IKEv2 Group-Assisted Key Establishment

IPsec Workshop 2026

Steffen Klassert

Why a new key exchange?

The Problem: Full-Mesh IKE Does Not Scale

- $O(N^2)$ pairwise SAs required for N nodes
- Each SA needs: IKE state, certificates, nonces, traffic selectors
- Operational overhead grows quadratically with group size

AI/ML clusters, HPC, large enterprise networks are all affected

Shared Group Keys: Convenient, but Risky

- Single key shared among all N nodes — used directly as ESP traffic key
- Compromise of any one node reveals the group key to the attacker
- No cryptographic separation between pairs

One compromised node – all traffic readable

Architecture

Logical Components

- **Group Key Management Server (GKMS)** — trusted authority
  - Authenticates nodes, distributes group policy
  - Issues the group keys
  - Relays DH messages between peers
  - Coordinates SA deletion and rekeying
- **Group members (nodes)**
  - Authenticate to GKMS, receive credentials and group key
  - Perform DH exchange relayed by GKMS to derive pairwise ESP keys

System Architecture

- GKMS acts as a trusted relay between two nodes A and B:
- A and B enroll with GKMS
  - Each receives group credentials and key
- A requests a pairwise SA with B via GKMS
- A and B derive the same ESP traffic key independently
  - HKDF(DH_secret, group_key, IDs, SPIs, nonces)
- GKMS coordinates deletion and rekeying on behalf of nodes

Peer Keys can be long living – Rekeying done via Group Key

Protocol Overview

Node Enrollment (G-IKEv2 GSA_AUTH)

- Each node performs an initial G-IKEv2 GSA_AUTH exchange with GKMS
- GKMS authenticates the node
- GKMS distributes:
  - A group identifier
  - A current group key
  - Policy for peer communication
- Group key is refreshed on group membership changes

GKMS_CREATE_CHILD_SA

- IKEv2-style exchange, relayed by GKMS
- Two new IKEv2 payloads:
  - GMS (GKMS-to-Node Coordination): carries DH values, nonce, SPI
  - GMV (GKMS-to-Node Verification Token): HMAC for tamper-evidence
- Message flow:
  - Initiator A sends GMS proposal to GKMS
  - GKMS forwards GMS to responder B
  - B responds with its DH value (relayed by GKMS to A)
  - GKMS forwards verification token (GMV) to both parties
- Both nodes compute DH shared secret — GKMS never sees it

Key Derivation: HKDF with Group Key as Salt

- Each pair gets a unique ESP key — no shared group key across pairs
- GKMS knows neither the DH secret nor the ESP key
- Fresh DH for each SA — PFS

Tamper Evidence

- GKMS relays DH public values between A and B
- A compromised GKMS could substitute DH values to intercept traffic
- Solution: Verification Token (GMV payload)

A compromised GKMS cannot inject a false key

Three Operational Modes

- GKMS-Assisted (default) — full DH + group key
  - DH shared secret + group key = pairwise ESP key
  - Provides PFS
  - Compromise of one node does NOT reveal other pairs' keys
- Group-Key-Derived Pairwise Key Mode
  - Group key only, no DH — SA key is group key + SA context
  - Simpler, but compromise of any node reveals the group key
- Direct Group Key Mode
  - Group key used directly as ESP key for all SAs
  - Maximum simplicity, but…

Default: GKMS-Assisted — PFS

Rekeying the Group Key

- GKMS refreshes the group key (time-based or packet-based)
- Triggers re-establishment of all ESP SAs with new derived keys
- New key = HKDF(old_key, new_group_key, context)
- Former group key is discarded — previous ESP traffic unreadable

Rekeying: Membership Changes

- **Adding a member:**
  - GKMS issues new group key to existing members + new member
- **Removing a member:**
  - GKMS distributes new group key to remaining members
  - Former member cannot crypt future traffic

Per-Node State: O(1) vs O(N)

- Full-Mesh IKE: O(N) per-node state
  - Quadratic growth in control-plane overhead
  - All N nodes: N × O(N) = $O(N^2)$
- GKMS-Assisted: O(1) per-node state
  - One IKE SA to GKMS (shared across all peers)
  - Limited ESP SAs (no full mesh required)
- GKMS-Assisted: constant per-node state regardless of group size

GKMS-Assisted — Scales to large groups without quadratic blowup

Security Properties

- PFS: DH fresh for each SA
- GKMS does not learn DH shared secret — cannot derive ESP keys
- Tamper-evident: HMAC verification token prevents GKMS fraud
- Dynamic group membership: group key refreshed on join/leave
- Delegated operations: GKMS coordinates SA management without revealing keys

Summary

- GKMS acts as trusted coordinator
- Nodes perform a DH exchange relayed by GKMS
- GKMS never learns shared secret
- HKDF derives unique ESP keys
- PFS without $O(N^2)$ IKE state
- Extends IKEv2 with two new payloads: GMS and GMV

draft-antony-ipsecme-ikev2-group-key-distribution-01