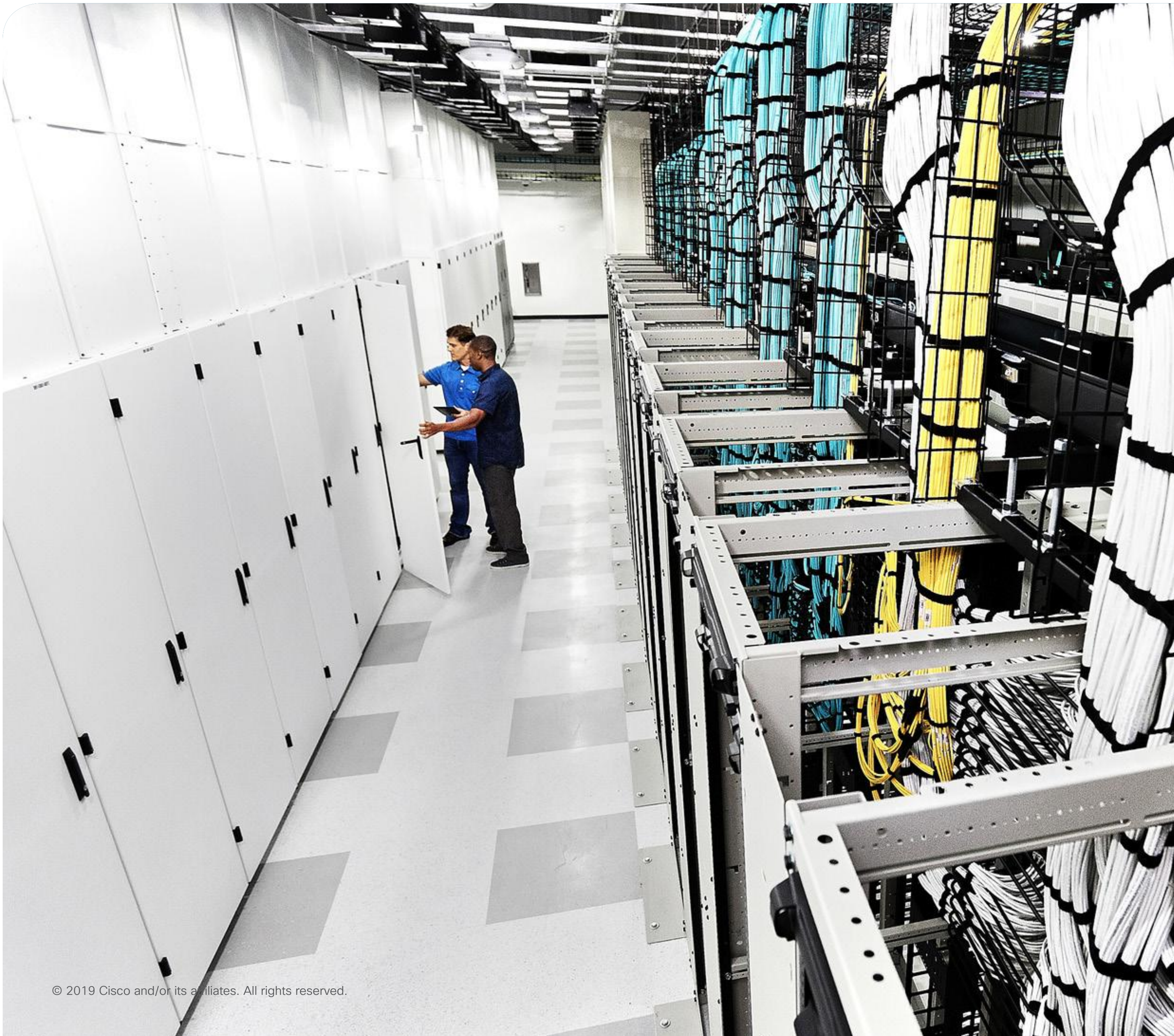
White paper
Cisco public

Cisco Software-Defined WAN for Secure Networks

Redefining WAN Delivery in the Cloud Era

Steven Mosher – Customer Solutions Architect
Craig Hill – Distinguished Systems Engineer



Contents

Next-generation WAN built for agility

Many organizations are moving their network infrastructure and applications to the cloud. This trend, combined with the rapid growth in multitenant LANs, media-rich applications, and networked devices, is placing increasing demands on WAN service delivery. As digitization expands, your organization is changing the way it approaches technology. Applications—both in the cloud and on premises—need predictable and fast performance. The network is gaining the intelligence to handle media-rich applications and enrich user experiences. While these digital interactions are beneficial, your WAN must evolve to handle this activity efficiently across cloud, data center, hub, branch, and remotely deployed sites.

The WAN must shift from playing a supporting role in the network to being a leader and provider of innovation. Due to the relatively high cost of traditional WAN connectivity and support, transforming the WAN has become a necessity. The modern WAN must find a balance between providing customers dynamic access while giving your organization the agility it needs to respond to changing business demands. In addition, the modern WAN must deliver:

Optimized cloud access: Many networking cloud solutions offer an inconsistent patchwork of options, and cloud-based applications can deliver a poor user experience. Enterprise organizations need an agile solution to onboard public cloud access on Amazon Web Services (AWS) and Microsoft Azure. In addition, the WAN must provide optimized performance for your cloud providers.

Reliable application performance and availability: Business-critical applications require predictable performance, and these applications must meet Service-Level Agreements (SLAs) even during link outages, brownouts, and other network events.

Reduced WAN expenses: The WAN is usually one of the most expensive IT budget line items. As WAN costs exceed US$100 per Mbps in bandwidth, many organizations cannot afford the expense. This results in insufficient bandwidth at branches and other locations, leading to an inadequate user experience.

A transformational overlay architecture

Cisco® Software-Defined WAN (SD-WAN) (formerly Viptela) is an overlay architecture that helps to overcome the biggest drawbacks of the traditional WAN. It builds secure, unified connectivity over any transport technology (Multiprotocol Label Switching [MPLS], broadband, Long-Term Evolution [LTE], Very Small Aperture Terminal [VSAT], and others). It also provides simplified operations with centralized management, policy control, and application visibility across the enterprise. With Cisco SD-WAN, you can provide secure connectivity everywhere, deploy new services and applications faster, and simplify operational complexity in the WAN.

Cisco SD-WAN also helps you connect and manage multiple branch offices while lowering WAN costs and improving security. The solution provides a secure hybrid overlay technology that virtualizes the enterprise WAN with centralized management and control. Cisco SD-WAN builds an overlay fabric that is carrier- and transport-agnostic. This allows networkwide segmentation for lines of business, compliance, and business partners. It also offers optimized performance for public clouds and the Internet.

The Cisco SD-WAN advantage

Cisco SD-WAN offers a broad set of options to facilitate the management and organization of your WAN. The Secure Extensible Network (SEN) platform delivers secure end-to-end network virtualization. Your organization can use the SEN platform to build large-scale networks with full integration of routing, security, centralized policy, and orchestration. This creates a network that is easy to manage while eliminating disconnects between business and IT.

Figure 1. Benefits of Cisco SD-WAN

Cisco SD-WAN

Centralized management, policy control, and application visibility across the enterprise

Cloud-first management with flexible deployment options

Accelerate key SD-WAN use cases; cloud-edge and segmentation

Sophisticated, but still simple to deploy and operate

Transport-independent secure fabric

Cisco SD-WAN builds an overlay fabric that is carrier-and transport-agnostic. This gives you a consistent WAN that can be built on any type of transport. Transports can be considered networks with similar attributes, such as performance, geographic paths, or security postures. Grouping transports by their attributes allows SD-WAN routers to make forwarding decisions that use transports based on policy.

Separation of control plane and data plane

Cisco SD-WAN provides a clear separation between management plane, control plane, and data plane. This allows each component to work independently and efficiently. It also facilitates scaling of the different components based on the needs of the network.

Zero-trust security

Cisco SD-WAN is based on the zero-trust model. All of the components mutually authenticate each other, and all of the edge devices are authorized before they are allowed onto the network. Every packet that flows through the network across data plane, control plane, and management plane is encrypted using SSL and IP Security (IPsec) technologies. The Cisco SD-WAN solution has unique differentiated capabilities to build a large-scale IPsec network across tens of thousands of sites.

Cloud-delivered

Cisco SD-WAN is cloud-delivered. All of the controllers are hosted in the cloud. You can log in to the Cisco vManage dashboard to centrally manage the WAN. vManage provides the ability to manage all aspects of the WAN, from provisioning, monitoring, and upgrading routers to having visibility into applications and troubleshooting the WAN. (Cisco SD-WAN controllers can also be deployed on premises.)

Zero-touch provisioning

All Cisco vEdge Routers are configured and managed using Zero-Touch Provisioning (ZTP). This allows you to significantly reduce your operational expenses in provisioning and maintenance.

Advanced analytics

Cisco SD-WAN vAnalytics

The WAN is often made up of disparate underlay infrastructure elements that are not directly controlled by your organization's IT. This infrastructure is often controlled by multiple providers. Because of this complexity, IT professionals often struggle to identify the source of network problems, have no real-time visibility into application or network performance, and cannot proactively plan future infrastructure growth.

Cisco SD-WAN vAnalytics is an analytics engine that provides the assurance and analytics elements of intent-based networking for the WAN. It provides IT with the visibility and insights necessary to isolate and resolve issues in the WAN. Additionally, Cisco SD-WAN vAnalytics delivers intelligent data analysis for planning and what-if scenarios.

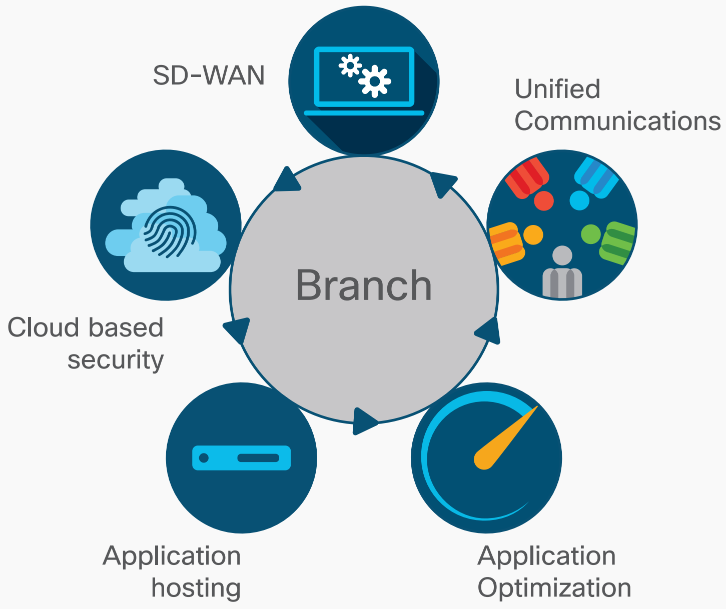
The major components of Cisco SD-WAN vAnalytics include:

- Comprehensive visibility into applications and infrastructure across the WAN
  - Provides real-time information for failure correlation, cross-customer benchmarking, and application performance scores
- Forecasting and what-if analysis
  - Enables future planning based on application and bandwidth, branch expansion analysis, and policy changes
- Intelligent recommendations
  - Recommendations for application Quality of Service (QoS) categorization and policy changes for predictable application performance

Figure 2. Cisco SD-WAN can reduce the complexity of remote sites

Reduce complexity for remote sites

Single rich services branch platform



- ✓ Easy to deploy and manage services on-demand
- ✓ On-demand physical and virtual form factors
- ✓ Best in-class trusted network services

Cisco SD-WAN benefits

Table 1. Features and benefits of Cisco SD-WAN

Features	Benefits
Centralized policy and distributed enforcement	The Overlay Management Protocol (OMP) centrally influences all routes and policy information for each segment of the network. This feature eliminates any bottlenecks in building the largest topologies and facilitates quick turnaround when making changes to the network.
Automated secure bring-up	The Cisco vEdge Routers have a factory-installed Trusted Platform Module (TPM) chip with a signed certificate. This built-in security helps ensure automated, foolproof authentication of any new Cisco vEdge Routers joining the network and is a major advantage when deploying tens of thousands of endpoints.
Encrypted control and data traffic	The default mode of operation of the Cisco SD-WAN network is “secure” and “encrypted.” Keys can be rotated as frequently as required without affecting performance. The SEN can scale to tens of thousands of network endpoints and 100,000+ routes while still providing multipoint security.

Features	Benefits
Scale-out architecture with redundancy	Multiple devices can be added to supplement capacity and provide redundancy. The architecture can withstand multiple failures in the overlay network for both the control and the data plane, effectively providing 99.999 percent availability.
End-to-end network segmentation	End-to-end network segmentation can be facilitated rapidly without additional control plane protocols. This segmentation provides robust protection of the network from outside attackers and provides secure separation internally within the multiple application segments.

Cisco SD-WAN solution components

Figure 3. Solution components

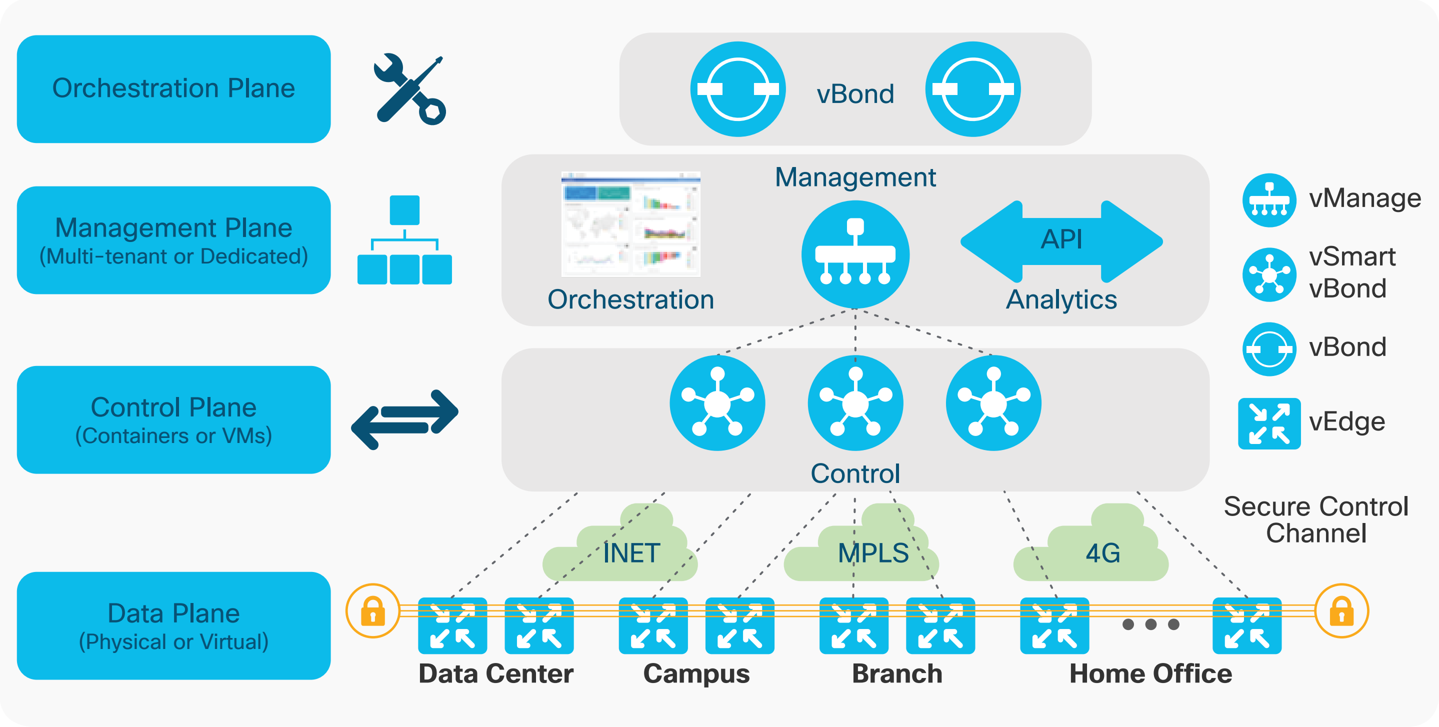


Table 2. Component descriptions

Component	Description
Cisco vManage	Cisco vManage is a centralized dashboard that facilitates automatic configuration, management, and monitoring of the overlay network. Users log in to vManage to centrally manage all aspects of the network lifecycle from initial deployment, ongoing monitoring, and troubleshooting to change control and software upgrades.
Cisco vSmart controller	Cisco vSmart controllers establish secure SSL connections to all other components in the network. They also run OMP to exchange routing, security, and policy information. The centralized policy engine in the vSmart controllers provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.
Cisco vEdge Routers	Cisco vEdge Routers are full-featured IP routers that perform standard functions such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Access Control Lists (ACLs), QoS, and various routing policies in addition to the overlay communication. These routers establish secure connectivity to all of the control components and also connect IPsec sessions with other vEdge routers in the WAN network.
Cisco vBond orchestrator	The Cisco vBond orchestrator facilitates the initial bring-up by performing authentication and authorization of all elements into the network. The vBond orchestrator also provides information on how each of the components connects to other components. The orchestrator plays an important role in facilitating communication with devices that sit behind the Network Address Translation (NAT).
Cisco SD-WAN vAnalytics	Cisco SD-WAN vAnalytics provides deep insight into the operations of the WAN, including visibility into network operations and applications. In addition, customers can run through various “what-if” scenarios and fine-tune their network based on the recommendations.

Network design recommendations

Topology options for secure SD-WAN

The purpose of these design recommendations is to provide guidance on Cisco’s preferred recommendations for implementing SD-WAN when external IPsec VPN devices (IVDs) are required for the purpose of network encryption. These recommendations target both single- and dual-homed edge router designs and highlight key features to gain the most benefit from SD-WAN capabilities, specifically regarding intelligent application-aware routing and the ability to constantly monitor the available transports to assure that the path meets those application requirements beyond shortest routing costs. There are also several key assumptions that are fundamental to these designs, including:

- vManage, vSmart, and vBond must have IP reachability at all times.
  - Black: via the underlying WAN transport
  - Red: via the routing infrastructure within the IVD routing tables

- Allowing the DSCP markings to bypass through the IVD unchanged
- The IP IVD of choice for the design must support the ability of pinning a single DSCP marking to a unique Security Association (SA) to the destination IP IVD (described in more detail below)

Finally, Cisco understands that there are multiple designs and requirements that could require different design features and topologies, but feels that the recommendations proposed in this paper target the most common topologies and for those requirements.

Single-router dual-encryptor topology design (inner side of IVD)

While the internal and external network IVD design offers two distinct topologies for the internal (red) design, there are several key differences from the topology of a commercial SD-WAN deployment. First, the management and controller cluster (vManage, vSmart, vBond) must be located and restricted to connectivity within the secure network space, specifically behind the IVD routing and security infrastructure. Second, the encapsulation for SD-WAN will not require IPsec encryption of the Generic Routing Encapsulation (GRE) tunnels between SD-WAN edge devices, as the IVDs handle the encryption requirements between locations.

Figure 4. Single-router dual-homed topology

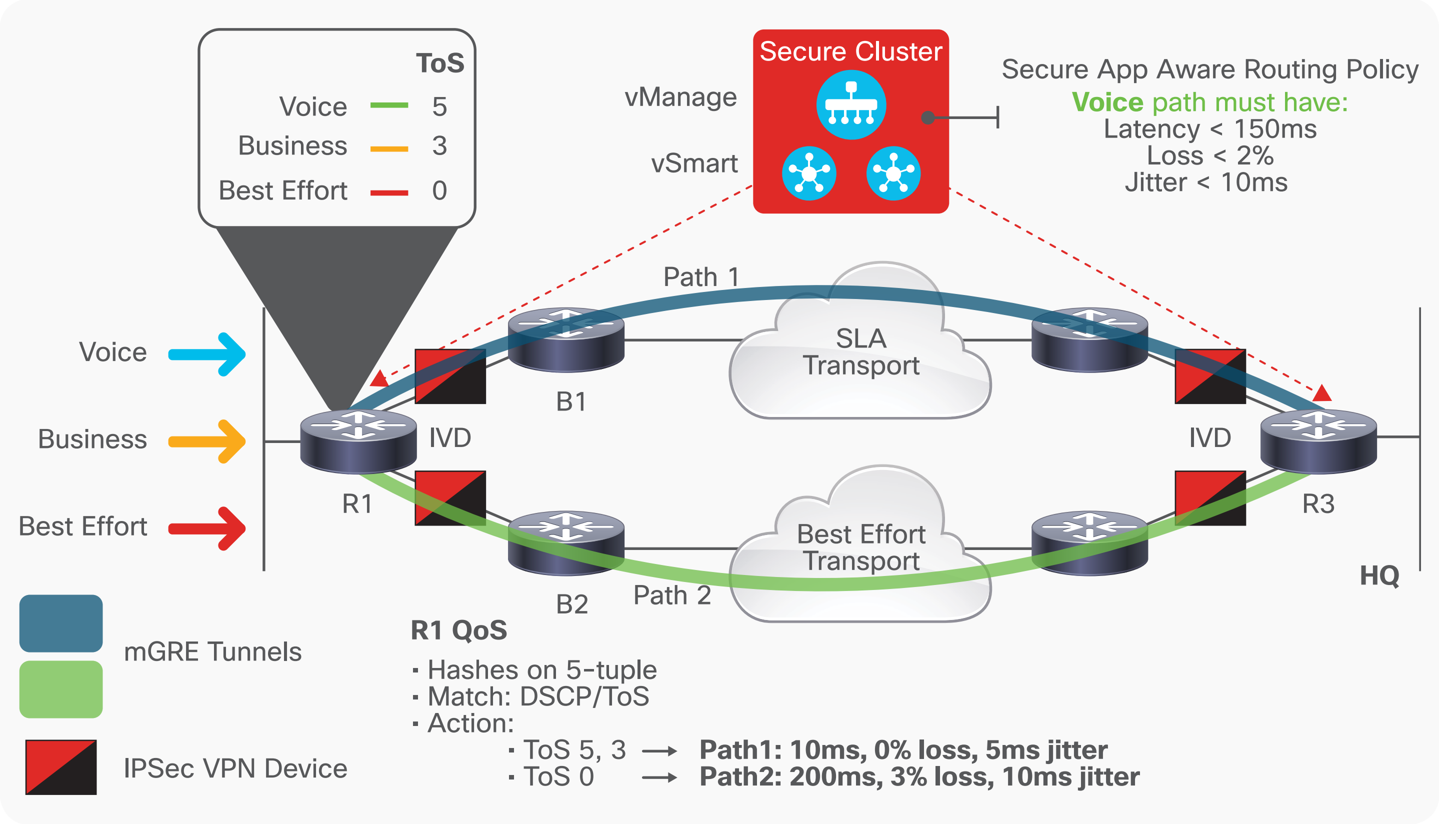


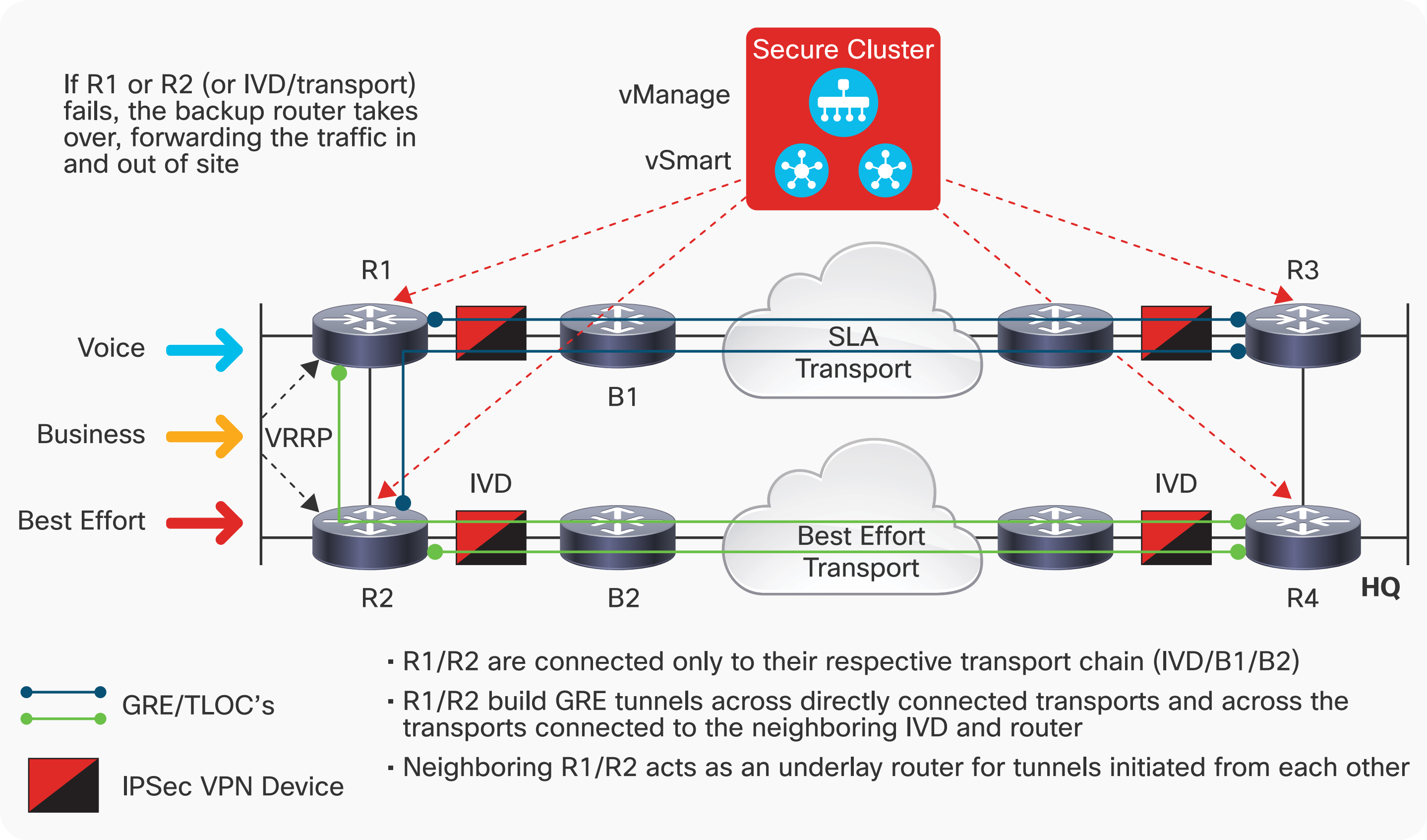
Figure 4 depicts the typical topology for a single-router dual-homed IVD design. Aside from the caveats above, the Cisco SD-WAN solution fits perfectly into this IVD topology. R1 will leverage two physical router interfaces, each pinned to a Transport Locator (TLOC). Recall that the TLOC provides that transport attachment point for the overlay tunnel, and is also the attachment point for supporting the liveliness probes that are sent to measure various QoS attributes (latency, packet loss, jitter) for link quality. In the IVD design, each TLOC will need to route to the destination TLOC within the secure routing space of the IVD and, like any other IVD network, will perform routing of specific IP addresses. In this case, these will be the source/destination TLOC address endpoints. While the Cisco SD-WAN solution is capable of running VRFs over IP (GRE), the SD-WAN solution reserves VPN 0 for control plane traffic. In the case of the IVD design, all VPN 0 traffic will be routable via the IVD secure transport, including the secure controller cluster, which must be reachable by all edge devices (R1 and R3 in Figure 4) and secured by the IVDs. This allows all control plane traffic (routing updates, Bidirectional Forwarding Detection [BFD] probes, key exchange for controller access) in the Cisco SD-WAN solution to be secured by the IVDs, as well as the router-to-router data plane traffic, creating an end-to-end secure infrastructure.

Dual-router dual-encryptor topology design (inner side of IVD)

The single- and dual-router designs share many capabilities and requirements, specifically the design requirements for securing VPN 0 traffic and access to the secure controller cluster. However, the dual-router dual-IVD design targets a higher level of availability than the single-router design, offering a fail-safe redundant design for those customers needing a higher level of uptime.

There are two key additions to the dual-router/dual-IVD design compared to the single-router design. First, because the two TLOCs on each router will be able to measure the link quality over each path, the application-aware forwarding decision can be made local, regardless of which router the packet landed on, via the Virtual Router Redundancy Protocol (VRRP). Second, because VRRP is used for load balancing of incoming host traffic from the branch campus network, Cisco recommends the use of a feature called TLOC extensions. TLOC extensions allow TLOCs to be configured in a redundant mode, allowing a partial mesh of TLOC topologies that offers connectivity redundancy as well as SLA transport liveliness from more sources and destination routers.

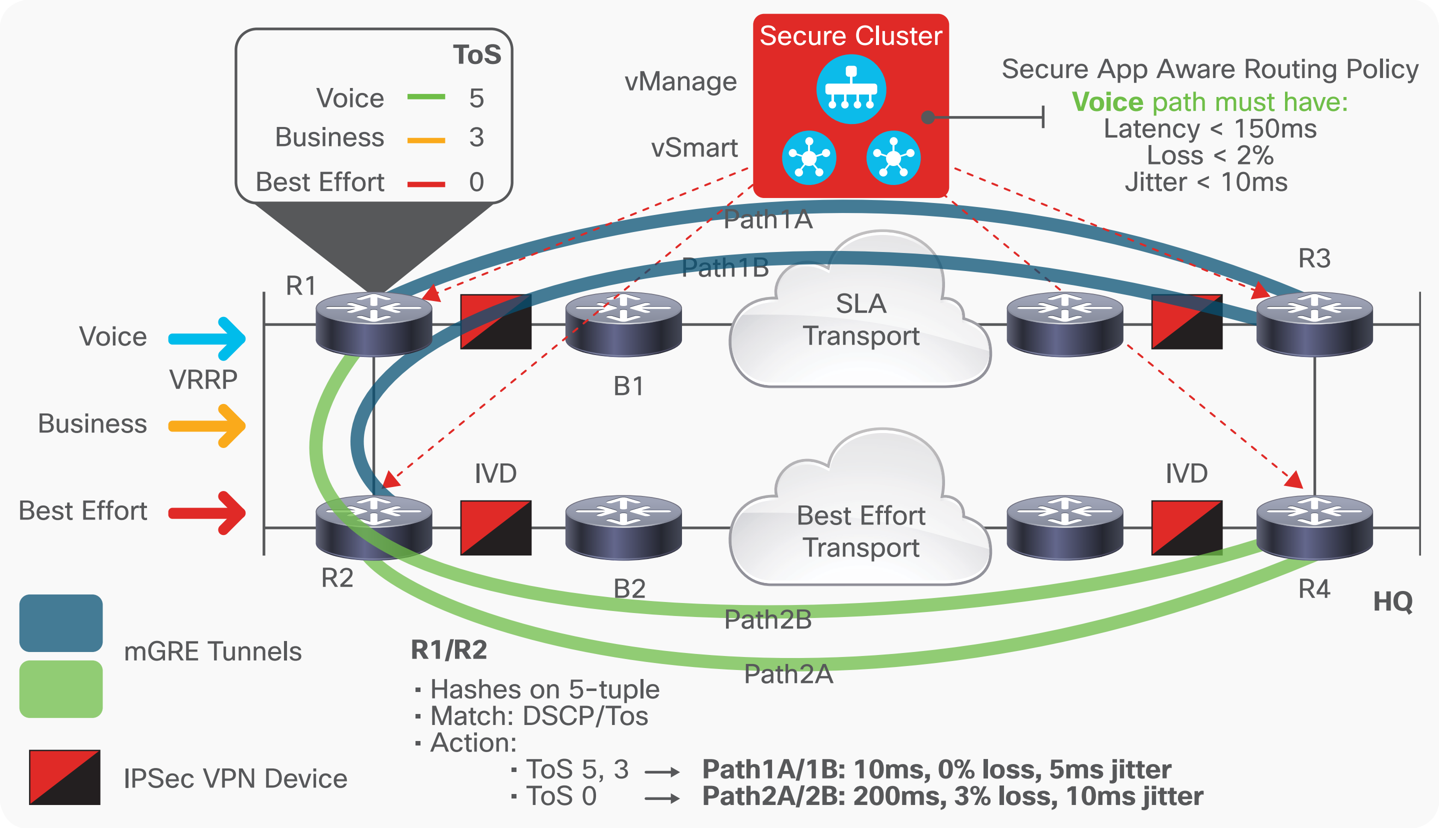
Figure 5. Dual-router dual-homed topology



- R1/R2 are connected only to their respective transport chain (IVD/B1/B2)
- R1/R2 build GRE tunnels across directly connected transports and across the transports connected to the neighboring IVD and router
- Neighboring R1/R2 acts as an underlay router for tunnels initiated from each other

As shown in Figure 5, the use of TLOC extensions gives the network designer the ability to originate indirectly connected TLOCs through its backup router. In the example shown in the figure, R2 would establish a directly connected TLOC to R4, but would add a second TLOC to R3 as well (via the R1 path), offering path redundancy to the remote site, even in the event that an IVD or the router/transport fails between R2 and R4. The TLOC extension extends a backup TLOC (GRE) across R1 to R3, with R1 acting as a transit path for that TLOC to R3. This TLOC extension design offers two key enhancements to the design. First, it provides another level of redundancy in the event of an IVD, link, node, or transport failure. Second, regardless of which router the destination packet lands on from the branch campus network, the application-aware routing policy forwarding can be applied, in this case, R1 or R2.

Figure 6. Branch with two WAN transport options



R1/R2

- Hashes on 5-tuple
- Match: DSCP/Tos
- Action:
  - ToS 5, 3 → **Path1A/1B: 10ms, 0% loss, 5ms jitter**
  - ToS 0 → **Path2A/2B: 200ms, 3% loss, 10ms jitter**

For example, as shown in Figure 6, a branch location has two WAN transport options (SLA based and best effort based) to the regional headquarters. Leveraging the real-time liveliness detection in the SD-WAN branch location that monitors per-path over each TLOC, a path can be chosen for voice traffic, leaving R1 (or R2) that complies with the required SLA, in this case latency less than 150 ms, loss less than 2%, and jitter less than 10 ms. Application probing is constantly generated and monitored from R1/R2, and assures that the voice traffic, classified as ToS=5, takes Path 1 to the central location at headquarters. The TLOC extension capability allows each transport to be measured from both R1 and R2 and the application-aware policy forwarding to be done directly from R1 or R2.

This application awareness is what differentiates Cisco SD-WAN from other WAN solutions, and the end-to-end measurement, in the case of Figure 6, from each router via TLOC extensions also takes into account the aggregated latency, loss, and jitter, including those induced by the IVDs, as well as the external transport network (black) directly connected to the transport services. The variations of path selection can change based on the agency's operators and how they handle specific applications, especially those in failure scenarios (for example, should low-latency voice take Path 2 if Path 1 fails?), so the options are endless through policy provisioning and the needs of the mission.

Single-homed Dual-Transport design (outer side of IVD)

While the dual-homed IVD designs can benefit greatly from SD-WAN offerings and capabilities, as described above, the single-homed solution while economical, does require one key capability within the IVD that is critical for benefitting from SD-WAN capabilities.

Understanding the Per Security Association (SA) to DSCP Marking Capability

For those customers requiring a single-homed topology but has the ability to leverage a dual-transport option in the public transport, these customers are able to take advantage of the SD-WAN application intelligence for forwarding encrypted traffic if several key caveats are met. The two key caveats were highlighted earlier in the paper above, specifically first, the ability to pass the DSCP markings in the clear, and second, the ability to leverage a capability in the IVD that offers per SA-to-DSCP peering.

Figure 7. Impact of a single SA for multiple DSCP markings

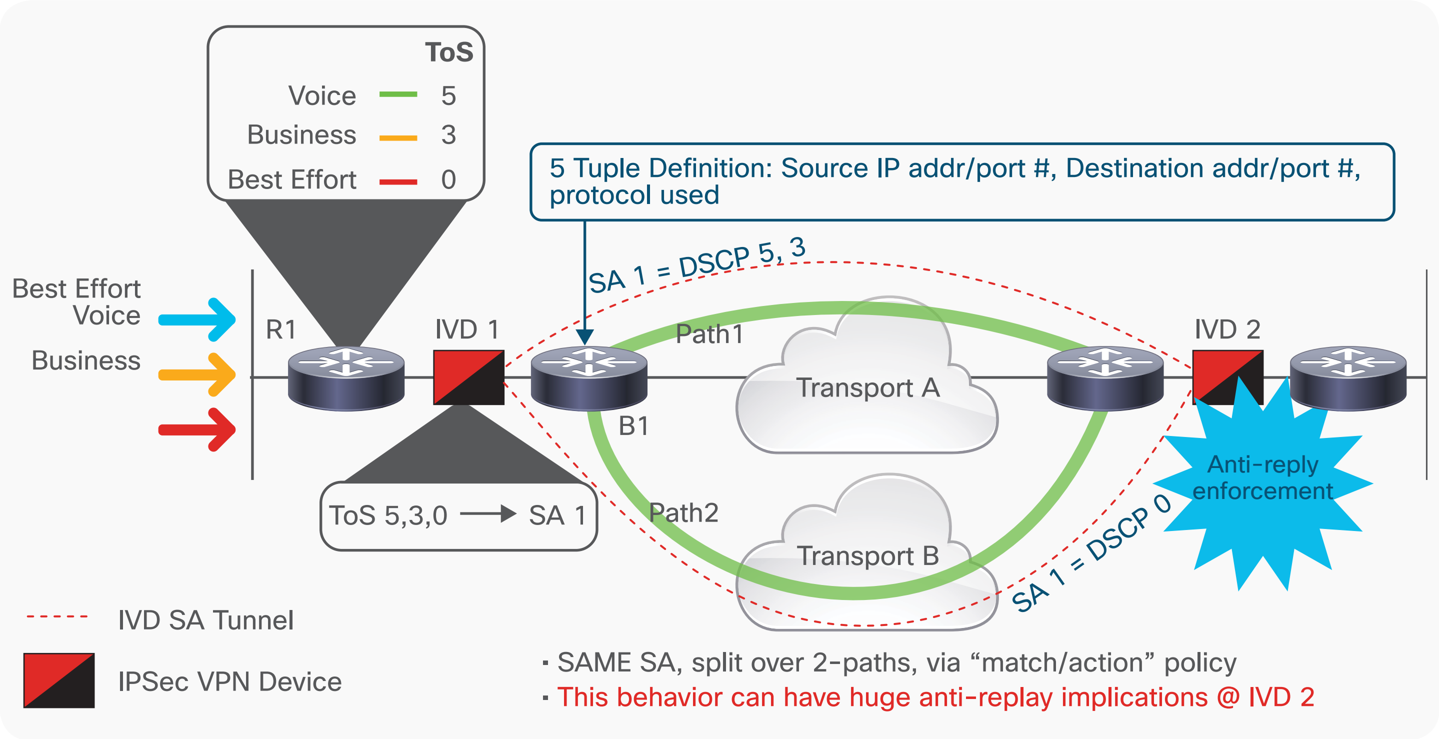

ToS
Voice 5
Business 3
Best Effort 0
5 Tuple Definition: Source IP addr/port #, Destination addr/port #, protocol used
SA 1 = DSCP 5, 3
Best Effort
Voice
Business
R1
IVD 1
Path1
IVD 2
Transport A
B1
Anti-reply enforcement
ToS 5,3,0 → SA 1
Path2
Transport B
SA 1 = DSCP 0
IVD SA Tunnel
IPSec VPN Device
▪ SAME SA, split over 2-paths, via "match/action" policy
▪ This behavior can have huge anti-replay implications @ IVD 2

Figure 7 above highlights the challenges where the IVDs are not able to offer per SA-to-DSCP peering. In the example, IVD 1 has a single SA established to IVD 2, and router B1 is leveraging Cisco SD-WAN traffic forwarding policy methods, forwarding DSCP 5,3 over "path 1", and DSCP 0 over "path 2". This splitting a traffic within a single SA can have huge security and quality issues due to anti-replay enforcement at IVD 2. Consider the policy above, and DCSP 5,3 getting higher priority than DSCP 0, so as traffic arrives at IVD 2, those packets having different priorities can have major ordering implications. So when IVD 2 does its anti-replay window checks, those DSCP 0 packets could easily fall outside the "window", causing the SA to drop and re-establish. This anti-replay issue is the crux of the issue in the topology and why the ability for the IVD vendor to support a unique SA per DSCP markings.

Figure 8. Unique SA per DSCP making

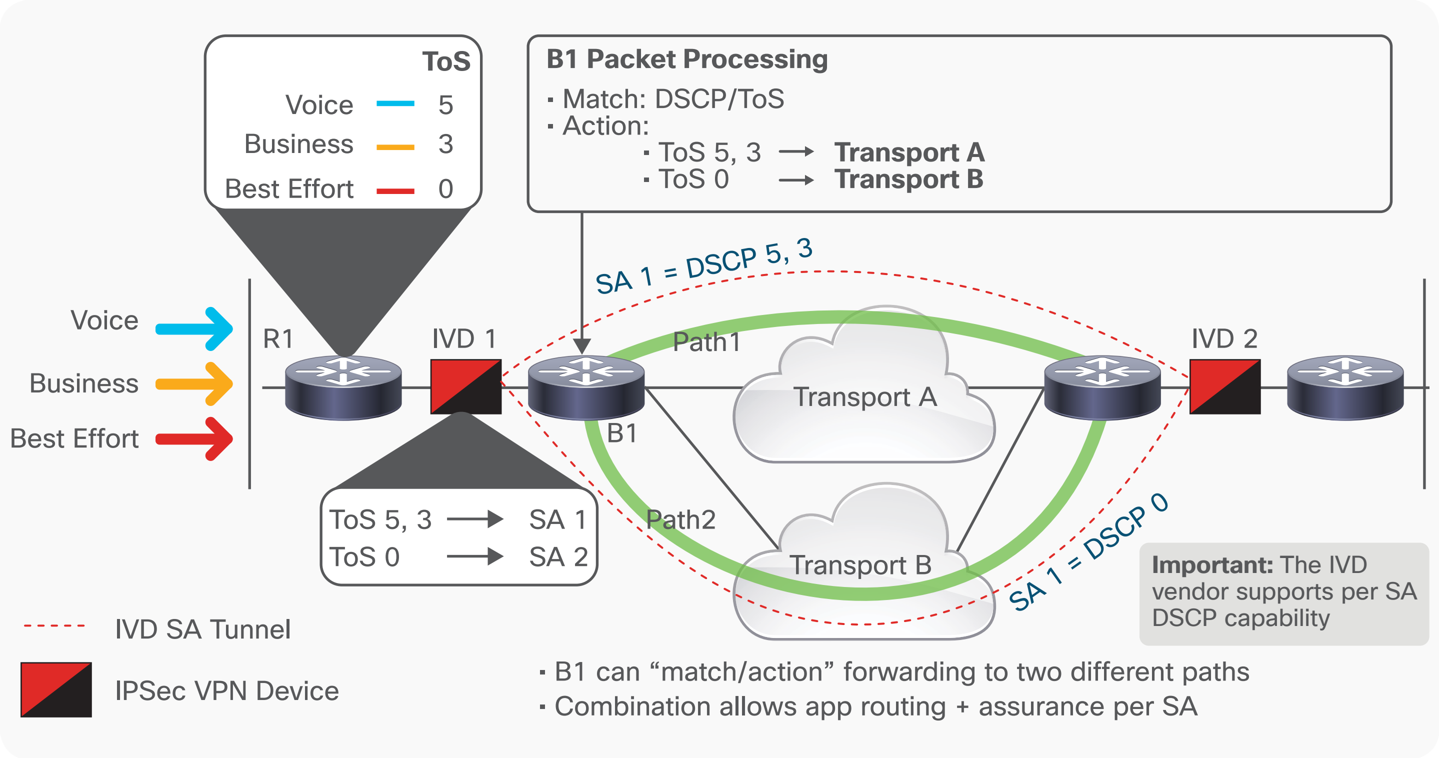
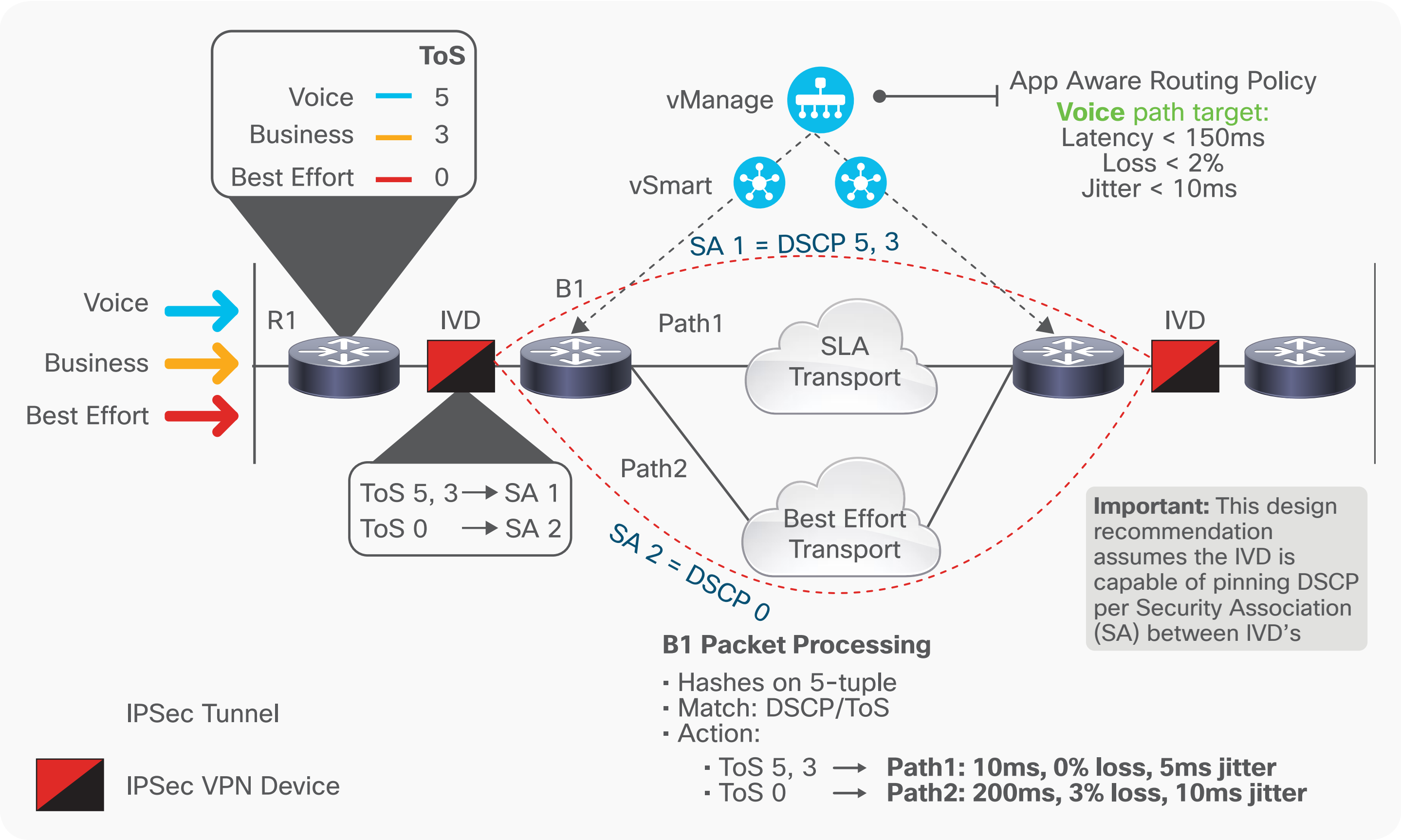


Figure 8 shows how SD-WAN can be leveraged if the IVD support the per SA-to-DSCP peering capability. In the example, the IVDs shown have the ability to create a unique SA per specific DSCP markings. This capability allows B1 to leverage application aware forwarding within the SD-WAN policy, and also eliminates those anti-replay window implications that can occur when a single flow is fragmented over various WAN transport paths. Thus, this SA per DSCP marking is critical to this topology to truly leverage the application intelligence of SD-WAN.

As was described above, if the DSCP bypass and per SA-to-DSCP peering is supported in the IVDs, the single-home dual-transport topology offers an economical method for leveraging SD-WAN intelligence in an IVD environment.

Figure 9. Single-homed Dual-Transport solution

As described above, if the DSCP bypass and SA per DSCP marking are supported, the single-home dual-transport topology offers an economical method for leveraging SD-WAN intelligence in an IVD environment.



In the single-homed dual-transport topology depicted in Figure 9, B1 will support the same SD-WAN capabilities as any other SD-WAN edge device, including the ability to explicitly forward traffic (per policy) over a specific path based on defined sets of "Match" policies. The SLAs derived from the specific path can be done via the inherent SLA probing per TLOC, over both the SLA transport and the best effort transport, as depicted in the figure.

Where the single-homed design varies the most from the dual-homed design is in the functions of R1. Because R1 is limited to a single interface egress to the IVD (and WAN), it does not have the ability to provide multiple TLOC capabilities to the WAN. With that caveat, this proposal is to leverage standard Class-Based Weighted Fair Queuing (CBWFQ) on R1 in order to properly prioritize and schedule the traffic in the defined QoS policy before sending it to the IVD. In this example, voice, business, and best effort will be classified as ToS=5, ToS=3, and ToS=0, respectively, as indicated below.

		Tos
Voice	━━	5
Business	━━	3
Best effort	━━	0

While R1 marks (or trusts) and schedules Type-of-Service (ToS) bits of each packet on ingress, the IVD, in addition to encrypting the packet, will bypass the ToS markings, leaving them untouched as each packet traverses the IVD. With this bypass capability in the IVD, as packets are forwarded from the IVD to B1, B1 has the ability to leverage these ToS markings as the needed match for classification, and to impose explicit SD-WAN policy options on the packets based on these markings. In the example shown in Figure 9, as packets ingress B1 from the IVD, B1's policies are configured for a match/action policy construct. In this example, B1 will "match" ToS markings as the classifier and, per those encodings, ToS markings 5 and 3 will be forwarded over the higher-quality transport Path 1. Traffic with ToS markings of 0 will be forwarded over the best effort transport via Path 2.

While the single-homed chain of R1-to-IVD-to-B1 limits per-path/per-application monitoring from the point of R1, the proposed solution does offer a rich set of application-aware capabilities, including:

- Prioritizing applications even after the packets are marked and encrypted after traversing the IVD
- Offering per-application policy forwarding on the WAN edge, for example at B1
- Allowing per-application policies and monitoring via QoE liveliness checks of those service levels per path in the WAN
- Providing operators the ability to leverage SD-WAN capabilities in the more complex designs where IVD-type encryption models are required

Given the benefits of the single-homed design, the question arises as to whether true SD-WAN capabilities are needed where R1 is located (that is, behind the IVD devices), since this solution targets per-hop QoS scheduling only. Where complex application routing capabilities are not needed, such as in the case with the dual-homed topology, the central controller and policy, as well as centralized management, could be enough for some to consider an SD-WAN edge router at R1's positioning, versus limiting an SD-WAN-capable router post-encryption, such as B1. This decision will be a case-by-case, customer-by-customer decision.

Summary

Customers looking to leverage a more intelligent WAN solution over an IVD-based infrastructure can do so with very innovative designs. Those customers wanting a very highly available WAN design with an application-aware routing capability should consider the dual-homed design using the TLOC extension enhancement. Customers that deploy only single-homed solutions but want to take advantage of the other operational capabilities SD-WAN has to offer can do so. Even those customers that require intelligence on the unsecure side of the IVDs can leverage a level of application intelligence with the advanced classification and application routing methods described in this paper.

Finally, in any of the WAN designs discussed in the paper, the SD-WAN edge routers do not have to be hardware based. There are Virtual Network Functions (VNF) routers that offer the same capabilities in a virtualized package. These can be run in multiple types of x86 offerings, including in public clouds such as AWS or Azure. This solution suite for Network Functions Virtualization (NFV) would also include the orchestration element and, because it is virtual, could include additional VNFs (firewall, intrusion detection system, third-party applications), including the Software-Defined Networking (SDN) orchestration capability for the day-0 configuration that NFV offers.