OpenSSL CONFERENCE

MASQUE

What's behind the MASQUE

Yaroslav Rosomakho

Chief Scientist, Zscaler

Member, Internet Architecture Board

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

20/10/2026

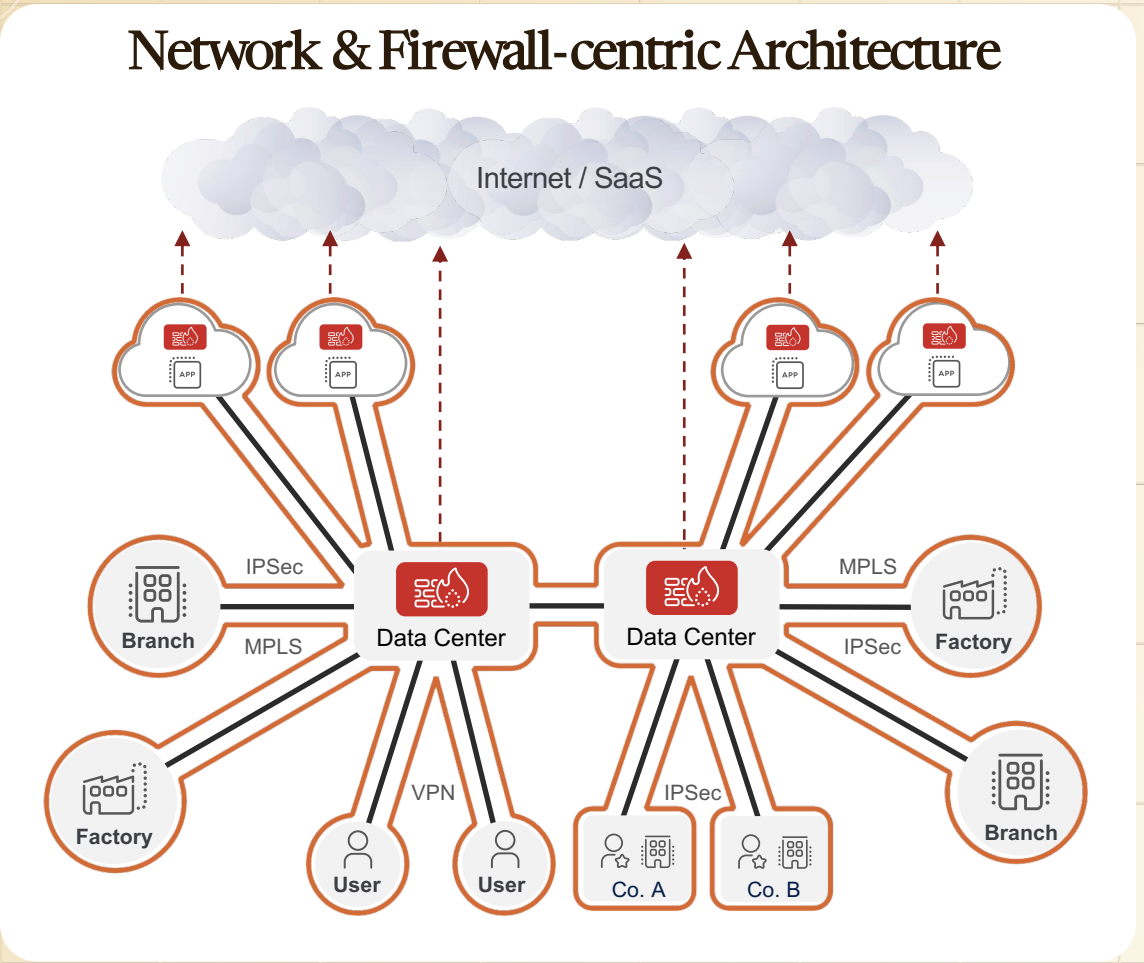
Desired Properties for secure tunnels

- Confidentiality
- Integrity and authentication
- Reliability and reachability
- Performance and efficiency
- Stealth and ossification resistance
- Deplorability and interoperability



What's wrong with IPSec?

- Easy to detect and block
- Inefficient for modern traffic patterns
- Operational and interoperability complexity
- Poor alignment with identity-centric security



What's wrong with Wireguard?

- Easy to detect and block
- Limited transport efficiency at scale
- No cryptographic agility
- Rigid key and identity model
- Deliberately narrow design scope



What's wrong with "SSL VPN"?



Proprietary and fragmented ecosystems



Limited interoperability and portability



Detectable traffic patterns despite TLS



Head-of-line blocking risks

Creating the MASQUE: background

Multiplexed **A**pplication **S**ubstrate over ***QU****IC* **E**ncryption

- Open, standards-based from IETF
- Born from:
  - Censorship resistance
  - Privacy-preserving proxies
  - QUIC + HTTP/3
- Designed to look like normal web traffic
- Survives hostile networks
- Avoids protocol ossification



Generalized MASQUE overview

- **A set of standards, not a single protocol**

Family of IETF standards, not a monolith. “Support” is meaningless without specifying the mechanism (e.g., CONNECT-IP vs. CONNECT).

- **HTTP-Based Tunnelling**

Not QUIC-exclusive. Provides tunnelling over any HTTP version (H1, H2, or H3), falling back as needed.

- **HTTP-Based Tunnelling**

General-purpose tunnelling foundation, not a turnkey VPN solution.



Key MASQUE properties

Satisfying secure tunnel requirements



CONFIDENTIALITY
TLS 1.3 based security model with no custom crypto

INTEGRITY & AUTHENTICATION
Cryptographic binding to HTTP/TLS identities

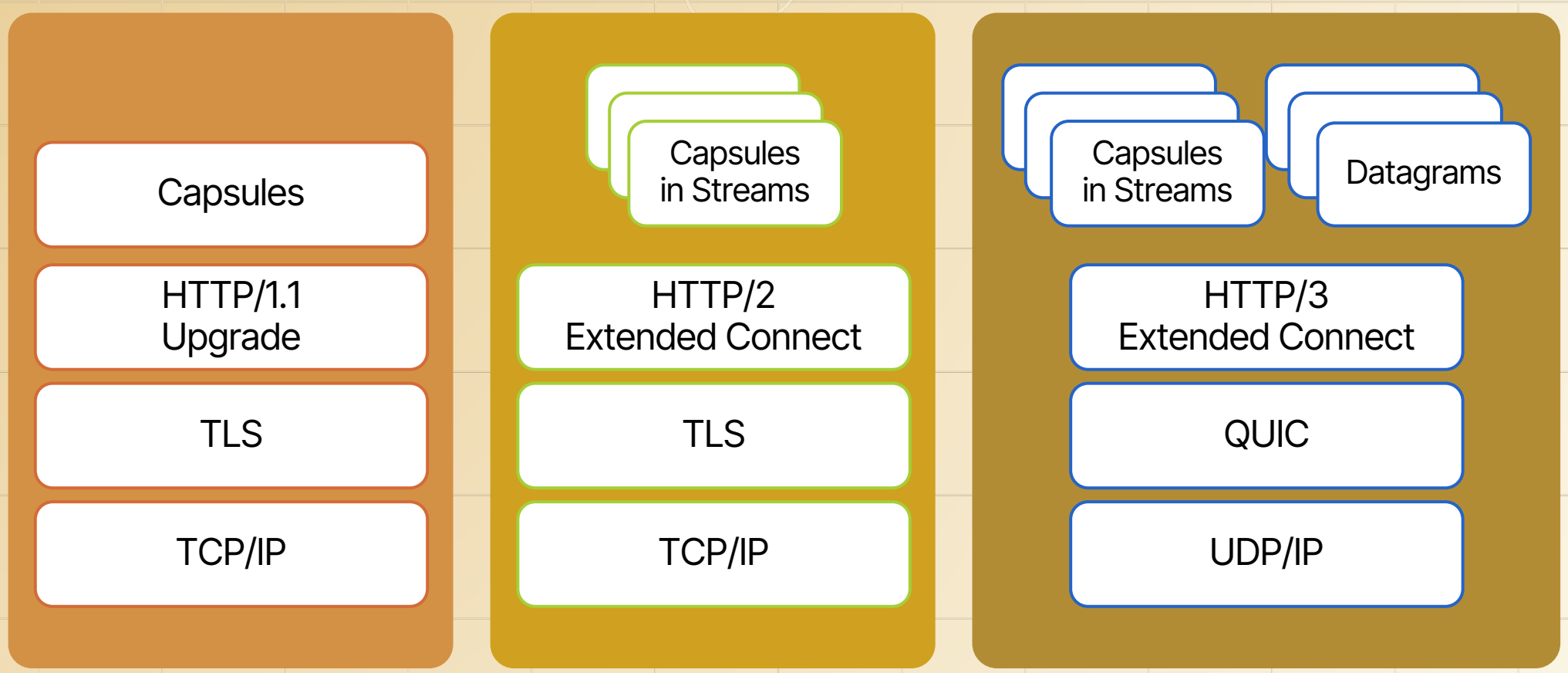
RELIABILITY & REACHABILITY
If the web (HTTP) works, MASQUE works

PERFORMANCE & EFFICIENCY
Multiplexed efficient tunnels without head-of-line blocking (when operated with HTTP/3)

STEALTH & OSSIFICATION RESISTANCE
Indistinguishable from normal HTTPS traffic

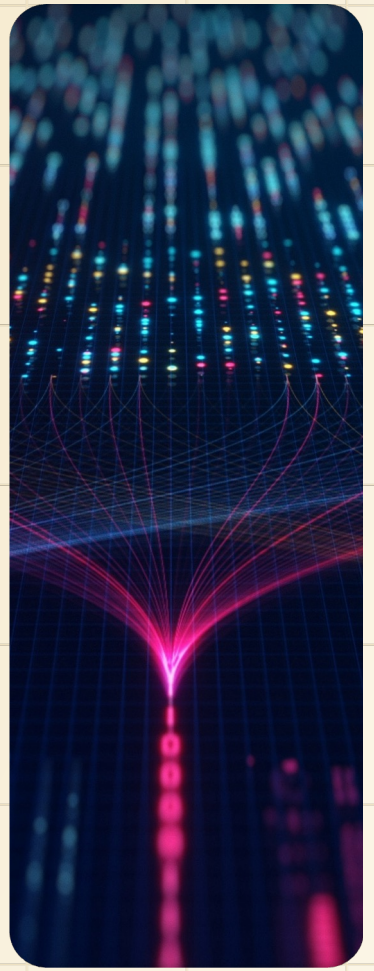
DEPLOYABILITY & INTEROPERABILITY
Open, standards-based mechanisms

MASQUE Protocol Stacks

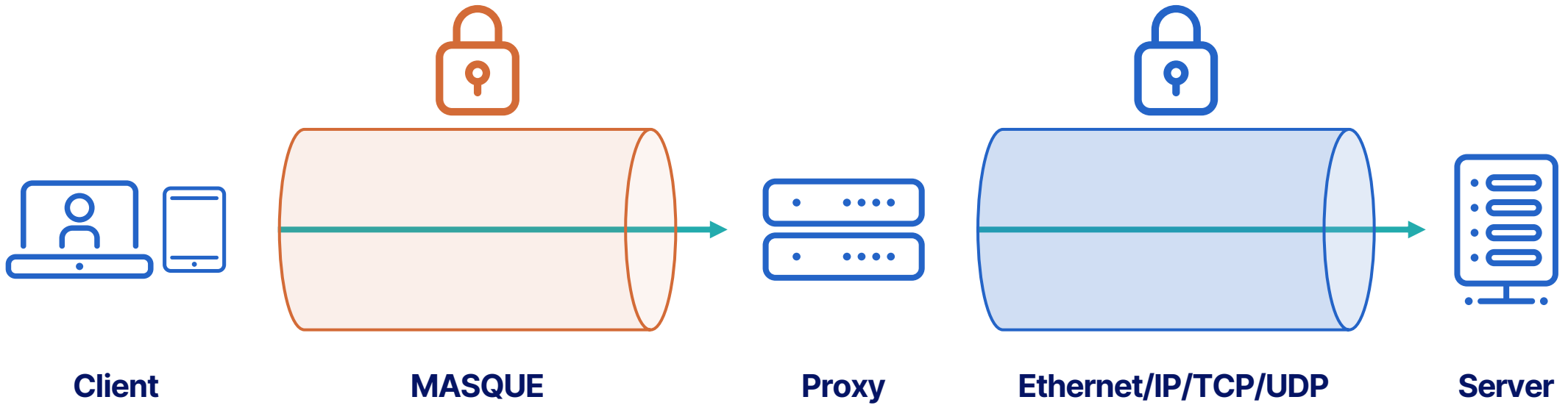


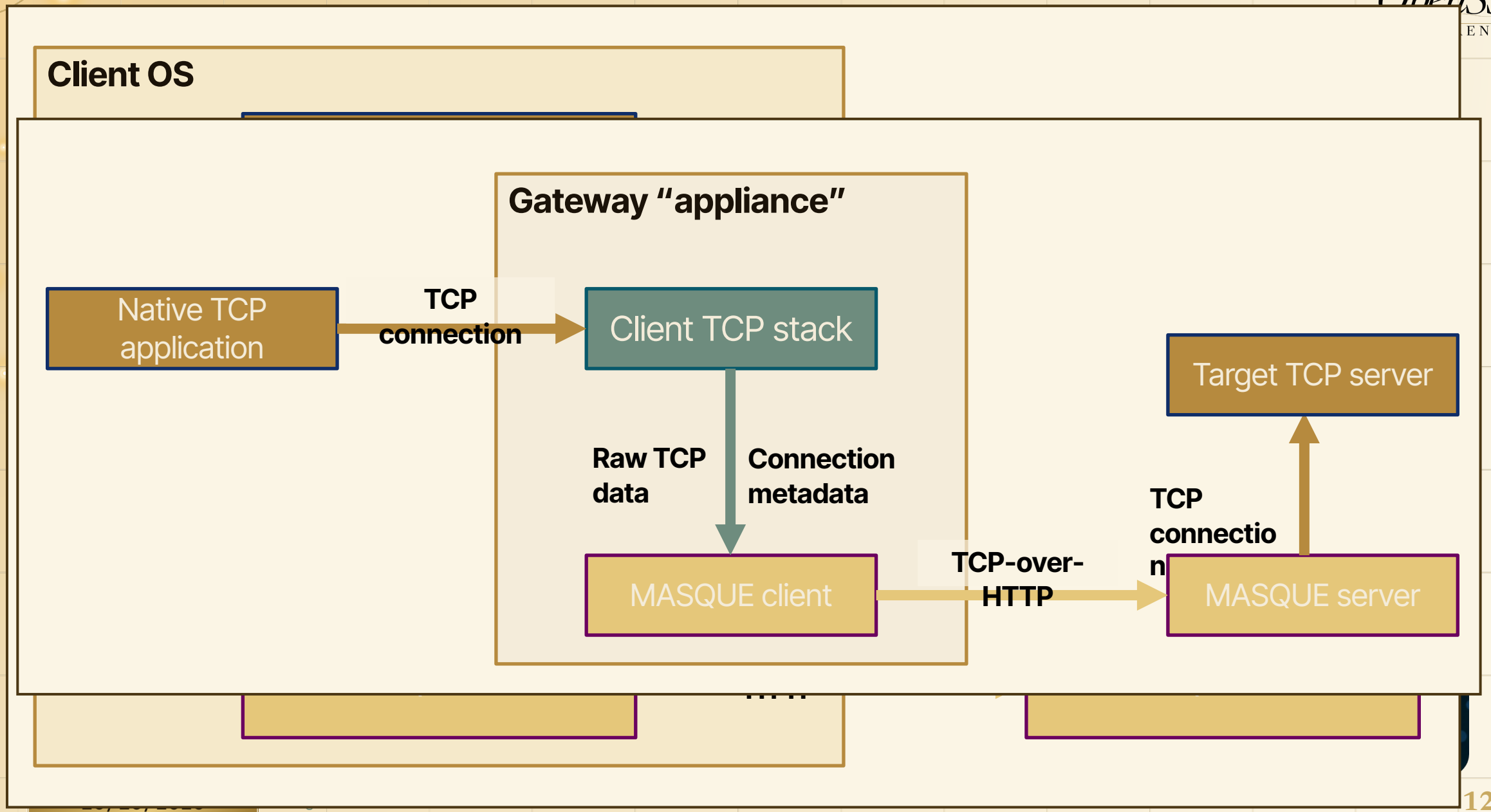
HTTP Capsule

- Just a structured binary message carried inside HTTP
- Transparent to intermediaries that don't understand them (hence the name)
- Simple TLV defined in RFC9297 with types registered in IANA
- Type and Length are coded as variable-length integers so there is little overhead
- Capsules are carried reliably and in order
- Used for signaling messages and to encapsulate UDP datagrams, IP packets or Ethernet frames when HTTP/3 datagrams are not available



How MASQUE “proxies” traffic




Client OS
Gateway “appliance”
Native TCP application
TCP connection
Client TCP stack
Raw TCP data
Connection metadata
MASQUE client
TCP-over-HTTP
MASQUE server
TCP connectio n
Target TCP server

UDP over HTTP


```
->
HEADERS
:method = CONNECT
:protocol = connect-udp
:scheme = https
:path = /.well-known/masque/udp/google.com/443/
:authority = example.com
capsule-protocol = ?1
<-
HEADERS
:status = 200
capsule-protocol = ?1

<->
Datagram Capsules .. Or Nothing (HTTP/3 Datagrams case)
```

IP over HTTP (CONNECT-IP, RFC9484)

- **Symmetrical Layer 3 tunnelling; a drop-in IPSec replacement**
- **Two delivery options (like CONNECT-UDP)**
  - Reliable over HTTP Capsules without MTU constraints
  - Unreliable over HTTP/3 Datagrams (limited by HTTP/3 Datagram size)
- **Lower overhead compared to IPSec, Wireguard or DTLS**
- **Capsule-driven integrated IP address allocation, routing, DNS and PREF64 signalling**
- **Ongoing work on header compression and checksum offload to further increase performance**



Specialised flavours: L2 and P2P



CONNECT-ETHERNET

draft-ietf-masque-connect-ethernet

- Raw Ethernet frame forwarding with MAC-level semantics
- Ideal for legacy protocols requiring L2 transparency

Bound UDP (proxy listener)

draft-ietf-masque-connect-udp-listen

- Enables Peer-to-Peer (WebRTC) by opening proxy-side inbound UDP socket
- Includes signalling for client-defined ACLs

TLS pitfall 1: AEAD limits



Cryptographic Limits

AEAD algorithms (AES-GCM, ChaCha20Poly1305) degrade gradually; there is no "hard" failure threshold.



The Rekeying Gap

- NIST Recommendation: Rekey every 2^{32} blocks (64 GB).
- TLS RFC 8446: Max $2^{24.5}$ full records (~360 GB).
- QUIC RFC 9001: Limits to 2^{23} packets (~12 GB).



The Implementation Trap

TLS 1.3/QUIC provide KeyUpdate mechanisms, but protocols do not enforce them.



Action

Ensure your library or stack explicitly triggers KeyUpdate before hitting these thresholds.

TLS pitfall 2: post-compromise security



The Vulnerability: The "Chain of Trust" Problem

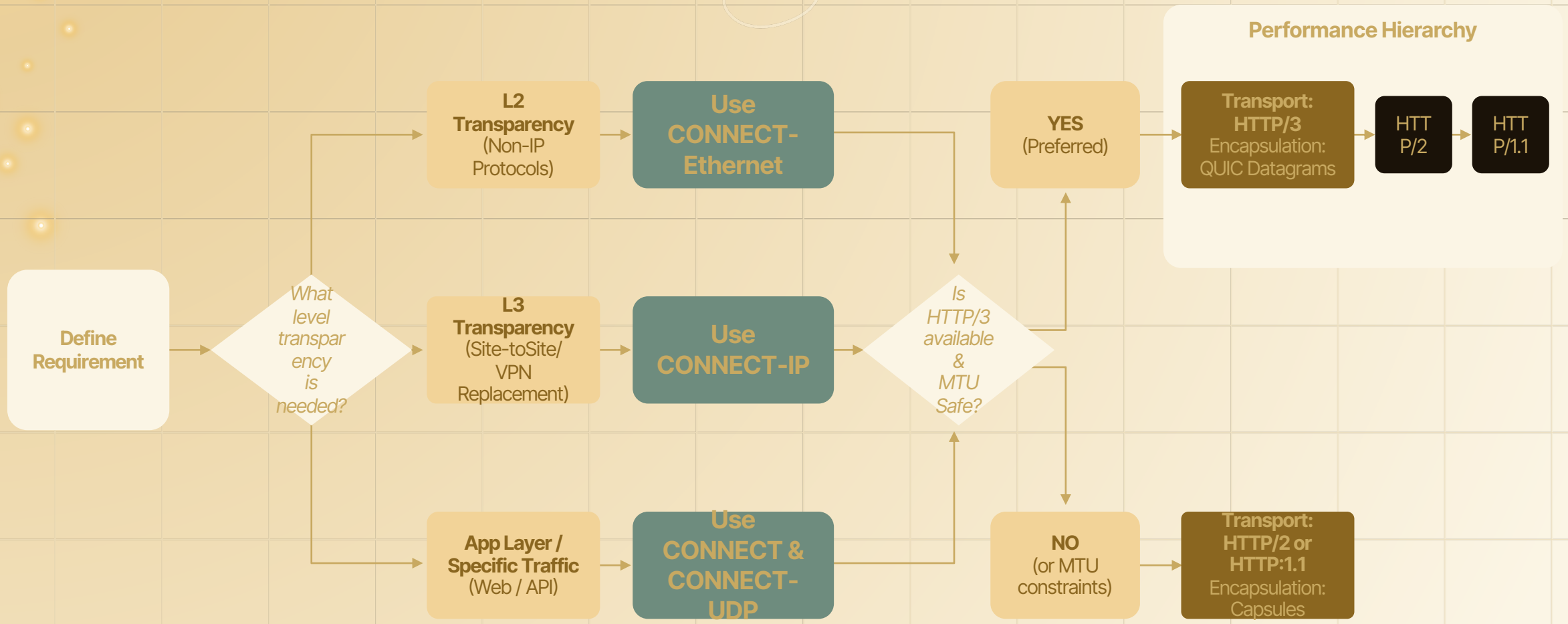
- **TLS 1.3 Limitation**: Standard rekeying derives the next key from the current one.
- **The Risk**: If an attacker compromises a single key, they can potentially derive all future keys in that session.
- **Tunnel Impact**: Long-lived MASQUE tunnels are prime targets for this "Stateful" compromise.

The Future Solution: Extended Key Update

draft-ietf-tls-extended-key-update/draft-ietf-quic-extended-key-update

- **Beyond Derivation:** Introduces fresh entropy into the key schedule mid-session.
- **True PCS:** Breaks the chain; a compromised key today does not compromise the tunnel tomorrow.
- **Outcome:** Essential for enterprise-grade, multi-day connectivity.

Which MASQUE to use?



MASQUE IETF working group

Working groups and materials

- **All IETF working groups are open to anyone and free to join**
- All working materials are freely available online at https://datatracker.ietf.org/wg/masque/documents/
- Most work is conducted online on the mailing list https://mailarchive.ietf.org/arch/browse/masque/

Meetings and events

- **IETF plenary meetings** are held three times a year (rotating around the globe)
- **Full remote participation** is available since before the pandemic

Internet **Get started at: www.ietf.org/participate**

How to apply MASQUE securely

1. Check if your ZTNA/VPN provider has a roadmap for MASQUE.
2. Are you a vendor? Consider MASQUE as your connectivity foundation.
3. Focus on secure and efficient MASQUE flavors: CONNECT, CONNECT-TCP, CONNECT-UDP over HTTP/3.
4. Extended Key Update is essential for security.
5. Auth Matters: Ensure your re-authentication strategy fits the use case.



Q&A