LCOS 11.00

Addendum

11/2026

ROHDE&SCHWARZ
Make ideas real

Inhalt

1 Addendum zur LCOS-Version 11.00....4
2 Konfiguration....5
2.1 **IPv6-Unterstützung für TCP- / HTTP-Tunnel**....5
2.2 Datei-Download von einem USB-Stick....5
3 Virtual Private Networks – VPN....6
3.1 Post-Quantum-Verfahren im IKEv2-Schlüsseltausch....6
3.1.1 Unterstützung von ML-KEM im IKEv2....6
3.1.2 Warum mehrere Schlüsselaustauschverfahren?....7
3.1.3 Auswirkungen auf die Performance....7
3.1.4 Einsatzempfehlungen....8
3.1.5 Konfiguration mit LANconfig....8
3.1.6 Ergänzungen im Setup-Menü....11
3.2 IKEv2: Unterstützung für RADIUS-Accounting-On....20
4 Voice over IP – VoIP....21
4.1 Voice Backup mittels VRRP....21
4.2 Ergänzungen im Setup-Menü....22
4.2.1 Vrrp-Interface....22
4.2.2 Vrrp-Interface....22
5 RADIUS....24
5.1 DHCPv6-Optionen im RADIUS-Auth-VSA übertragen....24
6 Ergänzungen im Menüsystem....26
6.1 Ergänzungen im Setup-Menü....26
6.1.1 CHAP-Reauth-Minuten....26
6.1.2 Schluesselaustausch-Algorithmen....26
6.1.3 Zugriffsart....27
6.1.4 Authentifizierungs-Typ....28

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Hinweis zur Unternehmensbezeichnung: LANCOM Systems heißt seit dem 01.07.2026 **Rohde & Schwarz Networks and Cybersecurity**. Produktinformationen und Kommunikationsmaterialien werden entsprechend unter der neuen Unternehmensbezeichnung geführt.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. Rohde & Schwarz Networks and Cybersecurity haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von Rohde & Schwarz Networks and Cybersecurity gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u. a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS) finden Sie auf der WEBconfig des Geräts unter dem Menüpunkt „Extras > Lizenzinformationen“. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage über einen Download-Server bereitgestellt.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*www.openssl.org*).

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.rohde-schwarz.com/networks-and-cybersecurity

1 Addendum zur LCOS-Version 11.00

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 11.00 gegenüber der vorherigen Version.

2 Konfiguration

2.1 IPv6-Unterstützung für TCP- / HTTP-Tunnel

Ab LCOS 11.00 können für TCP- / HTTP-Tunnel auch IPv6-Adressen angegeben bzw. verwendet werden.

2.2 Datei-Download von einem USB-Stick

Ab LCOS 11.00 kann eine Firmware-Datei oder ein Konfigurationsskript von einem angeschlossenem USB-Stick geladen werden. Beispiele:

1. Laden einer LCOS-Firmware vom USB-Stick aus dem Verzeichnis „Firmware“ auf dem USB-Stick:

```
loadfirmware file://usb/Firmware/LC-1800EF-4G-10.94.0327-RU4.upx
```

2. Laden einer WWAN-Firmware vom USB-Stick aus dem Verzeichnis „Firmware“ auf dem USB-Stick:

```
loadfirmware file://usb/Firmware/LC-1800EF-4G-EM060KEAAAR01A05M2G-A0.301.A0.301-RU2.upx
```

3. Laden einer Script-Konfiguration vom USB-Stick aus dem Verzeichnis „Config“ auf dem USB-Stick:

```
LoadScript file://usb/Config/Initital-Provisioning-V1.1.lcs
```

3 Virtual Private Networks – VPN

3.1 Post-Quantum-Verfahren im IKEv2-Schlüsseltausch

Ab LCOS 11.00 unterstützt LCOS im IKEv2 den Intermediate Exchange gemäß *RFC 9242* sowie Multiple Key Exchanges gemäß *RFC 9370*. Diese Verfahren dienen als Grundlage zum Einsatz von Post-Quantum-Verfahren im Schlüsseltausch.

Der Intermediate Exchange ermöglicht den Austausch zusätzlicher Schlüsselmaterialien auch bei großen Nachrichten, ohne diese vollständig in der ersten IKE_AUTH-Nachricht übertragen zu müssen. Mit Multiple Key Exchanges können mehrere, voneinander unabhängige Schlüsselaustauschverfahren kombiniert werden, beispielsweise ein klassisches Diffie-Hellman-Verfahren mit einem postquantenresistenten Verfahren wie ML-KEM. Dadurch entsteht ein hybrider Schlüsselaustausch, der sowohl die bewährte Sicherheit klassischer Verfahren als auch Schutz gegen zukünftige Angriffe durch leistungsfähige Quantencomputer bietet. Die zusätzliche Unterstützung von ML-KEM als neuer postquantenresistenter KEM-Gruppe ermöglicht es, IKEv2-Verbindungen bereits heute auf eine zukünftige Post-Quantum-Security-Strategie vorzubereiten.

Beide Verfahren sind im LCOS nicht explizit konfigurierbar, sondern werden automatisch verwendet, sofern dies erforderlich ist, z. B. bei Verwendung von zusätzlichen Runden im Schlüsseltausch sowie bei großen DH-Gruppen wie ML-KEM.

Im LCOS werden die ML-KEM-Gruppen DH37 (ml-kem-1024), DH36 (ml-kem-768) sowie DH35 (ml-kem-512) unterstützt. Diese Gruppen lassen sich nativ, sowie im hybriden Schlüsseltausch mit anderen zusätzlichen DH-Gruppen verwenden.

3.1.1 Unterstützung von ML-KEM im IKEv2

ML-KEM ist ein standardisiertes postquantenresistentes Key-Encapsulation-Mechanism-Verfahren und basiert auf gitterbasierten kryptografischen Problemen. Es wird häufig zur Absicherung gegen sogenannte „Store now, decrypt later“-Angriffe eingesetzt.

Bei einem solchen Angriff zeichnet ein Angreifer heute verschlüsselte Kommunikation auf, um sie später mit leistungsfähigen Quantencomputern zu entschlüsseln. Durch die Einbeziehung eines postquantenresistenten Verfahrens wie ML-KEM kann der IKEv2-Schlüsselaustausch bereits heute gegen dieses zukünftige Szenario abgesichert werden.

Wichtig ist grundsätzlich die Unterscheidung zwischen:

- **Schlüsselaustausch:** Erzeugung des gemeinsamen Geheimnisses, beispielsweise mit DH oder ML-KEM.
- **Authentisierung:** Nachweis der Identität der Kommunikationspartner, beispielsweise über Zertifikate oder digitale Signaturen.
- **Verschlüsselung:** Schutz der später übertragenen IPsec-Daten.

Die Verwendung von ML-KEM schützt primär den Schlüsselaustausch. Für eine vollständig postquantenresistente Gesamtlösung muss zusätzlich geprüft werden, ob auch die verwendeten Signatur- und Authentisierungsverfahren gegen Quantenangriffe geeignet sind.

3.1.2 Warum mehrere Schlüsselaustauschverfahren?

Ein hybrider Schlüsselaustausch soll die Sicherheit auch dann erhalten, wenn eines der verwendeten Verfahren später geschwächt oder gebrochen wird. Beispiel:

- Das klassische Diffie-Hellman-Verfahren ist heute gut etabliert.
- Ein zukünftiger Quantencomputer könnte bestimmte klassische Verfahren, insbesondere auf Basis des diskreten Logarithmus, mit Shor's Algorithmus gefährden.
- ML-KEM basiert auf einem anderen mathematischen Problem und ist für den Einsatz gegen Quantencomputer vorgesehen.
- Werden beide Verfahren kombiniert (hybrid), muss ein Angreifer grundsätzlich beide Geheimnisse überwinden, um das resultierende IKE-Schlüsselmaterial zu rekonstruieren.

Damit kann ein hybrider Austausch einen Übergangsschutz bieten: Die bestehende klassische Kryptografie bleibt nutzbar, während gleichzeitig ein postquantenresistenter Anteil ergänzt wird.

3.1.3 Auswirkungen auf die Performance

Der Einsatz von Post-Quantum-Verfahren im Schlüsseltausch hat Auswirkungen auf die Performance bzw. Geschwindigkeiten beim Aufbau von IKEv2-VPN-Tunnel. Der Datendurchsatz im IPSec wird dabei nicht beeinflusst.

Folgende Konsequenzen ergeben sich im praktischen Einsatz:

- **Zusätzliche Latenz**

  Mit RFC 9242 und RFC 9370 kann ein zusätzlicher Austausch hinzukommen. Dadurch entsteht mindestens ein zusätzlicher Request-/Response-Schritt. Die tatsächliche Verzögerung hängt deshalb stark von der Netzwerklaufzeit ab. Bei Verbindungen mit hoher Latenz – beispielsweise über Satelliten-, Mobilfunk- oder weit entfernte WAN-Strecken – kann dieser zusätzliche Round Trip deutlich messbar sein.

- **Zusätzlicher Rechenaufwand**

  Bei einem hybriden Schlüsselaustausch müssen mehrere kryptografische Verfahren ausgeführt werden. Neben dem klassischen Diffie-Hellman-Verfahren kommen bei ML-KEM insbesondere folgende Operationen hinzu:

  - Erzeugung beziehungsweise Verarbeitung des ML-KEM-Schlüsselmaterials,
  - Encapsulation auf der initiierenden Seite,
  - Decapsulation auf der antwortenden Seite,
  - zusätzliche Verarbeitung bei der Ableitung des gemeinsamen IKE-Schlüsselmaterials.

  Der Rechenaufwand ist typischerweise höher als bei einem alleinigen klassischen DH-Austausch. Besonders auf Geräten mit begrenzter CPU-Leistung kann sich das auf die Zeit zum Aufbau neuer VPN-Tunnel auswirken.

  Wichtig ist die Unterscheidung:

  - Der Aufbau neuer IKE-SAs kann länger dauern.
  - Die spätere Datenübertragung innerhalb einer bestehenden CHILD_SA wird durch den zusätzlichen Schlüsselaustausch in der Regel nicht wesentlich verlangsamt.
  - Bei häufigen Rekey-Vorgängen oder vielen gleichzeitig aufzubauenden Tunneln kann der zusätzliche Aufwand jedoch relevant werden.

- **Auswirkungen auf die Größe der IKEv2-Nachrichten**

  RFC 9242 reduziert nicht automatisch die insgesamt übertragene Datenmenge. Die Erweiterung verteilt zusätzliche Informationen lediglich auf mehrere IKE-Nachrichten.

Die Gesamtgröße aller Nachrichten kann durch zusätzliche Payloads sogar etwas steigen, da jede Nachricht eigene IKE-Header und Payload-Strukturen benötigt. Der Vorteil liegt hauptsächlich darin, dass einzelne Nachrichten kleiner und besser transportierbar werden.

Das kann Probleme mit folgenden Netzwerkeigenschaften reduzieren:

- begrenzter MTU,
- UDP-Fragmentierung,
- Firewalls und NAT-Geräte,
- VPN-Gateways mit Größenbeschränkungen,
- unzuverlässiger Übertragung großer UDP-Datagramme.

3.1.4 Einsatzempfehlungen

Grundsätzlich wird der Einsatz eines hybriden IKEv2-Schlüsselaustausch zum aktuellen Zeitpunkt empfohlen. Dazu wird ein klassisches Verfahren z. B. mit einem postquantenresistenten ML-KEM-Verfahren kombiniert. Für ein Sicherheitsniveau von etwa 128 Bit bietet sich die Kombination aus ECP256 (DH-Gruppe 19) oder X25519 (DH-Gruppe 31) und ML-KEM-768 an. Für höhere Sicherheitsanforderungen kann ECP384 (Gruppe 20) zusammen mit ML-KEM-1024 verwendet werden. Ältere MODP-Gruppen (z. B. DH14) sollten nur aus Kompatibilitätsgründen eingesetzt werden. Die konkrete Auswahl ist anhand der aktuellen BSI-Empfehlungen, des Schutzbedarfs und der von der Gegenstelle unterstützten Verfahren zu treffen.

Die Kombination aus klassischem DH und ML-KEM schützt zunächst den Schlüsselaustausch. Sie macht nicht automatisch die gesamte IKEv2-Authentisierung quantenresistent. Werden beispielsweise klassische RSA- oder ECDSA-Signaturen für Zertifikate verwendet, können diese langfristig weiterhin durch Quantencomputer gefährdet sein. Neuere Verfahren, z. B. für die Zertifikatsbasierte Authentifizierung, befinden sich bei der IETF in der Standardisierungsphase.

Es ist grundsätzlich möglich, den Schlüsseltausch mit Post-quantum Preshared Keys nach *RFC 8784* zu kombinieren.

3.1.5 Konfiguration mit LANconfig

Wählen sie im Bereich **VPN** > **IKEv2 / IPSec** > **Verschlüsselung** > **Verschlüsselung** ein Profil für den zusätzliichen Schlüsseltausch aus.

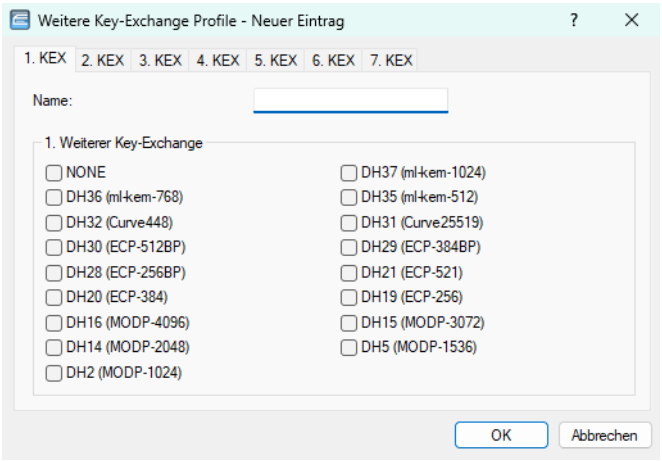
Zusätzlicher Schlüsseltausch

Profil

Name des Profils für den zusätzlichen Schlüsseltausch. Wird der Parameter leer gelassen, so wird kein zusätzlicher Schlüsseltausch durchgeführt und es wird nur die verhandelte DH-Gruppe des normalen Verschlüsselungsprofils verwendet. Die Profile definieren Sie unter **VPN** > **IKEv2 / IPSec** > **Verschlüsselung** > **Weitere Key-Exchange-Profile**.

Es ist möglich, bis zu sieben weitere Key-Exchanges zu konfigurieren. Die Key-Exchanges sind grundsätzlich optional und es kann z. B. nur die erste Runde verwendet werden. In jedem Key-Exchange wird ein Proposal, d. h. Auswahlmöglichkeiten in der Verhandlung zwischen den Verbindungspartnern, angelegt. Wie auch schon bei den regulären IKE-Proposals bzw. DH-Gruppen

muss es für die Kommunikationspartner eine gemeinsame Schnittmenge geben. Bei Nichtübereinstimmung scheitert die IKEv2-Verhandlung.



Name

Enthält den eindeutigen Namen dieses Key-Exchange-Profils. Diesen Namen ordnen Sie als zusätzliches optionales Schlüsseltauschprofil in der **Verschlüsselungs-Tabelle** zu. Sie können bis zu sieben weitere Key-Exchange-Profile definieren.

Weiterer Key-Exchange

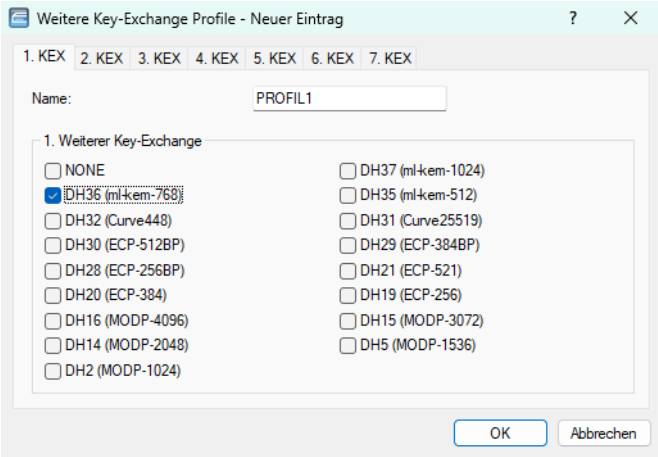
Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel. Aktuell werden folgende Gruppen unterstützt:

- DH-2 (1024-Bit Modulus)
- DH-5 (1536-Bit Modulus)
- DH-14 (2048-Bit Modulus)
- DH-15 (3072-Bit Modulus)
- DH-16 (4096-Bit Modulus)
- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)
- DH-31 (Curve25519)
- DH-32 (Curve448)
- DH-35 (ml-kem-512)
- DH-36 (ml-kem-768)
- DH-37 (ml-kem-1024)

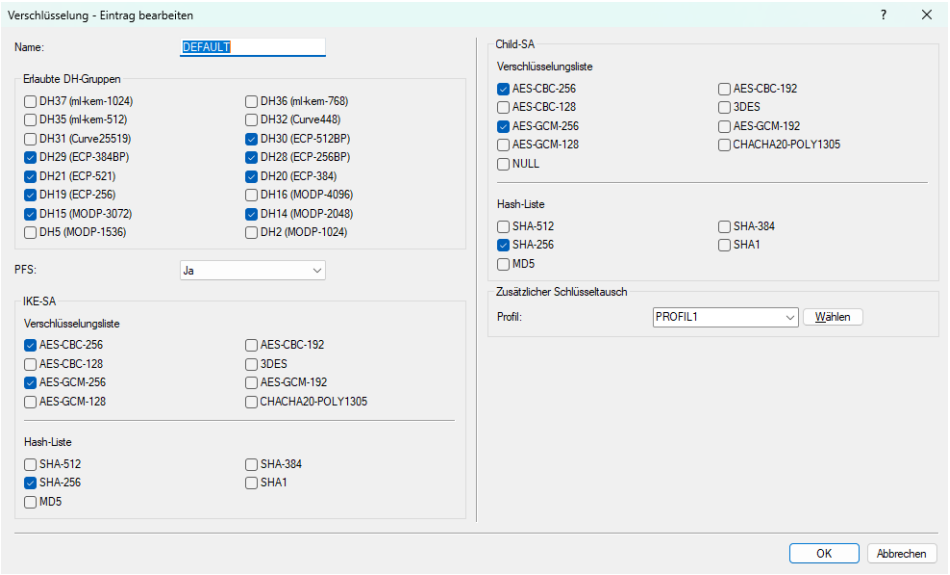
3.1.5.1 Beispiel 1

Es soll eine bestehende IKEv2-Verbindung mit ML-KEM 768 (DH36) mit einem zusätzlichen Schlüsseltausch (Runde 1) durch ein Hybridverfahren post-quantum-sicher gemacht werden.

1. Öffnen Sie die Tabelle **VPN** > **IKEv2 / IPSec** > **Verschlüsselung** > **Weitere Key-Exchange-Profile**. Vergeben Sie einen Namen für das Profil, z. B. „PROFIL1“ und aktivieren Sie DH36.



2. Öffnen Sie die Tabelle **VPN** > **IKEv2 / IPSec** > **Verschlüsselung** > **Verschlüsselung** des DEFAULT-Profils sowie ggf. im nächsten Schritt das Profil einer IKEv2-Verbindung:



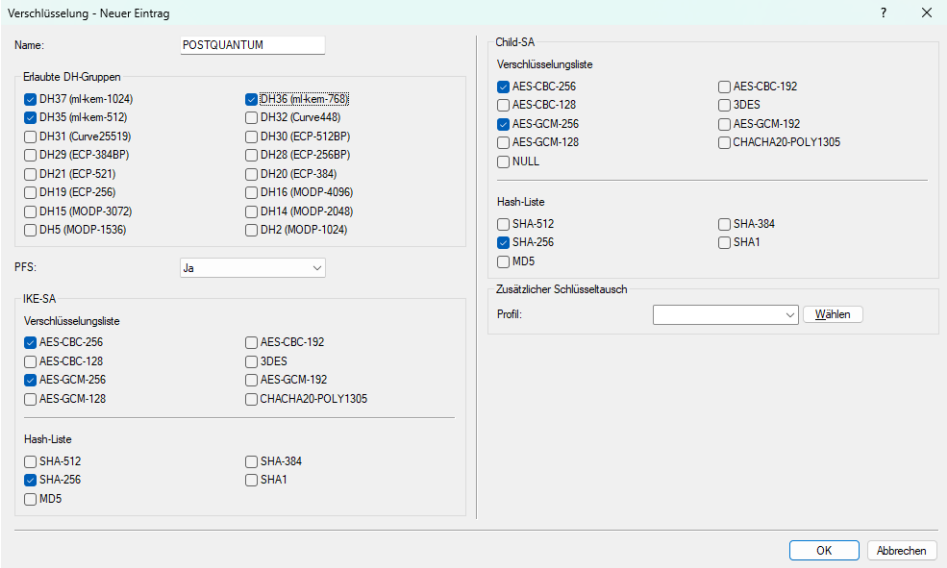
Tragen Sie unter Profil bei **zusätzlicher Schlüsseltausch** den Namen des Profils aus Schritt 1) ein. Im klassischen IKEv2-Schlüsseltausch werden die DH-Gruppen verwendet, die unter **erlaubte DH-Gruppen** konfiguriert sind. im weiteren Key-Exchange-Profil wird ML-KEM 768 (DH36) verwendet. Durch diese Konfiguration wird ein hybrides Post-Quantum-Verfahren eingerichtet.

3.1.5.2 Beispiel 2

Es soll eine IKEv2-Verbindung nur mit ML-KEM-Gruppen, d. h. ein reiner Post-Quantum-Schlüsseltausch, verwendet werden. Ein Hybridverfahren soll nicht zum Einsatz kommen. Daher ist der Einsatz von zusätzlichen Schlüsseltauschrunden nicht erforderlich.

1. Öffnen Sie die Tabelle **VPN** > **IKEv2 / IPSec** > **Verschlüsselung** > **Weitere Key-Exchange-Profile** des Profils einer IKEv2-Verbindung. Im klassischen

IKEv2-Schlüsseltausch werden unter **erlaubte DH-Gruppen** nur Post-Quantum-Gruppen basierend auf ML-KEM erlaubt, z.B. DH37, DH36, DH35.



3.1.6 Ergänzungen im Setup-Menü

3.1.6.1 DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen.

SNMP-ID:

2.19.36.2.2

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Verschlüsselung**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2

3.1.6.2 Add.-Key-Exchange-Profil

Name des Profils für den zusätzlichen Schlüsseltausch. Wird der Parameter leer gelassen, so wird kein zusätzlicher Schlüsseltausch durchgeführt und es wird nur die verhandelte DH-Gruppe des normalen Verschlüsselungsprofils verwendet.

SNMP-ID:

2.19.36.2.8

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Verschlüsselung**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

3.1.6.3 Add.-Key-Exchange-Profiles

Es ist möglich, bis zu sieben weitere Key-Exchanges zu konfigurieren. Die Key-Exchanges sind grundsätzlich optional und es kann z. B. nur die erste Runde verwendet werden. In jedem Key-Exchange wird ein Proposal, d. h. Auswahlmöglichkeiten in der Verhandlung zwischen den Verbindungspartnern, angelegt. Wie auch schon bei den regulären IKE-Proposals bzw. DH-Gruppen muss es für die Kommunikationspartner eine gemeinsame Schnittmenge geben. Bei Nichtübereinstimmung scheitert die IKEv2-Verhandlung.

SNMP-ID:

2.19.36.36

Pfad Konsole:

Setup > **VPN** > **IKEv2**

3.1.6.3.1 Name

Enthält den eindeutigen Namen dieses Key-Exchange-Profils. Diesen Namen ordnen Sie als zusätzliches optionales Schlüsseltauschprofil in der **Verschlüsselungs-Tabelle** zu. Sie können bis zu sieben weitere Key-Exchange-Profile definieren.

SNMP-ID:

2.19.36.36.1

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

3.1.6.3.2 ADDKE1

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.3

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37
ml-kem-1024 (ab LCOS-Version 11.00)

DH36
ml-kem-768 (ab LCOS-Version 11.00)

DH35
ml-kem-512 (ab LCOS-Version 11.00)

DH32
Curve448

DH31
Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.3 ADDKE2

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.4

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.4 ADDKE3

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.5

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.5 ADDKE4

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.6

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.6 ADDKE5

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.7

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.7 ADDKE6

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.8

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.1.6.3.8 ADDKE7

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel.

SNMP-ID:

2.19.36.36.9

Pfad Konsole:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Mögliche Werte:

DH37

ml-kem-1024 (ab LCOS-Version 11.00)

DH36

ml-kem-768 (ab LCOS-Version 11.00)

DH35

ml-kem-512 (ab LCOS-Version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

Bei der Konfiguration von „NONE“ wird erlaubt, dass von der Gegenseite auch kein Proposal bzw. ein leeres Proposal für diese Runde akzeptiert wird.

3.2 IKEv2: Unterstützung für RADIUS-Accounting-On

Ab LCOS 11.00 wird RADIUS-Accounting-On bzw. Off unterstützt.

Im IKEv2 werden bei der Verwendung von RADIUS-Accounting die RADIUS-Nachrichten „Accounting-On“ und „Accounting-Off“ unterstützt. Beim Start versendet das Gerät „Accounting-On“ an die aktiven RADIUS-Accounting-Server. Beim Herunterfahren versendet das Gerät „Accounting-Off“ an die aktiven RADIUS-Accounting-Server. Diese Funktion ist automatisch aktiv, wenn RADIUS-Accounting verwendet wird. RADIUS-Server können durch diese Nachrichten den Betriebsstatus des NAS übermittelt bekommen.

4 Voice over IP – VoIP

4.1 Voice Backup mittels VRRP

Das Virtual Router Redundancy Protocol (VRRP) ist ein Netzwerkprotokoll, welches mehrere physische Router zu einem einzigen virtuellen Router zusammenschließt, um die Ausfallsicherheit zu erhöhen. Auch der Voice Call Manager kann auf diesem virtuellen Interface betrieben werden.

Kommen mehrere virtuelle Netzwerke zum Einsatz, muss der Voice Call Manager an eines dieser Netzwerke gebunden werden. Dazu muss im Voice Call Manager die virtuelle ID (VRRP-ID) sowie der Interface-Name des virtuellen Routers (VRRP-Interface) angegeben werden. Diese beiden Werte beziehen sich auf die Angaben „Schnittstelle/Interface“ und „Router-ID“ der Tabelle „Virtuelle Router“ in den VRRP-Einstellungen. Wird als VRRP-ID „0“ angegeben, wird die VRRP Funktion im Voice Call Manager deaktiviert.

Zur Registrierung der SIP Telefone wird die entsprechende virtuelle IP-Adresse der Routers als Registrar im Telefon hinterlegt. Alternativ kann hier auch die VoIP-Domäne verwendet werden, sofern diese sich von der DNS-Domäne unterscheidet. Zu beachten ist hierbei allerdings, dass sich die SIP-Endgeräte erst nach Ablauf des Re-Register Timeouts am neuen Master-Router registrieren.

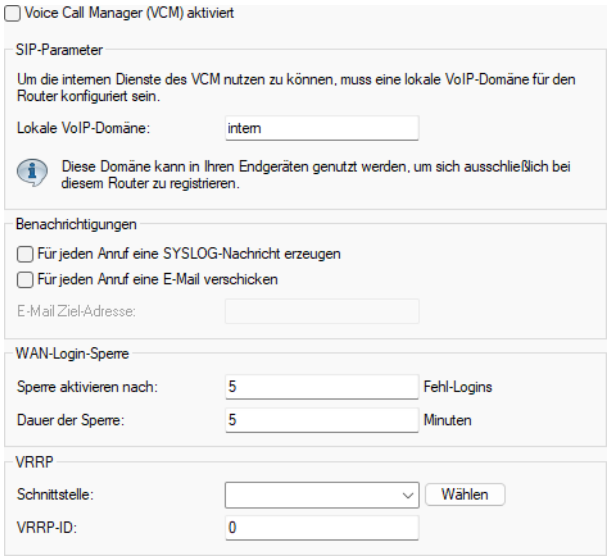
Übernimmt ein Standby-Gerät die Netzwerkkommunikation, sind die SIP-Endgeräte, bis zum erneuten Register, nicht verfügbar.

Ein Mischbetrieb, bei denen sich Telefone an der virtuellen und physikalischen IP-Adresse registrieren, ist nicht vorgesehen.

ISDN- und Analog-Telefone können im Backupfall nicht weiterverwendet werden.

Konfiguration in LANconfig

Die Einstellungen zum Voice Backup mittels VRRP konfigurieren Sie unter **Voice Call Manager** > **Allgemein**.



VRRP-Schnittstelle

Interface-Name des virtuellen Routers.

VRRP-ID

Virtuelle Router-ID.

4.2 Ergänzungen im Setup-Menü

4.2.1 Vrrp-Interface

Interface-Name des virtuellen Routers.

SNMP-ID:

2.33.2.27

Pfad Konsole:

Setup > **Voice-Call-Manager** > **General**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

4.2.2 Vrrp-Interface

Virtuelle Router-ID.

SNMP-ID:

2.33.2.28

Pfad Konsole:

Setup > **Voice-Call-Manager** > **General**

Mögliche Werte:

1 … 255

5 RADIUS

5.1 DHCPv6-Optionen im RADIUS-Auth-VSA übertragen

Ab LCOS 11.00 wird ein neues vendorspecific RADIUS-Attribut LCS-DHCPv6-Option mit der Nummer 35 unter dem Vendor LCS (2356) unterstützt. Es ist ein RADUS-Text-Attribut, das nur in Access-Accept-Nachrichten (d. h. den Antwortpaketen des RADIUS-Servers für die RADIUS-Authorization) vorkommt und mehrfach in derselben Nachricht vorkommen darf. Damit das LCOS diese Option verarbeiten kann, muss der Text die unten angegebene Form haben.

Das Attribut kann für die RADIUS-Authorization benutzt werden, wenn das Gerät RADIUS-Client und entweder PPPoE-Server oder IKEv2-Responder (VPN) ist. Jede Instanz des Attributs definiert eine DHCPv6-Option, die der DHCPv6-Server im LCOS an den DHCPv6-Client auf der PPPoE- bzw. VPN-Verbindung schicken soll, sofern der DHCPv6-Client in seiner Option-Request-Option danach fragt. Das Feature erfüllt damit denselben Zweck wie die statische Tabelle **Setup** > **IPv6** > **DHCPv6** > **Server** > **Additional-Options** [2.70.3.1.8].

Der Attribut-Text muss aus den drei Teilen Option-Number, Option-Type und Option-Value bestehen, die durch je ein Komma, aber ohne Leerzeichen oder anderen Trennzeichen voneinander getrennt sind. Der Option-Value darf zwar leer sein, das zweite Komma ist dann aber trotzdem erforderlich. Die drei Teile orientieren sich an den gleichnamigen Spalten der o. g. Setup-Tabelle sind wie folgt formatiert:

- Option-Number gibt die Options-Nummer (den DHCPv6-Option-Code) als Zahl an, und zwar entweder dezimal oder oktal mit „0“-Präfix oder hexadezimal mit „0x“-Präfix. Die Zahl muss im Bereich von 1 bis 65535 liegen.
- Option-Type ist entweder eine Zahl im Bereich von 0 bis 6, die ansonsten wie Option-Number kodiert ist, oder einer der Strings „Integer8“, „Integer16“, „Integer32“, „IPv6-Addresses“, „Domain-List“, „String“ oder „Hexdump“, wobei die hier angegebene Groß-/Kleinschreibung beachtet werden muss.
- Option-Value ist genauso formatiert wie die Option-Value-Spalte der o. g. Setup-Tabelle, wobei das Format hier genau wie dort vom Option-Type abhängt. Hier zitiere ich die Beschreibung aus der aktuellen Menüreferenz, die im RADIUS-Attribut gleichermaßen gilt. Alle Typen außer String sind komma- und leerzeichenseparierte Listen, wobei leere Listenelemente ignoriert werden und auch eine leere Liste erlaubt ist und zu einer Option der Länge 0 führt.
  - „Integer8“ oder Zahl 0: 8-Bit Integer von -128 bis 127 wahlweise dezimal, oktal mit Präfix „0“ oder hexadezimal mit Präfix „0x“.
  - „Integer16“ oder Zahl 1: 16-Bit Integer von -32768 bis 32767 wahlweise dezimal, oktal mit Präfix „0“ oder hexadezimal mit Präfix „0x“.
  - „Integer32“ oder Zahl 2: 32-Bit Integer von -2147483648 bis 2147483647 wahlweise dezimal, oktal mit Präfix „0“ oder hexadezimal mit Präfix „0x“.
  - „IPv6-Addresses“ oder Zahl 3: IPv6-Adressen ohne Beachtung der Groß-/Kleinschreibung in allen zulässigen Darstellungen inklusive der gemischten IPv4-/IPv6-Darstellung von Mapped-V4-Adressen wie z. B. ::ffff:1.2.3.4.
  - „Domain-List“ oder Zahl 4: Domain-Namen in normaler Schreibweise als Strings, die durch Punkte in Labels unterteilt sind, die jeweils höchstens 63 Zeichen lang sind. Leere Labels sind zulässig, werden aber ignoriert. Die DHCPv6-Option wird als Folge von Labels mit führendem Längenbyte kodiert, so wie es *RFC 3315*, Kapitel 8 bzw. *RFC 1035*, Kapitel 3.1 vorsehen. Eine Domain endet grundsätzlich mit dem leeren Label 0.

- „String“ oder Zahl 5: Die Zeichen werden als String übernommen. Der String beginnt unmittelbar hinter dem zweiten Komma und kann auch weitere Kommata, Leerzeichen oder Anführungszeichen enthalten, die dann als Teil des String interpretiert werden. Sollte hinter dem zweiten Komma erst noch ein Leerzeichen folgen, dann gehört auch dieses Leerzeichen bereits zum String.
- „Hexdump“ oder Zahl 6: Erwartet in jedem Block nur Hexziffern ohne „0x“-Präfix und füllt jeden Block ggf. mit einer führenden 0 zu gerader Länge auf. Der Block wird als Bigendian übernommen.

Die Option-Number muss eindeutig sein, d. h. in der RADIUS-Antwort dürfen nicht mehrere LCS-DHCPv6-Option-Attribute mit derselben Option-Number vorkommen, so wie es im DHCPv6 ja auch nicht mehrere Optionen mit gleichem Option-Code in derselben Nachricht geben darf.

Beispiele für gültige LCS-DHCPv6-Option-Attribute:

```
2356,0,0,-128,255,+13,-0200,0377,+0xD,0xff,-0x80,0X12
200,1,0,-32768,65535,+13,-0100000,0177777,+0xD,0xffff,-0x8000,0X12d
201,02,0,-2147483648,4294967295,+13,-020000000000,037777777777,+0xDEF,0xffffffff,-0x80000000,0X12d
202,03,::,2001:db87::beef,2001:004:00:0:56::,::ffff:192.168.0.4,fe80::02:a0:57:ff:fe:12:45:82,FE80::BDE
203,0x4,www.lancom.de,fully.qualified.,ThisIsAVeryLongLabelNamelyExactly63CharactersLongWhichIsMaximum.de
204, 5, alskdflaweiurqtow34875qor87aef<ynbxcv  4365o  7q64@!$&(/==%=?(
205,6,0123456789,abcdef,ABCDEF,8,123
0x2356,Integer8,,,,0, -128, 255, +13, -0200, 0377, +0xD, 0xff, -0x80, 0X12
0x200,Integer16,,,,0, -32768, 65535, +13, -0100000, 0177777, +0xD, 0xffff, -0x8000, 0X12d
0x201,Integer32,,,,0, -2147483648,4294967295,+13,-020000000000,037777777777,+0xDEF,0xffffffff,-0x80000000,0X12d
0x202,IPv6-Addresses,,,,::,2001:db87::beef,2001:004:00:0:56::,::ffff:192.168.0.4,fe80::02:a0:57:ff:fe:12:45:82,FE80::BDE
0x203,Domain-List,,,, www.lancom.de, fully.qualified., ThisIsAVeryLongLabelNamelyExactly63Characters.de
0x204,String,,,, alskdflaweiurqtow34875qor87aef<ynbxcv  4365o  7q64@!$&(/==%=?(
0x205,Hexdump,,,, 0123456789, abcdef, ABCDEF, 8, 123
```

Beispiele für ungültige LCS-DHCPv6-Option-Attribute:

```
666,666,666
777,Integer64,12345
65536,0,1,2,3
144,4
```

6 Ergänzungen im Menüsystem

6.1 Ergänzungen im Setup-Menü

6.1.1 CHAP-Reauth-Minuten

Die CHAP-Rechallenge bzw. CHAP-Reauthentifizierung im PPP-Server (PPTP, L2TP, PPPoE) ist hier konfigurierbar. Geben Sie hier die Zeit bis zu einer CHAP-Reauthentifizierung in Minuten ein.

Der Default ist 0, wodurch CHAP-Reauthentifizierung abgeschaltet wird.

Wird ein CHAP-Paket nicht beantwortet, so gibt es noch 4 Wiederholungen im Abstand von 5 Sekunden (insgesamt also 5 Versuche), bis die Verbindung mit einem Timeout abgebrochen wird.

SNMP-ID:

2.2.80

Pfad Konsole:

Setup > **WAN** > **QoS**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

0

6.1.2 Schluesselaustausch-Algorithmen

Ab LCOS-Version 11.00 werden im SSH mit „mlkem768nistp256-sha256“ und „mlkem1024nistp384-sha384“ zwei weitere neue Hybride-Post-Quantum-Algorithmen unterstützt.

Die MAC-Schluesselaustausch-Algorithmen dienen der Aushandlung des Schlüssel-Algorithmus. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

SNMP-ID:

2.11.28.3

Pfad Konsole:

Setup > **Config** > **SSH**

Mögliche Werte:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
sntrup4591761x25519-sha512
mlkem768x25519-sha256
Hybrid-Post-Quantum-Algorithmus mlkem768x25519. Hierbei wird der Post-Quantum-Algorithmus ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) mit dem bekannten klassischen Verfahren Curve25519 kombiniert.
mlkem768nistp256-sha256
Hybrid-Post-Quantum-Algorithmus mlkem768nistp256-sha256.
mlkem1024nistp384-sha384
Hybrid-Post-Quantum-Algorithmus mlkem1024nistp384-sha384.

Default-Wert:

diffie-hellman-group-exchange-sha256

ecdh-sha2

curve25519-sha256

curve448-sha512

sntrup761x25519-sha512

diffie-hellman-group14-sha256

diffie-hellman-group15-sha512

diffie-hellman-group16-sha512

mlkem768x25519-sha256

6.1.3 Zugriffsart

Ab LCOS 11.00 können Sie die Zugriffsrechte eines Wireguard-Tunnels auf WAN herunterstufen. Konfigurieren Sie hier die Zugriffsart des Wireguard-Tunnels per Peer.

SNMP-ID:

2.19.70.3.17

Pfad Konsole:

Setup > **VPN** > **WireGuard** > **Peers**

Mögliche Werte:

VPN
WAN

Default-Wert:

VPN

6.1.4 Authentifizierungs-Typ

Ab LCOS 11.00 werden bei OSPFv2 weitere Algorithmen nach RFC 5709 bei der kryptografischen Authentifizierung unterstützt. Neue zusätzliche Methoden sind SHA1, SHA256, SHA384 und SHA512.

Authentifizierungsmethode, die für diese Schnittstelle verwendet wird.

SNMP-ID:

2.93.3.4.11

Pfad Konsole:

Setup > **Routing-Protokolle** > **OSPF** > **Interfaces**

Mögliche Werte:

Null
Simple-Password
Cryptographic-MD5
Cryptographic-SHA1
Cryptographic-SHA256
Cryptographic-SHA384
Cryptographic-SHA512

Default-Wert:

Null