APPLICATION BULLETIN

NUMBER: AB18001
April 2018

MDS Orbit Series

GE MDS, LLC. 175 Science Parkway, Rochester, NY 14620 USA

Phone +1 (585) 242-9600, FAX +1 (585) 242-9620 Web: www.gemds.com

Orbit MCR/ECR IPsec VPN Interoperability

Introduction

This document describes various types of IPsec VPN setups that are supported by Orbit and their interoperability with third party IPsec VPN devices.

Scope

This bulletin is intended for system engineers and end users who would like to understand the Orbit IPsec VPN interoperability with third party devices.

Firmware Compatibility

This is bulletin is applicable to Orbit MCR devices running firmware version 6.1.2 or greater.

Terms

ACL	Access Control List
CLI	Command Line Interface
DMVPN	Dynamic Multipoint VPN
GRE	Generic Routing Encapsulation
NHRP	Next Hop Resolution Protocol
SA	Security Association
VPN	Virtual Private Network
VTI	Virtual Tunnel Interface

General Information

The IPsec based VPNs can be classified at a high level into route-based VPNs and policy-based VPNs.

Route Based VPN

Route-based tunnels are represented in the device as a virtual network interfaces and allow any arbitrary traffic to be sent over them. The routes can be configured statically or dynamically using routing protocols. The route-based VPNs are classified further into following types:

IPsec Tunnel Mode Based

The IPsec tunnel is represented as a virtual interface and IPsec tunnel mode is used with implicit local and remote traffic selectors of 0.0.0.0/0. This allows any traffic to match the IPsec policy. The traffic on particular tunnel interface (like st0.0 on JUNOS or Cisco VTI) is tied to a particular IPsec VPN connection by explicit binding. The tunnel can further be in following modes:

- *Point-to-Point Mode* – A unique tunnel interface is required for each peer.
- *Point-to-Multipoint Mode* – A single multipoint tunnel interface can be used for all peers.

GRE Tunnel Based

The GRE tunnel is represented as a virtual interface. The GRE traffic is then protected with transport mode IPsec SA. The tunnel can further be in following modes:

- *Point-to-Point – A unique tunnel interface is required for each peer.*
- *Point-to-Multipoint – A single multipoint tunnel interface can be used for all peers (see DMVPN below).*

Policy-Based VPN

Policy based VPNs using IPsec tunnel mode and explicitly specify the traffic that needs to be sent via the tunnel using traffic selectors (e.g. local-ip-subnet/remote-ip-subnets on Orbit or by security policies in JUNOS or by traffic selectors on st0 interface on JUNOS etc.) in IPsec connection configuration. The tunnel is not represented by a virtual interface. Any traffic that does not match policy, cannot enter the tunnel. In such configuration, dynamic routing protocols cannot be used since arbitrary traffic to advertised subnets cannot be sent via the tunnel. This is the most interoperable mode between devices from different vendors.

Deployment Considerations

For large scale deployments, where remotes need to scale to thousands and/or where failover is desired between tunnels across two HUB routers, route-based tunnels are preferred since dynamic routing protocols like BGP can be used for exchanging routes and for failover across HUB routers.

- Cisco DMVPN is one mechanism to achieve such a setup using Cisco ISR/ASR HUB routers. DMVPN is an open standard and combines multipoint GRE, IPsec transport mode SA and NHRP to build scalable hub-n-spoke VPNs. In this setup, any dynamic routing protocol can be used and arbitrary traffic can be sent over the tunnel.
- Juniper AutoVPN in point-to-multipoint mode is another mechanism but it uses proprietary signaling. Hence, both Hub and Spoke need to be SRX devices.
  https://www.juniper.net/us/en/local/pdf/app-notes/3500214-en.pdf

Interoperability Considerations

GE MDS Orbit

- Orbit supports policy-based VPN tunnels (net-to-net IPsec connection). This mode **is interoperable** with all third-party devices that implement policy-based VPNs.
- Orbit does not support route-based VPN tunnels using IPsec tunnel mode. Therefore, it is **not interoperable** with route-based VPNs as implemented by Juniper JUNOS or Cisco IOS/IOS-XE.
- Orbit supports route-based VPN tunnels using GRE tunnels protected by **transport** mode IPsec SA (host-to-host IPsec connection). Both point-to-point and point-to-multipoint modes (DMVPN) are supported. This mode **is interoperable** with Cisco DMVPN.

Cisco IOS/IOS-XE

- Cisco IOS/IOS-XE supports policy-based VPN tunnels using crypto-map directive (on the physical interface) that references an ACL with traffic selector configuration.
- Cisco IOS/IOS-XE supports route-based VPN tunnels using IPsec tunnel mode and represented the tunnels as VTIs.
- Cisco IOS/IOS-XE supports route-based VPN tunnels using GRE tunnels protected by **transport** mode IPsec SA (host-to-host). Both point-to-point and point-to-multipoint modes (DMVPN) are supported.

Juniper JUNOS

- JUNOS supports policy-based VPN tunnels using IPsec tunnel mode where IPsec traffic selectors are either configured by security policies or explicitly configured on the tunnel interface (st0) using traffic selectors.
- JUNOS supports route-based VPN tunnels using IPsec Tunnel mode and represented the tunnels as VTIs. Both point-to-point and point-to-multipoint IPsec tunnel modes are supported. **The point-to-multipoint mode is proprietary**. The mapping of remote traffic to the specific IPsec VPN is signaled through proprietary IKEv2 NOTIFY payload that signals the remote's tunnel (st0) IP address to build up NHTB table in the Hub.
- JUNOS supports point-to-point GRE tunnels. However, it does not support transport mode IPsec SA. A point-to-point GRE tunnel layered on top of policy-based IPsec tunnel can be used to interoperate with Orbit if there is a desire to run dynamic routing protocol between Orbit and JUNOS over IPsec. This will add additional overhead of 24 bytes and require additional virtual IP address space for GRE tunnels.
- JUNOS does not support point-to-multipoint GRE tunnels (DMVPN).

End of application bulletin.