Overview of Policy-Based Forwarding in an SD-WAN Network

For supported software information, click here.

In a traditional network, the default path selection method is for routing protocols to determine the best path to use to forward traffic towards a destination. Paths are selected based on the characteristics of the routing protocol itself and based on the entries in the route table.

For an SD-WAN network, the Versa Operating System^{TM} (VOS^{TM}) software supports powerful traffic forwarding capabilities that go beyond routing-based forwarding. The VOS software provides two forwarding methods, SD-WAN VPN path selection and policy-based path selection.

The first forwarding method, SD-WAN VPN path selection, uses SD-WAN policy rules to control traffic forwarding. With this method, the first step in determining how to forward a packet is to perform a route lookup on the packet. If the route lookup identifies a route that points to a remote SD-WAN site (also referred to as a VPN next hop), the VOS software uses SD-WAN policy rules to determine how to forward the traffic over the VPN. The policy rules can include SLA-based forwarding and packet conditioning. For more information about the VOS SD-WAN path selection capabilities, see Configure SD-WAN Traffic Steering.

With the second method, policy-based path selection (also referred to as policy-based forwarding, or PBF), you can override the route lookup altogether and instead forward the traffic over any desired next hop. The next hop can be a non-VPN next hop, such as a WAN interface or a GRE tunnel, or it can be an SD-WAN next hop, such as a specific SD-WAN hub. When the next hop is an SD-WAN next hop, you can apply all the standard VOS SD-WAN path selection behavior to determine how to forward the traffic to SD-WAN.

For releases prior to Release 20.1, you configure policy-based forwarding using either PBF policies or SD-WAN policies. For traffic whose route does not point to the SD-WAN VPN, the VOS software uses PBF policies. With PBF policy, traffic can be forwarded to only one non-VPN next hop. For routes that point to an SD-WAN VPN, the VOS software uses SD-WAN policies, and again, the traffic can be forwarded to only one non-VPN next hop.

For Releases 20.1 and later, the VOS software allows you to configure the following policy-based forwarding use cases:

- You can use SD-WAN policies to configure policy-based forwarding even when the route does not point to an SD-WAN VPN. This means that you can use SD-WAN policies for both SD-WAN VPN path selection and policy-based forwarding.
- You can forward traffic to a non-VPN next hop as well as to a VPN next hop. Again, this means that you can use SD-WAN policies for both SD-WAN VPN path selection and policy-based forwarding.
- You can specify multiple next hops in priority order, much like you specify circuit priorities, for forwarding over a

VPN.

- You can configure performance-based next-hop selection, using SLAs that use either active or passive monitoring of performance metrics.

A key use case for policy-based forwarding of traffic is direct internet access (DIA) for SaaS and other internet application traffic. You can create policies that define static DIA-related properties, such as how to load-balance among multiple WAN circuits and how to fail over from one WAN circuit to another. You can also create policies that dynamically monitor internet reachability and take the current reachability into account when making the path selection.

When you configure internet access and DIA, it is often important to ensure that DNS queries follow the same egress as the actual application traffic For example, if a particular application uses local breakout or local egress, the DNS queries for the domain names associated with that application should also use local egress. You use the VOS DNS proxy to achieve this goal. You can configure the DNS proxy to provide split DNS functionality, which resolves enterprise internal names using an enterprise DNS server and public domain names using a public DNS server, all while maintaining affinity with the path of application traffic.

For more information about using DIA to configure policy-based forwarding in an SD-WAN network, see Configure Direct Breakout to the Internet.

Performance-Based Path Selection

Performance-based path selection is an extension of policy-based forwarding that factors in the performance of the next hop when selecting the path. Performance-based path selection checks each next hop for liveness and does application performance monitoring. While you can use performance-based path selection for any purpose, a typical use is to select the best path to reach cloud-based SaaS applications. This section provides an overview of performance-based path selection as it relates to SaaS applications.

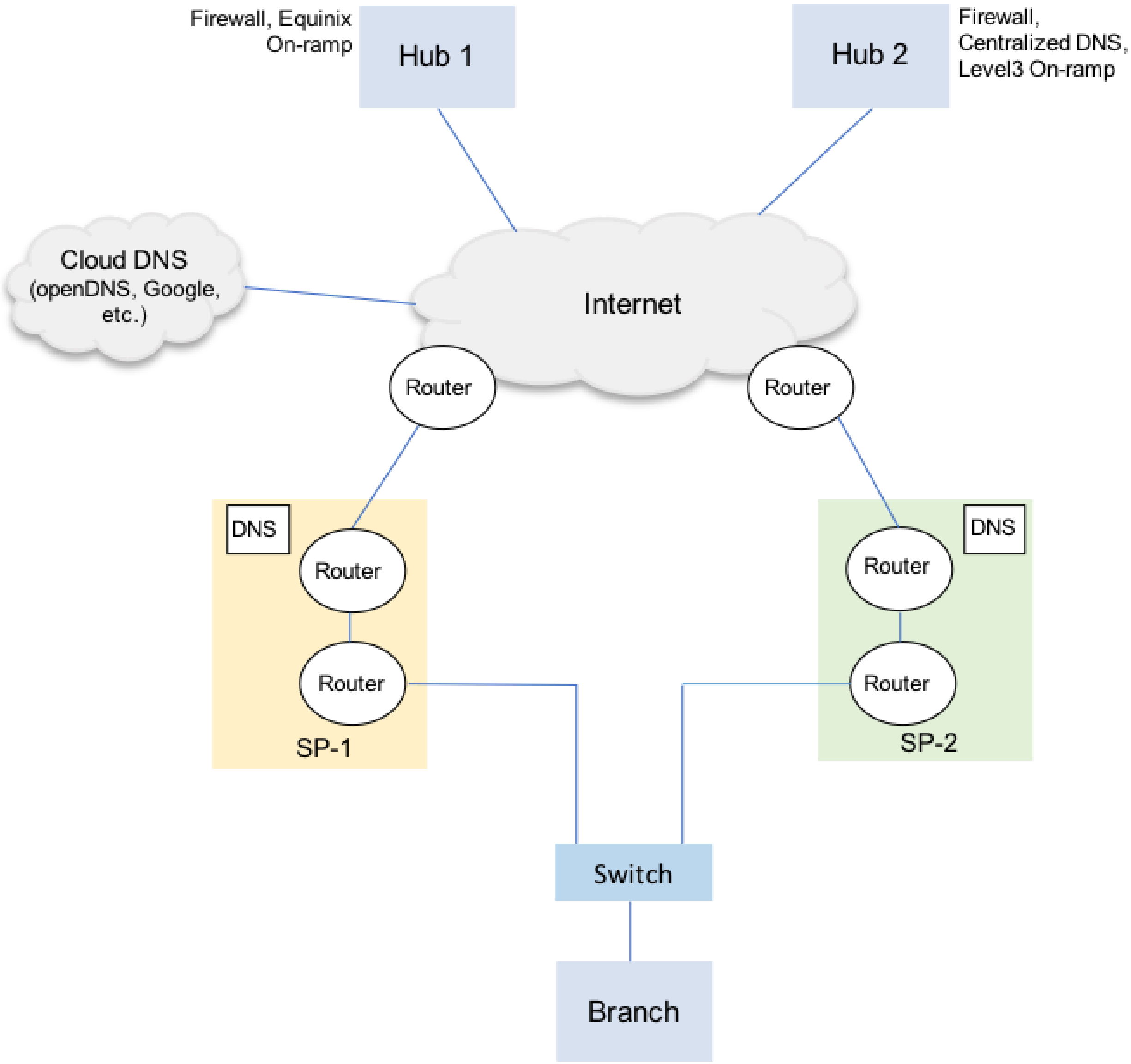
In an SD-WAN network, a tenant or organization can reach a SaaS application using multiple WAN links. These WAN links can use different paths and even different transport networks. Because the transmission latency among different paths can vary, it is important to choose the best available path for optimal SaaS-application performance.

To address this scenario, the VOS traffic-steering software allows you to select the best forwarding path using two monitoring methods:

- Passive monitoring—Uses passively collected, single-ended application performance metrics. Single-ended deployments are ones that do not require another participating VOS device.
- Active monitoring—Uses active performance monitoring data.

In a deployment scenario with direct internet access (DIA) connections, such as one with a single broadband link or multiple broadband links connected directly to a branch site, the best path to a SaaS application may be a direct connection from the branch, or it may be through a VOS device deployed as a cloud interconnection hub. The cloud interconnection hub can be deployed in a variety of locations, such as a customer data center, an internet interconnection or a hosting facility such as Equinix, or the SaaS provider’s data center. In addition, customers may require that all their internet traffic egress through one or more cloud security gateways, such as Zscaler.

The following figure shows a branch device (Branch) that has direct internet access using WAN links from two providers, SP-1 and SP-2. These links are also part of the SD-WAN overlay that includes Hub 1, Hub 2, and other branches (not pictured).


Firewall, Equinix On-ramp
Hub 1
Hub 2
Firewall, Centralized DNS, Level3 On-ramp
Cloud DNS (openDNS, Google, etc.)
Internet
Router
Router
DNS
Router
Router
SP-1
DNS
Router
Router
SP-2
Switch
Branch

When you enable passive application monitoring (also known as inline application monitoring), VOS spoke and hub devices collect transport and application layer metrics for TCP-based SaaS application sessions as application traffic passes through the devices. These metrics include network and server response times and packet loss estimates in each direction. The VOS traffic-steering software uses these metrics to assess the quality of an application using different paths and then to select the best path for the application. A path can be a direct internet access path (through a local WAN circuit) or an indirect path through a hub.

You can use passive SaaS application monitoring in the following scenarios:

- Most traffic uses a central breakout from a spoke to a hub, and only some traffic uses a local breakout
- Most traffic uses a local breakout, and only some traffic uses a central breakout

To configure passive SaaS application monitoring, you first configure an SD-WAN traffic-steering forwarding profile. Then, in an SD-WAN policy rule, you configure a match condition and associate the rule with the SD-WAN traffic-steering forwarding file.

Active SaaS application monitoring sends ICMP, TCP, and HTTP active monitoring to measure the responsiveness of commonly used cloud-based SaaS applications. To configure active SaaS application monitoring, you configure the monitor, which you reference in an SLA profile. Then you reference the SLA profile in and SD-WAN traffic-steering forwarding profile, and then you reference the profile in and SD-WAN policy rule.

You can configure hubs to export both active and passive monitoring metrics to spoke sites over the MP-BGP control plane. Spoke sites then have two ways to derive application performance metrics for hub paths:

- Use only locally collected, passive end-to-end performance metrics.
- Combine metrics exported by hubs with SLA monitoring metrics towards the hubs.

The metrics are consolidated into a single score called the Versa link rank (VLR), which represents the application's performance. The VLR score, which is updated regularly, is used to determine which path offers the best performance. The VLR is a number from 0 (best performance) through 100 (worst performance).

For information, see Configure SaaS Application Monitoring.

DNS Resolution

DNS name server resolution is a key aspect of application performance. While it is not required that you configure DNS resolution for DIA, it is recommended. for best performance.

An application transaction starts with a DNS query for the application server's domain. After the domain is resolved to an IP address, one or more HTTP or HTTPS sessions are initiated to that IP address as part of the application transaction.

Typically, an enterprise has a DNS server at a central location that is responsible for resolving both corporate internal and public domain names. Using a centralized DNS resolver works well in a network in which all internet-bound traffic from all branches and remote sites is backhauled through the central location.

In a scenario where you want to provide local (direct) access to the internet from a branch, performing the DNS resolution using a central DNS server generally results in less than optimal performance. This reduction in performance occurs in part because all internet-bound traffic must fist be backhauled through a centralized server. Performance is also reduced because DNS servers normally examine the source IP address of the query to determine which application server can best serve the client. Therefore, it is important to ensure path affinity between the DNS query and the subsequent application traffic for the entire transaction. To effect this, local internet access should be combined with local DNS resolution, and application access through a hub should be combined with DNS resolution through the same hub.

The VOS software combines DNS proxy with the path selection service to ensure path affinity, without requiring configuration changes across the network. The simplest way to do this is to configure DNS proxy with split DNS so that corporate internal domain names are resolved by a centralized DNS server behind an SD-WAN site, such as a data center or a headquarters, and external domain names are resolved by internet, cloud, or internet provider–hosted resolvers. When the DNS proxy resolves external names, it cooperates with the path selection service to select an appropriate path for the application corresponding to the DNS query.

For resolving external domain names, you can configure a DNS resolution policy for specific applications. One use case is when a specific SaaS provider recommends using a specific DNS server. For example, Microsoft recommends using the Cloudflare DNS server instead of the Google DNS server. For this, you would have one extra DNS proxy rule that matches all Office365 domain names and sets the action to use the Cloudflare resolver.

To reduce DNS response times and further improve application performance, you can configure the DNS proxy as a caching proxy.

For information about VOS DNS resolution features, see the Configure DNS Proxy, Configure HTTP/HTTPS Proxy, and Configure DNS Proxy with SD-WAN Traffic Steering for DIA articles.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 20.2.1 supports the configuration of additional use cases.

Additional Information

Configure Direct Breakout to the Internet
Configure a DNS Proxy
Configure DNS Proxy with SD-WAN Traffic Steering for DIA
Configure HTTP/HTTPS Proxy
Configure Policy-Based Forwarding
Configure SaaS Application Monitoring
Configure SD-WAN Traffic Steering