Data Center Interconnect Using VPLS over GRE over IPsec on MX Series Routers

Use Case

October 2016
Version 1.0
## Contents

Introduction ............................................................................................................................................................................ 1  
Use Case .................................................................................................................................................................................. 1  
Configuration .......................................................................................................................................................................... 2  
  Interfaces Configuration ..................................................................................................................................................... 2  
  IPsec Configuration ............................................................................................................................................................. 3  
  GRE Configuration ............................................................................................................................................................... 4  
  VPLS Configuration .............................................................................................................................................................. 4  
Verification and Operation ..................................................................................................................................................... 5  
  Route Table Verification ..................................................................................................................................................... 5  
  IPsec Verification ................................................................................................................................................................. 6  
  GRE Verification .................................................................................................................................................................. 6  
  VPLS Verification ................................................................................................................................................................. 7  
  Intersite Traffic Verification ................................................................................................................................................ 8  
Conclusion ............................................................................................................................................................................... 9  
Useful Links and References ................................................................................................................................................... 9
Introduction

MPLS-based Layer 2 VPNs, such as virtual private LAN service (VPLS), are typically used to provide intersite communications between separate Layer 2 domains, such as data centers, over a Wide Area Network (WAN). However, there may be instances where the network providing connectivity between the Layer 2 domains is IP-based and does not support MPLS. A common solution is to use IP-based generic routing encapsulation (GRE) to tunnel the IP and MPLS traffic between sites. As an additional option, you can secure the GRE tunnel within an IP Security (IPsec) VPN tunnel. The resulting solution is known as VPLS over GRE over IPsec.

Use Case

Figure 1 shows a network emulation of two data centers separated by an IP network configured with MX240 routers running Junos OS Release 12.2 R2.4. The endpoints of the GRE and IPsec tunnels are on the onsite routers, R1 and R2. Both of these routers contain a Trio-based MPC in slot 1, and an MS-DPC in slot 2. A single Internet router represents the service provider’s network that provides IP connectivity between the two data center sites.

![Figure 1 – Data Centers Network Separated by an IP Network](image)

An OSPF adjacency forms between the GRE tunnel endpoints. This allows an Internal Border Gateway Protocol (IBGP) session to form through the tunnel for VPLS control plane signaling. Finally, a Resource Reservation Protocol—Traffic Engineering (RSVP-TE) signaled label-switched path (LSP) is signaled between R1 and R2 to provide a forwarding path for VPLS traffic.

To transmit data between the two sites, two Ixia tester ports were configured.
Configuration

The following code shows the configuration for Router 1 (R1). For brevity, the configuration for R2 is not shown because it is essentially configured using similar statements. The MX240 router, which represents the Internet router, is configured with two IP interfaces.

Interfaces Configuration

1. Configure the WAN IP interface on R1.

   set interfaces xe-1/2/0 description "WAN to Site DC2"
   set interfaces xe-1/2/0 unit 0 family inet address 10.13.1.1/24

2. Configure the loopback interface with two IP addresses. The first IP address (for example, 172.16.0.1) is the router-id and runs OSPF, BGP, and MPLS; the second IP address (for example, 198.51.100.11) is the GRE tunnel endpoint.

   set interfaces lo0 unit 0 family inet address 172.16.0.1/32
   set interfaces lo0 unit 0 family inet address 198.51.100.11/32

3. Configure the inside and outside Services Processor, for example, the sp, interfaces. The inside interface receives unencrypted GRE packets. Once the data is encrypted, it is transmitted with the source IP address 192.0.2.10 towards the destination IPsec gateway, R2, through the outside interface. In this network example, the MS-DPC is in slot 2.

   set interfaces sp-2/0/0 unit 1 description "IPsec interface to DC2"
   set interfaces sp-2/0/0 unit 1 family inet address 192.0.2.10/30
   set interfaces sp-2/0/0 unit 1 service-domain inside
   set interfaces sp-2/0/0 unit 2 family inet
   set interfaces sp-2/0/0 unit 2 service-domain outside

Note: You configure the GRE interface in a section described later in this document.
IPsec Configuration

Internet Key Exchange (IKE) and IPsec proposals and policies correspond to the two phases of establishing an IPsec VPN. You group policies in an IPsec rule and then apply them to the service processor interface using a service set, as shown in Figure 2.

![Figure 2 – IKE and IPsec Proposals and Policies](image1)

1. To configure IPsec on the MX Series device, define the IKE policy that references the IKE proposal.

   ```
   set services ipsec-vpn ike proposal IKE-PROPOSAL authentication-method pre-shared-keys
   set services ipsec-vpn ike proposal IKE-PROPOSAL dh-group group5
   set services ipsec-vpn ike proposal IKE-PROPOSAL authentication-algorithm sha1
   set services ipsec-vpn ike proposal IKE-PROPOSAL encryption-algorithm aes-256-cbc
   set services ipsec-vpn ike proposal IKE-PROPOSAL lifetime-seconds 21600
   set services ipsec-vpn ike policy IKE-POLICY mode main
   set services ipsec-vpn ike policy IKE-POLICY proposals IKE-PROPOSAL
   set services ipsec-vpn ike policy IKE-POLICY pre-shared-key ascii-text company123
   ```

2. Configure an IPsec policy that references an IPsec proposal, and configure the MX Series device to establish the IPsec session immediately and not wait for data to establish to the tunnel.

   ```
   set services ipsec-vpn ipsec proposal IPSEC-PROPOSAL protocol esp
   set services ipsec-vpn ipsec proposal IPSEC-PROPOSAL authentication-algorithm hmac-sha1-96
   set services ipsec-vpn ipsec proposal IPSEC-PROPOSAL encryption-algorithm aes-256-cbc
   set services ipsec-vpn ipsec proposal IPSEC-PROPOSAL lifetime-seconds 3600
   set services ipsec-vpn ipsec policy IPSEC-POLICY perfect-forward-secrecy keys group
   set services ipsec-vpn ipsec policy IPSEC-POLICY proposals IPSEC-PROPOSAL
   set services ipsec-vpn establish-tunnels immediately
   ```

3. Define an IPsec VPN rule to specify which traffic to protect, the IP address of the remote router used to terminate the VPN tunnel, and the policies to use. Additionally, configure a static route on R1 to reach the remote router R2 through the WAN.

   ```
   set services ipsec-vpn rule DC2-VPN-RULE term 1 then remote-gateway 10.23.1.2
   set services ipsec-vpn rule DC2-VPN-RULE term 1 then dynamic ike-policy IKE-POLICY
   set services ipsec-vpn rule DC2-VPN-RULE term 1 then dynamic ipsec-policy IPSEC-POLICY
   set services ipsec-vpn rule DC2-VPN-RULE match-direction input
   set routing-options static route 10.23.1.0/24 next-hop 10.13.1.3
   ```

4. Configure a next-hop style service set to apply the VPN rule to the sp interfaces.

   ```
   set services service-set DC2-VPN-SET next-hop-service inside-service-interface sp-2/0/0.1
   set services service-set DC2-VPN-SET next-hop-service outside-service-interface sp-2/0/0.2
   set services service-set DC2-VPN-SET ipsec-vpn-options local-gateway 10.13.1.1
   set services service-set DC2-VPN-SET ipsec-vpn-rules DC2-VPN-RULE
   ```
DCI Using VPLS over GRE over IPsec on MX Series Routers

GRE Configuration

1. Enable tunnel-services on a Packet Forwarding Engine and configure a corresponding GRE tunnel interface, for example, gr-1/3/0. Both IPv4 and MPLS are enabled on the GRE interface so that it can process the protocol packets, including the OSPF, BGP, and RSVP control protocols.

   ```
   set chassis fpc 1 pic 3 tunnel-services
   set interfaces gr-1/3/0 unit 0 description "GRE to DC2"
   set interfaces gr-1/3/0 unit 0 tunnel source 198.51.100.11
   set interfaces gr-1/3/0 unit 0 tunnel destination 203.0.113.2
   set interfaces gr-1/3/0 unit 0 family inet
   set interfaces gr-1/3/0 unit 0 family mpls
   ```

2. Create a static route to direct traffic to the remote GRE tunnel endpoint through the IPsec tunnel.

   ```
   set routing-options static route 203.0.113.2/32 next-hop sp-2/0/0.1
   ```

3. Enable OSPF over the GRE tunnel so that loopback addresses can be advertised for IBGP peering.

   ```
   set protocols ospf traffic-engineering
   set protocols ospf area 0.0.0.0 interface lo0.0 passive
   set protocols ospf area 0.0.0.0 interface gr-1/3/0.0
   ```

VPLS Configuration

1. Define the VPLS access interface.

   ```
   set interfaces xe-1/3/0 encapsulation ethernet-vpls
   set interfaces xe-1/3/0 unit 0 description "LAN for VPLS to DC2"
   set interfaces xe-1/3/0 unit 0 family vpls
   ```

2. Configure MP-BGP required for VPLS signaling.

   ```
   set routing-options autonomous-system 12
   set protocols bgp group iBGP type internal
   set protocols bgp group iBGP local-address 172.16.0.1
   set protocols bgp group iBGP family l2vpn signaling
   set protocols bgp group iBGP neighbor 172.22.0.2
   ```

3. On the GRE interface, enable MPLS and RSVP. Then, create the LSP from the loopback interface of R1 to the loopback interface on R2. This LSP populates the inet.3 route table used to forward VPLS traffic.

   ```
   set protocols rsvp interface gr-1/3/0.0
   set protocols mpls interface all
   set protocols mpls label-switched-path From-DC1-to-DC2 from 172.16.0.1
   set protocols mpls label-switched-path From-DC1-to-DC2 to 172.22.0.2
   set protocols mpls label-switched-path From-DC1-to-DC2 no-cspf
   ```
4. Configure the VPLS instance.

    set routing-instances VPLS instance-type vpls
    set routing-instances VPLS interface xe-1/3/0.0
    set routing-instances VPLS route-distinguisher 172.16.0.1:100
    set routing-instances VPLS vrf-target target:12:100
    set routing-instances VPLS protocols vpls no-tunnel-services
    set routing-instances VPLS protocols vpls site-range 10
    set routing-instances VPLS protocols vpls site DC1 site-identifier 1

Verification and Operation

Route Table Verification

From the `show route` output, the routing table on R1 indicates that the GRE tunnel is up and running. The loopback addresses from R2 have been learned through OSPF.

As shown from the inet.3 table, a packet that enters the VPLS interface on R1 is forwarded to R2 through an LSP using the gr-1/3/0 interface. To reach the remote endpoint of the GRE tunnel, for example, 203.0.113.2, R1 forwards traffic using the static route to the inside services processor interface sp-2/0/0.1. Traffic is then encrypted and forwarded in the IPsec tunnel towards the destination.

user1@R1> show route

inet.0: 15 destinations, 17 routes (15 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

    172.16.0.1/32  *[Direct/0] 5w4d 02:02:40
                     > via lo0.0
    172.22.0.2/32  *[OSPF/10] 01:43:13, metric 1
                     > via gr-1/3/0.0
    10.8.0.0/16    *[Static/5] 5w4d 02:02:40
                     > to 10.8.2.254 via fxp0.0
    10.8.2.0/24    *[Direct/0] 5w4d 02:02:40
                     > via fxp0.0
                      [Direct/0] 5w4d 02:02:35
                     > via fxp0.0
    10.8.2.135/32  *[Local/0] 5w4d 02:02:40
                     Local via fxp0.0
    10.8.2.137/32  *[Local/0] 5w4d 02:02:35
                     Local via fxp0.0
    10.13.1.0/24   *[Direct/0] 04:12:27
                     > via xe-1/2/0.0
    10.13.1.1/32   *[Local/0] 04:12:27
                     Local via xe-1/2/0.0
    10.23.1.0/24   *[Static/5] 02:03:13
                     > to 10.13.1.3 via xe-1/2/0.0
    198.51.100.11/32 *[Static/5] 02:03:51
                     > to 10.13.1.3 via xe-1/2/0.0
    198.51.100.12/32 *[Static/5] 02:03:51
                     > via sp-2/0/0.1
    203.0.113.2/32  *[Static/5] 02:03:51
                     > via sp-2/0/0.1
                      [OSPF/10] 01:43:13, metric 1
                     > via gr-1/3/0.0
    100.0.0.8/30    *[Direct/0] 02:03:51
                     > via sp-2/0/0.1
    192.0.2.10/32   *[Local/0] 02:03:51
                     Local via sp-2/0/0.1
    172.16.0.0/12   *[Static/5] 5w4d 02:02:40
DCI Using VPLS over GRE over IPsec on MX Series Routers

> to 10.8.2.254 via fxp0.0
224.0.0.5/32  *[OSPF/10]  ld 00:41:13, metric 1
MultiRecv

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.22.0.2/32  *[RSVP/7/1] 01:42:43, metric 1
> via gr-1/3/0.0, label-switched-path From-DC1-to-DC2

**IPsec Verification**

The following CLI commands output show that both IKE and IPsec are operating normally. IPsec VPN tunnels are unidirectional.

user1@R1> show services ipsec-vpn ike security-associations
Remote Address State Initiator cookie Responder cookie Exchange type
10.23.1.2 Matured 267f60c8acd2ebbb baa178c991ad541e Main
{master}
user1@R1> show services ipsec-vpn ipsec security-associations
Service set: DC2-VPN-SET, IKE Routing-instance: default
Rule: DC2-VPN-RULE, Term: 1, Tunnel index: 1
Local gateway: 10.13.1.1, Remote gateway: 10.23.1.2
IPSec inside interface: sp-2/0/0.1, Tunnel MTU: 1500
Direction SPI AUX-SPI Mode Type Protocol
inbound 1760940036 0 tunnel dynamic ESP
outbound 3786679352 0 tunnel dynamic ESP

user1@R1> show services ipsec-vpn ipsec statistics
PIC: sp-2/0/0, Service set: DC2-VPN-SET
ESP Statistics:
Encrypted bytes: 2110183872
Decrypted bytes: 2118356032
Encrypted packets: 7328594
Decrypted packets: 7356966

**GRE Verification**

To verify the status of the GRE tunnel, use the show interfaces interface detail CLI command to review the interface details and statistics.

user1@R1> show interfaces gr-1/3/0 detail
Physical interface: gr-1/3/0, Enabled, Physical link is Up
Interface index: 156, SNMP ifIndex: 635, Generation: 159
Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 100000mbps
Hold-times : Up 0 ms, Down 0 ms
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes : 1986650571 2047568 bps
Output bytes : 1948243752 2015568 bps
Input packets: 7762202 999 pps
Output packets: 7731126 999 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Logical interface gr-1/3/0.0 (Index 333) (SNMP ifIndex 637) (Generation 145)
Flags: Point-To-Point SNMP-Traps 0x4000 IP-Header
Encapsulation: GRE-NULL
Copy-tos-to-outer-ip-header: Off
Gre keepalives configured: Off, Gre keepalives adjacency state: down
Traffic statistics:
Input bytes: 1986650571
Output bytes: 1948526938
Input packets: 7762202
Output packets: 7733834
Local statistics:
Input bytes: 218315
Output bytes: 283186
Input packets: 2701
Output packets: 2708
Transit statistics:
Input bytes: 1986432256 2047568 bps
Output bytes: 1948243752 2015568 bps
Input packets: 7759501 999 pps
Output packets: 7731126 999 pps

Protocol inet, MTU: 9168, Generation: 164, Route table: 0
Flags: Sendbcast-pkt-to-re
Protocol mpls, MTU: 9156, Maximum labels: 3, Generation: 165, Route table: 0
Flags: Is-Primary

VPLS Verification

If the GRE tunnel is in the up state, then OSPF adjacency, BGP peer, and LSP should be also be in the up state.

user1@R1> show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.22.0.2          gr-1/3/0.0             Full      172.22.0.2          128    37

user1@R1> show mpls lsp
Ingress LSP: 1 sessions
To              From            State  Rt P     ActivePath       LSPname
172.22.0.2         172.16.0.1         Up     0 *                      From-DC1-to-DC2
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions
To              From            State  Rt Style Labelin Labelout LSPname
172.16.0.1         172.22.0.2         Up       0  1 FF       3        - From-DC2-to-DC1
Total 1 displayed, Up 1, Down 0

user1@R1> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table         Tot Paths  Act Paths Suppressed  History Damp State  Pending
bgp.l2vpn.0    1           1            0          0          0          0
Peer          AS  InPkt  OutPkt  OutQ  Flaps  Last Up/Dwn
State|Active/Received/Accepted/Damped...
bgp.l2vpn.0: 1/1/1/0
VPLS-100.12vpn.0: 1/1/1/0
As a result, the VPLS connection to Data Center 2 (DC2) is up.

user1@R1> show vpls connections
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid  NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch  WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down  NP -- interface hardware not present
CM -- control-word mismatch  -> -- only outbound connection is up
CN -- circuit not provisioned  <- -- only inbound connection is up
OR -- out of range         Up -- operational
OL -- no outgoing label     Dn -- down
LD -- local site signaled down  CF -- call admission control failure
LD -- local site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated  RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch           MI -- Mesh-Group ID not available
BK -- Backup connection      ST -- Standby connection
PF -- Profile parse failure  PB -- Profile busy
RS -- remote site standby    SN -- Static Neighbor
LB -- Local site not best-site  RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: VPLS-100
Local site: DC1 (1)

<table>
<thead>
<tr>
<th>connection-site</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>rmt</td>
<td>Up</td>
<td>Jan 9 11:52:51 2013</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote PE: 172.22.0.2, Negotiated control-word: No
Incoming label: 262146, Outgoing label: 262145
Local interface: lsi.1048576, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS-100 local site 1 remote site 2

{master}

user1@R1> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : VPLS-100
Bridging domain : __VPLS-100__, VLAN : NA

MAC     MAC Logical
address  flags interface
00:00:23:d5:f0:03  D      xe-1/3/0.0
00:00:38:6d:b7:26  D      lsi.1048576

Intersite Traffic Verification
Using IxNetwork, the two Ixia tester ports were configured to transmit bidirectional traffic between the two data center sites. It was confirmed that the traffic flows were received without packet loss in both directions.

<table>
<thead>
<tr>
<th>Source/Dest Endpoint Pair</th>
<th>Tx Frames</th>
<th>Rx Frames</th>
<th>Frames Delta</th>
<th>Loss %</th>
<th>Tx Frame Rate</th>
<th>Rx Frame Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.33-192.168.1.31</td>
<td>86,843</td>
<td>86,843</td>
<td>0</td>
<td>0.000</td>
<td>1,000,000</td>
<td>1,000,000</td>
</tr>
<tr>
<td>192.168.1.33-192.168.1.31</td>
<td>86,843</td>
<td>86,843</td>
<td>0</td>
<td>0.000</td>
<td>1,000,000</td>
<td>1,000,000</td>
</tr>
</tbody>
</table>
Conclusion

This use case documents the configuration and verifies the functionality of VPLS over GRE over IPsec. It is meant to be a starting point for more advanced configurations.

Useful Links and References

- Juniper Networks TechLibrary for product documentation http://www.juniper.net/documentation/
