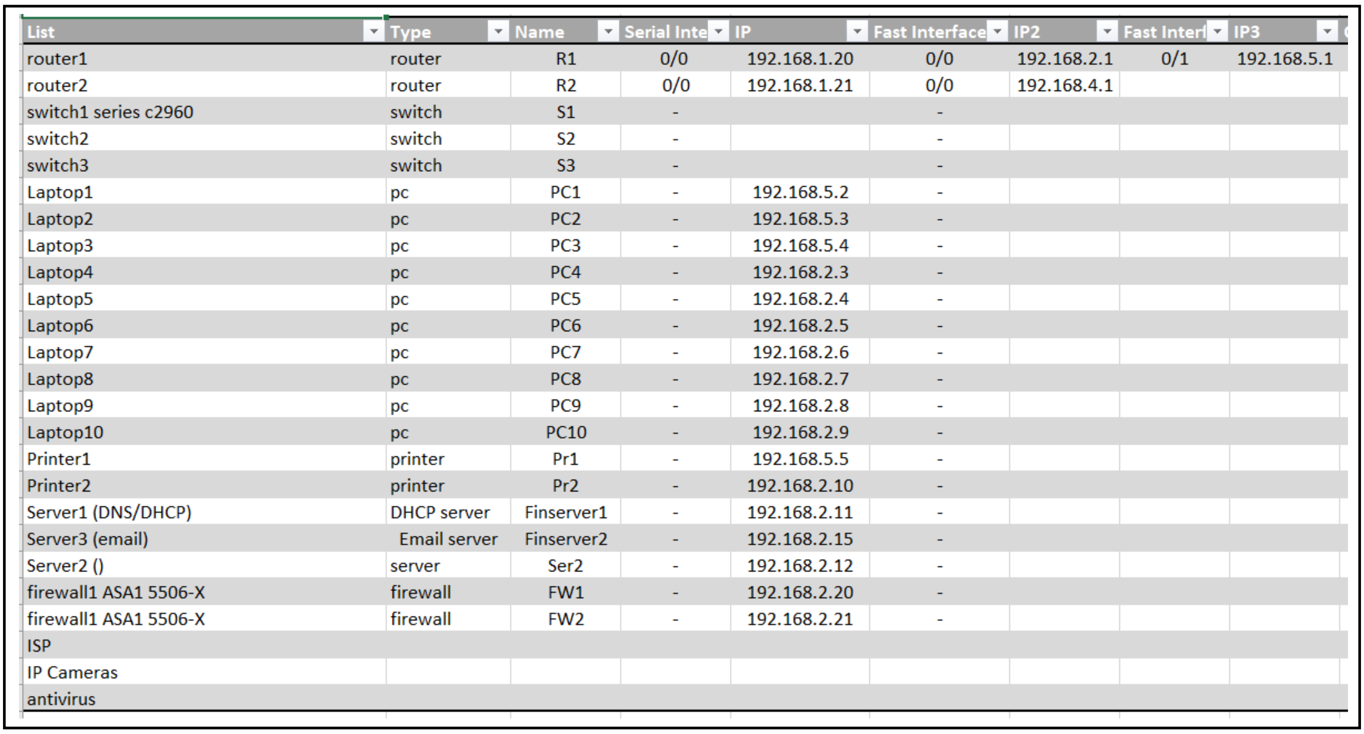
3. Network Topology



4. ‘0’ and ‘1’ Visibility Matrix

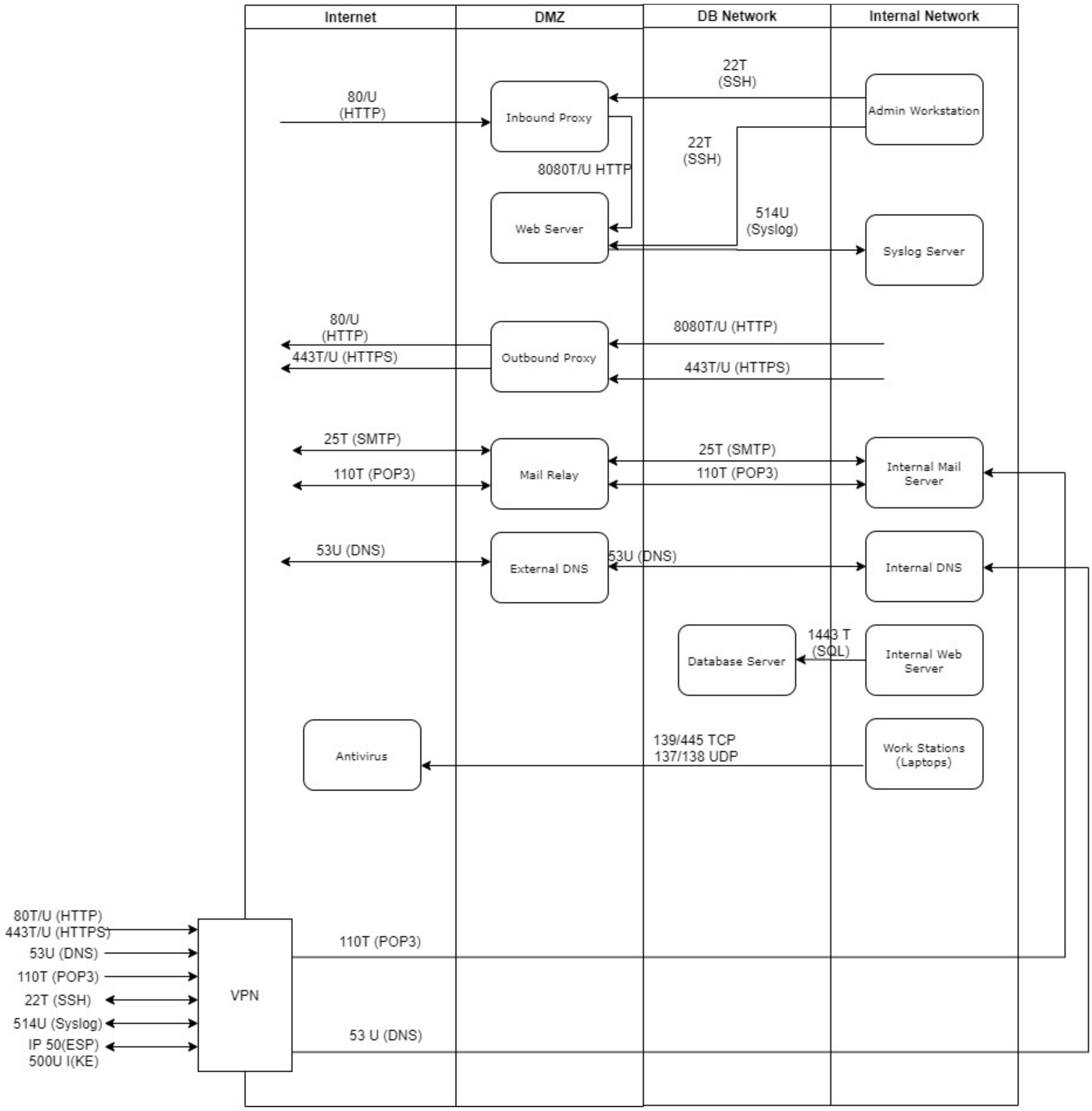


	CEO	CFO	CTO	AFRH	ITC	Dev	OMS	ITSec	Finance Drive	Common Drive	dev database server
CEO (2 devices : 1 Laptops, 1 phones)	1	0	0	0	0	0	0	0	0	1	0
CEO (2 devices : 1 Laptops, 1 phones)	1	0	0	0	0	0	0	0	0	1	0
CFO (2 devices : 1phone,1 laptop)	0	1	0	0	0	0	0	0	1	1	0
CTO (2 devices : 1 phone, 1 laptop)	0	0	1	0	0	0	0	0	0	1	0
AFRH (2 devices : 1 laptops, 1 phones)	0	0	0	1	0	0	0	0	1	1	0
AFRH (2 devices : 1 laptops, 1 phones)	0	0	0	1	0	0	0	0	1	1	0
ITC (2 devices : 1 laptop, 1 phone)	0/1	0/1	0/1	0/1	1	0/1	0/1	0/1	0/1	1	0/1
Dev (2 devices : 1 laptop, 1 phone)	0	0	0	0	0	1	0	0	0	1	1
OMS (2 devices : 1 laptop, 1 phone)	0	0	0	0	0	0	1	0	0	1	0
ITSec (2 devices : 1 laptops, 1 phones)	0	0	0	0	0	0	0	1	0	1	0
ITSec (2 devices : 1 laptops, 1 phones)	0	0	0	0	0	0	0	1	0	1	0
1 shared drive (Finance Drive)	0	0	0	0	0	0	0	0	1	0	0
1 Common drive for all (Common Drive)	0	0	0	0	0	0	0	0	0	1	0
dev database server	0	0	0	0	0	0	0	0	0	0	1



List	Type	Name	Serial Inte	IP	Fast Interface	IP2	Fast Interf	IP3
router1	router	R1	0/0	192.168.1.20	0/0	192.168.2.1	0/1	192.168.5.1
router2	router	R2	0/0	192.168.1.21	0/0	192.168.4.1		
switch1 series c2960	switch	S1	-		-			
switch2	switch	S2	-		-			
switch3	switch	S3	-		-			
Laptop1	pc	PC1	-	192.168.5.2	-			
Laptop2	pc	PC2	-	192.168.5.3	-			
Laptop3	pc	PC3	-	192.168.5.4	-			
Laptop4	pc	PC4	-	192.168.2.3	-			
Laptop5	pc	PC5	-	192.168.2.4	-			
Laptop6	pc	PC6	-	192.168.2.5	-			
Laptop7	pc	PC7	-	192.168.2.6	-			
Laptop8	pc	PC8	-	192.168.2.7	-			
Laptop9	pc	PC9	-	192.168.2.8	-			
Laptop10	pc	PC10	-	192.168.2.9	-			
Printer1	printer	Pr1	-	192.168.5.5	-			
Printer2	printer	Pr2	-	192.168.2.10	-			
Server1 (DNS/DHCP)	DHCP server	Finserver1	-	192.168.2.11	-			
Server3 (email)	Email server	Finserver2	-	192.168.2.15	-			
Server2 ()	server	Ser2	-	192.168.2.12	-			
firewall1 ASA1 5506-X	firewall	FW1	-	192.168.2.20	-			
firewall1 ASA1 5506-X	firewall	FW2	-	192.168.2.21	-			
ISP								
IP Cameras								
antivirus								

5. Data Flow Depiction



6. Firewall Security Policy

Inbound from internet

7. Rule.no:	Source	Destination	Port	Protocol	Action	Rule
1	Any	Inbound Proxy	80(TCP)	HTTP	Permit	Public access to our website
2	Any	Mail Relay	110(TCP)	POP3	Permit	Incoming E-mail
3	Any	Inbound	443(TCP)	HTTPS	Permit	Incoming traffic
4	Any	Any	Any	Any	Deny	Block all other traffic from internet

Public DMZ

Rule.no:	Source	Destination	Port	Protocol	Action	Rule
1	Outbound Proxy	Internal Networks	80(TCP)	HTTP	Deny	Blocks web traffic from hitting proxy
2	Outbound Proxy	Internal networks	443(TCP)	HTTPS	Deny	Blocks web traffic from hitting proxy
3	Outbound Proxy	Internal networks	443(UDP)	HTTPS	Deny	Blocks web traffic from hitting proxy
4	Outbound Proxy	Any	80(TCP)	HTTP	Permit	Employee web access from proxy to internet
5	Outbound Proxy	Any	80(UDP)	HTTP	Permit	Employee web access from proxy to internet
6	Outbound Proxy	Any	443(TCP)	HTTPS	Permit	Employee web access from proxy to internet
7	Outbound Proxy	Any	443(UDP)	HTTPS	Permit	Employee web access from proxy to internet

8	Mail relay	Internal mail server	110(TCP)	POP3	Permit	Inbound mail traffic from mail relay to internal mail server
9	Any	Any	Any	Any	Deny	Block all other traffic

Database DMZ

Rule.no:	Source	Destination	Port	Protocol	Action	Rule
1	Database DMZ	Syslog server	541(UDP)	Syslog	Permit	Log export from devices to central log server
2	Any	Any	Any	Any	Deny	Blocks all other traffic

Internal Network To DMZ / Internet

Rule.no:	Source	Destination	Port	Protocol	Action	Rule
1	Any	Outbound proxy	8080(TCP)	HTTP	Permit	Web access for employees
2	Any	Outbound proxy	8080(UDP)	HTTP	Permit	Web access for employees
3	Any	Outbound proxy	443(TCP)	HTTPS	Permit	Web access for employees
4	Any	Outbound proxy	443(UDP)	HTTPS	Permit	Web access for employees
5	Internal mail server	Mail relay	25(TCP)	SMTP	Permit	Outbound email to internet
6	Internal DNS	DMZ DNS	53(UDP)	DNS	Permit	DNS queries for internet host
7	Internal web-sever	Database server	1443(TCP)	SQL	Permit	SQL connections for

						database operations
8	Admin Workstation	Public DMZ	22(TCP)	SSH	Permit	Admin access for public DMZ
9	Any	Any	Any	Any	Deny	Blocks all other traffic