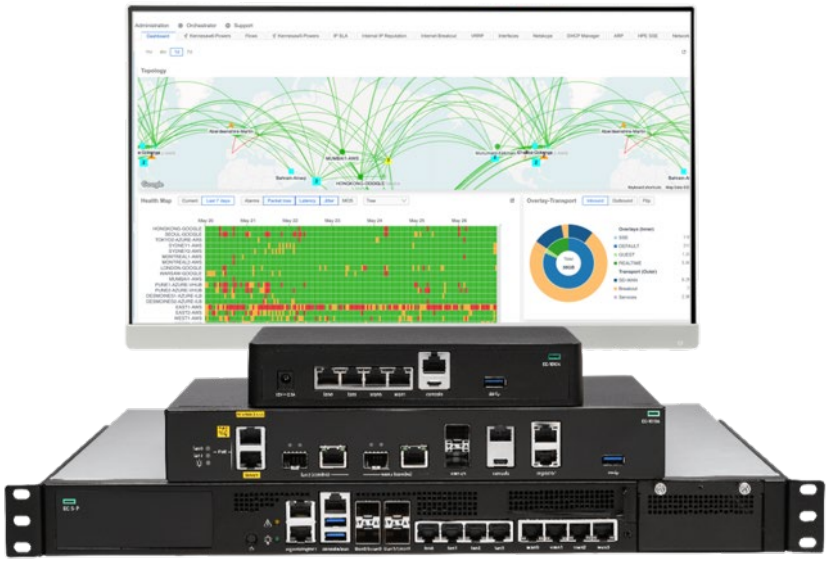
HPE Networking EdgeConnect

Advance secure cloud access with unified SASE built on self-driving SD-WAN and agentic AI



* Product configuration and appearance may vary”

AI is reshaping the cybersecurity landscape. While organizations use AI to improve efficiency and accelerate operations, attackers can use increasingly advanced AI to identify vulnerabilities and scale attacks faster. As applications move to the cloud and users connect from anywhere, this raises a critical concern: not simply whether vulnerabilities exist, but whether applications and resources are exposed to potential attackers.

Reducing exposure requires a zero trust approach that eliminates implicit trust and limits access based on identity and business need. HPE Networking EdgeConnect helps accelerate zero trust adoption by bringing a secure, self-driving SD-WAN together with advanced branch security and HPE Networking security service edge (SSE) as part of a unified SASE architecture. Integration with HPE Networking SSE extends zero trust protection with cloud-delivered security for private applications, SaaS, and internet access, helping reduce the attack surface while simplifying SASE adoption.

HPE Networking EdgeConnect also integrates with HPE Mist, bringing WAN telemetry together with wired, wireless, and data center networking within a broader AI-native operational framework. HPE Marvis uses cross-domain telemetry to provide greater end-to-end visibility, accelerate root-cause identification and troubleshooting, and enable increasingly self-driving network and security operations. It complements HPE Networking EdgeConnect SASE copilot, which provides specialized AI capabilities for SD-WAN and SASE operations.

At the same time, HPE Networking EdgeConnect delivers the advanced SD-WAN capabilities enterprises need to modernize the WAN. Application-aware routing, tunnel bonding, path conditioning, and dynamic traffic steering across broadband, MPLS, and other transports help improve application performance, resiliency, and efficiency while reducing the cost and complexity of traditional WAN architectures.

HPE Networking EdgeConnect platform

The HPE Networking EdgeConnect platform comprises:

- **HPE Networking EdgeConnect** physical or virtual EdgeConnect appliances (supporting any common hypervisors and public clouds) are deployed in branch offices to create a secure, virtual network overlay. This enables customers to move to a broadband WAN at their own pace, whether site by-site or via a hybrid WAN approach that leverages MPLS and broadband internet connectivity.
- **SASE orchestrator**, included with the HPE Networking EdgeConnect platform, it brings SD-WAN and SSE into a unified console for simplified management and consistent policy enforcement. It provides an AI-powered assistant with SASE copilot, streamlining day-to-day management through intelligent analytics and natural language interaction. It also offers unprecedented levels of visibility into both legacy and cloud applications, and centrally assigns policies based on business intent to secure and control all WAN traffic.
- **Threat defense**: HPE Networking EdgeConnect provides advanced threat protection with a built-in firewall including IDS/IPS, Adaptive DDoS, Smart SYN Cookie, web classification and reputation (URL filtering), and IP reputation. These capabilities help detect and block malicious traffic, dynamically mitigate attacks, and strengthen branch security against evolving cyber threats while replacing legacy branch firewalls.
- **WAN optimization** is an optional performance pack that combines WAN optimization technologies with EdgeConnect to create a single, unified WAN edge platform. WAN optimization accelerates performance of latency-sensitive applications and minimizes transmission of repetitive data across the WAN in a single, unified edge platform.

AI-driven operations

- **HPE Networking EdgeConnect in HPE Mist**

Integrating HPE Networking EdgeConnect with HPE Mist and HPE Mist Networking WAN Assurance brings WAN telemetry into a unified, AI-driven operational experience across WAN, wired, and wireless, domains. Network teams gain organization-wide visibility and can drill down from service health into device, application, transport, and security insights. The WAN edge view provides centralized visibility into device, application, and tunnel health, while service-level expectations (SLEs) help identify network conditions affecting user experiences. WAN insights combines real-time and historical telemetry to analyze utilization, latency, jitter, packet loss, congestion, and gateway events. Integrated network and security events, including IDS/IPS, provide additional context for investigating traffic behavior and validating policy enforcement.

Managed by HPE Marvis and advanced agentic AI, these capabilities help teams interpret and correlate telemetry, identify root causes, accelerate troubleshooting, and move toward increasingly self-driving network and security. Driver-Assist HPE Marvis actions for conditions such as MTU mismatch, bad WAN uplink, intermittent WAN connectivity, VPN path down, and negotiation issues, provide recommendations and operational insights, while self-driving actions for automated remediations, including intermittent WAN connectivity actions, will be supported in a future release.

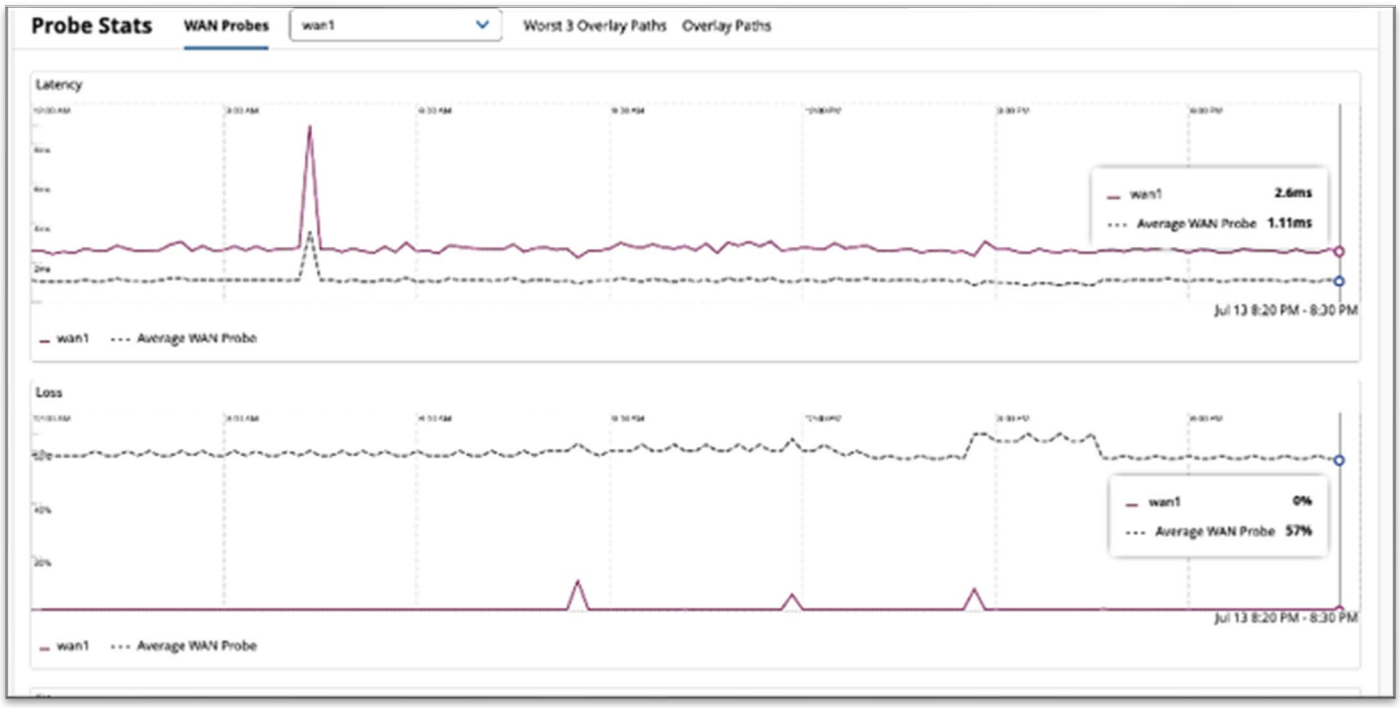


Figure 1. HPE Networking EdgeConnect WAN insights in the HPE Mist platform (here loss and latency)

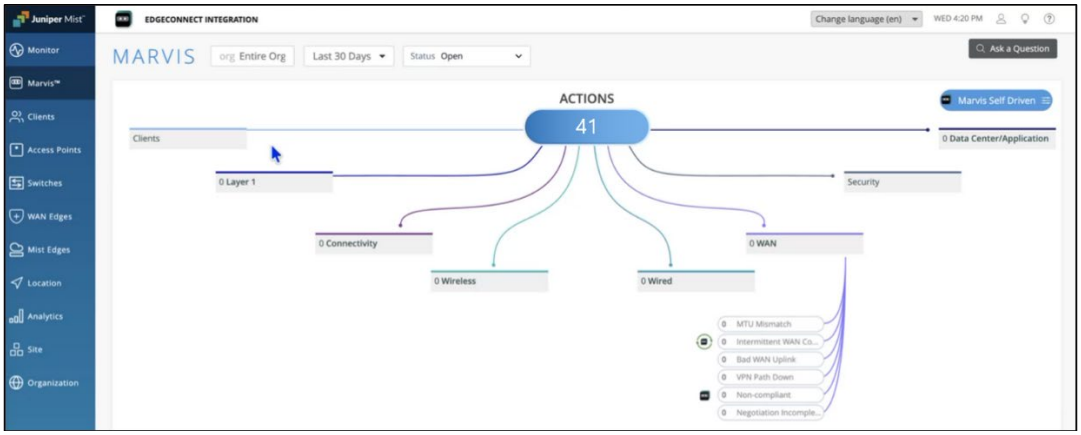


Figure 2. Find issues affecting user experience and get recommendations into resolutions with HPE Marvis actions

– **SASE copilot:** SASE copilot, the built-in AI assistant from HPE Networking EdgeConnect complements HPE Marvis by leveraging AI-powered analytics and natural language queries enabled by generative AI (large language models). This capability streamlines configuration, troubleshooting, and day-to-day management for SD-WAN and SASE by providing intelligent insights, guided recommendations, and automated operational assistance. SASE copilot also simplifies how administrators interact with the EdgeConnect platform by enabling natural language searches across solution capabilities and documentation, making it easier to configure policies, automate workflows, and troubleshoot issues faster.

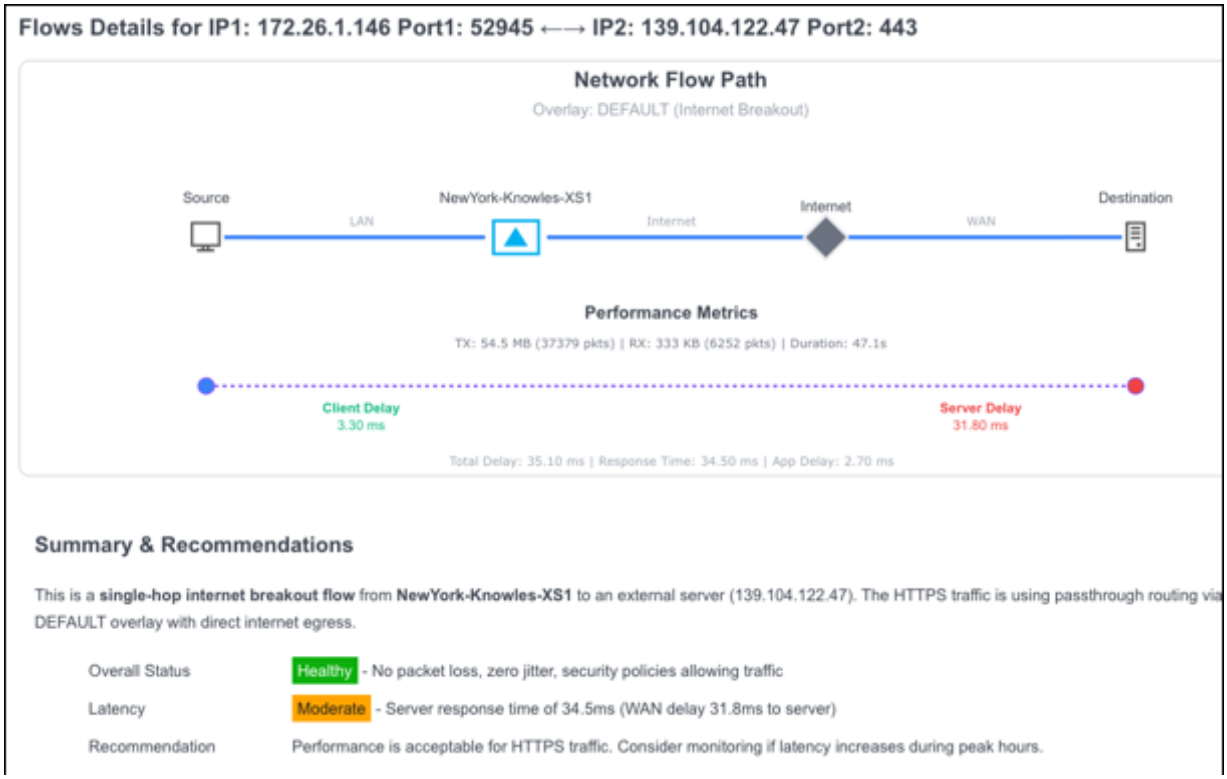


Figure 3. Accelerate issue resolution with SASE copilot, the built-in HPE Networking EdgeConnect AI assistant

HPE Networking EdgeConnect key features

SASE capabilities

– **SASE orchestrator:** HPE Networking EdgeConnect unifies SD-WAN and SSE management through a single SASE orchestrator, enabling administrators to configure connectivity, security, and access policies from one console. This integrated approach simplifies operations by reducing the need to switch between multiple tools while providing centralized visibility and control across users, applications, devices, and locations.

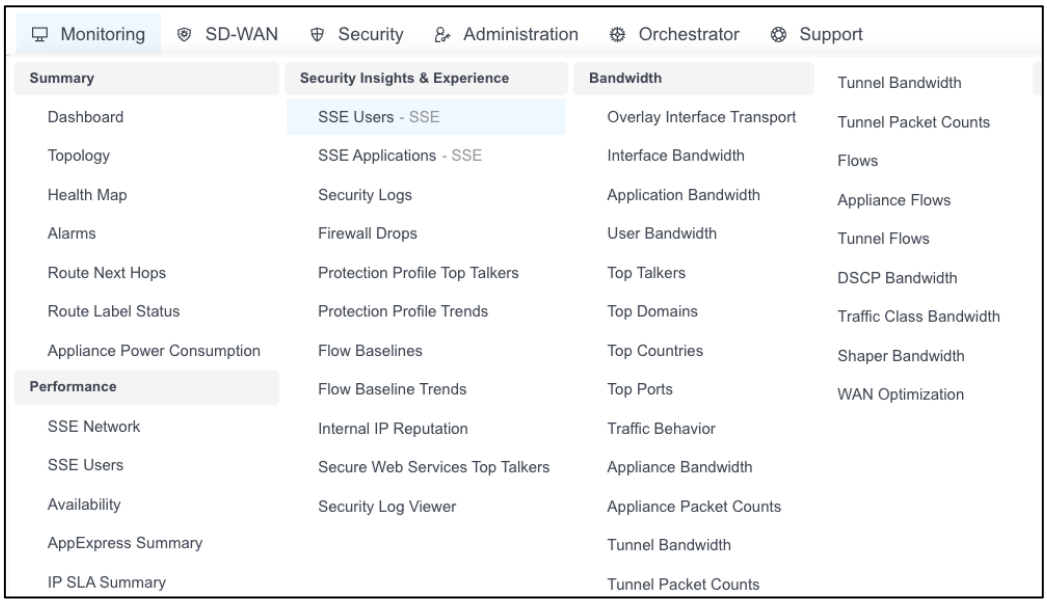


Figure 4. Simplify operations by managing SD-WAN and SSE connectivity, security, and access policies from one unified SASE console.

By bringing networking and security operations together, the unified platform also helps NetOps and SecOps teams collaborate more effectively, streamline change management, and reduce configuration complexity.

With shared visibility into users, applications, and traffic, teams can better understand interactions across the enterprise and consistently enforce policies. This convergence supports zero trust architectures by bringing networking and security together within a unified operational model.

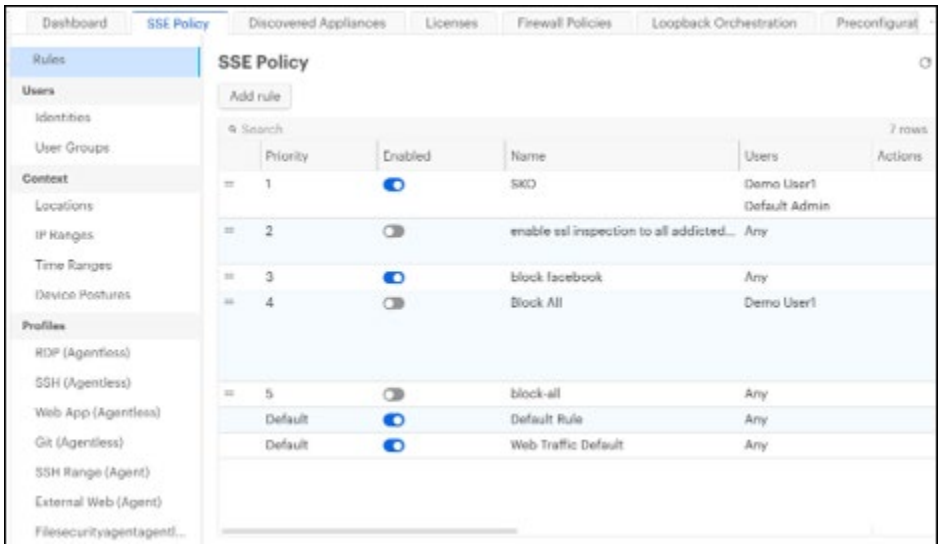


Figure 5. Configure SD-WAN and SSE policies in HPE Networking EdgeConnect

– **Unified SASE**

HPE Networking EdgeConnect not only encompasses the functionalities of SD-WAN but also extends its capabilities to meet the security needs of modern cloud architectures and hybrid workers by optionally adding security service edge capabilities from HPE Networking SSE. Zero trust network access (ZTNA) replaces traditional VPNs with identity-based, least-privilege access to private applications, helping reduce the attack surface. Secure web gateway (SWG) protects users from malicious websites and web-based threats such as phishing and ransomware by inspecting web traffic in real time and enforcing security policies. Cloud access security broker (CASB) provides visibility and control over SaaS applications, helping identify shadow IT and prevent data loss by controlling risky activities such as unauthorized uploads and file sharing. Firewall as a service (FWaaS) provides cloud-delivered firewall protection that continuously monitors and filters network traffic to protect remote users and branch offices from cyber threats. Finally, Digital experience monitoring (DEM) provides visibility into application and network performance to help optimize user experiences and streamline operations.

ZTNA, SWG, CASB, FWaaS and DEM are seamlessly integrated into a single codebase for simplified policy management through a single interface and a single policy engine. Additionally, the solution harmonizes access across the world via Amazon Web Services, Microsoft Azure, and Google Cloud backbone.

HPE Networking EdgeConnect also automates integration with third party SSE partner solutions from Zscaler, Netskope, Palo Alto Networks, Skyhigh Security, Broadcom, and others to create a seamless SASE architecture. Automated orchestration, using a drag-and-drop interface, enables IT to configure consistent enterprise-wide security policies based on business requirements.

– **SSE connector** HPE Networking EdgeConnect simplifies secure access to private applications by embedding an SSE Connector directly within the SD-WAN appliance, enabling ZTNA users to seamlessly reach private resources across the SD-WAN fabric while simplifying ZTNA deployment.

  Traditional ZTNA approaches often require deploying and managing dedicated connectors in data centers or cloud environments to provide access to private applications. This adds operational complexity, introduces additional infrastructure overhead, and can lead to performance bottlenecks.

EdgeConnect eliminates these challenges with a natively integrated SSE Connector, removing the need for additional hardware or virtual appliances. This streamlined approach reduces deployment complexity, optimizes performance through local access, enhances resiliency, and accelerates ZTNA adoption, without requiring extra infrastructure.

Connectors are automatically created from HPE Networking SSE, streamlining deployment and reducing configuration overhead. Connector zones can group multiple connectors into a single logical zone, improving scalability and simplifying policy management. In addition, the integrated connector supports EdgeConnect High Availability (EdgeHA), ensuring resilient access and continuous connectivity for ZTNA users, particularly for demanding applications such as voice and video.

– **SWG service** HPE Networking EdgeConnect provides SWG capabilities for all types of devices on the enterprise network, without the need for an SSE agent. In a traditional setup, securing unmanaged devices such as guests and IoT from web-based threats can be challenging, leading to potential vulnerabilities. The solution extends SWG protective capabilities to these unmanaged devices, ensuring a secure network environment for all. The device traffic is directed to HPE Networking SSE through EdgeConnect using a dedicated 10 Mbps SWG tunnel, eliminating the need to install an SSE agent on each device. For managed devices (devices with an HPE Networking SSE SWG user-based license), traffic is sent directly to HPE Networking SSE, bypassing this tunnel.

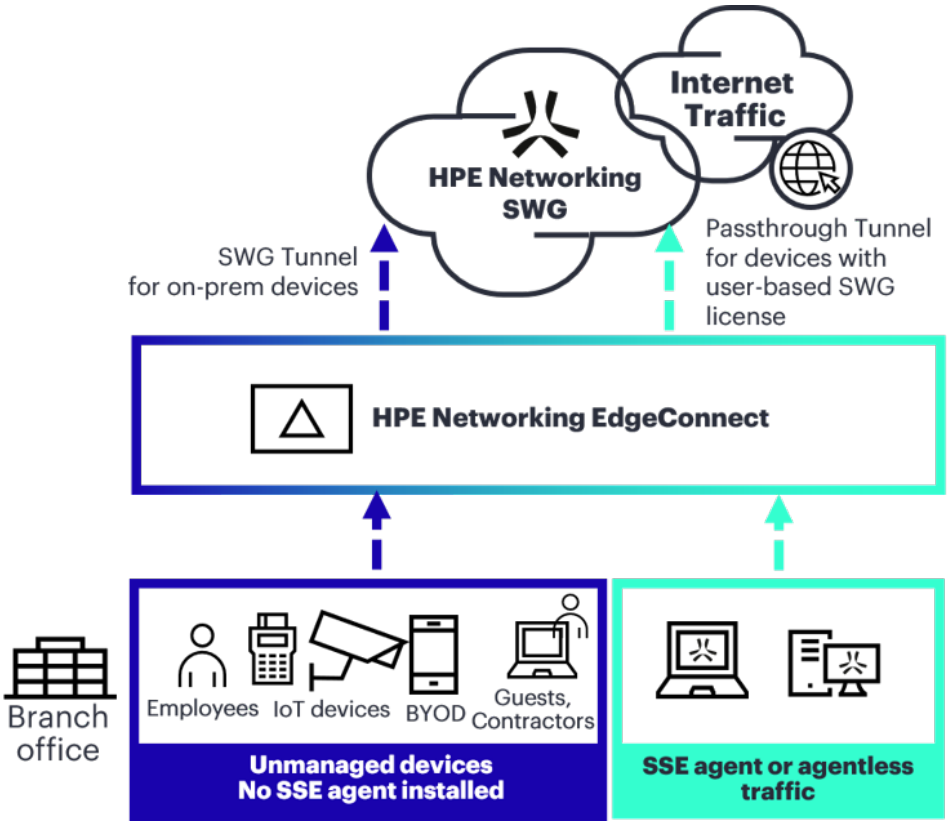


Figure 6. Protect all devices from web-based threats without an SSE agent using the SWG service

HPE Networking EdgeConnect built-in security

– Built-in firewall: EdgeConnect includes an advanced firewall that provides, in a single entity, advanced security features such as intrusion detection and prevention (IDS/IPS), DDoS defense, URL filtering and role-based segmentation, as well as application and user identity awareness. It blocks malware from entering the network based on application, identity, and context, regardless of the port/protocol used and provides increased visibility into network activity and potential risks.

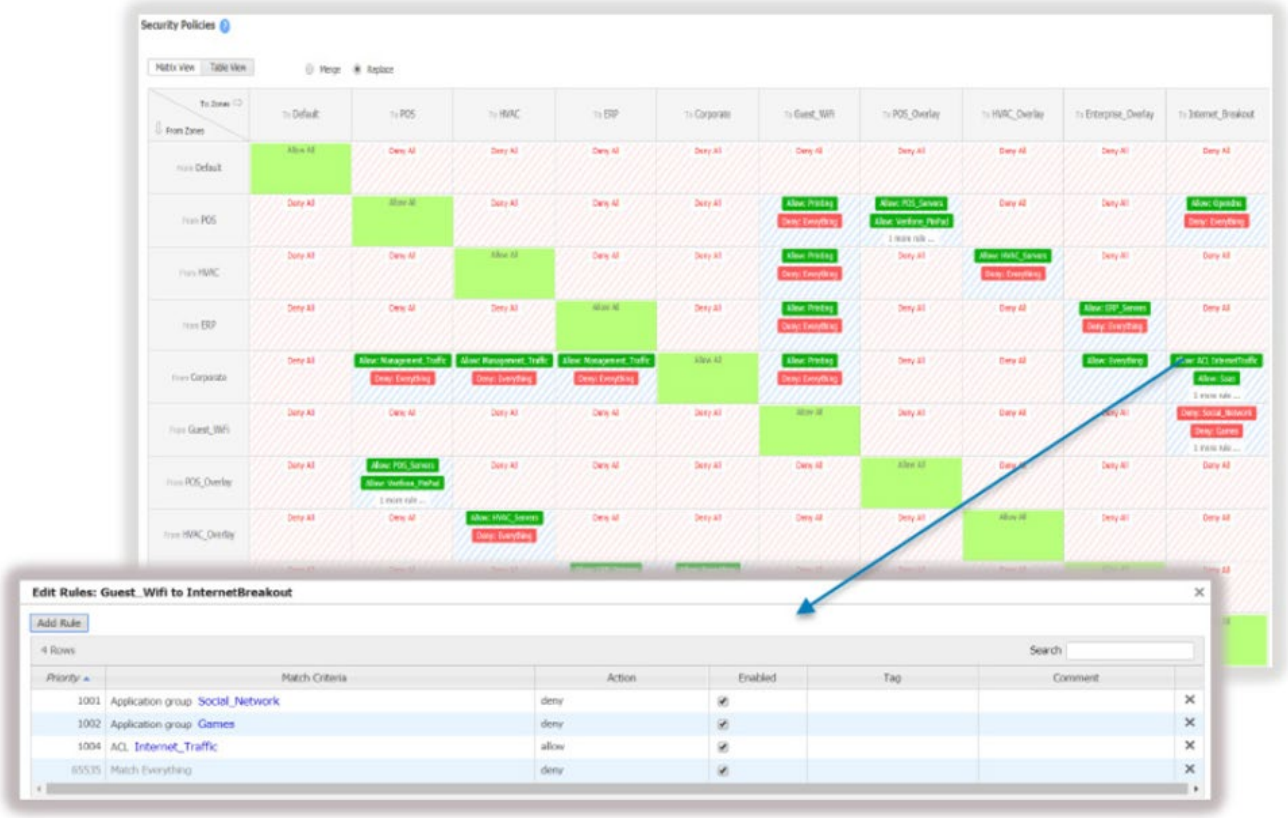


Figure 7. HPE Networking EdgeConnect enables administrators to define firewall zone-based policies.

– Role-based segmentation: Assign roles to users and devices and create role-based policies to micro-segment the network. IT teams can also define zone-based policies by creating secure end to-end zones across any combination of users, application groups and virtual overlays. Moreover, HPE Networking ClearPass Policy Manager integration with EdgeConnect augments application intelligence with user and device identity and role based policy, enabling fine-grained segmentation. The additional identity-based context offers consistent security policy enforcement that can be enforced network wide, from edge to cloud, while also accelerating troubleshooting and problem resolution.

  The solution also integrates NetConductor capabilities from HPE Aruba Central to implement an enterprise wide zero trust architecture, even in complex multi-vendor LAN environments, leveraging EVPN/VXLAN open standards. EdgeConnect can transport role information across the entire fabric, whether the traffic is directed towards a VXLAN-based campus fabric managed via NetConductor or a third-party campus fabric solution supporting EVPN/VXLAN group-based policy. IT architects can easily create role-to-role micro-segmentation policies that can be applied to the entire enterprise. In case the network does not support VXLAN, radius snooping derives the role directly from RADIUS transactions for authentication and authorization or receives them as login and logout events from HPE Networking ClearPass Policy Manager via API.

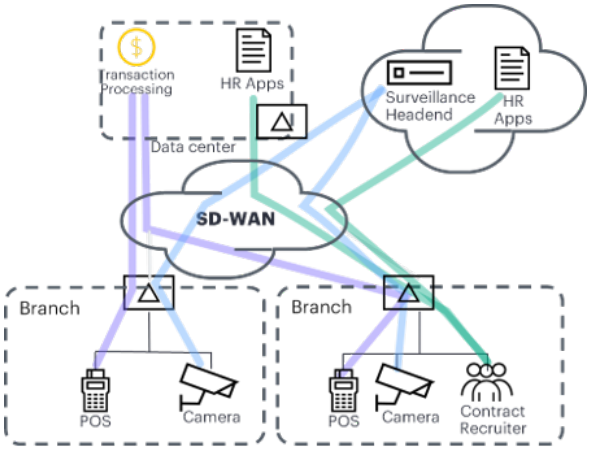


Figure 8. Role-based segmentation ensures that users and devices communicate only with destinations authorized for their roles within the organization.

– **NAC Security:** The integration of HPE Networking ClearPass Policy Manager with HPE Networking EdgeConnect enables administrators to secure EdgeConnect ports using 802.1X and MAC authentication. This is ideal for small locations, home offices, or any place where ports may be vulnerable to unauthorized access. With Network Access Control (NAC) enabled, the EdgeConnect appliance authenticates traffic using 802.1X, supporting EAP-TLS, EAP-TTLS, and EAP-PEAP authentication methods. MAC authentication is also available for devices such as IoT that don't support the 802.1X protocol.

– **Virtual routing and forwarding (VRF) segmentation**

  Network managers can configure and manage separate addressing, routing, and security policies consistently with HPE Networking EdgeConnect across end-to-end segments and microsegments for traffic traversing large-scale multinational enterprises and federations of independent companies. Advanced segmentation eliminates the arduous task of manually stitching together VRF, firewall, and NAT policies in a consistent manner, dramatically simplifying the management of diverse scenarios and providing unprecedented flexibility when contending with overlapping IP address spaces.

– **Threat intelligence with secure web services:** HPE Networking EdgeConnect enhances security with advanced web classification and reputation, as well as IP reputation analysis.

  Web classification and reputation (also known as URL filtering) helps organizations block access to harmful, inappropriate, or illegal websites that propagate malware, spam, spyware, and phishing attacks, as well as websites with sensitive content such as adult or gambling content. The solution tracks more than 1 billion domains and 43 billion URLs and classifies them into more than 85 site categories including high-risk categories, by leveraging machine learning to increase speed and accuracy. To determine web reputation, the service uses site history, age, rank, location, networks, links, real-time performance, and other contextual and behavioral trend data to determine a URL reputation score from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk.

  In addition to web classification and reputation, the IP reputation service strengthens security by providing real time threat intelligence and global visibility into millions of malicious IPs, with new threats detected daily. IPs are categorized by threat types, including Windows exploits, web attacks, phishing, botnets, scanners, reputation, spam sources, mobile threats, and proxies. Using data analysis and correlation, the service assigns a predictive risk score from 1 to 100 for each IP address.

  Based on this score, IPs are classified into five tiers similar to URL reputation scores. This enables administrators to quickly identify and block high-risk IPs, helping prevent cyber threats such as malware, ransomware, phishing, and command-and-control attacks.

– **Intrusion Detection and Prevention (IDS/IPS):** HPE Networking EdgeConnect integrates an intrusion detection and prevention system (IDS/IPS) leveraging signature-based inspection to detect network traffic patterns associated with known attacks. Integrated with EdgeConnect firewall, the system allows application-level selection for inspection based on firewall zones and provides actions such as drop or allow traffic. The system can operate either in inline mode or performant mode. In inline mode, the traffic passing through the sensor is immediately blocked if an intrusion occurs. In performant mode, traffic is analyzed out of path, providing more efficiency without impacting network performance.

  Threat events can be sent to the built-in security log viewer or to an external SIEM such as Splunk for security analytics to monitor real-time threats, enabling IT to quickly act on them.

– **Security log viewer:** EdgeConnect includes a built-in security log viewer within Orchestrator, providing real time visibility into security and network events without requiring external log exports or separate log analysis tools. Network and security teams can directly view and analyze Firewall, IDS/IPS, WAN drops, and Firewall Protection Profile (FPP) logs from a single page, with correlation between log records and flow details. This helps teams identify traffic behavior, validate policy actions, accelerate troubleshooting, and streamline day-to-day security operations.

– **The integration with Splunk** is performed through a custom application, called HPE Networking EdgeConnect Security App, easily downloadable from Splunk base. Compatible with both Splunk Enterprise and Splunk Cloud, the EdgeConnect Security App provides a dashboard view of IDS/IPS events stemming from EdgeConnect. Using Splunk, administrators can filter, sort, navigate, and view the collective security event notifications, overall trends, and top talkers.

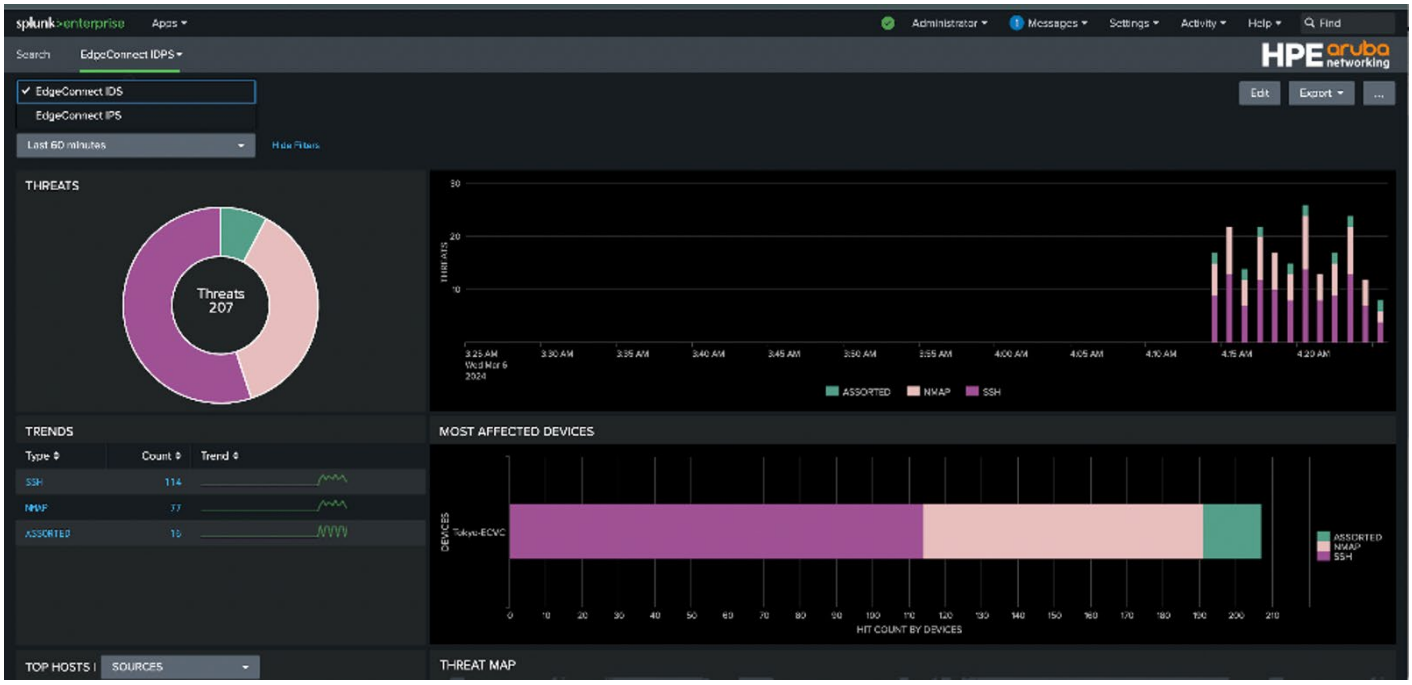


Figure 9. View IDS/IPS events in Splunk stemming from HPE Networking EdgeConnect

– **DDoS defense and firewall protection profile:** HPE Networking EdgeConnect detects and prevents DDoS attacks such as protocol attacks, ICMP floods, SYN floods, IP spoofing attacks and more. The solution enforces strict state handling and limits the number of malicious requests through actions such as rapid aging, drop excess and block source, defined for preset or configurable DoS thresholds. With firewall protection profiles, administrators can enforce different levels of DDoS protection levels across the organization by binding firewall protection profiles to firewall zones.

  To configure DoS thresholds, the solution combines three categories including threshold classification (source-level and zone-level), metrics to monitor (flows per second, concurrent flows and embryonic flows) and IP protocol (TCP, UDP, ICMP, others, and all). Each threshold is associated with a minimum and maximum value. The minimum threshold helps spot problems early on, while the maximum threshold makes sure traffic doesn't drop prematurely. This gives administrators better control, making sure that they only drop traffic when necessary. For each threshold, the solution provides the following actions: log, rapid aging, drop excess, block source, and enables SYN cookies for maximum action. The use of SYN cookies prevents legitimate connections from being dropped when the SYN queue fills up during SYN flood attacks. This is achieved by embedding a cookie in the SYN-ACK response, which verifies that the client IP address is real and not spoofed.

– **Adaptive DDoS** uses machine learning to automatically adjust DoS thresholds, simplifying DoS threshold configuration and eliminating the need for frequent updates due to changing network conditions. Traditionally, administrators set DoS thresholds manually, often based on estimates, requiring frequent adjustments. Adaptive DDoS automates this process with two key functionalities: Auto Rate-Limiting and Smart Burst. Auto Rate-Limiting uses machine learning to regularly calculate a new baseline based on network statistics and patterns. This baseline sets the minimum DoS threshold. Smart Burst is applied to the maximum threshold, automatically allocating unused flow capacity across configured firewall zones. Smart Burst manages "good traffic bursts" (e.g., login spikes in the morning or backups at night) while preventing bad traffic from consuming bandwidth. It offers four modes: Baseline Plus (adds a buffer to the baseline), Committed Burst (proportionally allocates extra flow capacity to firewall zones), Excess Burst (unused Committed Burst capacity is pooled and shared as an additional layer of support), and a custom setting.

– **DDoS analytics:** HPE Networking EdgeConnect includes a comprehensive set of reports for DoS defense such as threshold violations, flow drops, denied hosts and packets counts, top talkers, and alarms such as exceeded DoS thresholds.

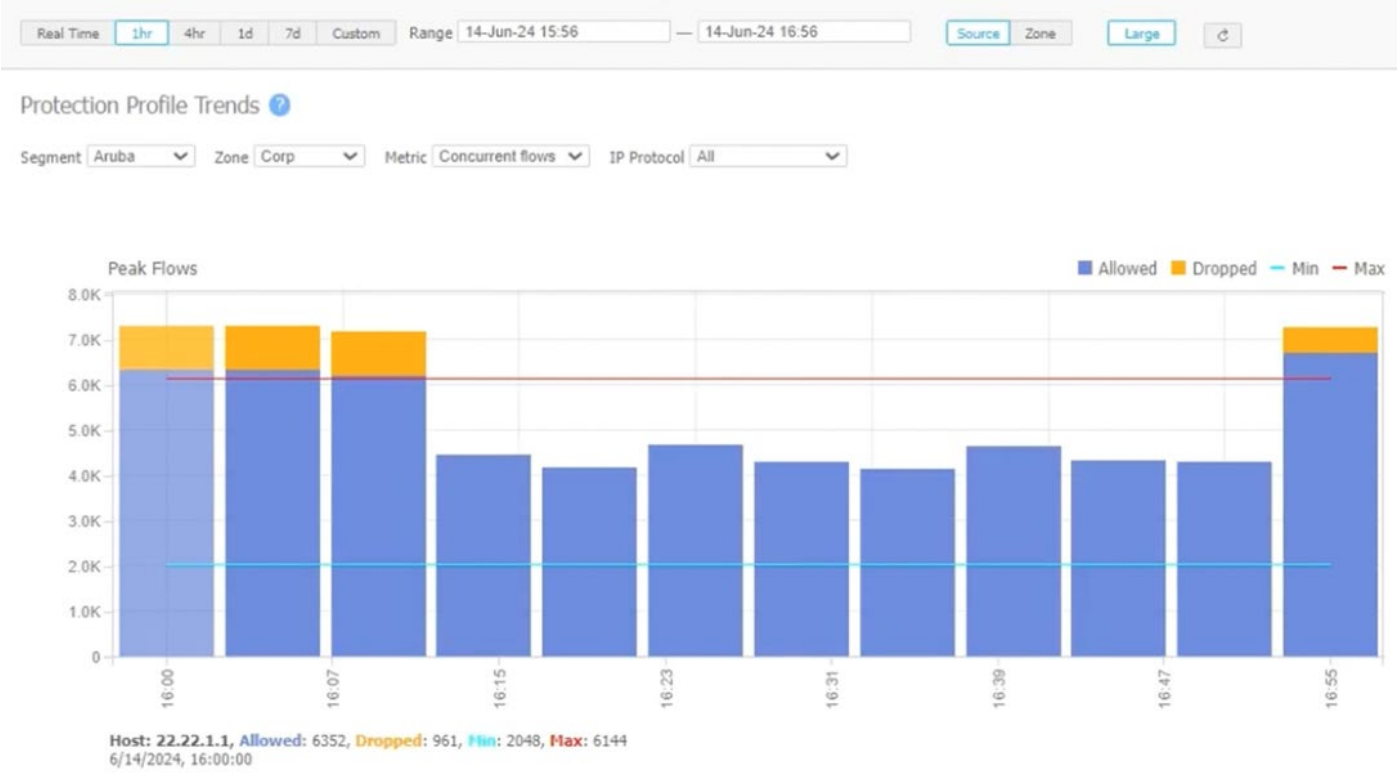


Figure 10. View the number of flows allowed and dropped for each five-minute time interval per firewall zones in EdgeConnect

- **Smart SYN cookie** adds intelligence to the traditional SYN cookie mechanism, optimizing performance where cookie generation can be resource intensive. A cap is automatically enforced on the number of SYN cookies generated to prevent resource exhaustion. SYN packets exceeding the limit are dropped to preserve system stability. The system also evaluates the reputation of the source IPs based on historical behavior. IP reputation applies to "internal" IPs (or LAN IPs) as well as external IPs. Depending on the IP reputation score, the solution decides whether to respond with a SYN cookie, allow a normal flow or denylist the source IP.
- **WAN hardening:** Each WAN overlay is secured edge-to-edge via 256-bit AES encrypted tunnels, meaning no unauthorized outside traffic can enter the branch. With the option to deploy EdgeConnect directly onto the internet, WAN hardening secures branch offices without the appliance sprawl and operating costs of deploying and managing dedicated firewalls. The platform uses either an Internet Key Exchange (IKE)-less IPSec protocol or IKE-based IPSec protocol to encrypt tunnels. It supports IKEv2 with options for certificate-based PKI (Public Key Infrastructure) authentication, pre-shared keys (PSK), and post-quantum PSK to protect data from decryption by quantum computers. The system supports these encryption algorithms: AES-GCM-128, AES-GCM-256, AES-CBC-128, AES-CBC-256, and these hash functions: SHA2-256, SHA2-384 and SHA2-512.

  Cipher Profiles can enable or disable ciphers for cryptographic services, facilitating operations and compliance. Preconfigured profiles, including FIPS, Common Criteria, and CSfC, are available to meet certification requirements.
- **Certifications:** HPE Networking EdgeConnect is certified for FIPS 140-2 Level 1, Common Criteria, Commercial Solutions for Classified (CSfC), SOC2 Type 2, CSA Star level 2, and demonstrated compliance with NIST's guidelines for integrating security into the System Development Lifecycle (SDLC). Additionally, the solution helps comply with relevant industry regulations, including HIPAA, PCI DSS, GDPR, and others.

Performance optimization

- **Business Intent Overlays:** HPE Networking EdgeConnect is built upon an application-specific virtual WAN overlay model. Multiple overlays may be defined to abstract the underlying physical transport services from the virtual overlays, each supporting different QoS, transport, failover, and security policies. Groups of applications are mapped to different business intent overlays to deliver applications to users in alignment with business requirements. Business intent overlays may also be deployed to extend micro-segmentation of specific application traffic from the data center across the WAN to help maintain security compliance mandates.

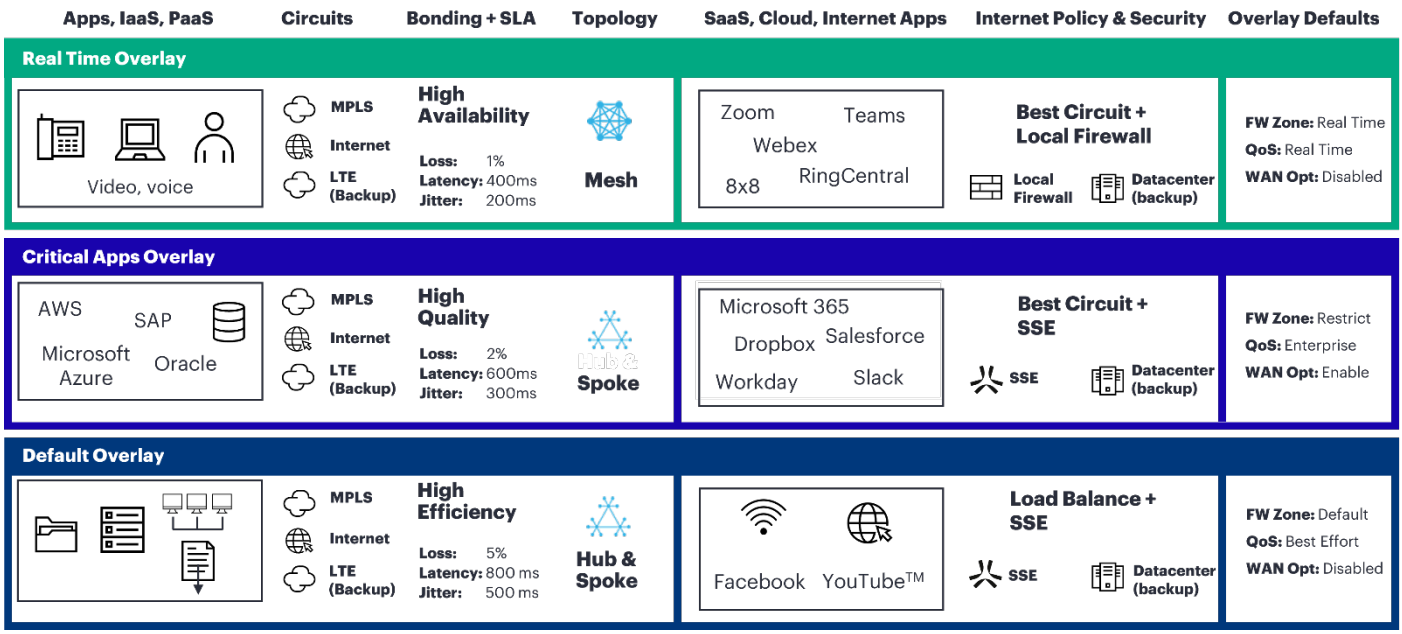


Figure 11. Business intent overlays configured within HPE Networking EdgeConnect

– **Path conditioning:** This feature provides private-line-like performance over the public internet. It includes techniques to overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections, thus improving application performance.

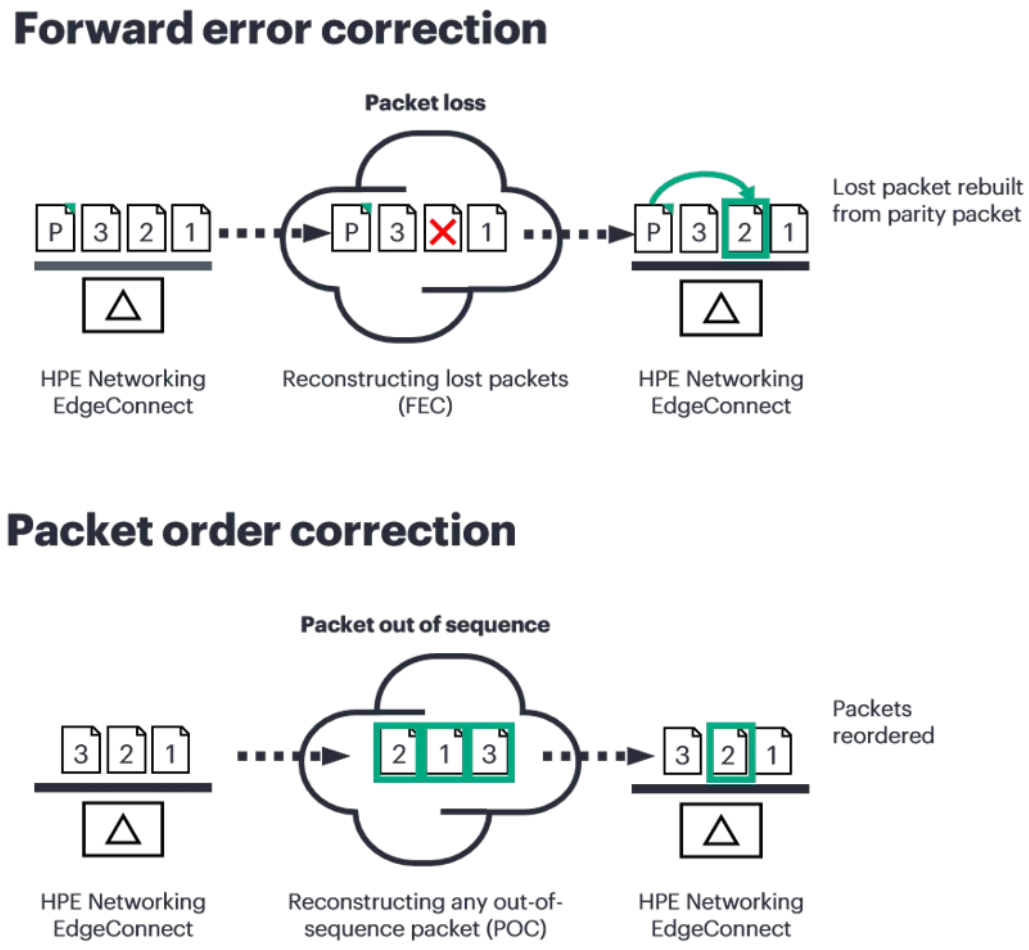


Figure 12. Path conditioning—advanced network and application performance capabilities

– **Tunnel bonding:** Configured from two or more physical WAN transport services, bonded tunnels form a single logical overlay connection, aggregating the performance of all underlying links. Real-time traffic steering is applied over broadband, MPLS, or any combination of links based upon company-defined policies that hinge on business intent. In the event of an outage or brownout, HPE Networking EdgeConnect automatically continues to carry traffic on remaining links or switches over to a secondary connection.

  Network traffic traversing an EdgeConnect can be tuned for availability, quality, throughput, and efficiency. This is accomplished on a per-application basis via business intent overlays. Multiple business intent policies can be created, each with its own specific bonding policy. As part of this policy definition, the customers can customize link prioritization and traffic steering policies based on multiple criteria, including physical performance characteristics, link economics, link resiliency characteristics, and customer-definable attributes.

  AppExpress optimizes user experience for up to 50 business-critical private and SaaS applications such as Zoom, Workday, SAP®, Microsoft 365, and other applications. AppExpress exploits SD-WAN path diversity by automatically selecting the best path for each application. The feature leverages synthetic polling and real-time user traffic observations to intelligently steer traffic regardless of how the application traffic is broken out. This includes:

  - **Local breakout:** It efficiently routes traffic over MPLS, Internet, 4G/5G, or satellite links, automatically choosing the best link for optimal performance.
  - **Optimized steering to IaaS:** the system automatically steers traffic to a virtual instance of EdgeConnect hosted in IaaS platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud™, ensuring efficient data flow.
  - **SSE PoP:** AppExpress selects the best SSE Point of Presence (PoP) that offers the highest performance, further enhancing user experience.

To determine how to steer the traffic and to report performance, AppExpress relies on the Application Performance Index or Apdex. Apdex is an industry standard that measures user experience based on a sample set of latency measurements to produce a normalized score ranging from 0 to 100. Each measurement is put into three levels of responsiveness including "Satisfied", "Tolerating" and "Frustrated" to calculate the Apdex score.

The Apdex score is continuously monitored so that the best path is dynamically selected depending on network conditions. This ensures that users consistently enjoy an unparalleled experience when accessing critical business applications.

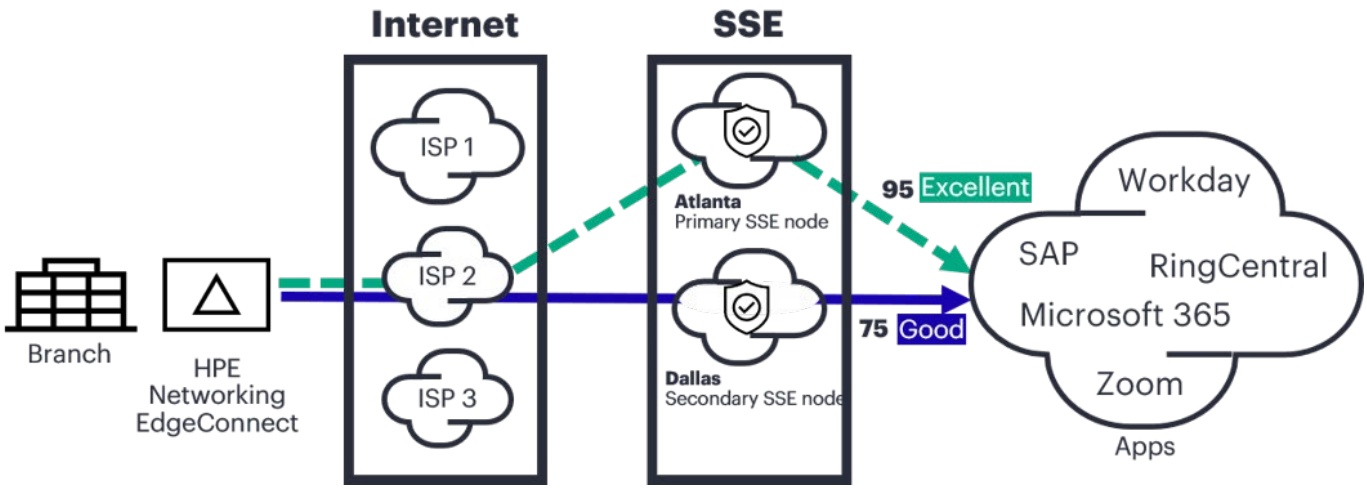


Figure 13. Optimize app performance, including SSE on ramp, with AppExpress.

- **First-packet iQ application classification:** HPE Networking EdgeConnect First-packet iQ application classification identifies applications on the first packet to deliver trusted SaaS and web traffic directly to the internet while directing unknown or suspicious traffic to the data center firewall or IDS/IPS. Identifying applications on the first packet is especially important when branches are deployed behind Network Address Translation (NAT); the correct path must be selected based on the first packet to avoid session interruption.
- **Secure Internet Breakout:** Granular, intelligent traffic steering enabled by First-packet iQ eliminates the inefficiency of backhauling all HTTP/HTTPS traffic to the data center. The solution eliminates the potential for wasted bandwidth and performance bottlenecks for trusted SaaS and web traffic. Trusted traffic is sent directly across the internet while unknown or suspicious traffic may be sent automatically to more robust security services in accordance with corporate security policies.
- **Routing:** HPE Networking EdgeConnect supports standard Layer 2 and Layer 3 open networking protocols such as VLAN (802.1Q), LAG (802.3ad), IPv4 and IPv6 forwarding, GRE, IPSec, VRRP, WCCP, PBR, BGP (version 4), OSPF.
- **Bridge group:** For small locations, HPE Networking EdgeConnect can act as a switch by providing layer 2 connectivity (bridging) between two to four ports of an EdgeConnect appliance, creating a bridge group. Interfaces in the bridge group can be configured with the same parameters available on physical or sub-interfaces, such as segmentation, firewall zones, labels, DHCP server and relay, VRRP, BGP, OSPF, multicast, and branch NAT.
- **High availability:** The HPE Networking EdgeConnect HA cluster protects from hardware, software and transport failures. High availability is achieved by providing fault tolerance on both the network side (WAN) and on the equipment side. The EdgeConnect appliances are interconnected with a HA link that allows tunnels over each underlay to connect to both appliances.
- **Zero-touch provisioning:** Plug-and-play deployment enables branch office deployment of HPE Networking EdgeConnect in seconds, automatically connecting with other EdgeConnect instances in the data center, other branches, or in cloud Infrastructure as a Service (IaaS) such as Amazon Web Services, Microsoft Azure, Oracle® Cloud Infrastructure and Google Cloud Platform™.

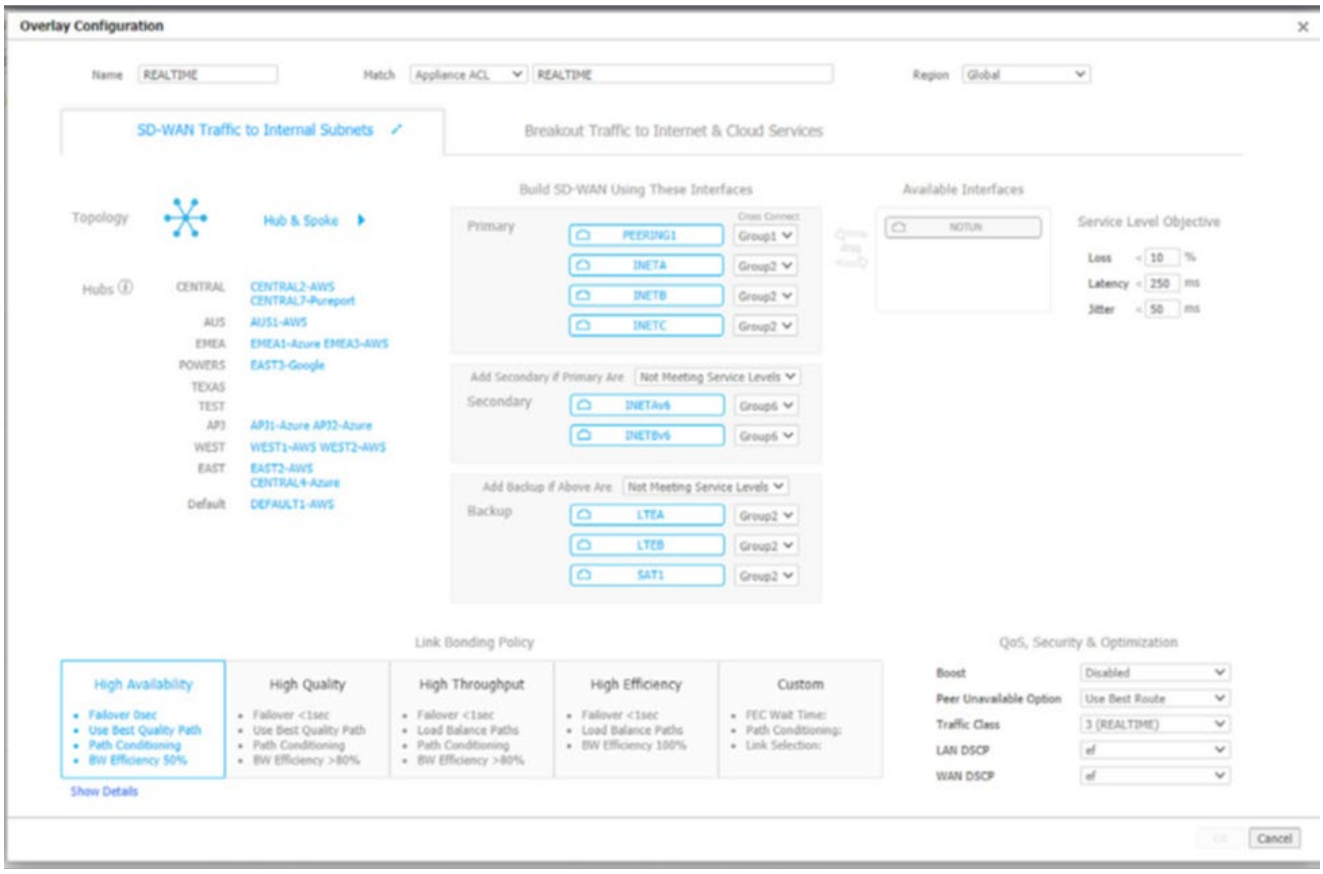


Figure 14. Centrally define and automate distribution of network-wide business intent policies to multiple branch offices.

– **5G cellular bridge/LTE links:** HPE Networking provides flexibility to support high-speed WAN connectivity for enterprise branch offices, pop-up locations, and small office/home offices with either a 5G cellular bridge or USB LTE modem. By using the HPE Networking 100 Series Cellular Bridge or a plug-and-play HPE Networking USB LTE modem with EdgeConnect, enterprises can fully manage their equipment through HPE Networking EdgeConnect Orchestrator, while ensuring optimal connectivity to critical applications and resources, even when primary connectivity experience a failure. The 5G Cellular Bridge and the USB LTE modem features global support for nearly all major carriers and works with many EdgeConnect gateway models. The 5G Cellular Bridge can be mounted anywhere and powered via power over Ethernet (PoE). This provides the option for optimal mounting for enhanced coverage and signal quality.

HPE Aruba Central orchestration

HPE Aruba Central is able to orchestrate a unified SD-WAN fabric between HPE Networking EdgeConnect, HPE Networking SD-Branch and HPE Networking Microbranch devices. This integration allows EdgeConnect appliances to act as VPN concentrators (VPNC) in the SD-WAN fabric, connecting SD-Branch gateways and Microbranch APs to either SD-Branch VPNC or EdgeConnect VPNC in hub locations. Additionally, tunnels and routes are visible on both HPE Aruba Central and HPE Networking EdgeConnect Orchestrator. Organizations with an existing EdgeConnect deployment can leverage this feature to build a consistent networking and security strategy, seamlessly integrating with other HPE Networking products such as SD-Branch, Microbranch, switches and access points.

Multi-cloud networking

Deploy virtual HPE Networking EdgeConnect appliances in a public cloud such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Oracle Cloud, or Alibaba Cloud, as well as other network connectivity providers such as Equinix and Megaport. A virtual EdgeConnect appliance can also be deployed in AWS GovCloud, AWS China, AWS Outposts, AWS Local Zones, or Azure Government Cloud.

By deploying an EdgeConnect appliance in a cloud environment, organizations can optimize or "ruggedize" the first mile between the branch and the public cloud to deliver better network performance, reliability, and quality. This provides a cloud on-ramp to connect on-premises networks or other cloud environments to cloud workloads, removing the manual complexity of connecting branch offices to the cloud.

The virtual EdgeConnect appliances support establishing tunnels over the internet as well as other private connections such as AWS Direct Connect, Microsoft Azure ExpressRoute, Google™ Cloud Interconnect, Oracle Cloud FastConnect, or Alibaba Cloud Express Connect. If a brownout or blackout occurs when establishing SD-WAN tunnels over multiple WAN transports, the remaining link(s) continue to carry traffic so that users don't notice any disruption to voice calls, audio and video conferences, or any other application.

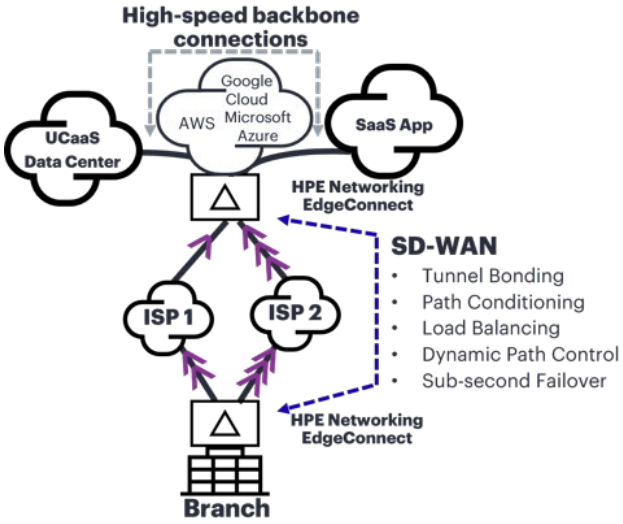


Figure 15. High-speed backbone connections

The EdgeConnect AWS Cloud WAN and AWS Transit Gateway integration is designed to provide seamless, scalable, and secure connectivity between enterprise branch locations, data centers, and AWS cloud infrastructure. This integration simplifies multi-region and global networking by leveraging the capabilities of AWS Transit Gateway and AWS Cloud WAN, in conjunction with the advanced features of EdgeConnect. EdgeConnect with AWS Cloud WAN preserves and extends on-premises network segments into AWS, thereby increasing overall data security, access control, and performance.

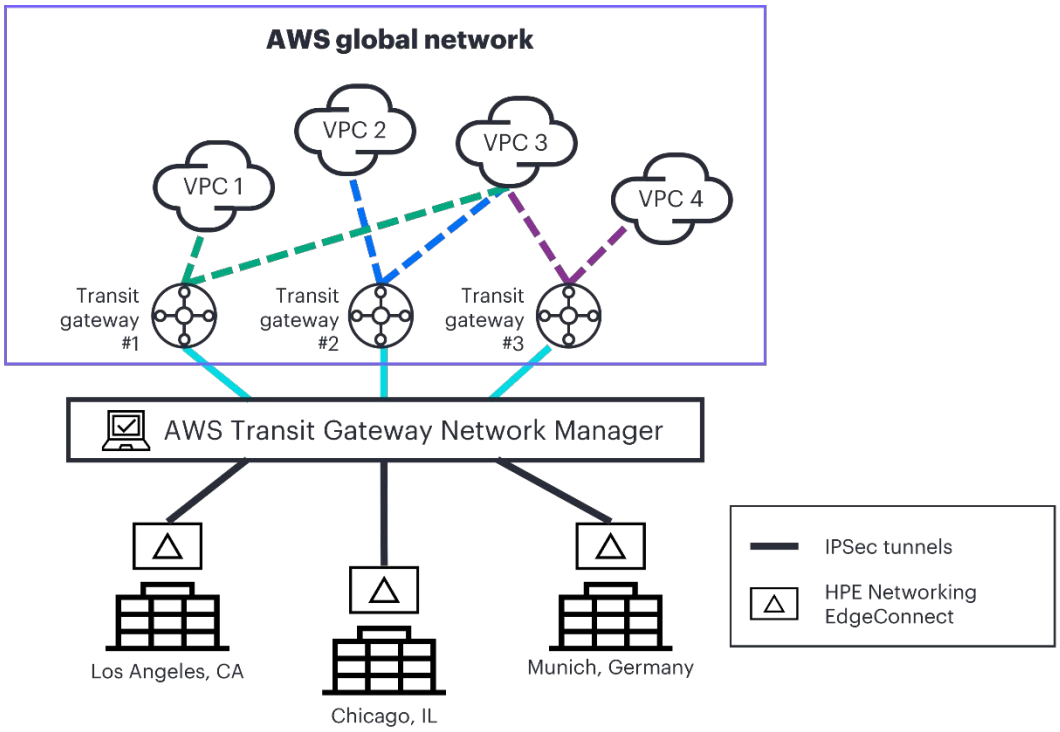


Figure 16. Branch-to-cloud and branch-to-branch connectivity using AWS TGNM

The Microsoft Azure integration allows an EdgeConnect appliance deployed in a Transit Virtual Network in Azure to seamlessly establish connectivity with an Azure Virtual WAN Hub, an Azure Route Server, or an Azure Internal Load Balancer depending on your use case. Additionally, this integration allows administrators to deploy EdgeConnect directly into an Azure Virtual WAN Hub from HPE Networking EdgeConnect Orchestrator. This enables organizations to extend their SD-WAN capabilities into Azure, ensuring optimized performance and security for Azure-hosted workloads and services.

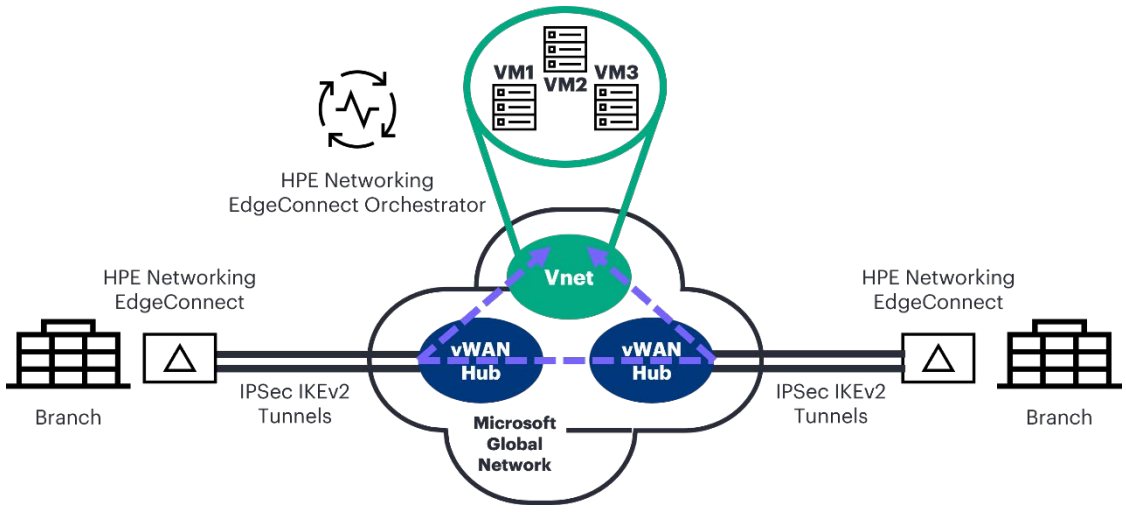


Figure 17. Branch-to-cloud and branch-to-branch connectivity using Azure Virtual WAN (vWAN)

On-ramp to express WAN backbones

This feature allows network administrators to create IPSec UDP SD-WAN tunnels inside third-party, standard IPSec tunnels, enabling direct traffic to the backbones of cloud service providers like AWS, Microsoft Azure, Google Cloud, Megaport, and Equinix. With a Virtual Tunnel Interface (VTI) connection between two locations, this protocol supports static routing, improving traffic flow. This setup leverages the fast, reliable backbones of cloud providers to enhance network performance and reduce latency.

Delivering the highest quality of experience for Microsoft 365

With the Microsoft 365 REST API integration, HPE Networking EdgeConnect continuously learns and discovers new Microsoft 365 end points and/or IP addresses and automatically re-configures EdgeConnect if a new, closer Microsoft 365 end point becomes available. By doing so, users can achieve optimal Microsoft 365 connectivity and performance by reducing the round-trip time (RTT). The EdgeConnect has been independently tested and certified to support the Microsoft 365 Connectivity Principles. As a result of the independent testing, the EdgeConnect platform has been inducted into the Microsoft 365 Networking Partner Program and has been given the official "Works with Microsoft 365" designation.

Boost application performance as needed

HPE Networking EdgeConnect WAN Optimization is an optional feature that includes:

- **Latency mitigation:** TCP and other protocol acceleration techniques are applied to all traffic, minimizing the effects of latency on application performance and significantly improving application response times across the WAN.
- **Data reduction:** Data compression and deduplication eliminates the repetitive transmission of duplicate data. WAN optimization inspects WAN traffic at the byte level and stores content in local data stores. Advanced fingerprinting techniques recognize repetitive patterns for local delivery. Data reduction can be applied to all IP-based protocols, including TCP and UDP.

Why add HPE Networking WAN Optimization?

HPE Networking EdgeConnect appliances alone provide enhanced application performance for broadband or hybrid WAN deployments, utilizing the included packet-based tunnel bonding, dynamic path control (DPC), and path conditioning for overcoming the adverse effects of dropped and out-of-order packets that are common with internet connections.

However, sometimes additional performance is needed for specific applications or locations. As distance between locations increases over the WAN, application performance degrades. This has less to do with the available bandwidth and is more about the time it takes to send and receive data packets over distance, and the number of times data must be re-sent.

WAN optimization use case examples

- Customers replicating to a disaster recovery (DR) site thousands of miles away might want to add WAN optimization to ensure recovery point objectives (RPOs) are not compromised.

- Enterprises with remote sites located in rural areas, or with sites that are exceptionally farther away from the company's data center, might want to add WAN optimization to overcome the effects of high latency. With WAN optimization, customers gain the flexibility to enable enhanced WAN optimization capabilities where and when it is needed in a fully integrated solution. WAN optimization is licensed per Mbps, per month, so customers do not have to pay for WAN optimization across the entire network.

Overcome effects of latency

The time it takes for information to go from sender to receiver and back is referred to as network latency. Since the speed of light is constant, WAN latency is directly proportional to the distance traveled between the two network endpoints. HPE Networking offers a variety of TCP acceleration techniques to mitigate WAN latency, including Window Scaling, Selective Acknowledgement, Round-Trip Measurement, and High Speed TCP.

Microsoft Windows and other applications that rely on the Common Internet File System (CIFS) often take longer to perform common file operations over distance, such as retrieving and sharing files. WAN optimization helps these applications not only by improving the underlying TCP transport, but also by accelerating CIFS through CIFS read-ahead, CIFS write-behind, and CIFS metadata optimizations.

Increase throughput

As packets flow through EdgeConnect appliances, WAN optimization inspects WAN traffic at the byte level and stores content in local data stores. As new packets arrive, the solution computes fingerprints of the data contained within the packets and checks to see whether these fingerprints match data that is stored locally.

If the remote appliance contains the information, there is no need to resend it over the WAN. Instead, specific start stop instructions are sent to deliver the data locally.

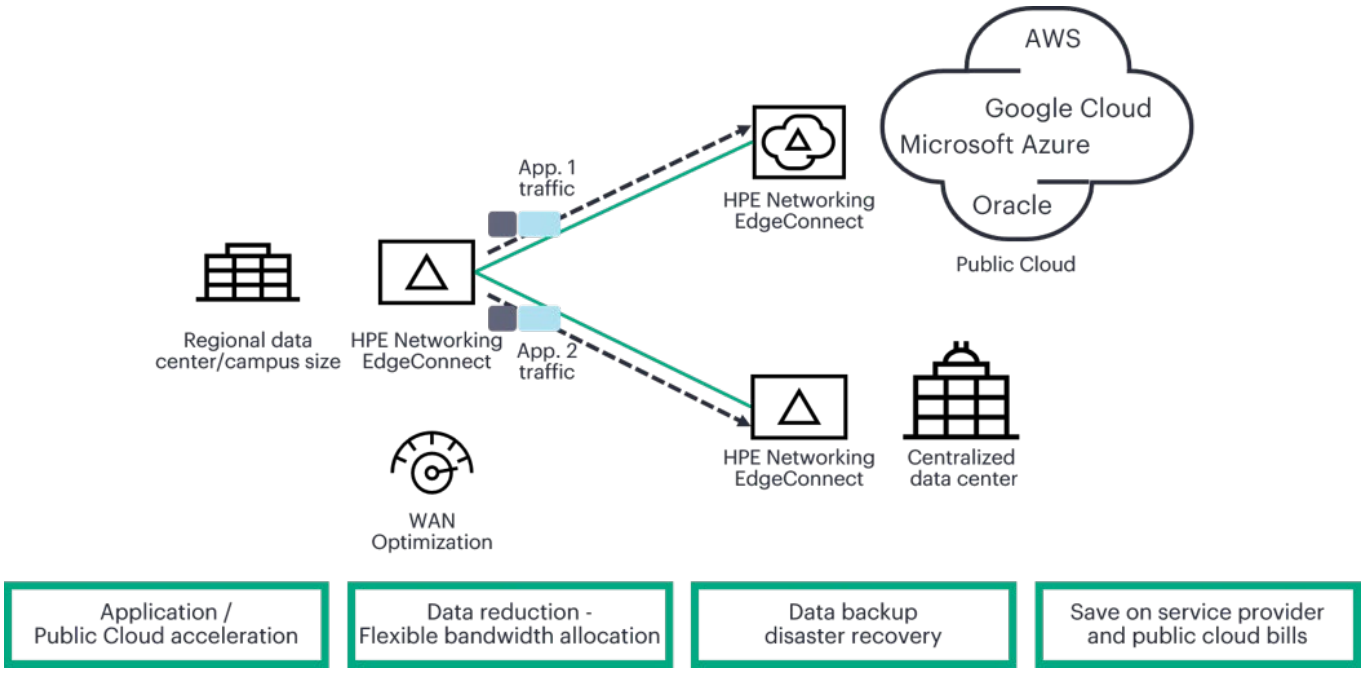


Figure 18. HPE Networking EdgeConnect WAN Optimization reduces latency effects and increases throughput

HPE Networking EdgeConnect gateways

	EdgeConnect EC10104	EdgeConnect EC10106	EdgeConnect EC10108	EdgeConnect EC-S-P
Model	**EC10104**	**EC10106**	**EC10108**	**EC-S-P**
Typical Deployment[1]	Small branch/home office	Small branch	Medium branch	Large branch
Typical WAN Bandwidth[2]	2-500 Mbps	2-1000 Mbps	2-2000 Mbps	10-3000 Mbps
Simultaneous Connections	256,000	256,000	256,000	256,000
Recommended WAN Optimization up to	200 Mbps	350 Mbps	500 Mbps	500 Mbps
IDS/IPS capacity (Performant mode) up to	400 Mbps	1000 Mbps	1500 Mbps	1500 Mbps
IDS/IPS capacity (Inline mode) up to	300 Mbps	750 Mbps	1000 Mbps	1000 Mbps
Redundancy/FRUs[3]	No	No	No	SSD and Power (AC or DC)
Datapath Interfaces[4]	4 x RJ45 10/100/1000	2x 10G SFP+ 2x Combo (SFP/1GbE) 2xGbE (PoE)	2x 10G SFP+ 2x Combo (SFP/1GbE) 2xGbE (PoE)	8 x RJ45 4 x 1/10G Optical

	EdgeConnect M-H	EdgeConnect L-H	EdgeConnect XL-H	EdgeConnect EC10150
Model	**EC-M-H**	**EC-L-H**	**EC-XL-H[5]**	**EC10150**
Typical Deployment[1]	Head office/ DC large hub	Data Center large hub	Data center large hub	Data center large hub
Typical WAN Bandwidth[2]	50-5000 Mbps	2-10 Gbps	2-10 Gbps	Up to 12 Gbps
Simultaneous Connections	2,000,000	2,000,000	2,000,000	2,000,000
Recommended WAN Optimization up to	1 Gbps	1 Gbps	5 Gbps	8 Gbps
IDS/IPS capacity (Performant mode) up to	4 Gbps	7.5 Gbps	7.5 Gbps	10 Gbps
IDS/IPS capacity (Inline mode) up to	2.5 Gbps	4 Gbps	4 Gbps	5 Gbps
Redundancy/FRUs[3]	SSD and Power	SSD and Power	SSD, NVMe, Power	SSD, NVMe, Power
Datapath Interfaces[4]	8 x RJ45 4 x 1/10G Optical	6 x 1/10G Optical	6 x optical interfaces EC-XL-H: 6 x 1/10G/25G EC-XL-H 10G: 6 x 1/10G	2x RJ45 10/100/1000,8 x 1/10G SFP+ or 10/25G SFP28

[1] For best performance, EdgeConnect Operating System Release 9.1 or higher is recommended.

[2] WAN bandwidth assumes bidirectional traffic (symmetric up link and down link). For total WAN throughput (Rx+Tx), multiply these numbers by 2.

[3] FRU Power Supplies are an additional SKU.

[4] EC10106, EC10108, EC-S-P, EC-M-H, EC-L-H, EC-XL-H, and EC10150 all support pluggable optics.

[5] EC-XL-H and EC-XL-H 10G comes pre-equipped with NVMe for maximum WAN optimization.

HPE Networking EdgeConnect gateway specification sheets

EC10104	EC10106	EC10108	EC-S-P
EC-M-H	EC-L-H	EC-XL-H	EC10150

HPE Networking EdgeConnect technical support

Term	Support is included as part of the HPE Networking EdgeConnect subscription license
Web-based support portal	Unlimited access 24x7x365 includes software downloads, technical documentation, and online knowledge base
Software updates	Major and minor features releases; maintenance releases
Technical support	24x7x365 phone / email / web (Global Technical Assistance Centers — TAC)
Response time	30 minutes for high priority (P1) — critical
HW warranty and maintenance	Refer to the HPE Networking EdgeConnect warranty and maintenance policies data sheet for further information

Flexible deployment models

- **HPE Networking EdgeConnect Virtual** — Download and install EdgeConnect from anywhere in the world. The software runs on all common hypervisors, including VMware ESXi™, Microsoft Hyper-V, Citrix XenServer, and KVM. HPE Networking customers who have an IaaS presence in AWS, Microsoft Azure, Oracle Cloud Infrastructure or Google Cloud Platform can deploy EdgeConnect within their hosted cloud environment.
- **HPE Networking EdgeConnect Physical** — For enterprises that are not virtualized in the branch, choose one of the EdgeConnect hardware appliance models for plug-and-play deployment.

HPE Networking EdgeConnect tiered subscription licensing

HPE Networking EdgeConnect licensing provides the SD-WAN capabilities that serve as the foundation for SASE. Customers can extend EdgeConnect with HPE Networking SSE by purchasing SSE licenses separately. HPE Networking SSE offers a range of packages to address different organizational requirements.

HPE Networking EdgeConnect platform is available as a software subscription. Two subscription tiers are available, Foundation and Advanced, in either single or multi-year increments (1, 3, 5, and 7 years) and at multiple bandwidth tiers. Subscription tier mixing is not supported, i.e., every EdgeConnect appliance in an SD-WAN fabric must run either Foundation or Advanced licenses.

Foundation License Tier: The Foundation license tier includes essential SD-WAN features and all of the advanced firewall features. The Foundation license is available at 100 Mbps, 1 Gbps, and unlimited bandwidth tiers. Moreover, the Foundation license supports Hub and-Spoke topology (4 Hubs/region), a limited number of VRFs, and includes a cloud-hosted orchestrator subscription (Foundation OaaS). The Foundation license supports three BIOS, all essential QoS parameters and fundamental data retention capabilities, making it ideal for customers who require a simple, easy-to-manage secure SD-WAN with comprehensive security features.

Advanced License Tier: Advanced license tier includes all HPE Networking EdgeConnect advanced SD-WAN features and all of the advanced firewall features. The Advanced license is available in 20 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, and unlimited bandwidth tiers. Moreover, the Advanced license supports unlimited topology, 64 VRFs and includes a cloud-hosted orchestrator subscription (Advanced OaaS). The Advanced OaaS appeals to enterprises that prefer a zero-CapEx SD-WAN management solution without the capital investment and the associated complexity of managing on-premises infrastructure. The Advanced license supports up to seven BIOS, advanced QoS parameters, and enhanced data retention capabilities making it ideal for customers who do not want to compromise on the secure SD-WAN features and want comprehensive security features.

Enterprises that require on-premises deployment of HPE Networking EdgeConnect Orchestrator can purchase a separate SKU set with the Advanced on-prem license tier. The on prem edition of the Advanced license offers the same rich capabilities as the Advanced license but enables enterprises to manage their own instance of HPE Networking EdgeConnect Orchestrator. It is well suited for customers that require a private installation of their SD-WAN management software.

Optional HPE Networking EdgeConnect WAN Optimization license

WAN optimization: HPE Networking EdgeConnect WAN Optimization is an optional WAN optimization performance pack that may be ordered and deployed flexibly to sites that require application acceleration. WAN optimization is offered in 100 Mbps or 10 Gbps blocks.

Moreover, large global enterprises with multiple business units (BU) or subsidiaries that have a requirement to support different regional QoS or security policies can optionally deploy HPE Networking EdgeConnect Orchestrator Global Enterprise (not applicable for Advanced on-prem license).

Learn more at

HPE.com/EdgeConnect

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

This data sheet is governed by the Hewlett Packard Enterprise current standard sales terms, which include the supplemental data sheet, or, if applicable, the Customer's purchase agreement with Hewlett Packard Enterprise.

Google Cloud Platform, Google Cloud, Google, and YouTube are registered trademarks of Google LLC. Azure, ExpressRoute, Hyper-V, Microsoft, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP is the trademark or registered trademark of SAP SE or its affiliates in Germany and in other countries. VMware ESXi is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. Oracle is a registered trademark of Oracle and/or its affiliates. All third-party marks are property of their respective owners

a00109847enw, Rev. 9

HEWLETT PACKARD ENTERPRISE

hpe.com