## Firewall: Rules









ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	6
	IPv4 ICMP	10.0.40.0/24	*	MGMT Workstations	*	*	none		Allow ICMP back to MGMT Workstations	
<b>23</b>	IPv4 ICMP	10.0.40.0/24	*	MGMT Workstations	*	*	none		Block ICMP back to Anything Else	
	IPv4 TCP	10.0.40.10	80 (HTTP)	*	*	*	none		Allow DMZ Web HTTP to Anywhere	
0	IPv4 TCP	10.0.40.10	443 (HTTPS)	*	*	*	none		Allow DMZ Web HTTPS to Anywhere	
0	IPv4 UDP	10.0.40.20	53 (DNS)	*	*	*	none		Allow DMZ DNS to Anywhere	
	IPv4 TCP	10.0.40.10	*	10.0.20.30	5998	*	none		Allow DMZ Web to Transaction DB Server	
×	IPv4 TCP/UDP	*	*		*	*	none		Deny All	



Description

Anti-Lockout

Allow ICMP

from MGMT

Anywhere

Deny ICMP

Allow Log

Server to send

Backups

DMZ Web

DMZ Web

HTTPS

HTTP

Allow LAN to

Allow LAN to

Allow HTTPS

Allow HTTPS

from USERS

to Internet Allow DNS

from MGMT

Allow DNS

to Internet

Out

Allow

from USERS

Allow SMTP

Transaction

DB Server to

Update DMZ Web

Deny All

to Internet

from MGMT

to Internet

from everywhere

else

Rule

Schedule





(X)

⊇l₄e

- Le

X

Q e

DX H

€ e

DX H

J.e

1X

-de

DX I

- e

(X)

J e

X

-de

XH

€ e

X +

- Le

(X)

ale

(X)

(X)







Port

\*

\*

25

(SMTP)

5998

Destination

LAN Address

27.18.160.120

10.0.40.10

10.0.40.10

8.8.8.8

8.8.8.8

10.0.40.10

Port

80

\*

443

80

443

443

443

53

53

\*

(DNS)

(DNS)

(HTTP)

(HTTPS)

(HTTPS)

(HTTPS)

\*

\*

\*

(HTTPS)

Floating WAN LAN OPT1

	ID	Proto	Source
		*	*
		IPv4 ICMP	MGMT Workstations
_ <b>E</b>		IPv4 ICMP	! MGMT Workstations
00		IPv4 TCP	10.0.10.30
		IPv4 TCP	A
		IPv4 TCP	. *
		IPv4 TCP	MGMT Workstations
		IPv4 TCP	10.0.30.0/24
		IPv4 UDP	MGMT Workstations

IPv4

UDP

IPv4 TCP

IPv4 TCP

IPv4

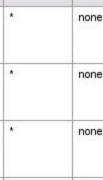
TCP/UDP

10.0.30.0/24

10.0.20.50

10.0.20.30

Source
*
MGMT Workstations
! MGMT Workstations



Gateway

**Oueue** 

none

none

none

none

none

none

none

none

none

## Firewall: Rules















ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	6
×		RFC 1918 networks	*	*	*	*	*		Block private networks	
×	*	Reserved/not assigned by IANA	*		*	*	*		Block bogon networks	30
	IPv4 TCP	*	443 (HTTPS)	MGMT Workstations	*	*	none		Allow HTTPS to MGMT	
	IPv4 TCP	*	443 (HTTPS)	10.0.30.0/24	*	*	none		Allow HTTPS to USERS	
	IPv4 UDP	8.8.8.8	53 (DNS)	MGMT Workstations	*	*	none		Allow DNS to MGMT	
	IPv4 UDP	8.8.8.8	53 (DNS)	10.0.30.0/24	*	*	none		Allow DNS to USERS	
	IPv4 TCP	27.18.160.120	443 (HTTPS)	10.0.10.30	*	*	none		Allow Log Backup back to Log Server	
	IPv4 ICMP echorep	*	*	MGMT Workstations	*	*	none		Allow Echo Replies back to MGMT Workstations	
<b>83</b>	IPv4 ICMP	*	*	! MGMT Workstations	*	*	none		Block ICMP Inbound except Echo Replies to MGMT WS	
	IPv4 TCP	A	*	10.0.40.10	80 (HTTP)	*	none		Allow Internet to DMZ Web HTTP	
C	IPv4 TCP	*	*	10.0.40.10	443 (HTTPS)	*	none		Allow Internet to DMZ Web HTTPS	
	IPv4 UDP	*	*	10.0.40.20	53 (DNS)	*	none		Allow Internet to DMZ DNS	
	IPv4 TCP	*	*	10.0.20.50	25 (SMTP)	*	none		Allow SMTP to Email Server	8
<b>23</b>	IPv4 TCP/UDP		*	*	*	*	none		Deny All	