NETWORK SECURITY PROJECT

FortiGate 60F
Secure SD-WAN Deployment

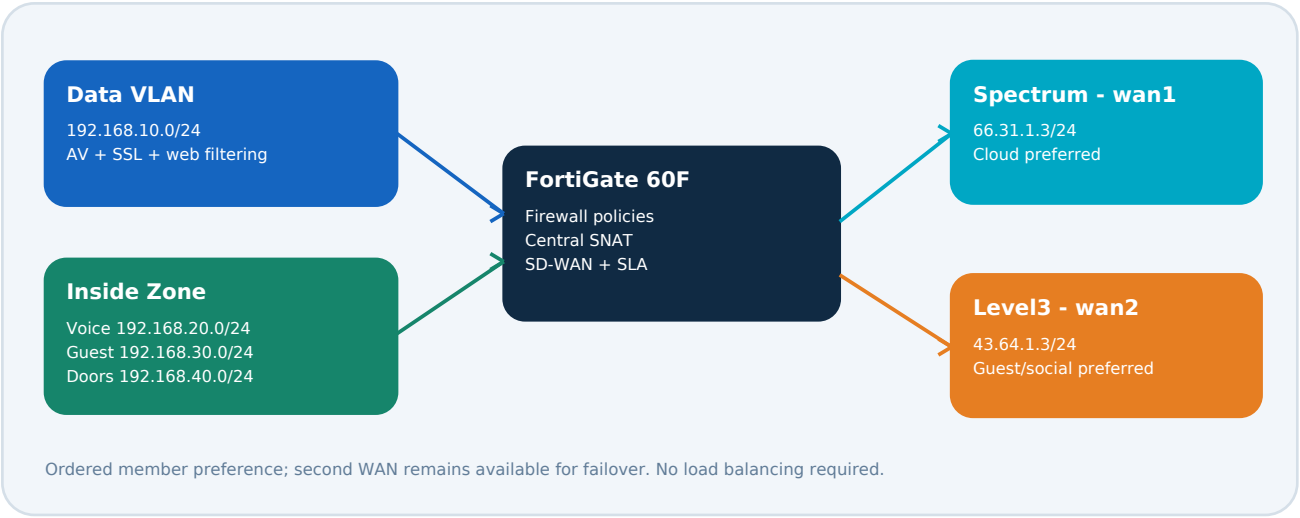
Application-aware path steering, centralized NAT, VLAN-specific security profiles, and dual-WAN failover validation.

Prepared by

Clovis Capellan

31 August 2026 | Version 1.0

1. Architecture and Design



The FortiGate 60F separates the Data network from the Inside Zone. Data users receive threat prevention and restricted web access; Doors, Guest, and Voice retain general Internet access. Both WAN circuits are members of the Outsize Zone and are selected by ordered SD-WAN rules.

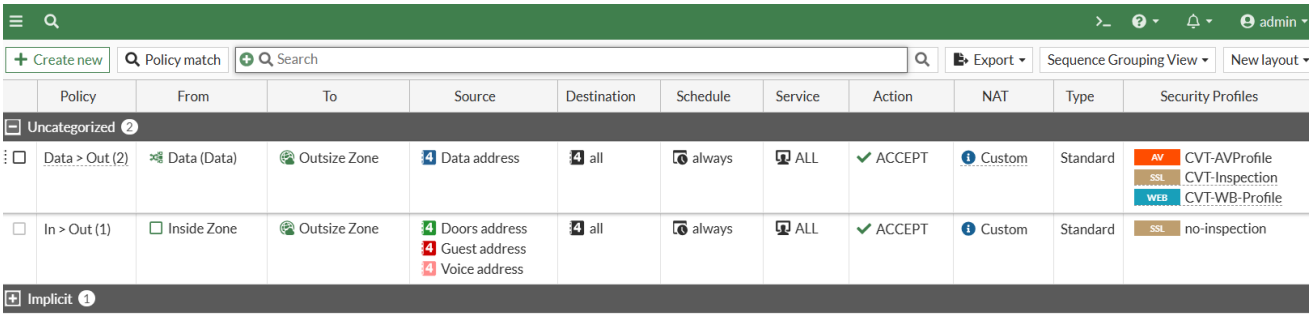
Interface and segmentation summary

NETWORK / INTERFACE	ADDRESS	ZONE / ROLE	DESIGN INTENT
Data	192.168.10.1/24	Dedicated interface/VLAN	Restricted Internet
Voice	192.168.20.1/24	Inside Zone	General Internet
Guest	192.168.30.1/24	Inside Zone	General Internet; WAN2 preferred
Doors	192.168.40.1/24	Inside Zone	General Internet
Spectrum (wan1)	66.31.1.3/24	Outsize Zone	GW 66.31.1.254
Level3 (wan2)	43.64.1.3/24	Outsize Zone	GW 43.64.1.254
Management	192.168.99.3/24	internal1	HTTPS/SSH/PING

2. Security Profiles, Policies, and Central NAT

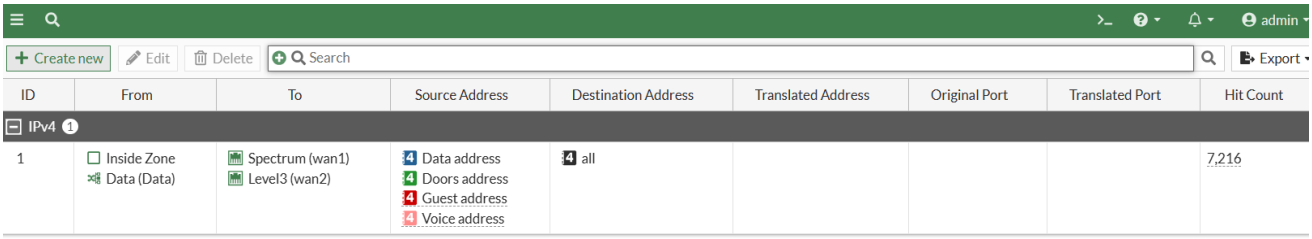
CONTROL	APPLIED TO	FUNCTION
CVT-AVProfile	Data only	Block detected malware across HTTP, SMTP, POP3, IMAP, and FTP; enable mobile malware and outbreak prevention.
CVT-WB-Profile	Data only	Block social media and streaming services, including YouTube and Netflix; allow other approved categories.
CVT-Inspection	Data only	Apply SSL inspection so HTTPS destinations can be categorized and security profiles can inspect encrypted sessions.
no-inspection	Doors / Guest / Voice	Permit general access without the Data VLAN restrictions; retain logging and least-privilege policy design.

Firewall policy evidence



The Data > Out policy applies CVT-AVProfile, CVT-Inspection, and CVT-WB-Profile. The Inside Zone policy covers Doors, Guest, and Voice with no-inspection.

Central SNAT evidence



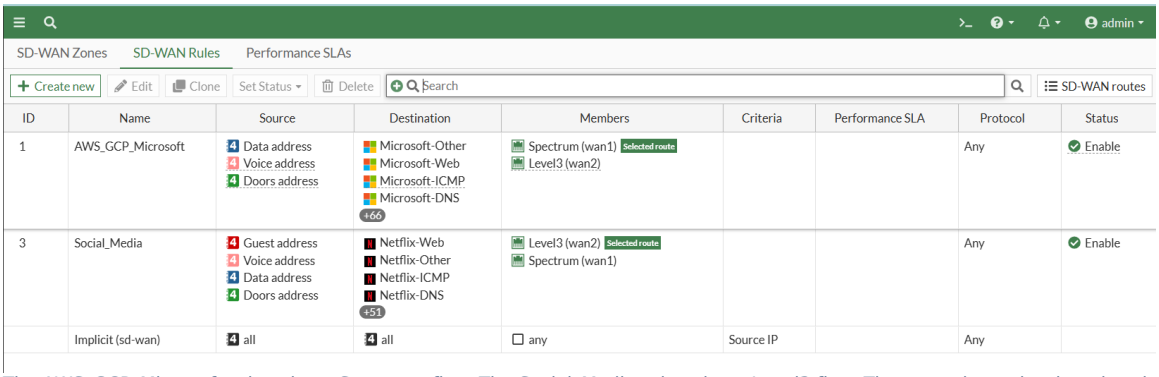
Central SNAT rule 1 covers Data and the Inside Zone toward both WAN interfaces. Translation follows the selected egress interface unless a dedicated IP pool is added.

Security note: blocking YouTube, Netflix, and social media reliably over HTTPS depends on current FortiGuard categorization, application signatures, and an SSL inspection method appropriate for managed endpoints.

3. SD-WAN Steering and Health Monitoring

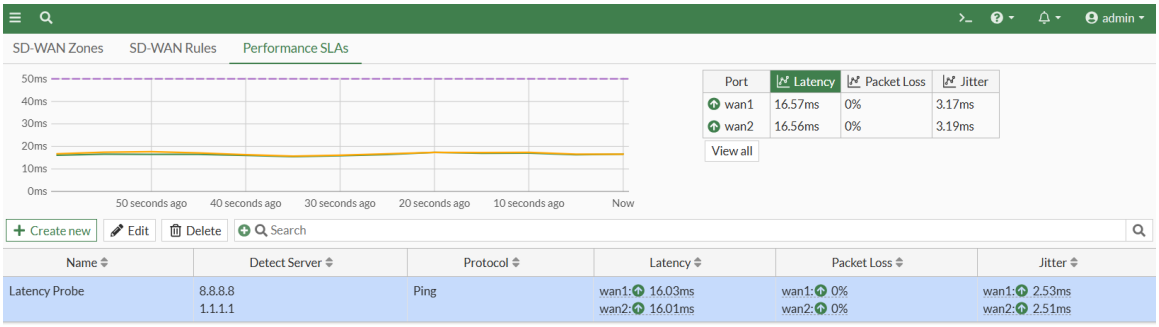
MEMBER	GATEWAY	PRIMARY USE	BACKUP
Spectrum (wan1)	66.31.1.254	Preferred: AWS, GCP, Azure/Microsoft	Level3
Level3 (wan2)	43.64.1.254	Preferred: Guest, social media, streaming	Spectrum

Application-aware rules



The AWS_GCP_Microsoft rule selects Spectrum first. The Social_Media rule selects Level3 first. The second member is ordered as the failover path rather than used for active load balancing.

Performance SLA



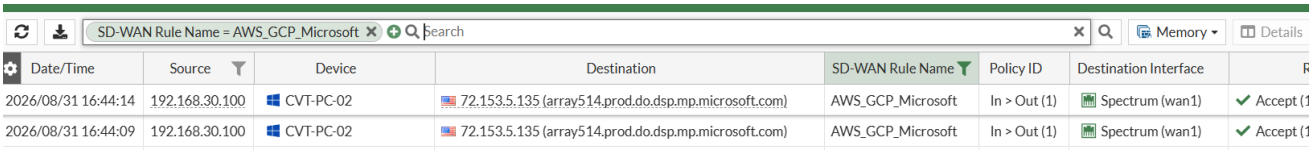
Captured SLA: approximately 16 ms latency, 0% loss, and 2.5-3.2 ms jitter using 8.8.8.8 and 1.1.1.1 probes.

Failover behavior observed in this lab: when an ordered, non-load-balanced path fails, reconvergence can drop approximately 1-2 packets. Existing sessions may also reset if the public NAT address changes, so the exact user impact depends on the application and protocol.

4. Validation, Operations, and Document Control

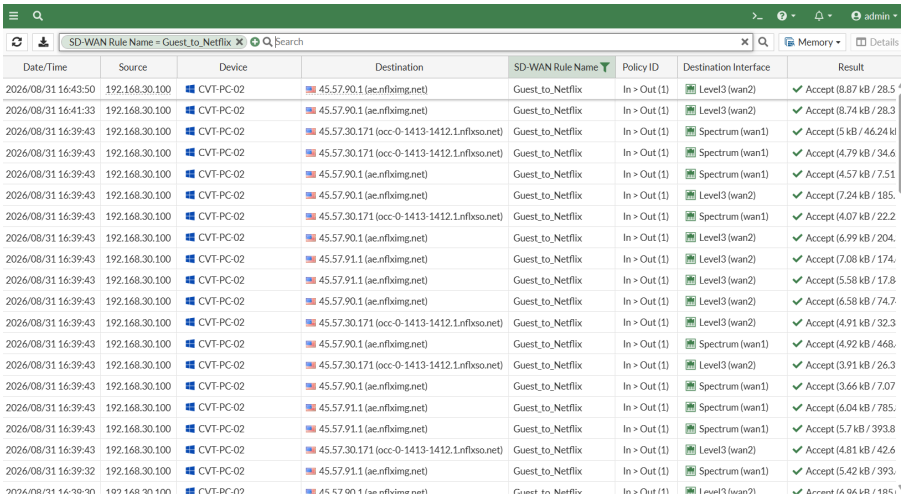
Forward traffic logs were used to confirm that the matched SD-WAN rule and destination interface agreed with the intended steering policy.

Cloud traffic validation - Spectrum wan1



Date/Time	Source	Device	Destination	SD-WAN Rule Name	Policy ID	Destination Interface	R
2026/08/31 16:44:14	192.168.30.100	CVT-PC-02	72.153.5.135 (array514.prod.do.dsp.mp.microsoft.com)	AWS_GCP_Microsoft	In > Out (1)	Spectrum (wan1)	Accept (1
2026/08/31 16:44:09	192.168.30.100	CVT-PC-02	72.153.5.135 (array514.prod.do.dsp.mp.microsoft.com)	AWS_GCP_Microsoft	In > Out (1)	Spectrum (wan1)	Accept (1

Guest / Netflix validation and failover testing



Date/Time	Source	Device	Destination	SD-WAN Rule Name	Policy ID	Destination Interface	Result
2026/08/31 16:43:50	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (8.87 kB / 28.5
2026/08/31 16:41:33	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (8.74 kB / 28.3
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (5 kB / 46.24 kl
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (4.79 kB / 34.6
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (4.57 kB / 7.51
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (7.24 kB / 185.
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (4.07 kB / 22.2
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (6.99 kB / 204.
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.91.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (7.08 kB / 174.
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.91.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (5.58 kB / 17.8
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (6.58 kB / 74.7
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (4.91 kB / 32.3
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (4.92 kB / 468.
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (3.91 kB / 26.3
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.90.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (3.66 kB / 7.07
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.91.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (6.04 kB / 785.
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.91.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (5.7 kB / 393.8
2026/08/31 16:39:43	192.168.30.100	CVT-PC-02	45.57.30.171 (occ-0-1413-1412.1.nflxso.net)	Guest_to_Netflix	In > Out (1)	Level3 (wan2)	Accept (4.81 kB / 42.6
2026/08/31 16:39:32	192.168.30.100	CVT-PC-02	45.57.91.1 (ae.nflximg.net)	Guest_to_Netflix	In > Out (1)	Spectrum (wan1)	Accept (5.42 kB / 393.

Acceptance checklist

TEST	PASS CONDITION
Segmentation	Data, Voice, Guest, and Doors use the documented /24 networks and correct zones.
Security	Data blocks malware, social media, YouTube, and Netflix; other VLANs retain intended access.
Cloud steering	AWS, GCP, Azure/Microsoft sessions match AWS_GCP_Microsoft and exit Spectrum wan1.
Guest/social steering	Guest and social/streaming sessions match the intended rule and prefer Level3 wan2.
Failover	Disable each WAN in turn; verify SLA state, backup selection, NAT behavior, logs, and application recovery.

Document control

FIELD	VALUE
Version	1.0
Date	31 August 2026
Prepared by	Clovis Capellan
Approval status	Project Based
Platform	FortiGate 60F secure SD-WAN lab

Configuration evidence supplied from the FortiGate GUI. Validate object names, ISDB coverage, inspection mode, and supported commands against the installed FortiOS release before production deployment.