# IETF117: Path Selection in Multi Tunnel SD-WAN

Altanai B (altanai@outlook.com)
Cisco Meraki

# Many options for Path selection

Networks today have various ways to choose path, as

- Tunnelling protocol preference
  - ( IPSec, SSL , GRE or proprietary AutoVPN  ...)
- split tunnel
- DTLS , WS ...
- MASQUE tunnel
- PoP routing

so on

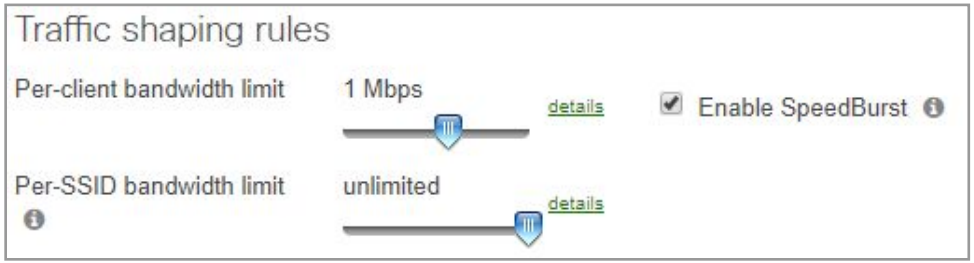
# Many options when there are multiple active tunnels

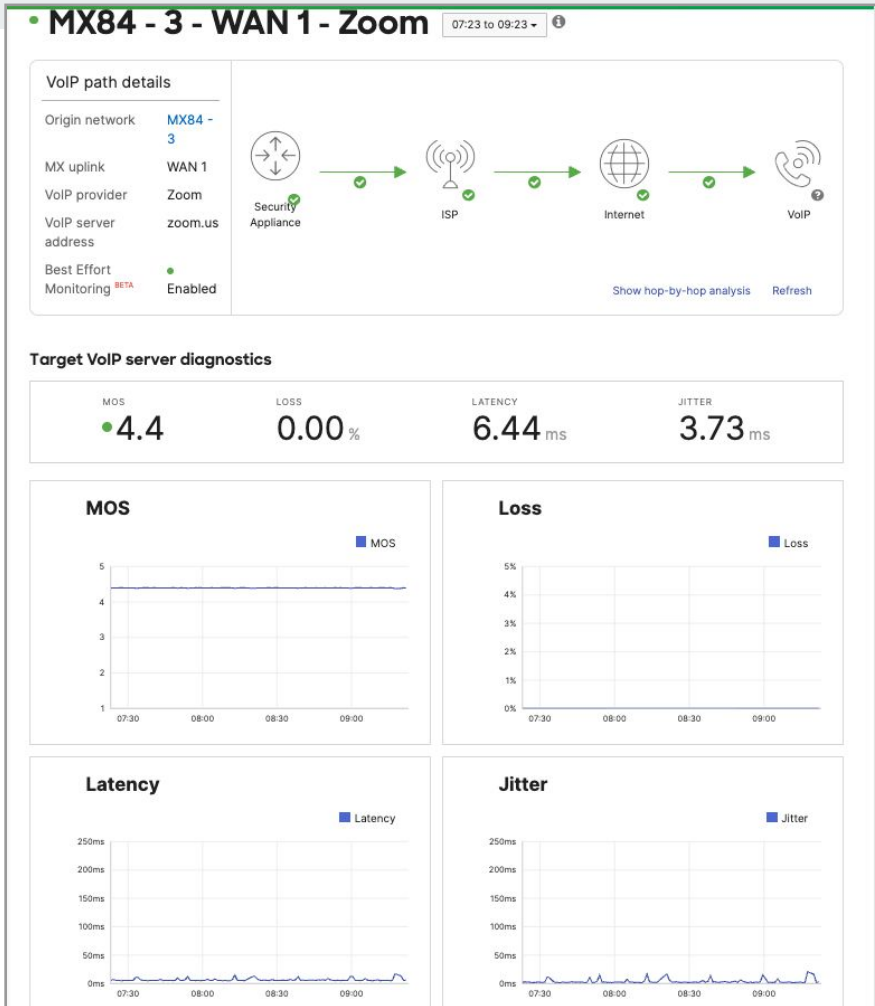
- Full or Split tunnel based on DSCP tags( Diffserv).

Example :

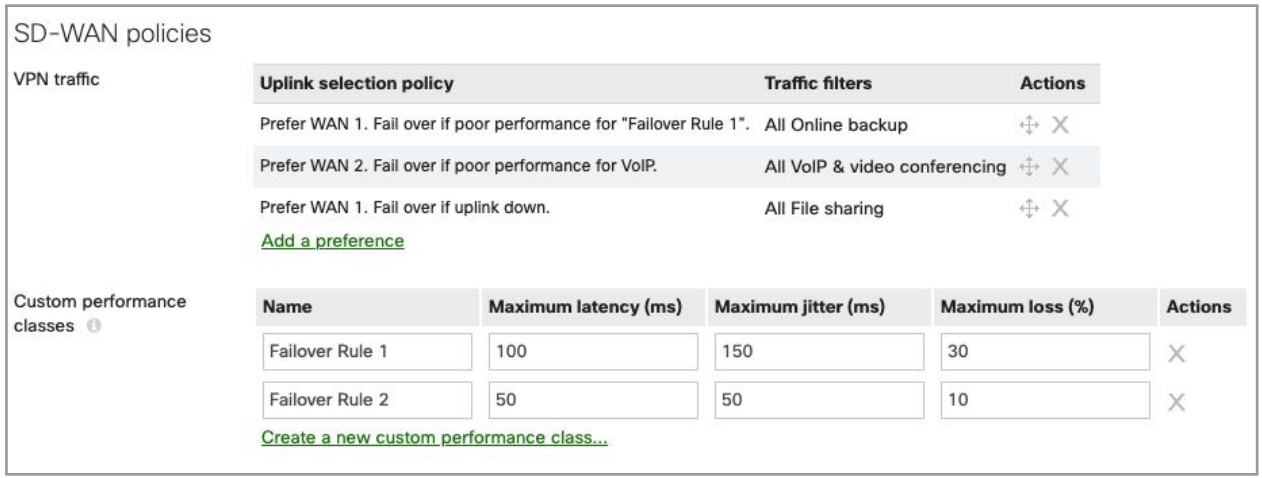
| Traffic Type | DSCP tag |
| --- | --- |
| SIP (Voice) | 46 (EF - Expedited Forwarding, Voice) |
| All Advertising, All Software Updates, All Online Backups | 10 (AF11 - High Throughput, Latency Insensitive, Low Drop) |
| WebEx, Skype | 34 (AF41 - Multimedia Conferencing, Low Drop) |
| All Video & Music | 18 (AF21 - Low Latency Data, Low Drop) |

- Weighted round robin order or ECMP
- Traffic Shaping generic rules based on
  - QoS ( such as MOS, jitter other customized score)
  - Attributes such as app type or address
  - Client identifier based rules

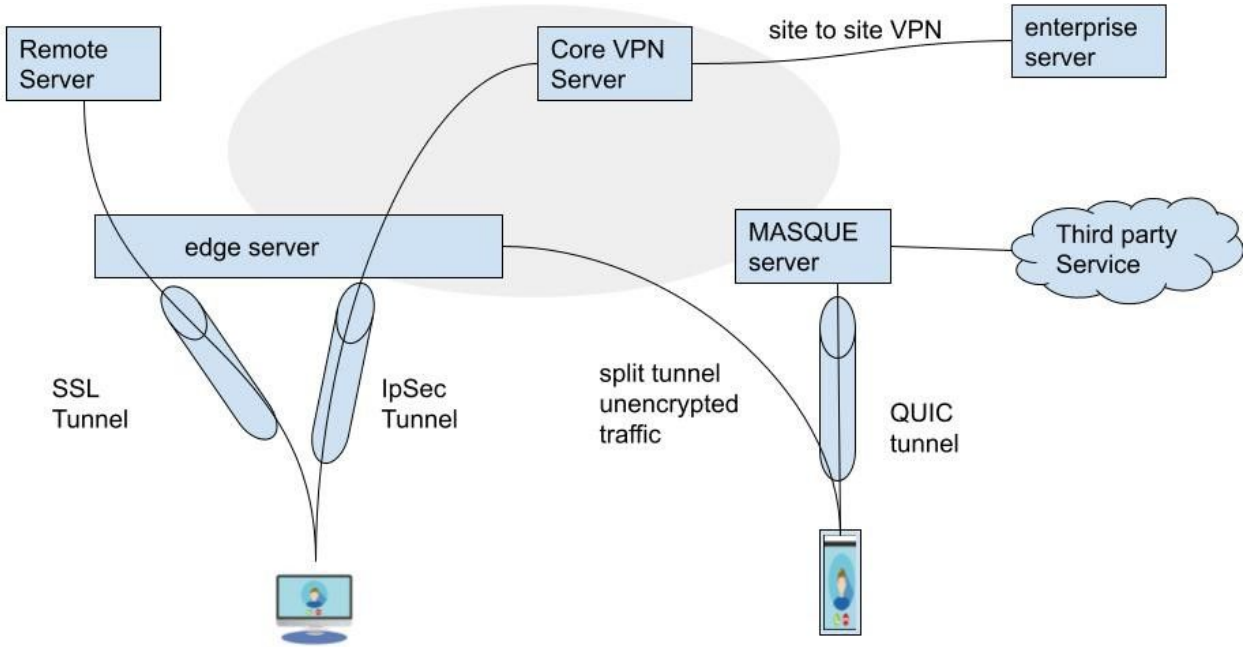


- Policy-Based routing
  - Flow preferences to pin traffic to a particular path.
  - Geo or proximity based rules.



- Dynamic Path Selection such as Network Based Application Recognition (NBAR) from Cisco
- MASQUE
  - QUIC multiplexing



# Standardised Algorithm for preferred Path Selection

# Overcomes

counter productive use cases as

- added latency on real time streaming
- added encryption for already end-to-end encrypted VoIP calls

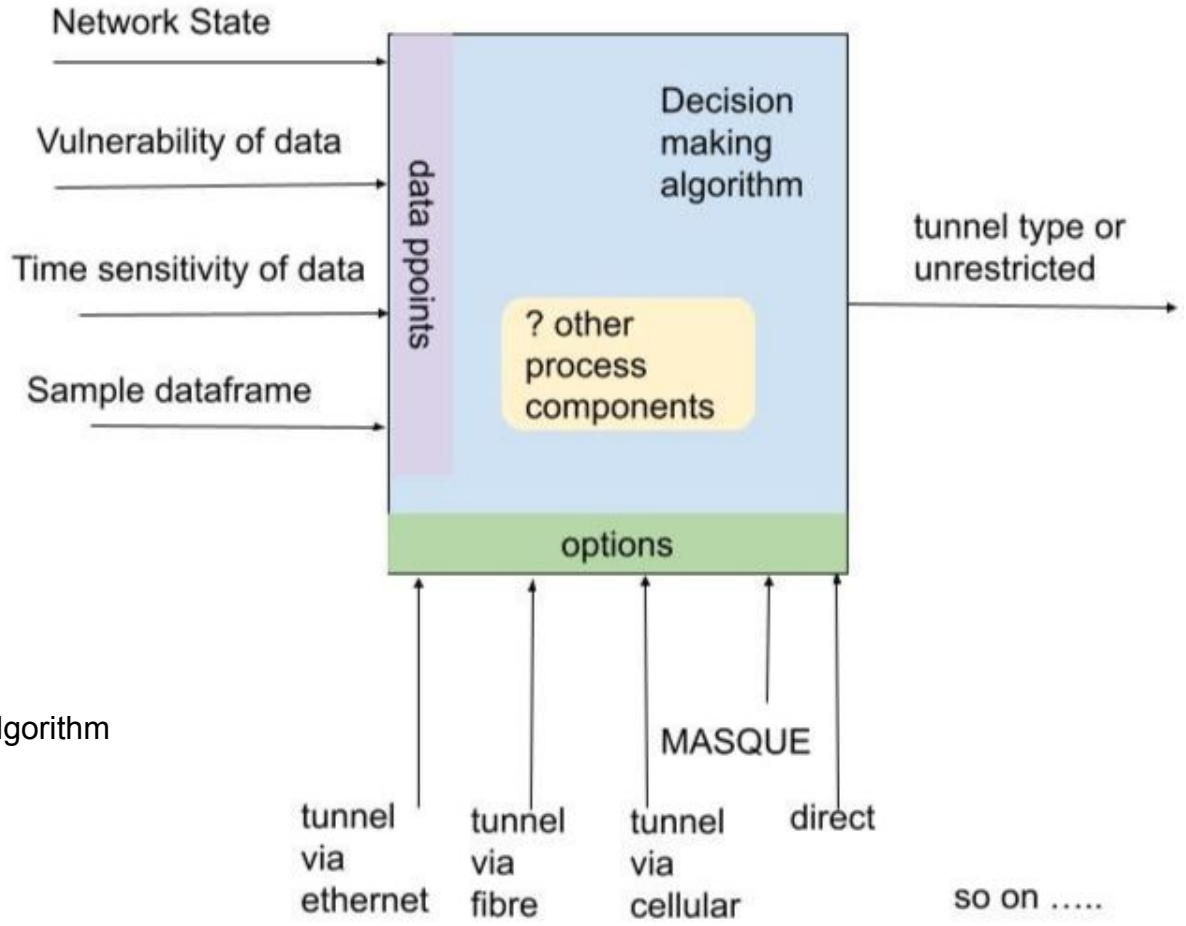
NAT traversal nightmare

nested tunneling and double congestion control

exhausting limited bandwidth available from VPN providers

strategies which unfairly maximize bandwidth usage in the public internet.

# Algorithm for preferred Path Selection



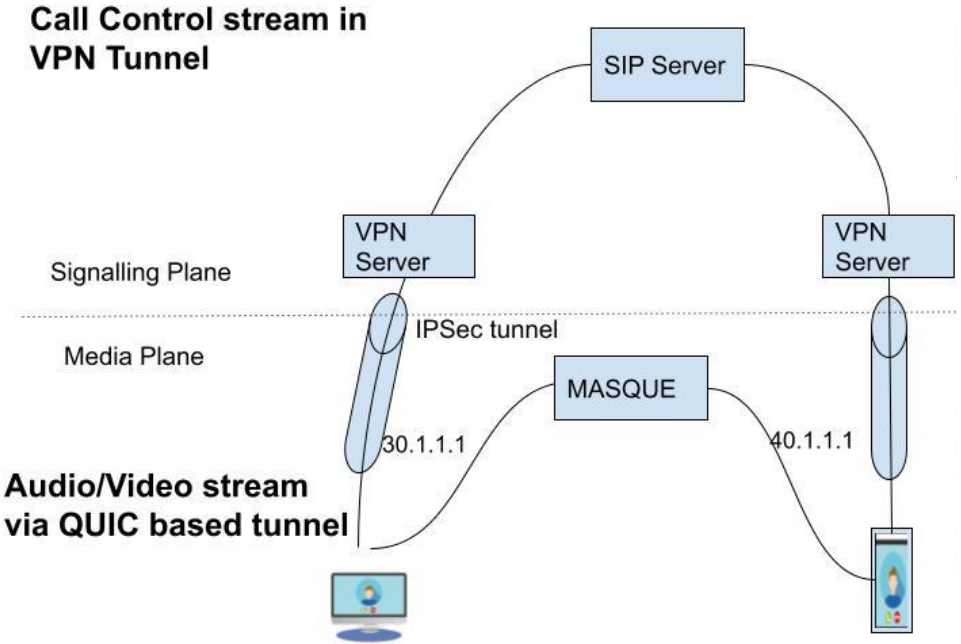

Suggestive data points for Decision making algorithm

Invite Discussions on the Algorithm itself

# Sample decisions

1. Direct connection for resource intensive application such as multiplayer games

2. Tunneling the VoIP traffic via separate routes,
   - signaling plane data on VPN tunnel,
   - media via MOQ.



# Sample decisions cont.

3. SIP trunk calls may actually benefit from a dedicated IPSec tunnel, pre NATed, pre authenticated and secure, as it would avoid the delay in resetting the path given the volume of calls expected between two endpoints.

4. Heavy file downloads such as VoD could benefit by load sharing between multiple tunnels.

# Thank you !

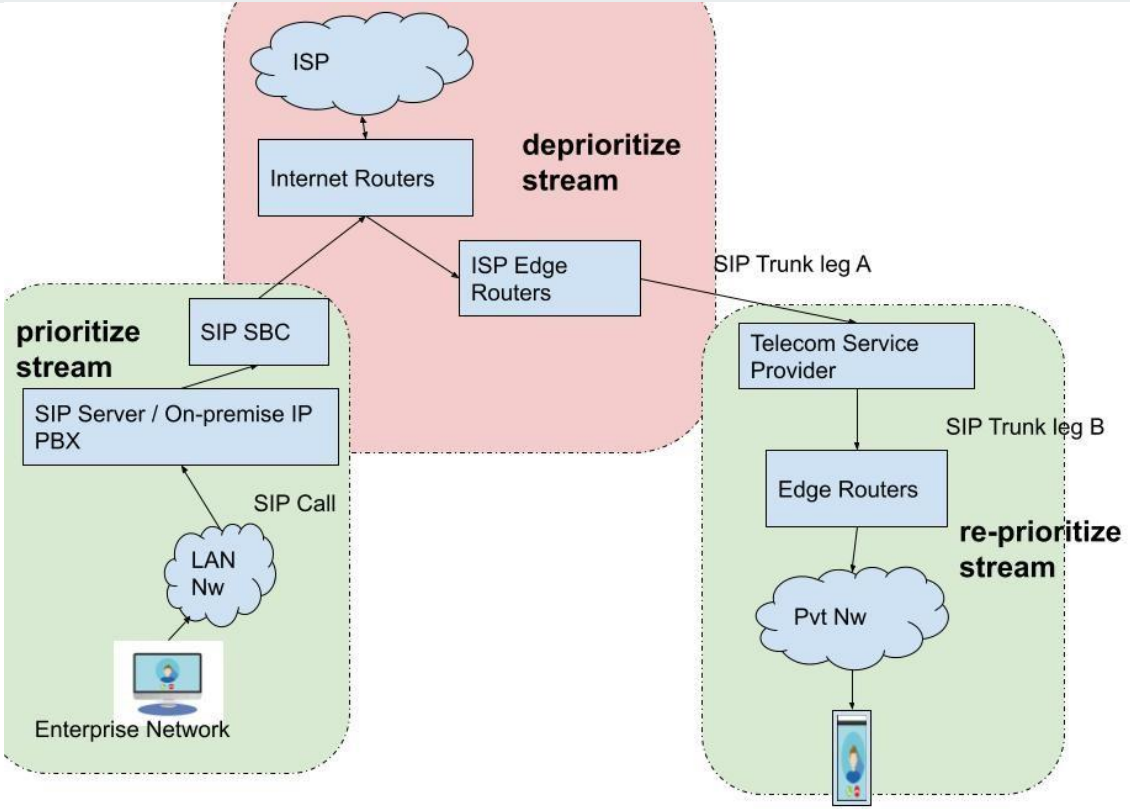
Email : altanai@outlook.com

# Scope of Further research

# Mismatched prioritization across networks

- Packet marking and queuing of other non critical traffic to optimize for real time streams
- VPN providers, CSPs and/or ISP may employ polar-opposite algorithms to shape traffic based on their interest

# Non-synchronized path handling




Same stream prioritized in some networks and deprioritized in others

# Advantages of standardized Path selection decision making algorithm

- ensure same treatment of the stream across heterogeneous networks
- edge gateway can decide if data is send to core VPN system be NATed and sent out unencapsulated.