SDWAN Edge Discovery

draft-dunbar-idr-sdwan-edge-discovery-03

Linda Dunbar
Sue Hares
Robert Raszuk
Kausik Majumdar
August 2021
SDWAN DRaft

• Use case: BESS/RTGWG drafts
• New Tunnel type (SDWAN-Hybrid)
  – Client routes: link to hybrid tunnel with IP-Sec (U1)
  – Tunnel next hop (SAFI-DSWAN Hybrid) – pass information regarding tunnel (IP-SEC SA, end point, Encaps)
• Purpose of Discussion: Answer questions
SDWAN topology (from IETF 109-110)

**BGP Route Controller - RR**

**MP-NLRI:** (AFI/Safi = 1/1)
Prefix: 10.1.1.x; 20.1.1.x
Nexthop: 2.2.2.2 /* C-PE-2 */
Encapsulation Extended Community: TunnelType = SDWAN-Hybrid
Color Extended Community: Color = RED

**L3VPN path**

- **C-PE 1**
  - lo: 1.1.1.1
  - ISP: 192.10.0.10
  - Client Route: 11.1.1.x

- **C-PE 2**
  - lo: 2.2.2.2
  - ISP1: 192.0.0.1
  - ISP2: 170.0.0.1
  - Client Route: 20.1.1.x

- **C-PE 3**
  - lo: 3.3.3.3
  - Client Route: 30.1.1.x

- **ISP3:** 192.10.0.10
  - Client Route: 20.1.1.x

**To indicate multiple types of underlay networks:** MPLS VPN, IPsec, etc.

**BGP UPDATE 1**

- Nexthop: x.x.x.x
- NLRI: SAFI = SDWAN
- Tunnel Encap Attr (SDWAN-Hybrid)
  - Tunnel-egress-endpoint SubTLV
  - GRE tunnel (via the L3VPN)
  - IPsec SA-ID Sub-TLVs

**BGP UPDATE 2**

- Nexthop: x.x.x.x
- NLRI: SAFI = SDWAN
- Tunnel Encap Attr (SDWAN-Hybrid)
  - Tunnel-egress-endpoint SubTLV
  - GRE tunnel (via the L3VPN)
  - IPsec SA-ID Sub-TLVs

Port 170.0.0.1 has multiple IPsec SAs
IPsec SA (RED) -> C-PE1
IPsec SA (Purple) -> C-PE3
Hybrid Tunnels: with Pre-configured IPsec SA IDs

Tunnel Type = SDWAN-Hybrid

- Site-Type = 1 (No GeoLoc SubTLV);
- Port-Local-ID = * (apply to all ports);
- Color (to correlate with client route UPDATE)

Node-ID

Tunnel Egress Endpoint Sub-TLV

GRE sub-TLV for (L3VPN Path)

IPsec-SA-ID sub-TLV #1

VxLAN sub-TLV

IPsec-SA-ID sub-TLV #2

multiple underlays tunnels
Hybrid Tunnels: with detailed IPsec SA sub-TLVs

- Tunnel Type = SDWAN-Hybrid
- Site-Type = 1 (No GeoLoc SubTLV)
- Port-Local-ID = # (apply to all ports)
- Color: to correlate with the client routes
- Node-ID

SDWAN NLRI

- Tunnel-Egress-Endpoint-SubTLV
- Extended Port Sub-TLV (Optional) or use Tunnel end point sub-TLV to describe the WAN Port Address
- IPsec SA Nonce Sub-TLV
- IPsec SA Public Key Sub-TLV
- IPsec SA Proposal Sub-TLV with Num Transforms
  {Transforms Substructure Sub-sub TLV}

multiple underlays tunnels
**NLRI: SDWAN-Hybrid SAFI = 74**

- **Site Type:**
  - Site-Type = 1: For simple deployment, with node ID to identify the precise geolocation.
  - Site-Type = 2: For large SDWAN heterogeneous deployment where a Geo-Loc Sub-TLV [LISP-GEOLoc] is used to identify the precise geolocation.

- **Port local ID:** SDWAN edge node Port identifier, which is locally significant. If the SDWAN NLRI applies to multiple ports, this field is NULL.

- **SDWAN-Color:** to correlate with the Color-Extended-community included in the client routes UPDATE.

- **Node-ID:** The node’s IPv4 or IPv6 address.
Backup slides
Tunnel Path Attributes and Sub-TLVs inside the SDWAN NLRI
Extended Port (NAT) Sub-TLV

Flags:
- I bit (CPE port address or Inner address scheme)
  - If set to 0, indicate the inner (private) address is IPv4.
  - If set to 1, it indicates the inner address is IPv6.
- O bit (Outer address scheme):
  - If set to 0, indicate the public (outer) address is IPv4.
  - If set to 1, it indicates the public (outer) address is IPv6.
- R bits: reserved for future use. Must be set to 0 now.

NAT Type:
- without NAT; 1:1 static NAT; Full Cone; Restricted Cone; Port Restricted Cone;
- Symmetric; or Unknown (i.e. no response from the STUN server).

Encap Type:
- the supported encapsulation types for the port facing public network, such as
  - IPsec+GRE, IPsec+VxLAN, IPsec without GRE, GRE (when packets don’t need encryption)

Transport Network ID:
- Central Controller assign a global unique ID to each transport network;
- RD ID: Routing Domain ID. Need to be global unique.

Local IP:
- The local (or private) IP address of the port; If NAT is not used, this field is set to NULL.

Local Port:
- used by Remote SDWAN edge node for establishing IPsec to this specific port. If NAT is not used, this field is set to NULL.

Public IP:
- The IP address after the NAT.

Public Port:
- The Port after the NAT.
### ISP of the Underlay Network Sub-TLV

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Flag</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Port Type</td>
<td>Port Speed</td>
<td></td>
</tr>
</tbody>
</table>

- **Type**: To be assigned by IANA
- **Length**: 6 bytes.
- **Flag**: a 1 octet value.
- **Reserved**: 1 octet of reserved bits. It SHOULD be set to zero on transmission and MUST be ignored on receipt.

- **Connection Type**: There are two different types of WAN Connectivity. They are listed below as:
  - Wired – 1
  - Wireless – 2
  - LTE – 3
  - 5G – 4

- **Port Type**: There are different types of ports. They are listed below as:
  - Ethernet – 1
  - Fiber Cable – 2
  - Coax Cable – 3
  - Cellular – 4

- **Port Speed**: The port seed is defined as 2 octet value. The values are defined as Gigabit speed.
Two Types of IPsec SA attributes (only use one)
Sub-Sub-TLV

- Full Set: with multiple Sub-TLVs for full suite of IPsec SA attributes
  - Nonce Sub-TLV
  - Public Key Sub-TLV
  - Proposal Sub-TLV: to indicate the number of Transform subTLVs to be included
    - Transforms Substructure Sub-TLV
- Simple Set: Simple Deployment with limited number of parameters
  - One Sub-TLV to represent Public Key, Nonce, ReKey, Transform
Nonce Sub-TLV, Public Key Sub-TLV

- **Nonce Sub-TLV:**

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>ID Length</td>
</tr>
<tr>
<td>IPsec SA ID</td>
</tr>
<tr>
<td>Nonce Data</td>
</tr>
</tbody>
</table>

- **Public Sub-TLV:**

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffie-Hellman Group Num</td>
</tr>
<tr>
<td>Key Exchange Data</td>
</tr>
<tr>
<td>Duration</td>
</tr>
</tbody>
</table>

**IPsec SA ID** - The 2 bytes IPSec SA ID could 0 or non-zero values. It is cross referenced by client route's IPSec Tunnel Encap IPSec-SA-ID or IPSec-SA-Group Sub-TLV in Section 5 of the Draft. When there are multiple IPsec SAs terminated at one address, such as WAN port address or the node address, they are differentiated by the different IPsec SA IDs.
### Simplified IPsec SA attributes advertisement

- **IPsec-simType**: to be assigned by IANA.
- **Flags**: for future usage.
- **Transform (1 Byte)**: the value can be AH, ESP, or AH+ESP.
- **Mode (1 byte)**: Indicate Tunnel Mode or Transport mode.
  - AH (1 byte): AH authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3.
  - ESP (1 byte): ESP authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3.
  - Each SDWAN edge node can have multiple authentication algorithms; send to its peers to negotiate the strongest one. Default algorithm is AES-256.
- **ReKey Counter (Security Parameter Index)**
- **Public Key**: IPsec public key
- **Nonce**: IPsec Nonce
- **Duration**: SA life span.

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec-simType</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Transform</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>ReKey Counter (SPI)</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>key1 length</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>key2 length</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
</tbody>
</table>

- IPsec-simType: to be assigned by IANA.
- Flags: for future usage.
- Transform (1 Byte): the value can be AH, ESP, or AH+ESP.
- Mode (1 byte): Indicate Tunnel Mode or Transport mode.
  - AH (1 byte): AH authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3.
  - ESP (1 byte): ESP authentication algorithms supported, which can be md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3.
  - Each SDWAN edge node can have multiple authentication algorithms; send to its peers to negotiate the strongest one. Default algorithm is AES-256.
- When node supports multiple authentication algorithms, the “Transform Sub-TLV” described by [SECURE-EVPN] can be used to describe the additional algorithms supported by the node.
- ReKey Counter (Security Parameter Index)
- Public Key: IPsec public key
- Nonce: IPsec Nonce
- Duration: SA life span.