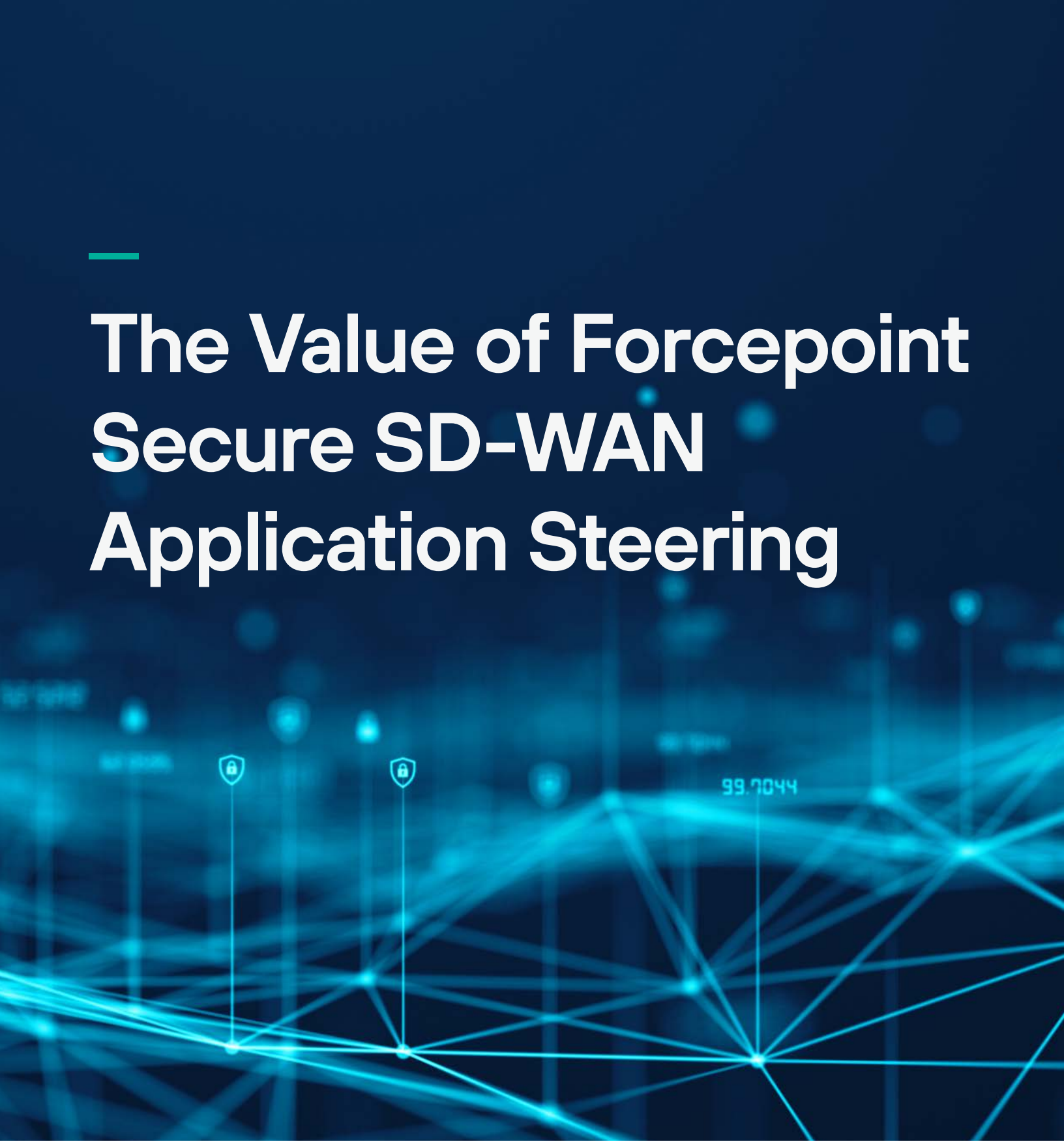
The Value of Forcepoint Secure SD-WAN Application Steering



Forcepoint

Whitepaper

Table of Contents

Introduction

As businesses continue to adapt to SaaS apps and cloud services, maintaining high application performance, enhanced network efficiency, and centralized control and management is more critical than ever. Traditional WAN architectures, such as MPLS, lack the necessary resources to support today's modern organizations. Software-Defined Wide Area Networks (SD-WAN) are a powerful solution, offering greater flexibility, improved application performance, and visibility into applications, ultimately delivering increased productivity and better user experience.

This technical whitepaper explores the role of application steering in Forcepoint Secure SD-WAN, focusing on how it addresses network inefficiencies and enhances application performance. Specifically, it will dive into the types of selection points, application identification methods, and more, providing real-world examples of how Forcepoint SD-WAN optimizes mission-critical applications.

Types of Selection Points

Within an SD-WAN infrastructure there are two types of traffic steering selection points: SD-WAN internet breakout, and tunnel selection within SD-WAN mesh.

1. SD-WAN internet breakout
With internet breakout, the traffic leaves an organization's network through one of many possible internet connections. The key factor is knowing which application the SD-WAN engine is selecting the link for, and choosing the optimal link for the application based on the administrator's configured preferences for that application.

2. Tunnel selection within SD-WAN mesh
When traffic flows within the organization's dedicated SD-WAN mesh, applications can be routed more efficiently by selecting optimal tunnels dynamically. What is most important, and is possible within Forcepoint Secure SD-WAN, is that connections dynamically take different paths based on changing network conditions without breaking the established application connection.

Application Identification Methods

General principles
Two major application detection methods are IP database-based and application fingerprinting-based.

IP database-based:

→ + Fast matching based on the first IP packet of the connection

→ + Lightweight

→ - Database needs constant updates and may still miss important applications

→ - No support for multiple applications at the same address

Application fingerprinting based:

→ + Accurate matching, with no need for huge databases and constant updates

→ - Requires more CPU power

Forcepoint SD-WAN application identification and routing

With Forcepoint Secure SD-WAN, applications are identified based on hybrid technologies, which use detailed application fingerprinting from the supported traffic and advanced analysis such as destination server certificate validation.

Certificate validation provides highly accurate application identification, which is typically released weekly and updated via dynamic updates. The updates are then easily distributed to all engines in the system with Forcepoint SD-WAN central management.

Forcepoint Secure SD-WAN link performance evaluation and optimization

Different methods are available for SD-WAN internet breakout and the SD-WAN tunnel selection use case.

SD-WAN internet breakout application identification and performance
With the SD-WAN internet breakout use case, the challenge is that a link needs to be selected before seeing what type of application is being routed. Forcepoint Secure SD-WAN solves this with advanced application routing.

The application is first identified through application identification capability. Then the best link is chosen based on the specific application, delivering the best possible application performance. Additional benefits include automated probe configuration and accurate application identification.

SD-WAN tunnel selection optimization
With the SD-WAN tunnel mesh scenario, link selection options and flexibility are much greater.

In this scenario, even established connections can move from one link to another dynamically. The connection can start through any available path and after the application is identified through traffic fingerprinting, the application can be moved to the most suitable path to provide users with the most optimal experience.

Forcepoint Secure SD-WAN Multi-Link uses advanced link performance evaluation to monitor bandwidth for latency, jitter and other factors that may impact application performance. Applications can then be configured to select the link that best meets the application's needs. For example, Forcepoint Secure SD-WAN Multi-Link will select a link to carry VoIP applications based on the requirements of low latency and jitter.

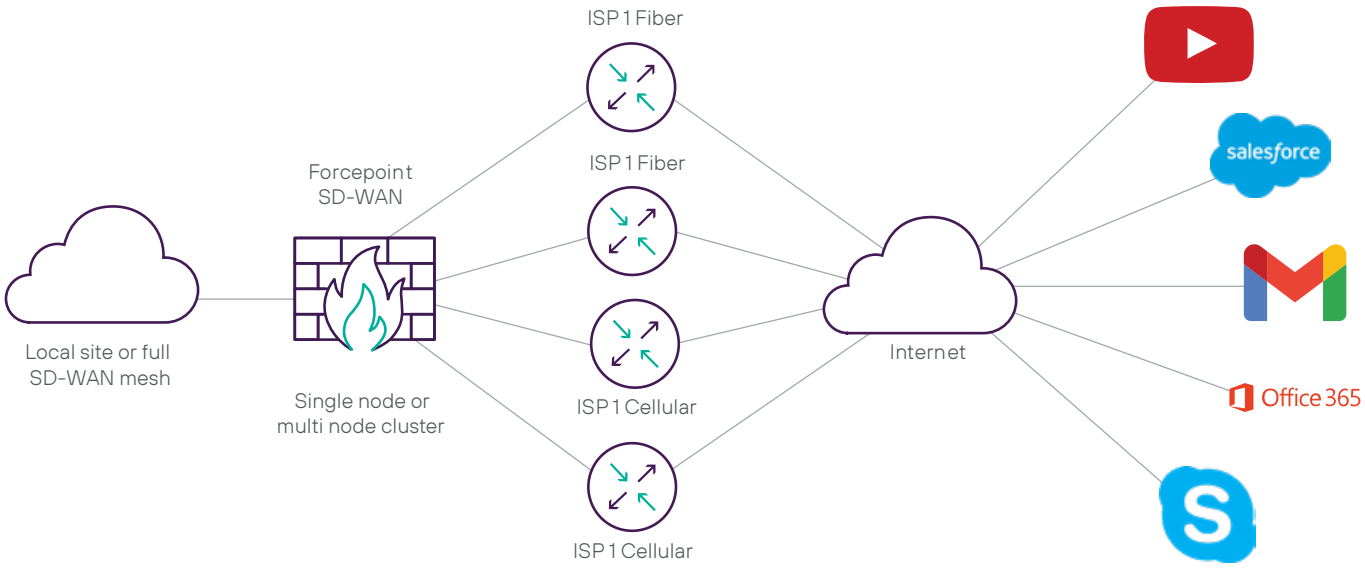


Figure 1. Internet breakout scenario with four different connections to the Internet.

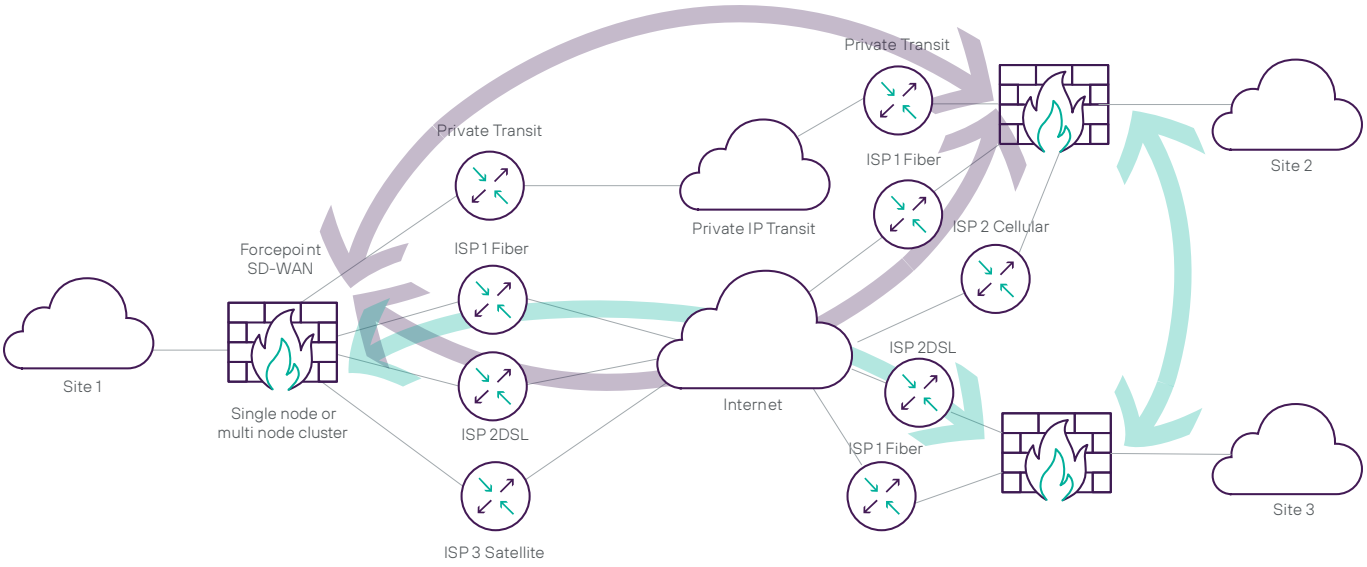


Figure 2. SD-WAN Multi-Link scenario that combines different connectivity types, even private transit.

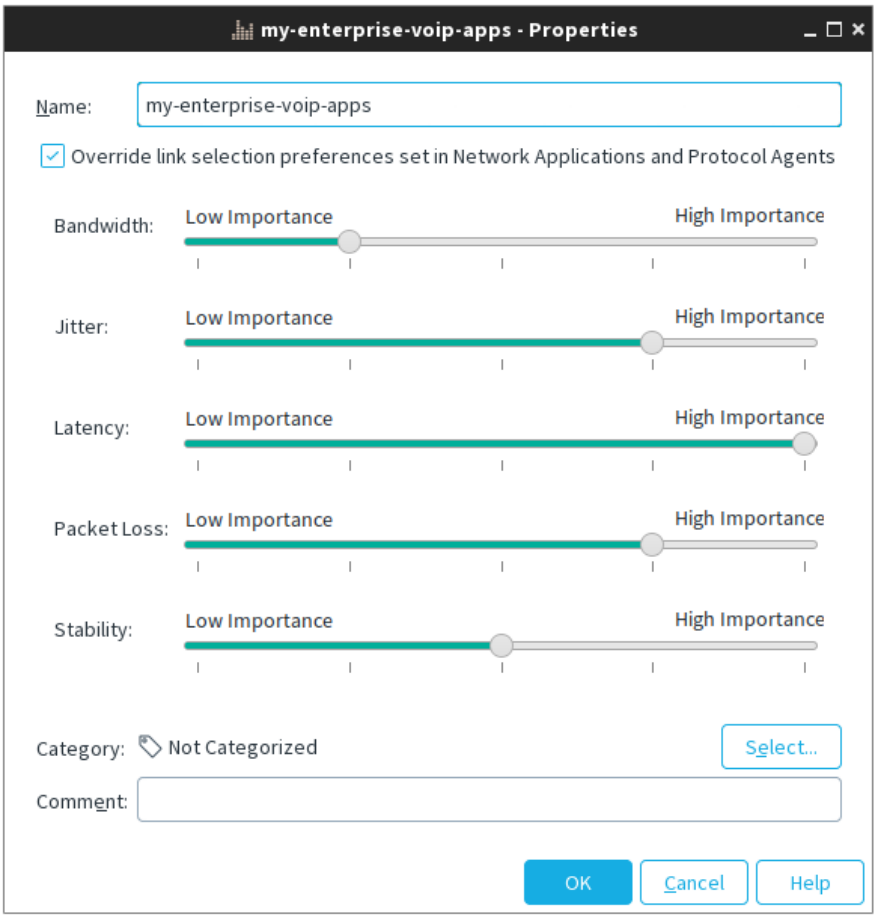


Figure 3. Configuration example for link quality selections for VOIP traffic.

By combining detailed application identification, accurate link monitoring capabilities, and the ability to direct applications to the most optimal link, Forcepoint Secure SD-WAN empowers administrators with industry-leading management for traffic direction.

Example of enterprise applications and how Forcepoint can handle and improve those

Internal VoIP application in SD-WAN
With the SD-WAN tunnel mesh scenario, link selection options and flexibility are much greater.

Scenario: An organization needs to improve internal VoIP traffic between branches. Branches have various connectivity types and performance sometimes varies, so it is ineffective to configure VoIP traffic to a particular link.

Utilizing Forcepoint Secure SD-WAN tunneling between sites, it applies link usage profile to prioritize low latency links for VoIP traffic. Forcepoint Secure SD-WAN continuously monitors tunnel performance on each node and then automatically directs VoIP traffic to the best available link.

Leveraging template policies and the easily laid out UI, Forcepoint Secure SD-WAN is extremely flexible and simple to implement for all branch types and multi-link configurations.

Public VoIP application directly from the public cloud

Scenario: A company needs to improve Microsoft Teams and Zoom call quality for their users in various branch locations having various connectivity types. Due to the varying conditions of the alternative links, it is not efficient to give static priority or preference for these applications versus available links.

Customer branches are directly connected to the internet, so traffic is best handled by selecting the link with the lowest latency when establishing the connection. By default, Forcepoint Secure SD-WAN uses round trip time measurements between the SD-WAN engine and the destination using the application protocol instead of ping-based probing – thus choosing the most optimal link for the application, not for the ping-probe.

Configuration scalability

In Forcepoint Secure SD-WAN, centralized management is a key component that enables administrators to manage thousands of engines with a single view.

Having a centralized management covers all facets of configuration and delivers benefits such as:

- → Consistent and secure configuration
- → Fast updates to entire fleet of engines
- → Easy of monitoring
- → Low total cost of ownership

Some of the features that deliver the above benefits are:

- → **Template-based policy structure with resource aliasing** to easily build policies that can be shared and managed with many different engines, even if the engine's network neighborhood is different.
- → **Certificate management for SD-WAN** to automate highly secure configurations without burdening administrators.
- → **Central management of the entire engine configuration.** Eliminate command line interface or similar non-scalable methods.
- → **SD-WAN configuration eliminates manual tunnel creation, even full mesh VPN topologies.** Easily drag and drop elements to the VPN, Multi-Link paths between potential endpoints are automatically established.
- → **Integrated Forcepoint Secure SD-WAN Orchestrator enables distribution of full-scale mesh configuration to thousands of peers,** each having multiple endpoints through different ISPs for full redundancy and load-balancing.
- → **Endpoint Context Agent allows endpoint executables to be used as policy selectors,** providing greater policy granularity and SD-WAN traffic visibility.
- → **Integration with Forcepoint Secure Service Edge (SSE) solutions** for a Zero-Trust single vendor solution.

Technical background

Link selection on SD-WAN internet breakout scenario

Because there is a need to apply source NAT for the traffic based on the selected link for the connection, it is not possible to dynamically adjust the selection for an existing connection without breaking it.
However, new connections can select new links as needed (cache timeout, link breakage). Since initial link selection is crucial to user experience, application identification prior to fully establishing the connection is critical.

The challenge in the SD-WAN internet breakout use case is the initial link needs to be identified for the very first packet of the connection. How can Forcepoint Secure SD-WAN provide proper link selection when the application identification is mostly based on traffic identification from the payload that is not yet available when the connection's initial SYN packet needs to be processed?

The solution is advanced application routing, where traffic from the client is duplicated over all possible links so that the initial application payload is visible for identification purposes. After the application is identified, the connection utilizing the appropriate link, based on configuration and performance factors, is allowed to continue while duplicated connections are terminated. Caching the dynamically learned application is used for correct link selection without duplication for every new connection.

When selecting the available link in the internet breakout scenario, simple solutions just use ping time to determine link viability. More advanced solutions can perhaps ping the assumed application target destination through available links, attempting to select a suitable link for the traffic and its destination.

The problem however is that ping (ICMP ECHO) can be treated very differently in the networks versus the actual application connection. Another problem in that kind of separate probing is the probe can test different targets than what the actual application is using due to the different DNS replies received by the prober and the client using the application. Modern cloud applications like Microsoft 365, Teams, Zoom, etc. are highly distributed and there simply is no single target to probe, which makes simplistic approaches fail in practice.

Therefore, the default method in Forcepoint Secure SD-WAN for link selection in the internet breakout is to replicate the TCP SYN packet from the client through all available links and select the link that first returned the SYN-ACK. This probing method is much more accurate as probing is directed to the actual remote endpoint with the same protocol and port as the application connection. The method is also simple and scalable for the administrator, without needing to configure application-specific probe targets.

This probing method is naturally combined with application-specific preferences configured by the administrator so that link usage can be also controlled instead of allowing it to be selected in a fully dynamic fashion. A typical use case is that one of the links is best suited for business traffic and therefore the administrator does not want that link to be utilized for low-priority traffic unless there is an exception in the behavior of the other links.

Reaction to link failure need to be fast to provide a good user experience. Due to the active use of all available links for connection opening (the number of active paths supported is not limited to any practical purposes), reaction to some or even multiple concurrent link failures is immediate for any new TCP connection.

Some applications also use UDP connections, especially to provide the best possible low-latency audio and video experience. Due to the lack of standard connection handshake in UDP connections, links for UDP connections are selected based on cached results for TCP connections to the same destination or previous TCP connection link selections if no specific cache entry is available.

Link selection on SD-WAN tunnel mesh scenario

There are greater link selection options and flexibility with the SD-WAN tunnel mesh scenario. In this scenario, even established connections can move from one link to another link dynamically because NAT is not used for link selection.

Application connections can start through any available path and later, when the application is identified by fingerprinting from the traffic, the application connection can be moved to the most suitable path to provide users with the most optimal experience.

Link selection is also done constantly when link performance changes. For example: if a link gets overloaded, critical application connections can be moved to a better-performing link.

Forcepoint SD-WAN Multi-Link tunnel mesh unique features

Core to the Forcepoint Secure SD-WAN Multi-Link secure tunneling mesh is the ability to build resilient and scalable connectivity over various link types. It builds one logical path between two gateways that can utilize the very different connections available to various locations

No matter if the connectivity is fiber, DSL, mobile broadband, satellite, MPLS, or any other IP transit, Forcepoint SD-WAN Multi-Link can form resilient, scalable and secure logical pathways between the locations – whether they be physical or cloud.

Common troublemakers like dynamic IP addressing from ISP or dynamic NAT are transparently handled and do not cause issues for the administrator. Private IP transit networks can be smoothly integrated and used as one of the network connectivity paths for the most critical traffic.

Combining multiple ISP links with Forcepoint Secure SD-WAN Multi-Link technology is not just for high availability or application-connectivity optimization. It increases the total available network bandwidth for sites as traffic is actively balanced over all available links. Sites may also have backup links that must not be used when other links are available; higher-cost links are only used as failover. These scenarios are also supported by standby link configuration. Such a link is activated only when other configured links are not available.

Usually, the user experience of an application is best guaranteed by selecting the most suitable link for the traffic. To augment this functionality, there are additional useful features that can be used in conjunction with SD-WAN Multi-Link tunneling:

- → **Rule and application based QoS tagging.** This allows the intermediate network to recognize even tunneled traffic correctly and apply, for example, expedited forwarding service based on the DCSP marks set by the SD-WAN engine for the traffic when such service is available.
- → **QoS policies to enforce traffic limits.** This is especially useful to limit bandwidth or link usage of non-critical traffic.
- → **Forward error correction (FEC) by packet duplication.** In some scenarios when link selection and QoS features are not enough, adaptive packet duplication based on observed packet loss for the most critical traffic can help improve the application experience for the most critical traffic.

Conclusion

The advanced application steering feature enables fast and secure site-to-cloud connection, resulting in greater applications performance and productivity. Site-to-site connectivity is also enhanced with Forcepoint Multi-Link capability, enabling administrators to use multiple connectivity options, from fiber, DSL, MPLS, mobile broadband, satellite, boosting the application's performance, network resiliency and bandwidth.

Forcepoint Secure SD-WAN provides centralized visibility and control with high performance that scales to thousands of sites by combining multi-link networking and intrusion prevention with zero-touch deployment and updates. When used with the Forcepoint SSE services, Secure SD-WAN delivers a single-vendor solution that boosts productivity, cuts costs, and reduces risk.

To learn more visit Forcepoint Secure SD-WAN

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, X and LinkedIn.

[FP-The Value of FP SD-WAN Application Steering-Whitepaper-US-EN] 03Feb2025