Leitfaden: Netzwerk- & Firewall-Konfiguration für YuLinc (WebRTC)

netucate systems GmbH

Technische Orientierungshilfe zur Firewall- und Proxy-Konfiguration für Behörden-IT-Abteilungen

Basis: Offizielle YuLinc-Infrastruktur-Dokumentation (inkl. Infrastruktur-Erweiterung Mai 2026)

Stand: Juli 2026

1. Der Gold-Standard: Freigabe auf Domain-Basis (Empfohlen)

Um den Administrationsaufwand zu minimieren und die Plattform zukunftssicher (z. B. bei Infrastruktur-Erweiterungen) zu betreiben, sollte die Freigabe in Ihrer Firewall und auf Ihren Proxys zwingend über Wildcard-Domains erfolgen:

- **Erforderliche Domains:** *.wbcnf.net und *.netucate.net
- **Basis-Ports (ausgehend):** Port 443 (TCP/UDP) sowie Port 3478 (UDP)

✓ **Vorteil:** Werden diese Domains freigegeben, entfällt die manuelle Pflege einzelner IP-Adressen komplett – alle Web-, Signalisierungs- und Medienserver sind automatisch abgedeckt, auch bei künftigen Infrastruktur-Erweiterungen wie der für Mai 2026 umgesetzten.

2. Drei Wege der Umsetzung (Architektur-Optionen)

Je nach den Sicherheitsrichtlinien Ihrer Behörde kann der Medienverkehr (Audio, Video, Screen-Sharing) über drei verschiedene Wege geroutet werden. Bitte prüfen Sie intern, welcher Weg für Ihr Netzwerk umsetzbar ist:

Weg A: Direkte Verbindung zu den Medienservern (Optimale Qualität)

- **Protokoll & Ports:** TCP und UDP auf den Ports 20000–40000

- **Ziel:** Alle dedizierten Medienserver-IPs von netucate sowie die IP-Bereiche für das elastische Cloud-Scaling (z. B. Scaleway-Bereiche bei Lastspitzen).
- **Bewertung:** Liefert die absolut beste Audio- und Videoqualität bei geringster Latenz. Erfordert jedoch die administrative Öffnung einer größeren ausgehenden Port-Range.

Weg B: Das UDP-Relay (TURN) (Der Behörden-Standard)

- **Protokoll & Ports:** UDP auf Port 3478 oder 443
- **Ziel:** Verbindung zu den zentralen TURN-Servern (turn.aquila-eu.wbcnf.net und turn.delphinus-eu.wbcnf.net).
- **Bewertung:** Fängt Probleme mit restriktivem NAT (Symmetric NAT) ab, wenn viele Teilnehmer aus demselben Netz kommen. Sehr gute Balance aus Sicherheit und Performance.

Weg C: Das TCP/TLS-Relay (Der restriktive Fallback)

- **Protokoll & Ports:** TCP / TLS auf Port 5349 oder 443
- **Ziel:** Gleiche TURN-Server-Adressen wie bei Weg B.
- **Bewertung:** Die "Nuclear Option", falls UDP in Ihrem Netzwerk komplett blockiert ist. Funktioniert fast immer, erzeugt aber durch das TCP-Protokoll eine höhere CPU-Last auf Ihrer Firewall (Session-Tracking) und kann zu minimalen Latenzen bei den Nutzern führen.

3. Architektur-Hintergrund: Gen2-Verbindungstechnologie (SFU / Simulcast)

YuLinc setzt auf die Gen2-Verbindungstechnologie. Deren besonderer Clou liegt darin, dass mehrere Video- und Audiostreams (inklusive verschiedener Qualitätsstufen) über nur eine einzige Peer-Verbindung laufen können. Diese Architektur hat gegenüber dem Aufsetzen mehrerer separater Verbindungen für jeden Stream entscheidende Vorteile – und ist auch für die Firewall-Dimensionierung relevant:

- **Geringerer Verbindungs-Overhead:** Es findet nur ein einziger Verbindungsaufbau (ICE, DTLS usw.) pro Teilnehmendem statt – weniger Signalisierungsaufwand und damit reduzierte Komplexität bei der Verwaltung.
- **Effizientere Nutzung von Ressourcen:** Eine Peer-Verbindung belegt weniger Arbeitsspeicher und CPU-Zeit, da nur ein Protokoll-Stack gehalten werden muss. Die Netzwerklast lässt sich besser steuern, da mehrere Streams im selben Verbindungskanal koordiniert werden.
- **Bessere Skalierbarkeit:** Wenn viele Teilnehmende gleichzeitig aktiv sind, bleibt das Setup schlanker, da nicht für jeden Stream eine eigene Verbindung eingerichtet wird. Die SFU steuert und verteilt alle Streams pro Teilnehmendem zentral, was die Bandbreite auf Empfängerseite optimiert.
- **Dynamische Anpassung dank Simulcast:** Trotz nur einer Peer-Verbindung können unterschiedliche Qualitätsstufen gesendet werden (z. B. High- und Low-Definition). Die SFU passt die Auslieferung an Netzwerk- oder Gerätekapazitäten an, ohne dass zusätzliche Peer-Verbindungen erforderlich sind.

✓ **Bedeutung für Ihre Firewall-Konfiguration:** Da alle Qualitätsstufen eines Teilnehmenden über eine einzige Verbindung laufen, entsteht pro Teilnehmendem nur ein UDP/TCP-Session-State Richtung Medien- bzw. TURN-Server – nicht mehrere. Das reduziert den benötigten Verbindungs- und Port-Overhead bei Weg A und wirkt sich günstig auf die NAT-Table-Größe aus (siehe Abschnitt 4), was die Kapazitätsplanung bei vielen gleichzeitigen Teilnehmenden planbarer macht.

4. Performance-Checkliste bei vielen Teilnehmern (Gleiche öffentliche IP)

Wenn sich 20, 50 oder mehr Personen gleichzeitig aus demselben Behördennetzwerk einwählen, entstehen Engpässe meist **lokal auf der internen Firewall** und nicht auf den Zielservern. Bitte prüfen Sie folgende Punkte in Ihrer Konfiguration:

- **Proxy-Ausnahme (Bypass) einrichten:** WebRTC-Medienströme sind via DTLS/SRTP bereits vollverschlüsselt und lassen sich nicht cachen. Ein Aufbrechen der Pakete durch Deep Packet Inspection (DPI) oder SSL-Verkehrsprüfung auf Web-Proxys führt unweigerlich zu Verbindungsabbrüchen. Für *.wbcnf.net und *.netucate.net muss ein kompletter Proxy-Bypass (Direct Routing) eingerichtet werden.
- **NAT-Table-Timeout (UDP-States):** Dank der Gen2-Verbindungstechnologie (siehe Abschnitt 3) benötigt jeder Teilnehmende ohnehin nur einen Session-State statt mehrerer pro Qualitätsstufe. Um dennoch ein Volllaufen ("Exhaustion") der State-Table auf der Firewall bei vielen gleichzeitigen Teilnehmenden zu verhindern, sollte das UDP-Timeout für die Ports 3478 und 443 auf einen niedrigen Wert gesetzt werden (Empfehlung: max. 30 Sekunden für inaktive UDP-States).
- **Quality of Service (QoS):** Der Echtzeit-Verkehr (Audio/Video) auf den Ports 3478 und 443 sollte im internen Netzwerk gegenüber normalen Daten-Downloads (z. B. großen Windows-Updates im Hintergrund) priorisiert werden.

Hinweis: *Die vollständige, detaillierte IP-Übersicht (inkl. aller Standort- und Zertifizierungsangaben) entnehmen Sie bitte der offiziellen „YuLinc by netucate – Infrastruktur-Dokumentation“ (Stand: März 2026, inkl. Infrastruktur-Erweiterung Mai 2026).*

---

netucate systems GmbH – Mondorfer Weg 30 – D-61352 Bad Homburg v.d.H.
Stand: Juli 2026 – Erstellt auf Basis der offiziellen, technisch verifizierten Infrastruktur-Dokumentation.