MKA over IP/UDP

Authors:

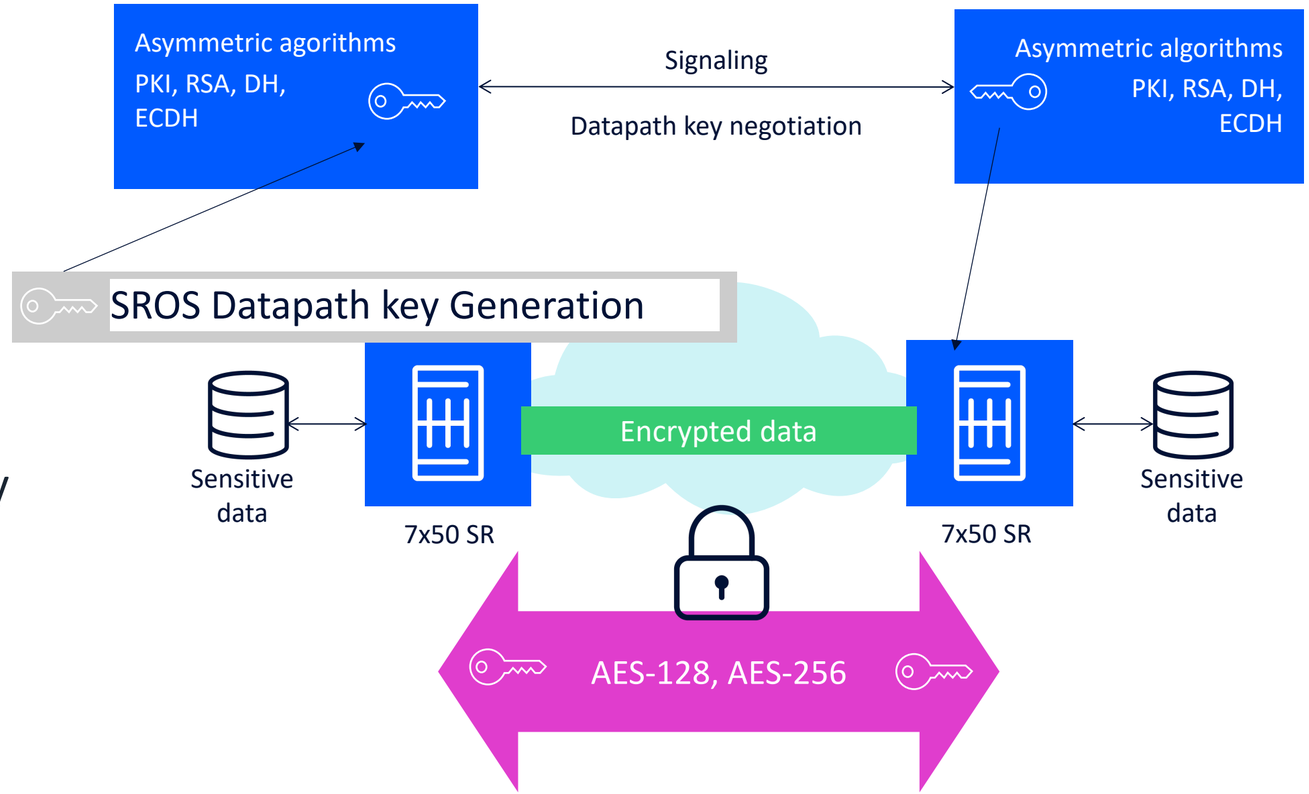
Hooman Bidgoli, Nokia
Nabeel Cocker, Redhat
Nicklous Morris, Verizon

IETF 118, Nov 2023 Prague

PQC issue with current encryption protocols

SSH, TLS, IPSec

- Symmetric keys, both Bob and Alice need to have the same key to encrypt and decrypt
  - Strong security
  - Key distribution can be the point of attack
- Asymmetric Keys, solves the exchange problem that plagued symmetric encryption. It does so by creating two different cryptographic keys (hence the name asymmetric encryption) — a private key and a public key
  - RSA, DSA, DH, ECDH
  - Longer Key lengths to achieve same security as symmetric keys
  - more processing overhead



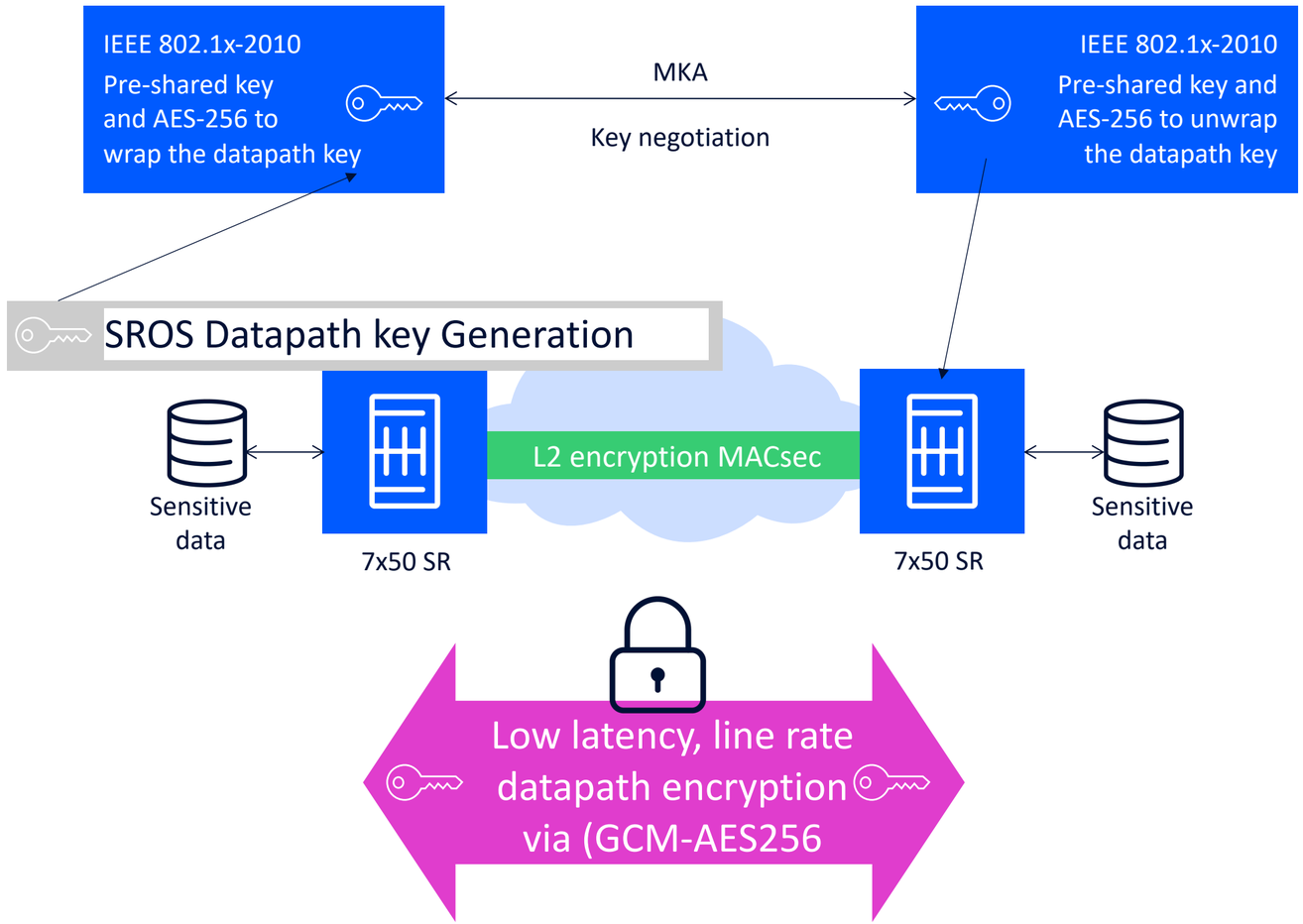
IEEE 802.1AE

Post quantum safe

- MACsec Key Agreement (MKA) uses Pre-Shared Key (PSK) to encrypt the datapath symmetric key (SAK)
  - PSK is a form of Symmetric Encryption, with length of 64 Hex (AES-256) or 32 Hex (AES-128)
  - CMAC-AES-128/256 to Encrypt the SAK
- SAK is generated from Random Number Generator of the SROS
  - Deviation Function uses the RNG to generate 128 bit or 256 bit keys for datapath encryption
  - **SROS RNG is (FIPS-140-2 and NIAP Certified)**
  - **Better then 256 bit entropy**

MACsec uses the SAK and GCM-AES-128/256 to create a Post Quantum Safe Transport

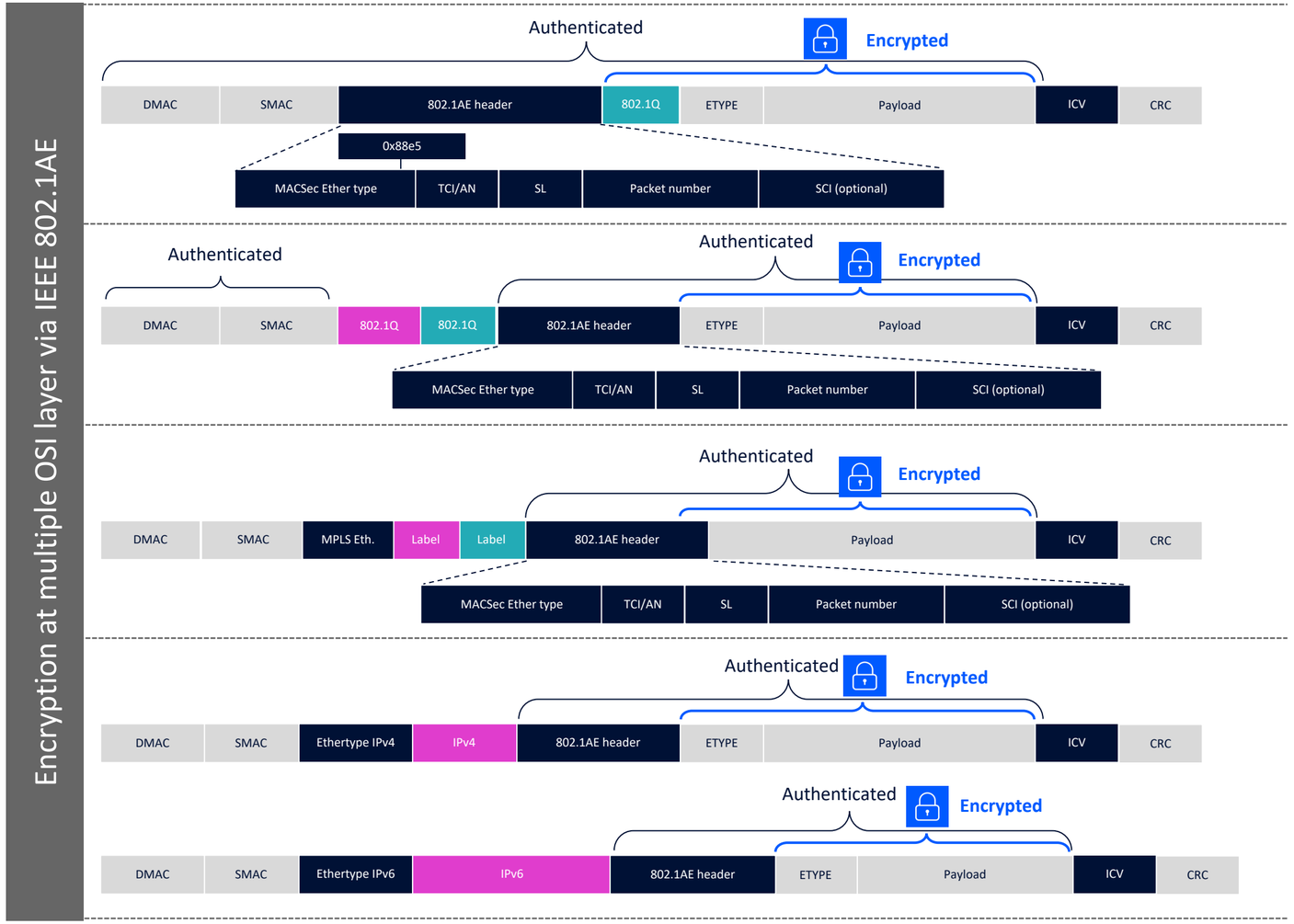
IEEE802.1AE MACsec



IEEE 802.1AE

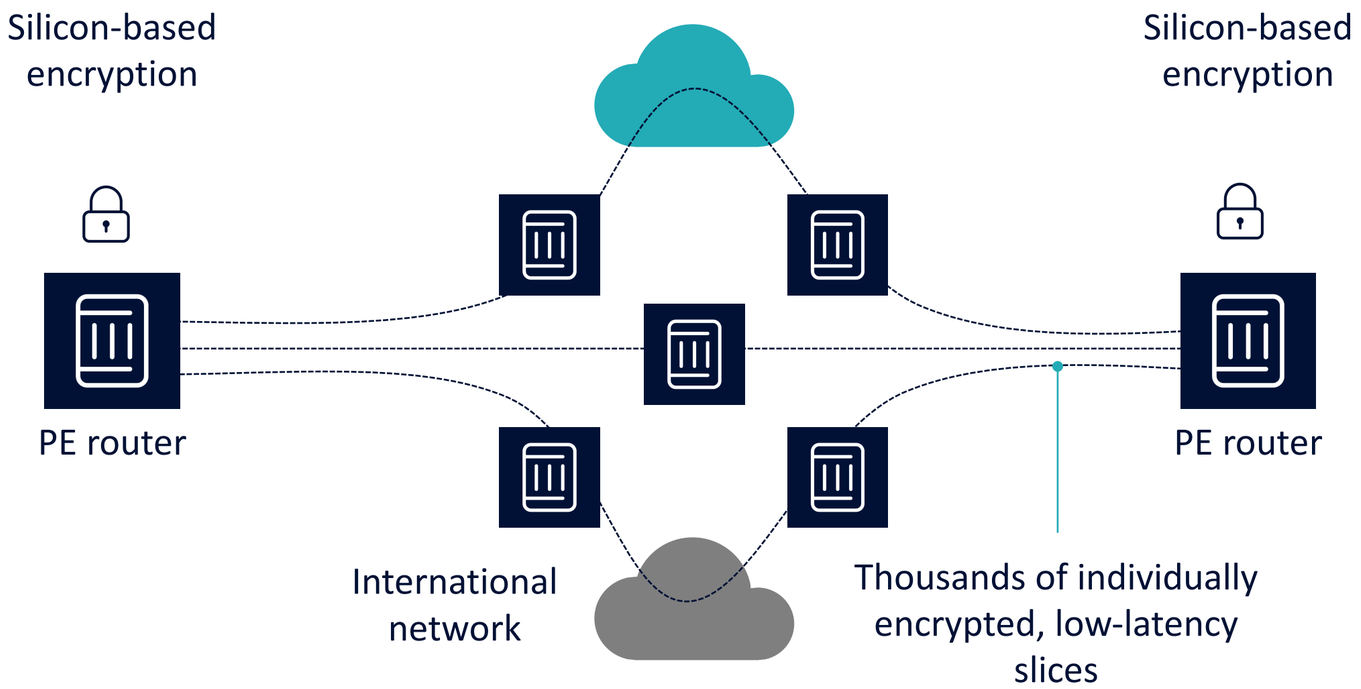
Enhanced

- Programmable encryption and authentication offset
- Capable of leaving L2, L2.5, L3 headers in clear
  - IEEE802.1AE MACSec standard encryption
  - WAN-MODE MACSec encryption, VLAN tags in clear
  - MPLS and services encryption, by leaving the MAC header, VLAN tags and MPLS label in clear
  - IPv4/IPv6 encryption, providing an alternative to IPSec. Leaving MAC, VLAN Tags and the IP header in clear
- Achieving encryption for multiple OSI layers via a single standard (IEEE802.1AE)



Highly secure, low latency line rate encryption

Post quantum safe encryption



Quantum Safe Encryption

- GCM-AES 256, IP/MPLS encryption
- Managed end-to-end encrypted services
- Reuses IEEE802.1AE and IEEE802.1x (MKA)

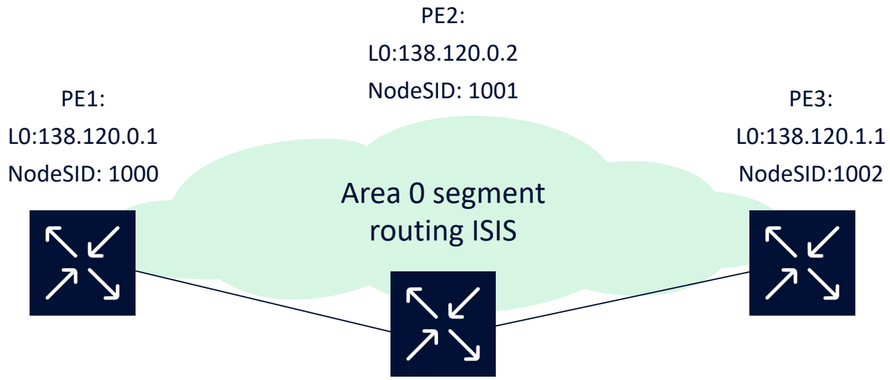
Encrypt existing services

- No need to re-engineer your network or services
- ANYsec encrypts existing tunnels with a flip of a switch
- Transparent to transit/LSR router

Encryption suited for any type of network

- Latency prune or low latency
- Encrypt at any network speed

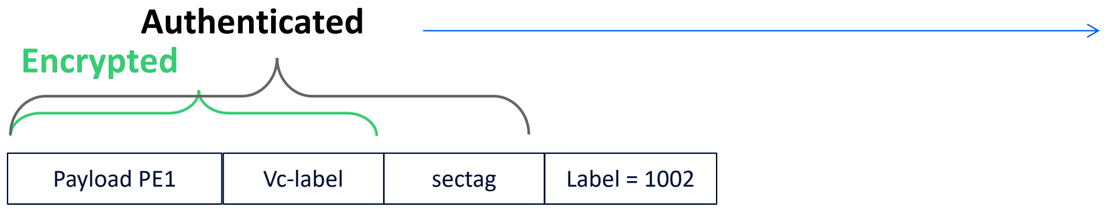
Traffic flow



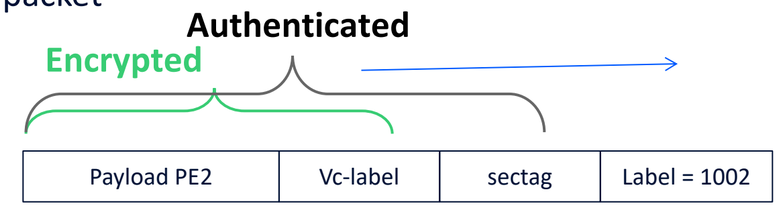
FP5 L3 TCAM encryption table			
Match label	Key 1	Key 2	Active key
1002	SAK-1	SAK-2	SAK-1

FP5 L3 TCAM encryption table			
Match label	Key 1	Key 2	Active key
1002	SAK-3	SAK-4	SAK-1

FP5 L3 TCAM decryption table		
Match label	Key 1	Key 2
1002	SAK-1	SAK-2



PE1 generated packet



PE2 generated packet

```
configure
|-+anysec
   |-+encryption-group 1
      |-+connectivity-association 1
      |-+ local-ip:138.120.0.1
      |-+ peers
         |-+ peer-ip: 138.120.1.1
```

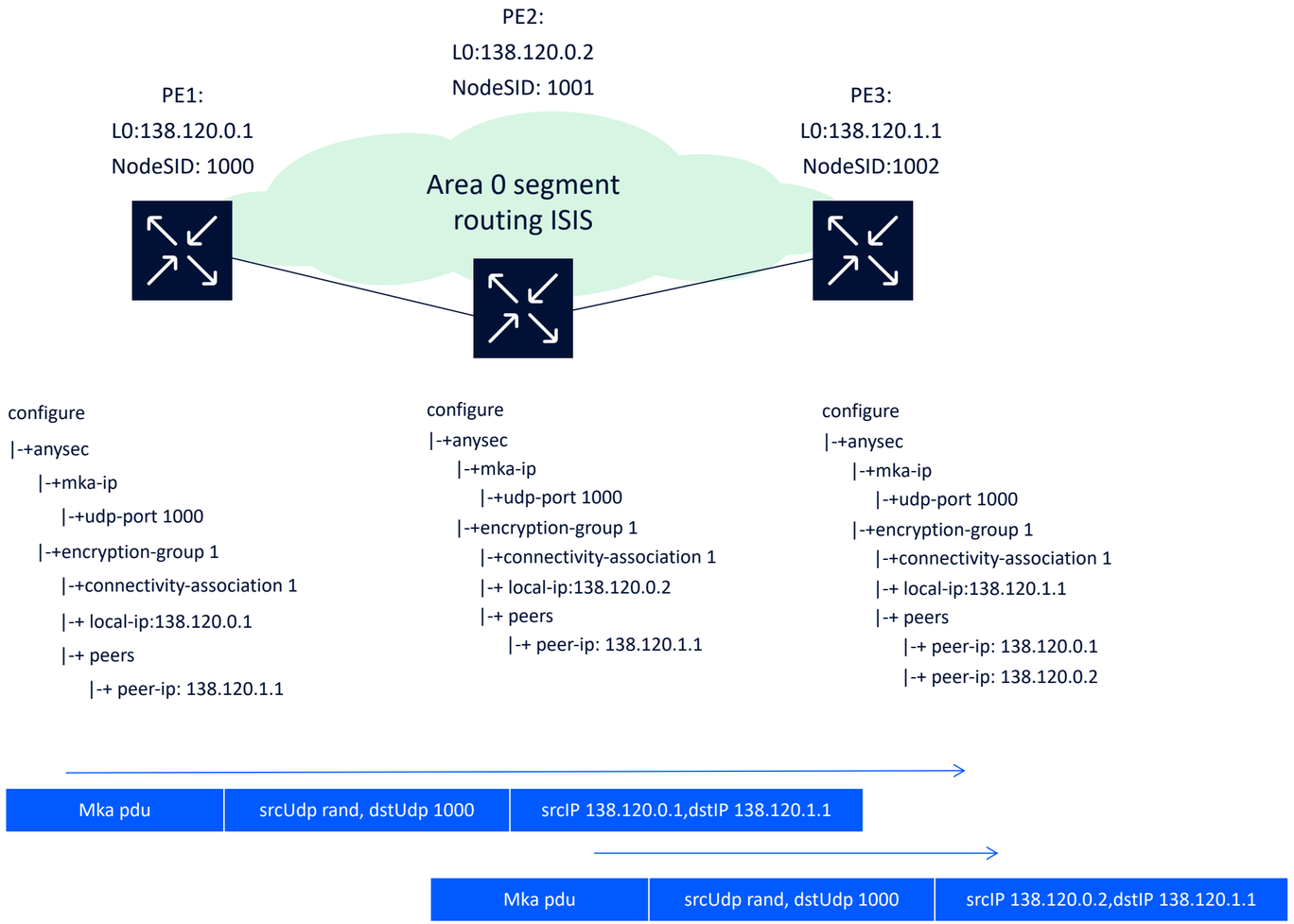
```
configure
|-+anysec
   |-+encryption-group 1
      |-+connectivity-association 1
      |-+ local-ip:138.120.0.2
      |-+ peers
         |-+ peer-ip: 138.120.1.1
```

```
configure
|-+anysec
   |-+encryption-group 1
      |-+connectivity-association 1
      |-+ local-ip:138.120.1.1
      |-+ peers
         |-+ peer-ip: 138.120.0.1
         |-+ peer-ip: 138.120.0.2
```

Tunnel encryption

- Any service ridding these tunnels will be encrypted

MKA over UDP/IP



Encryption key signaling via MKA

- MACSec key agreement over IP/UDP
- Configurable UDP port to extract MKA packets at destination
- MKA IP, source and destination IP address is based the configured “local-ip” and “peer-ip”