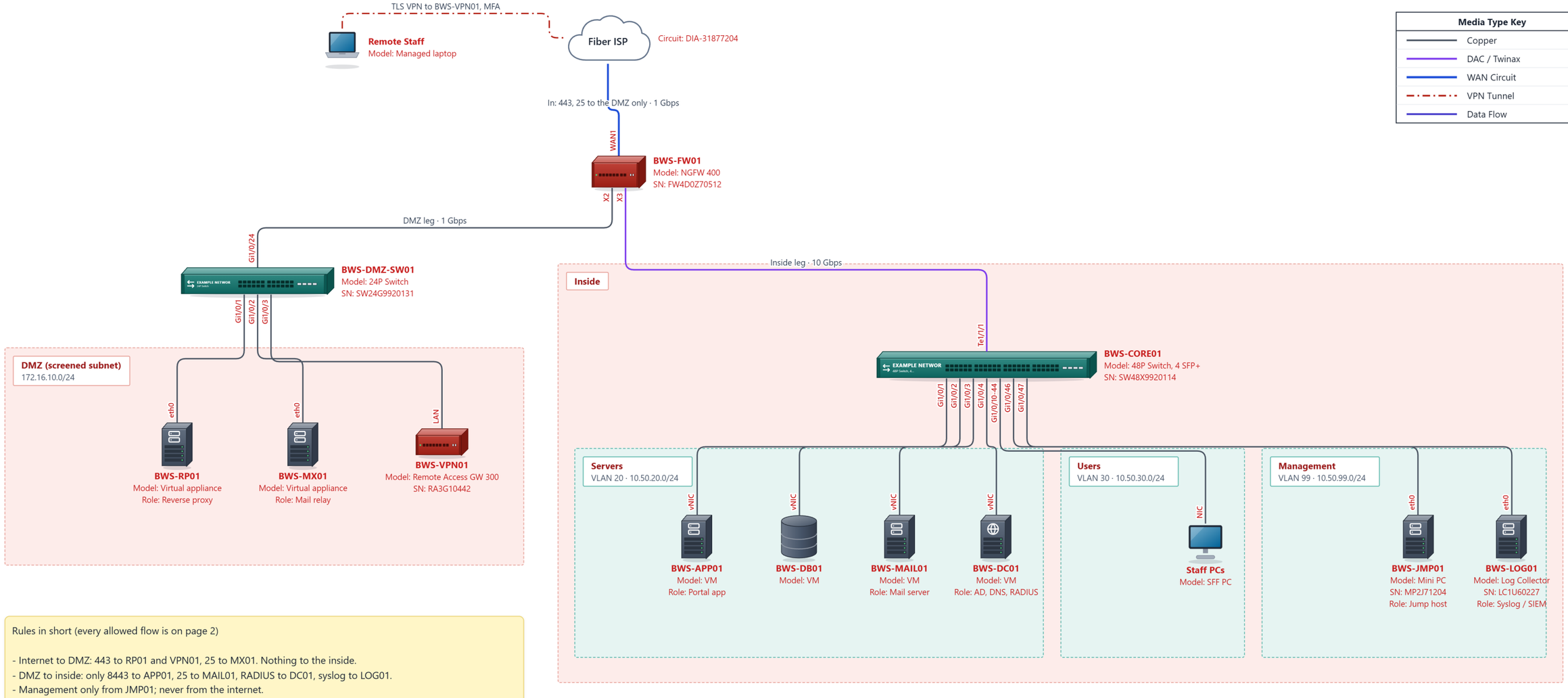
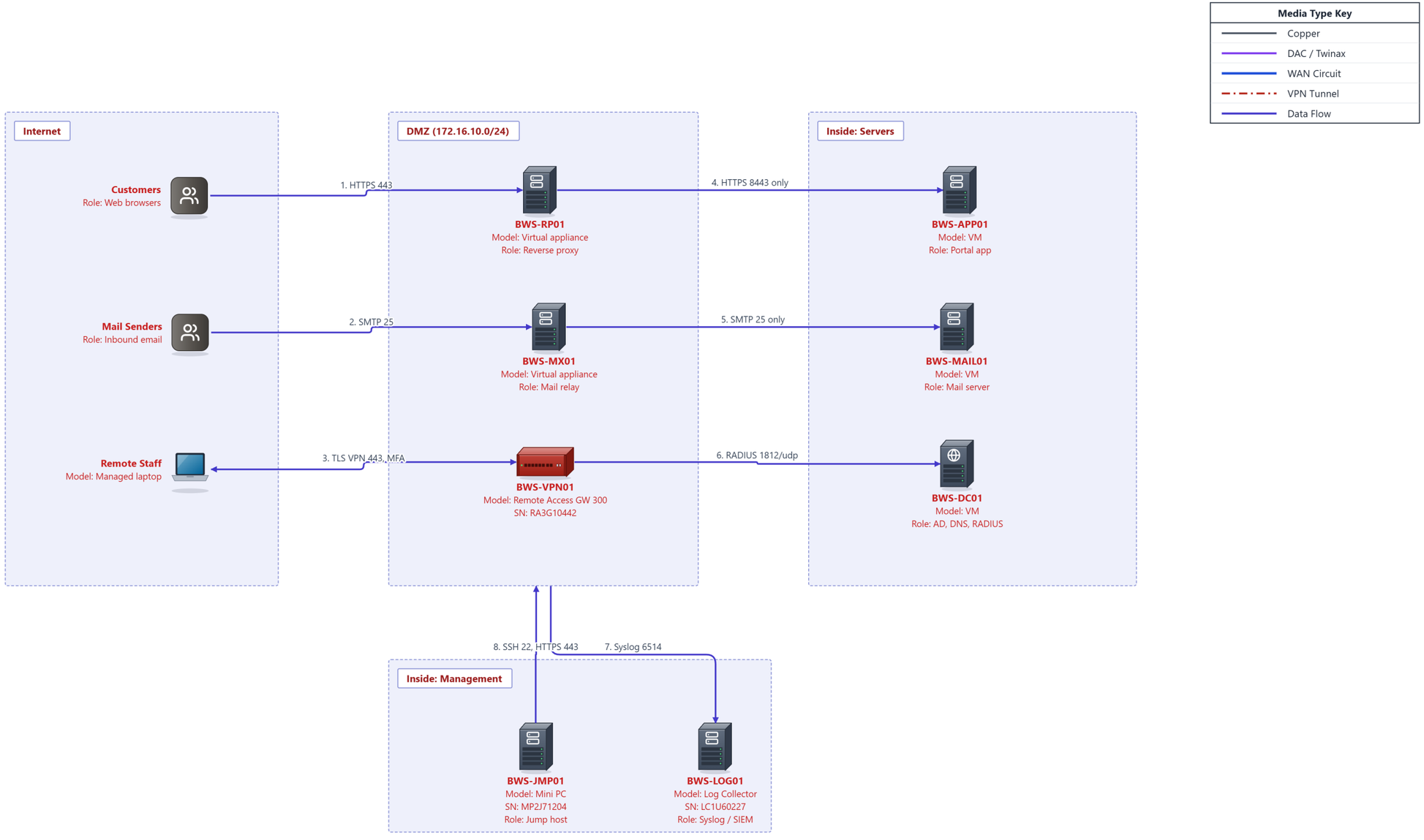


Rules in short (every allowed flow is on page 2)

- Internet to DMZ: 443 to RP01 and VPN01, 25 to MX01. Nothing to the inside.
- DMZ to inside: only 8443 to APP01, 25 to MAIL01, RADIUS to DC01, syslog to LOG01.
- Management only from JMP01; never from the internet.
- Everything else: denied and logged.

DOCUMENT **Brightwater Supply - DMZ and Firewall Zones** Brightwater Supply Co. · 75 Commerce Drive, Springfield	SHEET TITLE **Three-Legged DMZ**	VERSION 1.0	LAST CHANGED 2026-11-25	VERIFIED	SHEET 1 of 8
		DRAWN BY	LAST EDITOR	APPROVED	



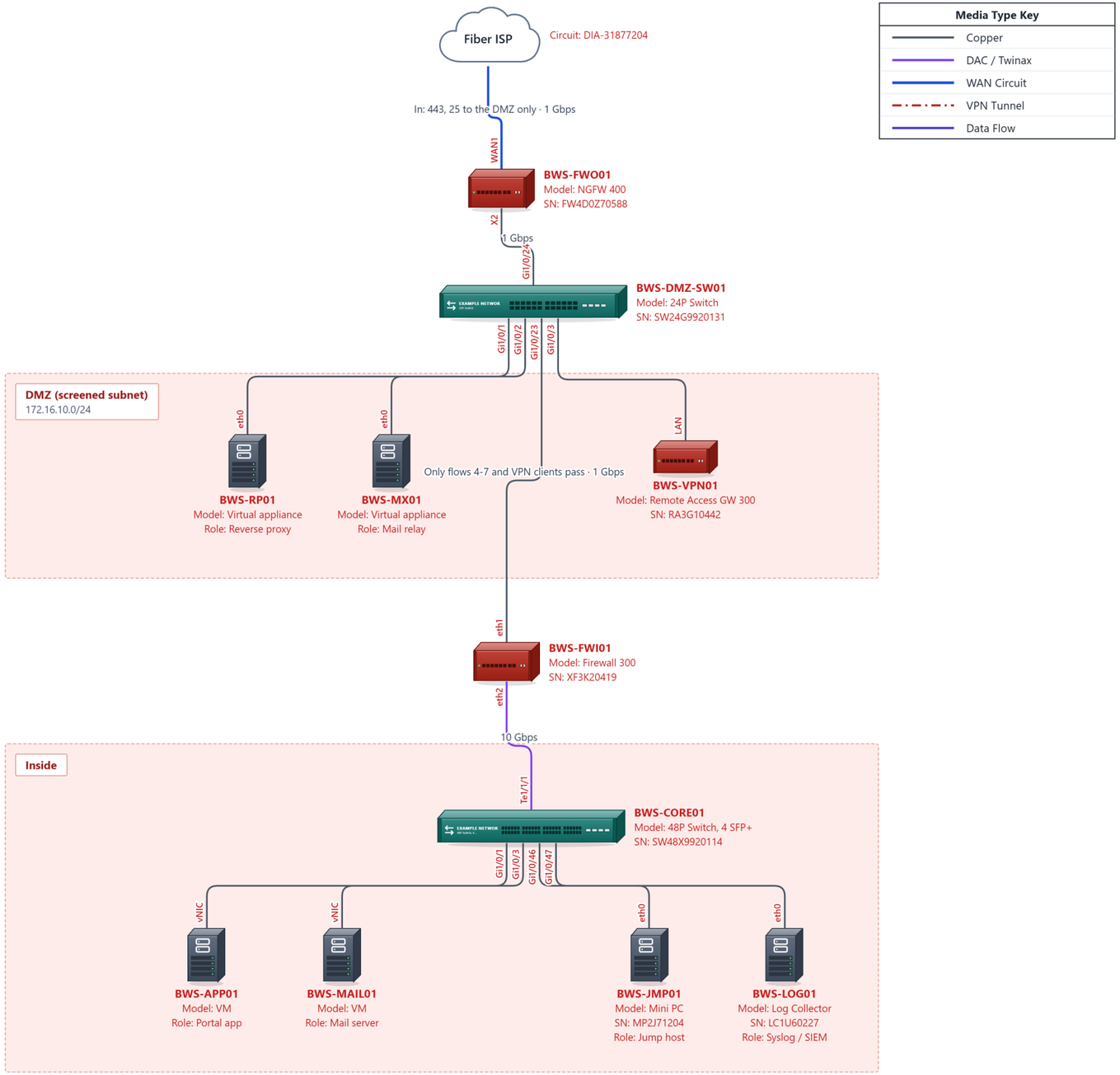
Also allowed: VPN clients (10.50.40.0/24) get the Users VLAN rules; DMZ hosts may reach DNS, NTP and their update servers on the internet.
Denied and logged: internet to the inside (any port), DMZ to the inside except flows 4-7, any other DMZ to internet traffic, and management from anywhere but BWS-JMP01.

DOCUMENT	SHEET TITLE	VERSION	LAST CHANGED	VERIFIED	SHEET
Brightwater Supply - DMZ and Firewall Zones Brightwater Supply Co. · 75 Commerce Drive, Springfield	**Allowed Flows**	1.0	2026-11-25		2 of 8
		DRAWN BY	LAST EDITOR	APPROVED	

Back-to-back DMZ

The DMZ sits between two firewalls. An attacker who gets past the outer one still faces the inner one, which only lets flows 4-7 and VPN client traffic in.

Two vendors means one bug or one bad rule does not open both. The cost: two rule bases to keep in step.



DOCUMENT	SHEET TITLE	VERSION	LAST CHANGED	VERIFIED	SHEET
Brightwater Supply - DMZ and Firewall Zones Brightwater Supply Co. · 75 Commerce Drive, Springfield	**Back-to-Back DMZ**	**1.0**	**2026-11-25**		**3** of 8
		DRAWN BY	LAST EDITOR	APPROVED	

Device Inventory 36 devices

Hostname	Type	Vendor / model	Serial	Mgmt IP	Area	Location	Page
Remote Staff	Laptop	Example Computers Managed laptop					Three-Legged DMZ
Fiber ISP	ISP / Carrier						Three-Legged DMZ
BWS-FW01	Firewall	Example Networks NGFW 400	FW4D0Z70512	10.50.99.1		Server room, Rack 1, U40	Three-Legged DMZ
BWS-DMZ-SW01	Switch	Example Networks 24P Switch	SW24G9920131	10.50.99.4		Server room, Rack 1, U36	Three-Legged DMZ
BWS-RP01	Server	Example Systems Virtual appliance		172.16.10.10	DMZ (screened subnet)		Three-Legged DMZ
BWS-MX01	Server	Example Systems Virtual appliance		172.16.10.20	DMZ (screened subnet)		Three-Legged DMZ
BWS-VPN01	VPN Gateway	Example Networks Remote Access GW 300	RA3G10442	172.16.10.30	DMZ (screened subnet)		Three-Legged DMZ
BWS-CORE01	Switch	Example Networks 48P Switch, 4 SFP+	SW48X9920114	10.50.99.2	Inside	Server room, Rack 1, U38	Three-Legged DMZ
BWS-APP01	Server	Example Systems VM		10.50.20.10	Servers		Three-Legged DMZ
BWS-DB01	Database	Example Systems VM		10.50.20.11	Servers		Three-Legged DMZ
BWS-MAIL01	Server	Example Systems VM		10.50.20.12	Servers		Three-Legged DMZ
BWS-DC01	DC / DNS / DHCP	Example Systems VM		10.50.20.5	Servers		Three-Legged DMZ
Staff PCs	Workstation	Example Computers SFF PC			Users		Three-Legged DMZ
BWS-JMP01	Server	Example Systems Mini PC	MP2J71204	10.50.99.20	Management		Three-Legged DMZ
BWS-LOG01	Server	Example Systems Log Collector	LC1U60227	10.50.99.30	Management		Three-Legged DMZ
Remote Staff	Laptop	Example Computers Managed laptop			Internet		Allowed Flows
BWS-RP01	Server	Example Systems Virtual appliance		172.16.10.10	DMZ (172.16.10.0/24)		Allowed Flows
BWS-MX01	Server	Example Systems Virtual appliance		172.16.10.20	DMZ (172.16.10.0/24)		Allowed Flows
BWS-VPN01	VPN Gateway	Example Networks Remote Access GW 300	RA3G10442	172.16.10.30	DMZ (172.16.10.0/24)		Allowed Flows
BWS-APP01	Server	Example Systems VM		10.50.20.10	Inside: Servers		Allowed Flows
BWS-MAIL01	Server	Example Systems VM		10.50.20.12	Inside: Servers		Allowed Flows
BWS-DC01	DC / DNS / DHCP	Example Systems VM		10.50.20.5	Inside: Servers		Allowed Flows
BWS-JMP01	Server	Example Systems Mini PC	MP2J71204	10.50.99.20	Inside: Management		Allowed Flows
BWS-LOG01	Server	Example Systems Log Collector	LC1U60227	10.50.99.30	Inside: Management		Allowed Flows
Fiber ISP	ISP / Carrier						Back-to-Back DMZ
BWS-FWO01	Firewall	Example Networks NGFW 400	FW4D0Z70588	10.50.99.11			Back-to-Back DMZ
BWS-DMZ-SW01	Switch	Example Networks 24P Switch	SW24G9920131	10.50.99.4		Server room, Rack 1, U36	Back-to-Back DMZ
BWS-RP01	Server	Example Systems Virtual appliance		172.16.10.10	DMZ (screened subnet)		Back-to-Back DMZ
BWS-MX01	Server	Example Systems Virtual appliance		172.16.10.20	DMZ (screened subnet)		Back-to-Back DMZ
BWS-VPN01	VPN Gateway	Example Networks Remote Access GW 300	RA3G10442	172.16.10.30	DMZ (screened subnet)		Back-to-Back DMZ
BWS-FWI01	Firewall	Example Security Firewall 300	XF3K20419	10.50.99.12			Back-to-Back DMZ
BWS-CORE01	Switch	Example Networks 48P Switch, 4 SFP+	SW48X9920114	10.50.99.2	Inside	Server room, Rack 1, U38	Back-to-Back DMZ
BWS-APP01	Server	Example Systems VM		10.50.20.10	Inside		Back-to-Back DMZ
BWS-MAIL01	Server	Example Systems VM		10.50.20.12	Inside		Back-to-Back DMZ
BWS-JMP01	Server	Example Systems Mini PC	MP2J71204	10.50.99.20	Inside		Back-to-Back DMZ
BWS-LOG01	Server	Example Systems Log Collector	LC1U60227	10.50.99.30	Inside		Back-to-Back DMZ

Link / Cabling Schedule 25 links

Cable ID	End A	Interface	End B	Interface	Media	Speed	VLANs	Length	Test	Label / notes	Page
	Remote Staff		Fiber ISP		VPN Tunnel					TLS VPN to BWS-VPN01, MFA	Three-Legged DMZ
	Fiber ISP		BWS-FW01	WAN1	WAN Circuit	1 Gbps				In: 443, 25 to the DMZ only	Three-Legged DMZ
BWS-C002	BWS-FW01	X2	BWS-DMZ-SW01	Gi1/0/24	Copper	1 Gbps	10	1 m	Pass	DMZ leg	Three-Legged DMZ
BWS-C003	BWS-FW01	X3	BWS-CORE01	Te1/1/1	DAC / Twinax	10 Gbps	20,30,99	1 m	Pass	Inside leg	Three-Legged DMZ
BWS-C011	BWS-DMZ-SW01	Gi1/0/1	BWS-RP01	eth0	Copper		10	2 m	Pass		Three-Legged DMZ
BWS-C012	BWS-DMZ-SW01	Gi1/0/2	BWS-MX01	eth0	Copper		10	2 m	Pass		Three-Legged DMZ
BWS-C013	BWS-DMZ-SW01	Gi1/0/3	BWS-VPN01	LAN	Copper		10	2 m	Pass		Three-Legged DMZ
	BWS-CORE01	Gi1/0/1	BWS-APP01	vNIC	Copper		20				Three-Legged DMZ
	BWS-CORE01	Gi1/0/2	BWS-DB01	vNIC	Copper		20				Three-Legged DMZ
	BWS-CORE01	Gi1/0/3	BWS-MAIL01	vNIC	Copper		20				Three-Legged DMZ
	BWS-CORE01	Gi1/0/4	BWS-DC01	vNIC	Copper		20				Three-Legged DMZ
	BWS-CORE01	Gi1/0/10-44	Staff PCs	NIC	Copper		30				Three-Legged DMZ
BWS-C046	BWS-CORE01	Gi1/0/46	BWS-JMP01	eth0	Copper		99	2 m	Pass		Three-Legged DMZ
BWS-C047	BWS-CORE01	Gi1/0/47	BWS-LOG01	eth0	Copper		99	2 m	Pass		Three-Legged DMZ
	Fiber ISP		BWS-FWO01	WAN1	WAN Circuit	1 Gbps				In: 443, 25 to the DMZ only	Back-to-Back DMZ
BWS-C102	BWS-FWO01	X2	BWS-DMZ-SW01	Gi1/0/24	Copper	1 Gbps	10	1 m	Pass		Back-to-Back DMZ
	BWS-DMZ-SW01	Gi1/0/1	BWS-RP01	eth0	Copper		10				Back-to-Back DMZ
	BWS-DMZ-SW01	Gi1/0/2	BWS-MX01	eth0	Copper		10				Back-to-Back DMZ
	BWS-DMZ-SW01	Gi1/0/3	BWS-VPN01	LAN	Copper		10				Back-to-Back DMZ
BWS-C103	BWS-DMZ-SW01	Gi1/0/23	BWS-FWI01	eth1	Copper	1 Gbps	10	1 m	Pass	Only flows 4-7 and VPN clients pass	Back-to-Back DMZ
BWS-C104	BWS-FWI01	eth2	BWS-CORE01	Te1/1/1	DAC / Twinax	10 Gbps	20,30,99	1 m	Pass		Back-to-Back DMZ
	BWS-CORE01	Gi1/0/1	BWS-APP01	vNIC	Copper		20				Back-to-Back DMZ
	BWS-CORE01	Gi1/0/3	BWS-MAIL01	vNIC	Copper		20				Back-to-Back DMZ
	BWS-CORE01	Gi1/0/46	BWS-JMP01	eth0	Copper		99				Back-to-Back DMZ
	BWS-CORE01	Gi1/0/47	BWS-LOG01	eth0	Copper		99				Back-to-Back DMZ

VLAN / Subnet Table 3 VLANs

VLAN	Name	Subnet	Gateway	DHCP scope / helper	Devices	Page
20	Servers	10.50.20.0/24	10.50.20.1	Static	4	Three-Legged DMZ
30	Users	10.50.30.0/24	10.50.30.1	BWS-DC01, .100-.250	1	Three-Legged DMZ
99	Management	10.50.99.0/24	10.50.99.1	Static	2	Three-Legged DMZ

Data Flows 8 flows

From	To	Data	Class.	Sensitive data	Protocol / port	Encryption	Purpose	Page
Customers (Internet)	BWS-RP01 (DMZ (172.16.10.0/24))	Portal traffic	Confidential	Personal info	HTTPS 443	TLS 1.3	Customer portal, published by the reverse proxy	Allowed Flows
Mail Senders (Internet)	BWS-MX01 (DMZ (172.16.10.0/24))	Inbound email	Internal		SMTP 25 (STARTTLS)	TLS 1.2	Receive email	Allowed Flows
Remote Staff (Internet)	BWS-VPN01 (DMZ (172.16.10.0/24))	Remote access sessions	Confidential	Credentials	TLS VPN 443	TLS 1.3	Staff remote access	Allowed Flows
BWS-RP01 (DMZ (172.16.10.0/24))	BWS-APP01 (Inside: Servers)	Proxied portal requests	Confidential	Personal info	HTTPS 8443	TLS 1.2	Reverse proxy to the one app server behind it	Allowed Flows
BWS-MX01 (DMZ (172.16.10.0/24))	BWS-MAIL01 (Inside: Servers)	Filtered email	Internal		SMTP 25	TLS 1.2	Deliver filtered mail to the mail server	Allowed Flows
BWS-VPN01 (DMZ (172.16.10.0/24))	BWS-DC01 (Inside: Servers)	Sign-in checks	Confidential	Credentials	RADIUS 1812/udp	Other encryption	Check VPN sign-ins and MFA	Allowed Flows
DMZ (172.16.10.0/24)	BWS-LOG01 (Inside: Management)	Logs from every DMZ host	Internal		Syslog over TLS 6514	TLS 1.2	Logging and monitoring	Allowed Flows
BWS-JMP01 (Inside: Management)	DMZ (172.16.10.0/24)	Admin sessions	Confidential	Credentials	SSH 22, HTTPS 443	SSH / SFTP	Administer DMZ hosts from the jump host	Allowed Flows

Data Stores 1 store

Data store	Stores	Class.	Sensitive data	Encrypted at rest	Kept for	Region	Owner	Boundary
BWS-DB01	Customer accounts and orders	Confidential	Personal info	Yes	7 years			