CVP2N: IR1800 Wired SD-WAN with LTE as Last Resort and DIA with SEA

Overview

This single-router SD-WAN configuration is for the Cisco Industrial Router IR1800 with added Secure Equipment Access (SEA) feature profile. SEA is a cloud-based service that provides remote access to devices reachable from the edge device and is intended as a service for OT to provide third-party access to assets.

At deployment time, this catalog will require user to provide a subnet with 2 IP. The IP addresses are for the SEA application and the default gateway which will be configured on the device for the user as a virtualportgroup7, and the corresponding mask for this network. This network will need to have a route to the internet for the SEA agent to register to cloud.

Configuration Catalog Details

Ethernet LAN connectivity is mapped into one VPN for security and granular control:

- Connected Devices (VPN 10): Secure network or DIA for corporate devices.
- One or more Hubs can be deployed as shown. The hubs are optional in this deployment since all edge devices can reach the internet thought NAT using VPN 0. If the user wants to route some traffic from edge to enterprise network, then a hub needs to be deployed using a configuration group not provided here that will also advertise routes to the edge routers (aka spokes). It will also be required to assign each edge device a unique Service VPN subnet and IP address to allow for return traffic. No default route from the hub should be advertised to the spokes in this deployment since it would conflict with the default route using NAT through VPN0.

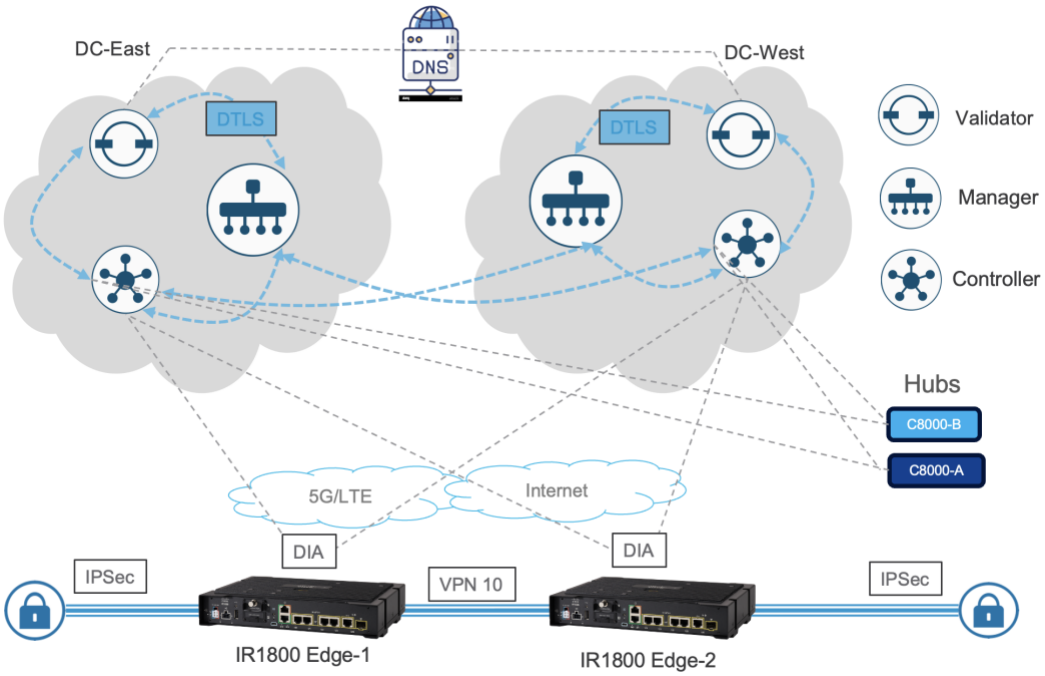

Fig 1: Configuration Catalog Design

Further details on functionality provided by this catalog entry which can be changed for the device at deployment time:

- The Service VPN (LAN) side is configured to advertise static and connected routes (VPN 10) or flexible integrations at sites with routed LAN access layer. If user decides to route connected subnets to a hub router, they will need to override the default subnet configured for VPN 10 with unique subnets across all edge devices to allow for proper routing. If left configured as default, the same subnet will be advertised to a Hub from all connected edge devices. Regardless, all default route traffic from VPN 10 will traverse the VPN 0 through NAT to the public internet.
- A DHCP Server is configured for VPN 10 allowing connected clients to receive IP addresses from service VPN 10. In addition, a few timers for BFD and OMP have been tuned to reduce LTE bandwidth usage while maintaining SD-WAN functionality (no defaults provided).
- A primary and secondary NTP servers with corresponding VPN for access can be configured with primary as preferred source. Also, NTP on wired can be disabled if needed.
- User can set the router console rate (default provided).
- Default DNS servers (Cisco DNS) are provided in both VPN 0 and VPN 10. User can change those in VPN 10 as needed.
- Point router logs to a server of their choice and provide the correct VPN and source interface for such traffic. The field is in the system section called “Logging Server IP Address” and is currently set to “0.0.0.0”, please change it at install time to a valid logging server IP address or set it to be the same as the “System IP” from the system section if one does not exist.
- Assign a loopback IP address to the field “VPN1 Loopback IP” under the service section. This can be assigned same IP address as “System IP” address and serves as a troubleshooting IP that can be advertised to and reachable from a hub router over the same VPN.
- Enter either a static GPS coordinates for the device to display in UI/MAP or if the device has LTE modem with GPS, then it can be enabled. Both GPS and NMEA must be enabled and the mode set to “standalone” to acquire GPS signal. Modem GPS coordinates will override static coordinates in UI/MAP. If NMEA data streaming is also required, source/destination IP and port should be provided to forward the GPS stream.

Direct Internet Access

Service VPN devices access the internet through a local breakout with a NAT-DIA default route in VPN 10. NAT trackers with endpoint IP tracking for connected devices are configured on the VPN 0, physical WAN Internet-facing interfaces, to detect when the external network becomes unavailable.