

SD-WAN for Multi-Branch Operations

A Procurement & Operations Playbook for Banking, Retail, and Telecom Buyers

Audience: Heads of IT Infrastructure, Network Architects, and CFOs evaluating WAN transformation across 50+ branches in banking, retail, telecom, and government.

Format: 11 pages · Reading time: ~22 minutes · Vendor-neutral perspective

Published by Inara Technologies · Islamabad, Pakistan · www.inara.pk

ISO 9001:2015 · ISO 27001 · Authorized partner: Cisco, Fortinet, Palo Alto, Juniper, Aruba

TABLE OF Contents

#	Section	Pg.
	Executive Summary	3
01	Why Branch WAN Modernization Is Now a Board-Level Question	4
02	MPLS, Internet, SD-WAN, SASE – What Replaces What	5
03	The Four-Pillar SD-WAN Capability Framework	6
04	Transport Strategy: How to Mix MPLS, Broadband, LTE, and 5G	7
05	Security Architecture: Where the Firewall Lives Now	8
06	Operations: NOC Model, SLAs, and Day-2 Reality	9
07	Cost & Commercial Model – What You Actually Save	10
08	The 16-Question SD-WAN Vendor Scorecard	11

EXECUTIVE

Summary

SD-WAN procurement decisions made between 2022 and 2026 will define enterprise branch connectivity costs and security posture for the next decade. For Pakistani banks operating 200–700+ branches, retailers running 100–500+ outlets, and telecom operators managing distributed PoPs, the WAN choice is no longer a routing question – it is a question about transport mix, security architecture, observability, and operational model.

The market has fragmented. MPLS providers are repositioning as SD-WAN providers. Firewall vendors are adding SD-WAN to existing security platforms. Cloud-first 'SASE' vendors are selling outside-in security overlays. Each of these positions favours a different architecture and a different commercial outcome. This guide gives the buyer the framework, the transport math, and the 16-item scorecard needed to choose deliberately rather than by vendor narrative.

Central Argument

Vendor selection is the second decision in an SD-WAN program, not the first. The first decision is the transport and security topology – specifically: where will inspection happen, how many internet break-outs will the branch carry, and what is the failover behaviour when the primary path degrades. Buyers who allow a vendor to lead with technology before this topology decision is made consistently over-pay and under-perform.

WHY BRANCH

WAN Modernization Is a Board-Level Question

Three Forces Are Converging on the WAN Budget

Branch WAN was a quiet line item until three forces collided. Each force on its own is manageable; together they are reshaping the WAN budget at every multi-branch enterprise in Pakistan.

Force	What It Changes	Buyer Implication
Bandwidth growth at the branch	Internal SaaS, branch video, biometric onboarding, real-time analytics each require 5-10x the bandwidth of the legacy core-banking dial-up era	MPLS-only WANs hit a price-per-Mbps wall above 100 branches
Security perimeter is now in the cloud	Microsoft 365, core-banking-adjacent SaaS, payment gateways, observability tools – the corporate perimeter has moved to the internet edge	Backhauling internet traffic to a central firewall over MPLS is operationally and economically untenable
Last-mile diversity	Multiple Pakistani last-mile carriers (PTCL, Wateen, Multinet, Nayatel, fiber + LTE + 5G + StarLink) make transport diversification practical at every branch	Mixed-transport SD-WAN can deliver MPLS-like reliability at internet-grade economics

The cumulative effect: a CFO who approved a MPLS extension three years ago for a 150-branch network is now looking at a 30-50% Opex reduction opportunity, if the architecture is right. The architecture decisions described in the rest of this paper are how that opportunity is realized – or missed.

MPLS, INTERNET, SD-WAN, SASE – What Replaces What

Clearing Up the Three Most Common Buyer Confusions

The terminology is genuinely confused, even among experienced network buyers. Use the table below as a reference when reviewing vendor proposals.

Term	What It Is	What It Replaces	Where It Falls Short
MPLS	A Layer-3 VPN service from a carrier with class-of-service queues	Frame Relay and ATM circuits of the 1990s-2000s	Costly per-Mbps; long provisioning; no cloud break-out; flat performance to the internet edge
Internet VPN (IPsec)	Branch-to-HQ tunnels over commodity broadband	Reduces MPLS spend; useful for low-traffic sites	No application-aware routing; failover takes seconds; QoS depends on carrier behaviour
SD-WAN	Overlay fabric with application-aware path selection across MPLS + internet + LTE	Replaces or augments MPLS; turns multiple transports into one logical network	Does not by itself provide cloud-delivered security; lacks SaaS optimization unless paired with SASE/SSE
SASE / SSE	Cloud-delivered security stack (FWaaS, SWG, ZTNA, CASB) consumed at the branch via SD-WAN	Replaces the central firewall + internet break-out architecture; integrates security into the WAN fabric	Strong only when the SD-WAN and the security cloud are tightly integrated; loosely-coupled SASE is fragile

THE FOUR-PILLAR SD-WAN Capability Framework

Score Every Provider 1–4 on Each Pillar

#	Pillar	What to Evaluate
01	Transport-Agnostic Fabric	Native support for MPLS, dedicated internet, broadband, LTE, 5G, StarLink. Application-aware path selection tuned to your application mix. Sub-second failover. Last-mile carrier diversity in Pakistan covered out of the box.
02	Integrated Security	On-box NGFW capability for branch internet break-out. SSE/SASE integration option for cloud-delivered security. IPS/AV signature update cadence. TLS inspection at line rate. Zero-trust segmentation between branch VLANs (e.g., ATM, staff, guest, IoT).
03	Observability & Application Visibility	Per-application performance dashboards. Path quality metrics (jitter, loss, latency) per transport. SaaS performance visibility (Microsoft 365, AWS, Azure, banking SaaS). Alerting integrated with the customer's NOC. Sample dashboards available pre-purchase.
04	Operations & Lifecycle	Zero-touch provisioning at the branch. Centralized policy push and audit trail. Template management at 100+ branch scale. Firmware lifecycle approach. Multi-tenant operator model for managed-service consumption.

TRANSPORT STRATEGY

How to Mix MPLS, Broadband, LTE, and 5G

Branch Tiering Drives the Transport Mix

A common procurement mistake is to choose a single transport pattern for the whole branch network. Branches have different criticality, different bandwidth needs, and different last-mile options. Tier the branches first, then assign transport per tier.

Branch Tier	Profile	Recommended Transport Mix	Bandwidth Sizing
Tier 1 – Flagship / Corporate	HQ, regional HQ, large urban branches; mission-critical; 100+ staff	Dedicated internet (primary) + MPLS or dedicated internet (secondary) + LTE/5G (tertiary)	200-1000 Mbps symmetric per circuit
Tier 2 – Urban Branch	City branches; 20-80 staff; full banking/retail services	Dedicated internet (primary) + broadband or MPLS (secondary) + LTE/5G (tertiary)	50-200 Mbps symmetric per circuit
Tier 3 – Sub-urban / Town	Smaller town branches; 5-20 staff; standard branch services	Broadband (primary) + LTE/5G (secondary)	20-80 Mbps; transport diversity essential
Tier 4 – Rural / Remote	Rural branches; 2-8 staff; limited last-mile choice	Best-available wireline (primary) + LTE/5G (secondary); StarLink for true remote	5-20 Mbps; design for graceful degradation

Buyer Insight

The bill at scale is dominated by Tier 2 and Tier 3 branches. A 1% per-month price difference per Tier-2 circuit across 250 branches is a six-figure annual swing. Do the per-tier math before signing a national contract.

SECURITY ARCHITECTURE

Where the Firewall Lives Now

The Branch Inspection Question

The single biggest architecture decision in SD-WAN is where security inspection happens. There are three viable patterns, each with different cost, latency, and operational properties. None is universally correct; the right choice depends on the buyer's regulatory posture and SaaS-adoption depth.

Pattern	Where Inspection Happens	Best For	Trade-offs
A. Backhaul All Internet	All branch internet traffic tunneled back to a central NGFW (Fortinet / Palo Alto) before going to the internet	Banks with strict regulator-driven inspection requirements; low-SaaS environments	Latency penalty on cloud apps; central firewall sizing is now N× branch bandwidth; bandwidth waste
B. Branch-Local Inspection (on-box NGFW)	Each branch SD-WAN device runs an NGFW for direct internet break-out; central NGFW for HQ-bound traffic only	Retail and mid-bank deployments; high-SaaS environments; cost-sensitive WAN budgets	Branch device complexity; per-branch licensing; signature update governance across the fleet
C. Cloud-Delivered (SASE/SSE)	SD-WAN tunnels each branch into a cloud security stack (FWaaS, SWG, ZTNA); inspection in the security cloud	Cloud-first organizations; geographically distributed users; modern security posture	Cloud-stack dependency; data residency questions; vendor maturity in Pakistan must be verified per provider

OPERATIONS

NOC Model, SLAs, and Day-2 Reality

The Day-2 Operating Model Decides Whether the Investment Pays Off

SD-WAN deployments succeed or fail on day-2, not on day-1. The vendor-led 'turn-up' phase always looks good; the real question is how the network behaves at month nine when a Tier-3 branch's primary broadband degrades from 50 ms latency to 250 ms and the application path-selection logic has to make calls automatically.

SLA Dimension	What to Demand	Red Flags in Provider Response
Branch availability	99.5–99.9% per branch with transport diversity; defined per tier	'Best effort' or no per-branch metric
Application performance	Per-app loss/latency/jitter thresholds with measurement; not just bandwidth	Bandwidth-only SLA; no application-aware measurement
Mean time to detect (MTTD)	<5 min for branch outage; auto-ticketing	Manual detection or customer-raised tickets only
Mean time to repair (MTTR)	Per-tier MTTR with carrier escalation matrix; spare-device logistics included	Hardware swap-out 'when available'; no carrier accountability
Change management	Per-policy push audit trail; staged rollout; rollback within minutes	Direct CLI changes by vendor with no audit; bulk pushes without staging
Reporting cadence	Weekly operational + monthly management review with named owner	Reports 'on request'; no proactive cadence

COST & COMMERCIAL

What You Actually Save

The Honest TCO Model

The 30–50% Opex reduction headline that drives many SD-WAN business cases is real – but it assumes a particular transport substitution, not a wholesale MPLS replacement. The honest TCO model below comes from actual Pakistan banking and retail deployments at 150–300 branch scale.

Cost Line	Legacy MPLS WAN	Mixed SD-WAN (Tiered)	Net Change
Transport (per-branch monthly)	PKR 60,000–80,000 (Tier-2)	PKR 20,000–35,000 (dedicated internet primary + LTE secondary)	–50% to –65%
Central NGFW capacity	Sized for full branch internet backhaul	Sized for HQ and Tier-1 only (if branch-local NGFW used)	–30% to –50%
Branch SD-WAN devices	Routers only (low cost)	SD-WAN appliances with NGFW licensing per branch	+50% to +100% on branch hardware
Operations (managed)	Carrier helpdesk only; thin SLA	Managed SD-WAN + Managed NOC; proactive ops; defined SLAs	+20% to +30%
Net WAN Opex (200–300 branches)	Baseline	Re-architected	Typical net reduction: –25% to –40%

Buyer Insight

The savings are real but not as large as vendor-led business cases suggest. Build the TCO model with operations cost included – not just transport. A poorly-operated SD-WAN that saves 50% on circuits but loses two hours of branch downtime per month is not a saving.

THE 16-QUESTION

SD-WAN Vendor Scorecard

Use these questions in RFP responses, vendor presentations, and reference checks. Score each 0/1/2. A provider scoring below 24/32 should not advance to commercial evaluation.

#	Category	Question	Score /2
Q1	Architecture	Draw your recommended branch architecture for our Tier-2 profile with primary, secondary, and tertiary transports.	__ /2
Q2	Architecture	Where will security inspection happen – branch, central, or cloud? Justify per tier.	__ /2
Q3	Transport	Which Pakistani last-mile carriers can you procure on our behalf? Show your sourcing matrix.	__ /2
Q4	Transport	What is your failover time when the primary path is hard-down? What about soft-fail (latency spike)?	__ /2
Q5	Security	Show your branch NGFW signature update model. Cadence? Bandwidth impact? Bypass options?	__ /2
Q6	Security	Describe your zero-trust segmentation between branch VLANs (ATM, staff, guest, IoT, biometric).	__ /2
Q7	Visibility	Provide a sample application-performance dashboard for a comparable customer (redacted).	__ /2
Q8	Visibility	Demonstrate SaaS-path visibility (Microsoft 365, core-banking SaaS) for a comparable client.	__ /2
Q9	Operations	Show your zero-touch provisioning flow end-to-end. What is the per-branch turn-up time?	__ /2
Q10	Operations	What is your NOC model for managed SD-WAN? PK-based? Shift coverage? Carrier escalation authority?	__ /2
Q11	Operations	Describe your firmware lifecycle approach for 200+ branches. Rollback model?	__ /2
Q12	SLAs	Provide per-tier MTTD and MTTR commitments with measurement methodology and consequence model.	__ /2
Q13	Commercial	Provide a 5-year TCO model for a 250-branch deployment using our tier mix. Include operations cost.	__ /2
Q14	Commercial	Are licenses portable across hardware refreshes? What is the exit cost if we terminate the engagement at year three?	__ /2
Q15	References	Two Pakistan multi-branch references at 100+ branch scale, deployed within the last 24 months.	__ /2

#	Category	Question	Score /2
Q16	Compliance	Show ISO 27001 certification with scope statement covering managed SD-WAN operations.	__ /2

Scoring Guide: Below 20/32: Do not advance / 20-26/32: Conditional / 27-32/32: Qualified for commercial evaluation.

Considering an SD-WAN transformation across 50+ branches?

Inara's 2-week SD-WAN Readiness Assessment delivers a branch-tiering analysis, transport-mix recommendation, and a 5-year TCO model specific to your branch profile and Pakistani last-mile options – before you go to RFP.

inara.pk | sdwan-readiness