USE CASE: SD-WAN

This use case helps enterprises utilizing SD-WAN aggregation appliances to monitor the performance and user experience of their hub and spoke remote office – home office networks. In the scenario depicted above passive TAPs would be inserted at the office router input to the SD-WAN appliance (TAPs 1 & 2) and on each WAN link terminating on the appliance. In this use case we show three types of WAN links:

IPsec inter-office tunnels over a private WAN (TAPs 3 & 4), internet WAN links with IPsec inter-office tunnels combined with internet cloud services access (TAPs 6 & 6), and GRE tunnels for enterprise security device inspection (TAPs 7 & 8).

The Cirries DART monitoring solution consists of three component products: PacketSensor packet capture, MetaSensor metadata collector, and the DART management center. When capacity allows these products can be combined in a common server for cost effectiveness.

The below diagram depicts a combined PacketSensor – MetaSensor software instance in the remote offices. The Cirries DART solution can provide the following metrics for performance assessment and trouble shooting.

These metrics and analytics allow the Enterprise to effectively monitor the performance of the WAN networks and SD-WAN appliance, automatically identify problems and instigate automated workflows for rapid resolution of any issue in the network.

DART Metrics

TAPs 1 & 2:
- Full user experience metrics – TCP, RTP, Application
- Full IP traffic metrics
- Correlate WAN input and output traffic across the SD-WAN appliance
- Correlate traffic anomalies with appliance SNMP recorded events

TAPs 3 & 4:
- Correlate send & receive packet counts in each IPsec tunnel direction
- IPsec tunnel IP traffic metrics
- Correlate traffic anomalies with appliance SNMP recorded events

TAPs 5 & 6:
- Correlate tunnel traffic & IP traffic metrics
- Full user experience metrics for non IPsec internet traffic
- Correlate traffic anomalies with appliance SNMP recorded events

TAPs 7 & 8:
- Correlate tunnel traffic & IP traffic metrics
- unwrap tunnel for full user experience metrics
- Correlate traffic anomalies with appliance SNMP recorded events