

FREE SD-WAN MIGRATION CHECKLIST

& Cutover Planner

A practical field guide for moving from an MPLS-centric WAN to a hybrid SD-WAN architecture - from discovery and baseline through pilot, cutover, validation and MPLS retirement.

ASSESS	BASELINE	DESIGN	PREPARE
PILOT	MIGRATE	VALIDATE	OPTIMIZE

Use this checklist to: inventory your existing WAN, map critical applications, define the target hybrid WAN, validate security readiness, run a representative pilot, plan migration waves, execute cutover safely, prepare rollback, validate the new service and decide where MPLS can be retained or retired.

Important: Adapt the thresholds, controls, approvals and test cases to your own enterprise architecture, security policies, carrier contracts and change-management process.

0. How to Use This Checklist

Use the sections in sequence for a greenfield program, or as a control framework for an existing migration plan.

- | | |
|---|--|
| ☐ Complete the current WAN inventory before finalizing the target design. | ☐ Capture application dependencies and current performance baselines. |
| ☐ Design the target hybrid WAN by site profile - not one universal design. | ☐ Plan security before changing internet breakout or backhaul patterns. |
| ☐ Run a representative pilot with explicit exit criteria. | ☐ Group sites into migration waves by risk and complexity. |
| ☐ Never begin cutover without a tested rollback path. | ☐ Complete post-cutover validation before considering MPLS retirement. |

Final decision rule: A production migration wave should be GO only when critical prerequisites are complete, no unresolved blocker remains, and the migration team has an executable rollback path.

1. Current WAN Inventory

Build a factual current-state view of sites, circuits, providers and contract constraints.

- ☐ List every branch, campus, data center, cloud edge and special site.
- ☐ Record primary and backup transports for each site.
- ☐ Capture provider, circuit ID, bandwidth, SLA and support details.
- ☐ Record contract expiry dates and termination constraints.
- ☐ Document WAN edge models, software versions and ownership.
- ☐ Identify local firewall, NAT, DNS and DHCP dependencies.
- ☐ Record existing monitoring and telemetry coverage.
- ☐ Flag sites with unusual routing, provider or access constraints.

Key output: one authoritative inventory that engineering, operations, procurement and project teams can use.

2. Application Dependency Matrix

Map the traffic that determines whether the migration succeeds or fails.

- ☐ Identify business-critical applications and their owners.
- ☐ Map user/site groups to application destinations.
- ☐ Document private data center, SaaS and public-cloud dependencies.
- ☐ Capture latency, jitter, loss and availability requirements where relevant.
- ☐ Identify applications requiring QoS or deterministic path behavior.
- ☐ Document segmentation and security requirements.
- ☐ Define preferred and backup path intent for critical applications.
- ☐ Create an application test script for migration windows.

Tip: Think in terms of Application -> Users/Sites -> Destination -> Performance Need -> Security Need -> Test Owner.

3. Performance Baseline

Measure the current network before migration so post-cutover issues can be compared objectively.

- ☐ Capture latency for representative critical flows.
- ☐ Capture jitter for real-time voice and video.
- ☐ Capture packet loss and retransmission indicators.
- ☐ Capture bandwidth utilization by site and circuit.
- ☐ Review recent incidents and recurring WAN failure patterns.
- ☐ Document current failover behavior and convergence time.
- ☐ Capture application or synthetic experience metrics where available.
- ☐ Agree acceptance thresholds before the pilot.

4. Target Hybrid WAN Design

Define the target architecture by site profile and business requirement.

- ☐ Define primary and backup underlays for each site profile.
- ☐ Decide where MPLS remains, where it becomes backup and where it can eventually be removed.
- ☐ Define the SD-WAN overlay, controller and management architecture.
- ☐ Define routing exchange with legacy networks, clouds and data centers.
- ☐ Define segmentation / VRF / policy boundaries.
- ☐ Define application steering and SLA-based path policy.
- ☐ Define local internet breakout policy by site / application.
- ☐ Define resilience for critical hubs, data centers and cloud connectivity.

Do not force every site into the same connectivity pattern. Site criticality, carrier availability, application needs and economics should drive the underlay design.

5. Security Readiness

Validate security architecture before changing traffic paths or enabling new internet breakout.

- ☐ Define internet egress locations and security enforcement points.
- ☐ Confirm firewall / NGFW policy changes are approved.
- ☐ Confirm DNS, web security and malware controls.
- ☐ Validate segmentation and access-policy preservation.
- ☐ Review identity-aware / Zero Trust requirements.
- ☐ Clarify whether SASE is in scope now, later, or not required.
- ☐ Confirm logging, SIEM and security telemetry coverage.
- ☐ Update incident-response and escalation procedures.

6. SD-WAN Pilot Checklist

Treat the pilot as a rehearsal for production migration, not just a proof that the edge can connect.

- | | |
|---|--|
| ☐ Select representative pilot sites - not only the easiest branch. | ☐ Validate every required underlay before overlay activation. |
| ☐ Validate SD-WAN control connections and overlay establishment. | ☐ Validate routing, redistribution and legacy interworking. |
| ☐ Validate segmentation and security policy. | ☐ Validate application-aware routing and path selection. |
| ☐ Validate QoS for real-time and critical traffic. | ☐ Validate SaaS / cloud paths and internet breakout. |
| ☐ Test transport failover and recovery behavior. | ☐ Confirm logs, alarms and monitoring are operational. |
| ☐ Confirm operations can troubleshoot and support the pilot. | ☐ Close or formally accept all critical pilot defects. |
| ☐ Update the migration runbook with pilot lessons learned. | |

Pilot exit criteria: Architecture validated, failover proven, critical applications accepted, security validated, monitoring active and operations ready.

7. Migration Wave Planner

Scale only after the pilot, and sequence sites based on risk and complexity.

Wave	Typical Scope	Purpose
Wave 0	Pilot sites	Validate architecture and process
Wave 1	Low-risk standard sites	Build operational rhythm
Wave 2	Standard production sites	Scale repeatable delivery
Wave 3	Complex sites / hubs	Handle advanced dependencies
Wave 4	Critical / exceptional sites	Migrate highest-risk environments last

- ☐ Track carrier delivery and hardware dependencies before assigning a migration date.
- ☐ Confirm change windows, site access and business blackout periods.
- ☐ Avoid using site count alone as the measure of delivery complexity.
- ☐ Define success and rollback criteria consistently across waves.

8. Pre-Cutover Checklist

Do not enter the change window until critical prerequisites are ready.

- ☐ Change / CAB approval confirmed.
- ☐ Site and business contacts confirmed.
- ☐ All required underlays active and tested.
- ☐ WAN edge installed, reachable and licensed.
- ☐ Configuration and routing changes peer-reviewed.
- ☐ Security policies approved and ready.
- ☐ Monitoring and telemetry prepared.
- ☐ Performance baseline captured.
- ☐ Critical application test script available.
- ☐ Service-provider escalation contacts available.
- ☐ Go / No-Go authority identified.
- ☐ Rollback steps reviewed and executable.

9. Cutover Checklist

Execute the production migration in a controlled, observable sequence.

- ☐ Confirm final GO decision.
- ☐ Record the pre-change state: routes, interfaces, alarms and key metrics.
- ☐ Activate or connect the SD-WAN edge.
- ☐ Verify each underlay is reachable.
- ☐ Verify overlay control connections and tunnels.
- ☐ Confirm expected routes and path preference.
- ☐ Apply traffic steering, QoS and segmentation policies.
- ☐ Apply required security and internet-breakout policy.
- ☐ Validate critical applications and traffic paths.
- ☐ Monitor alarms, logs and service quality continuously.
- ☐ Test failover if included in the approved change plan.
- ☐ Obtain business / site acceptance before closing the change.

10. Rollback Plan

Rollback is a pre-planned safety mechanism, not an emergency idea.

Trigger	Question to answer before cutover
Critical app failure	What exact condition requires rollback?
Routing instability	How long will the team troubleshoot before backing out?
Security failure	Which missing control makes the change unacceptable?
Performance degradation	What threshold is considered severe?
Monitoring loss	Can the site remain in production without required visibility?
Time threshold	What is the latest safe rollback decision time?
Authorization	Who can order rollback?
Recovery procedure	How will legacy routing/configuration be restored?

A good rollback plan names the trigger, decision authority, exact recovery steps and validation method for restored service.

11. Post-Cutover Validation

Immediate connectivity is not enough. Validate the service, resilience, security and operations.

- ☐ LAN and WAN reachability verified.
- ☐ DNS resolution verified.
- ☐ Critical private applications validated.
- ☐ SaaS and public-cloud applications validated.
- ☐ Voice / video quality accepted.
- ☐ Internet breakout behavior confirmed.
- ☐ Routing and path preference validated.
- ☐ QoS and application steering validated.
- ☐ Failover / recovery validated where approved.
- ☐ Security policy and segmentation validated.
- ☐ Logging and monitoring validated.
- ☐ Operations accepts steady-state ownership.

12. MPLS Retirement Decision

Do not disconnect MPLS simply because the first SD-WAN cutover was successful.

- ☐ Agreed stabilization period completed.
- ☐ Critical application performance accepted over time.
- ☐ Alternative-path failover proven.
- ☐ Operations comfortable supporting the new service.
- ☐ Security architecture stable with no critical gaps.
- ☐ Alternative underlays provide sufficient diversity.
- ☐ Carrier termination dates and penalties understood.
- ☐ Business owner approves retirement or reduction.
- ☐ A fallback strategy exists for any retained critical dependency.

Decision: RETIRE / RETAIN / REVIEW. The right answer can differ by site. The objective is not to eliminate MPLS everywhere - it is to justify every remaining transport.

13. Final Readiness Gate

Score eight dimensions before authorizing a production migration wave.

Area	Assessment	Owner	Evidence / Notes
Architecture	☐ Ready ☐ Partial ☐ Not Ready		
Connectivity	☐ Ready ☐ Partial ☐ Not Ready		
Applications	☐ Ready ☐ Partial ☐ Not Ready		
Routing	☐ Ready ☐ Partial ☐ Not Ready		
Security	☐ Ready ☐ Partial ☐ Not Ready		
Pilot	☐ Ready ☐ Partial ☐ Not Ready		
Rollback	☐ Ready ☐ Partial ☐ Not Ready		
Operations	☐ Ready ☐ Partial ☐ Not Ready		

GO

All critical prerequisites complete; residual risks accepted.

CONDITIONAL GO

Minor gaps remain with explicit owner, mitigation and acceptance.

NO-GO

Critical dependency, security, rollback or service prerequisite unresolved.

Final note: This checklist is designed as a planning aid. It does not replace your organization's architecture standards, security requirements, carrier procedures, change-management controls or vendor-specific implementation guidance.