

Post-Quantum Login and Authentication Problems in SD-WAN

Afshan Mulla · Technical Leader, Cisco CX, Professional Services · aafshan.mulla@gmail.com

Jaypal Baviskar · Technical Leader, Cisco CX, Service Provider Technology Group · jay.22kar@gmail.com

Position paper- IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication (pqws), Prague, 11–12 October 2026

Position. We argue that SD-WAN is one of the hardest places in the enterprise to deploy post-quantum authentication, and one where the consequences of getting it wrong are most concentrated. Three things combine.

First, in Cisco Catalyst SD-WAN, our documented example, every router proves who it is, by default, over DTLS 1.2 on UDP [3][6], where one lost datagram forces the whole handshake flight to be sent again, and post-quantum certificates turn an 8-datagram handshake into a 40-datagram one.

Second, SD-WAN runs on whatever links are available: broadband, LTE and satellite, exactly where loss and delay are highest.

Third, Catalyst SD-WAN does not use IKE. Data-plane keys are generated by each router and distributed by the controller over that same control connection [3], so the security of every tunnel in the fabric rests on control-plane authentication.

With ML-DSA-87, the parameter set CNSA 2.0 requires for national security systems [11], our model shows that fewer than one in three control-connection attempts on a 3%-loss circuit would complete without retransmission, against about four in five today. Because ML-DSA in TLS is specified only for TLS 1.3 [18], and no specification defines it for TLS 1.2, a standards-based control plane has to move to DTLS 1.3 anyway, and DTLS 1.3 acknowledgements can remove most of the penalty. We argue for migrating the transport first, and propose four fixes that need no new cryptography.

1. How SD-WAN login actually works, and why it is different

A WAN Edge router joins the fabric by building mutually authenticated control connections to the orchestrator, the controllers and the manager. Cisco Catalyst SD-WAN documents the design: control connections run over DTLS 1.2 (RFC 6347) on UDP by default, TLS 1.2 on TCP is an option, and each device authenticates with a certificate [3]. Controllers additionally check each router's serial and chassis number against an authorized-device list that the manager distributes to all control components [3][19]. Hardware routers hold a factory SUDI certificate in a tamper-resistant Trust Anchor module (TAM) [3][19]. Certificates today use 2048-bit RSA keys [3].

A single router does not build one control connection. It builds one persistent connection to the manager (over one transport), one to each controller over every transport, and transient connections to the orchestrator over every transport during bring-up [4][25]. With two transports and two controllers that is five persistent connections and seven handshakes at cold start, per router, per reload, and again after transport flaps.

The last difference is the one that matters most. Catalyst SD-WAN dispenses with IKE altogether [3]. Each router generates an AES key per TLOC and sends it to the controller in OMP route updates, and the controller distributes it to the other routers [3]; in pairwise-key mode the controller relays ECDH P-384 public values instead [16]. That removes much pairwise key-exchange work, which is why the design is good. It also means the confidentiality of every tunnel depends on the control connection. An attacker who can impersonate a controller, which requires recovering a classical CA or controller private key, for example with a cryptographically relevant quantum computer (CRQC), is not attacking one tunnel; they are positioned to receive the fabric's keys. The coupling also means that recorded control traffic whose key exchange is classical exposes data-plane keys to later decryption, so authentication and key establishment on this channel must move together. Some SD-WAN products use IKEv2 control channels instead [13]; IKEv2 fragmentation also resends every fragment of a message on loss [21].

2. What a post-quantum control connection costs

How this was worked out. Key and signature sizes are from FIPS 204 [1] and FIPS 205 [2]. Each certificate carries an assumed 500 bytes of X.509 structure beyond the key and signature; measured minimal ML-DSA certificates carry about 255 bytes (3,987 / 5,516 / 7,474 B for ML-DSA-44 / 65 / 87 [12]) and enterprise templates carry more. Each side sends a leaf, one intermediate and a handshake signature; both sides authenticate; the controller flight also carries a single key-exchange allowance (1,184 B for ML-KEM-768; 1,568 B for ML-KEM-1024 with ML-DSA-87); a full hybrid exchange adds about 1.1–1.6 kB, one or two datagrams. Records are assumed to fit 1,200 bytes, conservative once NAT and tunnel overhead are counted. Datagrams count all six flights of a DTLS 1.2 handshake [6]. “Clean” is the chance that a handshake completes with no retransmission, $(1 - \text{loss})^6$ datagrams, with loss independent per datagram. DTLS 1.2 retransmits an entire flight, not the lost datagram [6, §4.2.4], so a single loss re-sends about 20 kB, with a timer that starts at 1 s and doubles. Timing figures come from a Monte Carlo model (150,000 trials per point, 40 ms RTT, one datagram per small flight, independent loss); the script is available from the authors.

Signature algorithm	Controller sends	Edge sends	Total bytes	Datagrams	Clean @1% loss	Clean @3% loss
RSA-2048 (today)	2,388	2,356	4,744	8	92%	78%
ML-DSA-44	12,068	10,884	22,952	25	78%	47%
ML-DSA-65	16,015	14,831	30,846	31	73%	39%
ML-DSA-87 (CNSA 2.0)	21,633	20,065	41,698	40	67%	30%
SLH-DSA-128s	25,816	24,632	50,448	47	62%	24%

Table 1. One mutual control-connection handshake, in bytes and UDP datagrams (all six DTLS 1.2 flights),

and the chance it completes without a retransmission. ML-DSA in TLS is specified only for TLS 1.3 [18]; the rows show what today's transport would face.

- Loss stops being a nuisance and becomes the binding constraint.** A broadband or LTE TLOC at 3% loss today completes 78% of handshakes cleanly. At ML-DSA-87 that falls to 30%. Modelling the DTLS 1.2 timers (40 ms RTT), the 95th-percentile establishment time rises from about 1 s to about 15 s, and roughly one attempt in six takes longer than 5 s.
- A fabric-wide reconnection becomes a storm.** Take an illustrative 5,000-site fleet with five persistent control connections each. A fabric-wide re-establishment, for example after a root-CA rollover or a regional outage, means 25,000 handshakes: about 119 MB and 200,000 datagrams today, against roughly 1.04 GB and 1,000,000 datagrams at ML-DSA-87, with about 70% of handshakes at 3% loss resending at least one ~20 kB flight (22% today). Signature verification is not the problem (well under a millisecond for ML-DSA); the wire and the loss are.
- Satellite and high-latency TLOCs suffer first.** DTLS retransmission is timer-based with exponential backoff. On a 600 ms GEO path, one lost datagram in a 40-datagram handshake adds at least a second before anything is resent, and a second loss adds two more. A connection that comes up in about a second today can take tens of seconds, which sits badly with the timers driving fabric convergence.
- The transport has to move anyway, and that is the fix.** ML-DSA and hybrid ML-KEM key exchange are specified for TLS 1.3 [18][22], and no specification defines either for TLS 1.2, so a standards-based post-quantum control plane needs DTLS 1.3, which reuses the TLS 1.3 handshake [5], or TLS 1.3 over TCP. DTLS 1.3 acknowledges handshake records, and a sender SHOULD then retransmit only the unacknowledged portion [5, §5.8.1]. In the same model, ML-DSA-87 over DTLS 1.3 at 3% loss has a p95 of about 2 s, with about 0.2% of attempts over 5 s. Open-source DTLS 1.3 exists in wolfSSL [29] and is in beta for OpenSSL 4.1, planned for October 2026 [23].

3. Where the limits sit in an SD-WAN fabric

Where	What it is	Can it be changed?	What it means
DTLS 1.2 over UDP (default control transport)	One lost datagram retransmits the whole flight; no reliable stream underneath [3][6]	Config: TLS/TCP; DTLS 1.3 needs vendor support	Handshake stalls, control connection flaps

Where	What it is	Can it be changed?	What it means
Control connections per router	One to the manager, one to each controller per transport, plus transient orchestrator connections on every transport [4]	Architectural	Handshake cost multiplies five- to sevenfold per device
Transport quality	Broadband, LTE/5G and satellite TLOCs; we assume 1–5% loss and up to 600 ms RTT	No, that is the point of SD-WAN	Loss and delay multiply the flight count
Controller certificate keys	RSA-2048 today [3]	Yes, once platform crypto modules support ML-DSA	NIST IR 8547 draft proposes deprecating RSA-2048 after 2030; CNSA 2.0: PQ-only network gear in national security systems by 2030 [11][24]
SUDI in the Trust Anchor module	Certificate pre-programmed at manufacture [14][19]	Never	Classical for the device's 7–10 year life; a PQ operational identity is typically bootstrapped from it [14][20]
Data-plane keys	AES keys generated per router per TLOC and distributed in OMP routes over the control connection; IKE is not used [3]	Architectural	The whole fabric's tunnel keys rest on one control-plane identity
Authorized-device list and trust material	Manager distributes the device list to all controllers [19]; every router already holds the fabric root-CA trust chain and receives configuration over its control connection [3]	Yes, the opening	The fabric already ships trust material outside the handshake

Table 2. SD-WAN-specific pressure points. The last row is not a problem; it is the mechanism the proposals below build on.

4. What we propose

(1) Move the transport before the credential. A standards-based post-quantum control plane cannot stay on DTLS 1.2 [18][22], so the move to DTLS 1.3 is a precondition of the migration, not an extra cost, and in our model its acknowledgements are worth more than any certificate optimisation (ML-DSA-87 at 3% loss: p95 about 15 s on DTLS 1.2, about 2 s on DTLS 1.3). The same lesson applies to IKEv2 control channels, where an individual draft proposes fragment acknowledgement for exactly this reason [21]. Vendors should ship DTLS 1.3 control planes before, not after, post-quantum certificates.

(2) Keep the chain off the wire, where there is a chain. The manager already sends configuration to every router, and the authorized-device list to every controller, over authenticated control connections [3][19]. The same channel can pre-provision intermediates, so every handshake after the first sends a shorter path. Trust-anchor identifiers describe exactly this: relying parties predistribute intermediates as trust anchors and servers send shorter paths [9, §9.5]. Raw public keys [8] work in TLS 1.3; cached information [7] predates TLS 1.3 and would need a 1.3 profile. A fabric in which both ends and the CA belong to one organisation is the easy case for all three. Removing the intermediate from both directions saves 15.4 kB of 41.7 kB (37%) and takes the handshake from 40 datagrams to 27; raw public keys would save a further ~10 kB (to ~16 kB, 19 datagrams), since the handshake signature remains. Where the PKI is flat, this proposal gives little.

(3) Make the handshake survive a flap. LTE and broadband TLOCs flap routinely. Where a flap or reload triggers a full mutual handshake, post-quantum makes it almost nine times more expensive in bytes at the moment the link is at its worst. The protocol pieces exist: DTLS Connection IDs keep a session across address changes [5][26], and PSK resumption is not bound to a network path [5]. The gap is SD-WAN use of them, with policy for when resumption may replace re-authentication, so the full certificate exchange happens once per device per epoch rather than once per flap.

(4) Make the failure attributable, and account for it per TLOC. Today a handshake too large for a lossy circuit surfaces as a DTLS connection failure (DCONFALL) or a per-peer timeout, the same codes as a broken circuit [25], and an operator will reasonably blame the circuit. Add an explicit state for a handshake abandoned after repeated flight retransmission, and report handshake bytes, datagram count, retransmissions and establishment time per TLOC. It is small, and it lets an operator tell an oversized handshake from a failing circuit.

5. Questions for the workshop, and where the work belongs

- What is the real datagram-loss and RTT distribution, including burstiness, on production SD-WAN broadband, LTE and satellite TLOCs, and what handshake size does it support? Vendors and managed service providers hold this telemetry; we have not found it published.
- Is DTLS 1.3 adoption, rather than certificate size, the real gate on post-quantum SD-WAN? Should control planes move to DTLS 1.3, or to TLS 1.3 over TCP, accepting head-of-line blocking in exchange for reliable delivery of large flights?
- Because data-plane keys ride the control connection, control-plane security protects far more than itself. Does that argue for a stronger parameter set on the control plane, or for reducing the coupling?
- Factory SUDI certificates cannot be replaced and the routers holding them will be in service for 7–10 years. IEEE 802.1AR LDevIDs enrolled with BRSKI [14][20] can carry a post-quantum operational identity, but enrolment rests on the classical factory identity. By when must it happen, how is it repeated after RMA or factory reset, and who signs it?
- In multi-tenant managed SD-WAN, tenants will migrate at different rates. Must a fabric support mixed classical and post-quantum control connections indefinitely, and what does that do to the authorized-device model and to composite certificate sizes [15]?

Where the follow-up belongs. The reusable pieces have homes in the IETF: DTLS 1.3 guidance, resumption and trust-anchor negotiation in TLS; certificate size in LAMPS and PLANTS [10]; IKEv2 fragment acknowledgement (an individual draft) in IPSECME [21]; a per-TLOC handshake telemetry model in OPSAWG. IETF SD-WAN work exists in BESS and IDR [27][28], but none of it addresses post-quantum authentication of SD-WAN control connections. SD-WAN service definitions sit with MEF, and factory identity needs liaison with IEEE 802.1 and TCG. The EAP community documented the same class of large-certificate problem in 2022 [17]; SD-WAN has less margin, because DTLS 1.2 has no per-fragment acknowledgement, and a near policy deadline [11], so it should not wait its turn.

References

- [1] FIPS 204, Module-Lattice-Based Digital Signature Standard, NIST 2024.
- [2] FIPS 205, Stateless Hash-Based Digital Signature Standard, NIST 2024.
- [3] Cisco, Catalyst SD-WAN Security Configuration Guide, IOS XE 17.x, Security Overview, Jan 2026.
- [4] Cisco, Catalyst SD-WAN Getting Started Guide, Overlay Network Bring-Up Process.
- [5] RFC 9147, DTLS 1.3, 2022.
- [6] RFC 6347, DTLS 1.2, 2012.
- [7] RFC 7924, TLS Cached Information Extension, 2016.
- [8] RFC 7250, Using Raw Public Keys in TLS and DTLS, 2014.
- [9] draft-ietf-tls-trust-anchor-ids-06, TLS Trust Anchor Identifiers, Sep 2026.
- [10] draft-ietf-plants-merkle-tree-certs-07, Merkle Tree Certificates, Oct 2026.
- [11] NSA, Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), 2022, with later updates.
- [12] J. Gomez, The Great Certificate Size Explosion, Cisco Blogs, Aug 2026.
- [13] Versa Networks, Operationalizing Post-Quantum Cryptography in SASE and SD-WAN, Jun 2026.
- [14] IEEE Std 802.1AR, Secure Device Identity, 2018.
- [15] draft-ietf-lamps-pq-composite-sigs-19, Composite ML-DSA, Apr 2026 (RFC Editor queue).
- [16] Cisco, Catalyst SD-WAN Hardening Guide (pairwise keys, ECDH P-384).
- [17] RFC 9191, Handling Large Certificates and Long Certificate Chains in TLS-Based EAP Methods, 2022.
- [18] draft-ietf-tls-mldsa-05, Use of ML-DSA in TLS 1.3, Jul 2026.
- [19] Cisco, SD-WAN Control Components Certificates and Authorized Serial Number File (PDG).
- [20] RFC 8995, Bootstrapping Remote Secure Key Infrastructure, 2021.
- [21] draft-antony-ipsecme-ikev2-fragment-acknowledgment-03, Jan 2026.
- [22] draft-ietf-tls-ecdhe-mlkem-05, Hybrid ECDHE-MLKEM Key Agreement for TLS 1.3, May 2026.
- [23] OpenSSL Library, “The OpenSSL Library supports DTLS 1.3”, 9 Sep 2026; 4.1 Beta, 23 Sep 2026.
- [24] NIST IR 8547 (Initial Public Draft), Transition to Post-Quantum Cryptography Standards, Nov 2024.
- [25] Cisco, Troubleshoot Common SD-WAN Control and Data Plane Issues, Doc ID 222302.
- [26] RFC 9146, Connection Identifier for DTLS 1.2, 2022.
- [27] draft-ietf-bess-bgp-sdwan-usage-37, BGP Usage for SD-WAN Overlay Networks, Jun 2026.
- [28] draft-ietf-idr-sdwan-edge-discovery-30, SD-WAN Edge and Underlay Tunnel Discovery Using BGP, Sep 2026.
- [29] wolfSSL, “wolfSSL now supports DTLSv1.3”, Jun 2022.