Arista WAN Routing System

Modern WAN Evolution

The distribution of users and applications across campus, cloud, SaaS, edge, and data center environments is creating new challenges for wide-area networking architectures and Internet routing:

- Traditional WAN and SD-WAN architectures are often monolithic solutions that do not extend visibility or operational consistency into the campus, data center, and cloud environment
- Many SD-WAN vendors developed highly proprietary technologies that locked clients into their systems and made troubleshooting difficult
- Application architectural evolution often mandates transport diversity and the secure usage of Internet and Cloud Transit options.
- SD-WAN brought valuable features to customers; however, traditional federated routing systems are still the majority of the WAN market.

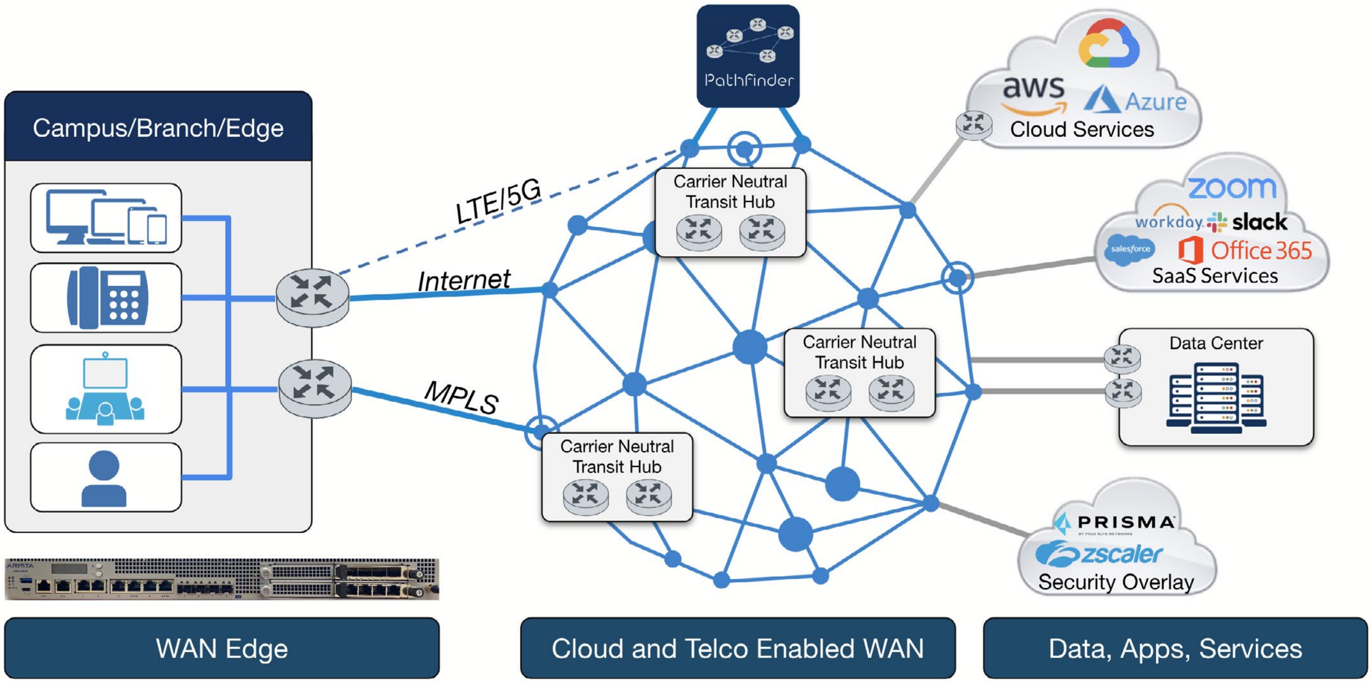


Figure 1: Arista WAN Routing System

Arista introduced the WAN Routing System (Figure 1) to address the challenges above with the following key capabilities:

- Enterprise Class Routing Systems: Physical, Virtual, and Cloud – all using identical EOS software with consistent capabilities. Physical systems are designed for dual-router and carrier-diverse deployments in critical sites, campus, and data centers as well as in carrier-neutral and cloud-adjacent transit hubs.
- Dual Modality: Systems can operate in a classic and stand-alone routing model with traditional federated routing protocols within public and private networks, or operate in a more 'SD-WAN'-like model with configurations procedurally rendered, tested, and automatically deployed with CloudVision Pathfinder Service.
- Multi-Transit: MPLS, Direct Internet, Cloud Transit, 5G/LTE, and SASE/ZTNA Overlay options.
- Transit Hubs: dynamic provisioning and scaling of carrier-neutral densely peered environments with Equinix Metal, Fabric, and Network Edge services (CloudEOS on Equinix).
- Application Identification: identify and classify applications into virtual Topologies which are then automatically traffic engineered.
- Adaptive Overlays: Adaptive Virtual Topology with traffic engineering, application awareness, IPsec AutoVPN cryptography and self-healing.
- Dynamic Path Selection and Path Computation: self-healing and traffic engineering for edge, aggregation, and core.

Solution Overview

The Arista WAN Routing System solution architecture (Figure 2), enabled with the CloudVision Pathfinder Service delivers the following key capabilities

- WAN Fabric - Secure Encrypted Transport
- Adaptive Virtual Topology - Application-Aware Routing
- CloudVision Pathfinder Service
- Service Onboarding
- Enterprise-Class Routing System

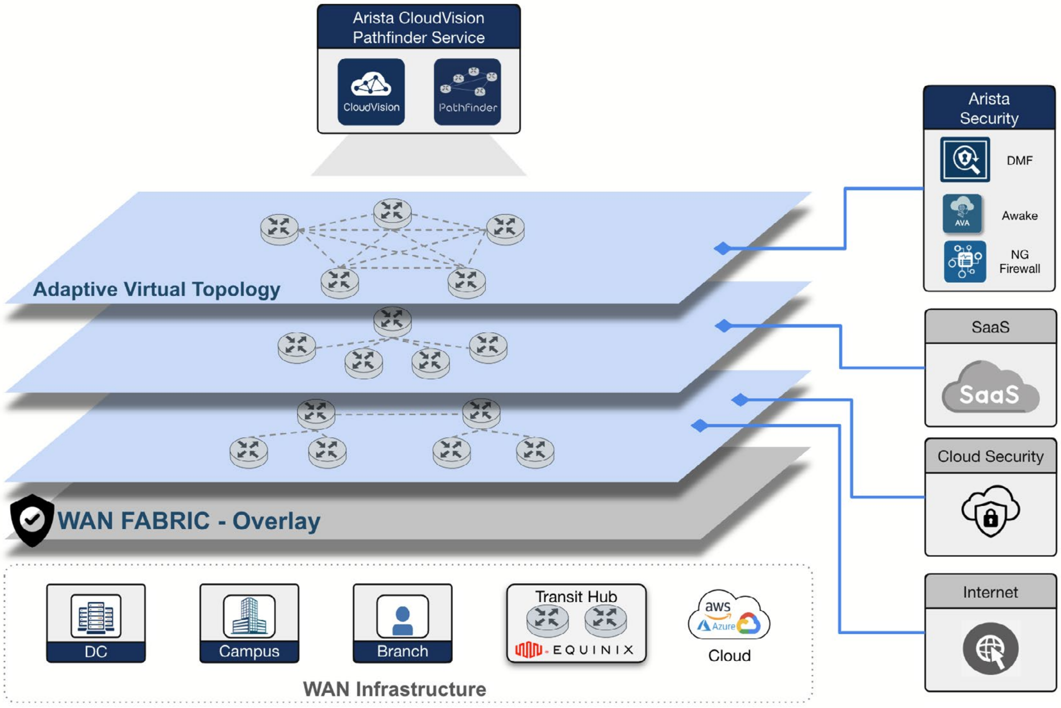


Figure 2: Arista WAN Routing System Solution Architecture

WAN Fabric - Secure Encrypted Transport

To provide secure encrypted transport over the end-to-end network, a WAN fabric is built between the routing systems deployed at each customer location - across data center, campus, branch, and cloud. The WAN fabric is a secure overlay network, built and maintained by combining Dynamic Path Selection (DPS), Inband Network Telemetry (INT), and Automated Virtual Private Network (Auto-VPN) technologies

DPS provides secure tunneled paths using IPSec encryption over MPLS, public internet, and 5G/LTE transport networks. Inband Network Telemetry (INT), monitors the network performance (latency, jitter, packet loss, throughput, and MTU) of each path and is significantly more accurate than out-of-band monitoring or probe-based solutions. DPS steers application traffic into these different paths based on the real-time performance attributes of the network. For example, if there is performance degradation on an MPLS link, sensitive real-time traffic such as IP voice can be rerouted to a different path with better performance.

Managing a large end-to-end network can be operationally challenging. Arista Auto-VPN automatically discovers the routing systems at remote sites, whether directly connected to the WAN or Internet including behind a NAT device, and establishes DPS tunnels between all of the sites greatly simplifying network operations.

Adaptive Virtual Topology - Application-Aware Routing

Arista Adaptive Virtual Topology (AVT) is a network abstraction construct on top of the WAN Fabric that allows customers to put applications into groups, applying different network policies, including:

- Application Group Policy and Ingress Classification: DPI (Deep Packet Inspection) based to identify thousands of applications automaticall, as well as classic interface, sub-interface, and 5-tuple based classification
- Network Topology Construction: hub-spoke, full mesh and regional full mesh
- Traffic Engineering: maps the AVT and its associated performance requirements to the available paths based on real-time path performance, business policy including path cost and billing model, and traffic prioritization
- Internet Exit Policy: local internet exit, remote internet exit through a firewall and internet exit through a cloud security/SASE provider
- QoS Policy:, marking, queuing and shaping are also bound to the AVT
- Cloud Transit: the ability to utilize a cloud provider’s high performance backbone can be set on a per-AVT basis

For example, call center voice traffic often requires full-mesh connectivity using the lowest latency paths available; a credit card processing application might specify a hub-spoke topology, with an MPLS link as primary and Internet link as backup, to meet compliance requirements; SaaS applications such as Office365 benefit by having traffic locally break out to the Internet and directed to the SaaS provider’s closest point of presence. The AVT construct allows customers to provision network services that meet and then automatically maintain application SLAs.

CloudVision Pathfinder Service with Transit Hubs - Traffic Engineering

The Enterprise WAN is getting more complex with the adoption of public cloud, SaaS, and a distributed workforce, the point-to-point tunnel-based approach from many SD-WAN vendors is often not enough to meet today’s IT requirements.

Arista introduced the CloudVision Pathfinder Service combined with Transit Hubs to provide a holistic traffic engineering approach to improving the end-to-end enterprise application experience and provide self-healing capabilities across the Internet, Cloud, critical sites, and campus and data center environments. Arista Pathfinder Service includes the Pathfinder Path Computation Engine that monitors and dynamically reprograms all of the routing systems within an enterprise and the network performance of all paths, computing the best possible path for every application. This could be a direct path between two sites or a multi-hop path that goes through a transit hub point.

Transit Hubs are physical or virtual WAN routing systems deployed in carrier-neutral and cloud-adjacent facilities with dense telecommunications interconnection. Arista has partnered with Equinix to allow enterprise customers to deploy Transit Hubs using CloudEOS on Equinix Network Edge and Bare Metal Cloud Platforms and leveraging the Equinix Fabric backbone to deliver a superior experience for enterprise applications.

- Fast access to the public cloud providers via Equinix's 27+ global metros
- End-to-end encryption from the data center, campus, and branch to the cloud
- Improving site-to-site connectivity using Equinix Fabric with Arista Pathfinder Service
- Flexible deployment with Equinix Network Edge and Bare Metal Cloud

Service Onboarding

Seamlessly enabling enterprise network services like firewalls, IPS, IDS, observability tools and many more are a key priority for IT teams. The Arista CloudVision Pathfinder solution allows customers to connect the Arista WAN Fabric to internal and external services and define an AVT policy to route traffic to wherever the service resides. Typical enterprise network services include:

- On-premises Firewall Insertion
- Secure Internet Exit (local or remote with firewall)
- Cloud Security Access (SASE) / ZTNA
- SaaS Application Access
- Enhanced Observability (with Arista DMF)
- Network Detection and Response (with Arista NDR and Edge Threat Management)

All of these can be easily inserted using the Arista CloudVision Pathfinder solution.

Enterprise-Class Routing Systems

The Arista 5000 Series of WAN Systems, powered by EOS, offer the right levels of performance, scale, and resilient systems design to meet modern enterprise WAN edge and aggregation requirements with the following highlights:

- Delivering from 5Gbps to over 50Gbps of bidirectional AES256 encrypted traffic
- Supporting 1/10/100GbE interfaces and flexible network modules
- Redundant power supplies and fan assemblies
- Arista 5310 is equipped with FTW (fail-to-wire) ports to ensure WAN link availability during power outages, system reloads, and other disruptive events.

Arista 5310 WAN Routing System (Figure 3), provides up to 5Gbps IPsec encrypted throughput, with 4x 1/10GbE RJ45 Ports (with 2x Fail to Wire Ports) and 4x 1/10GbE SFP+ Ports, and two expansion slots.

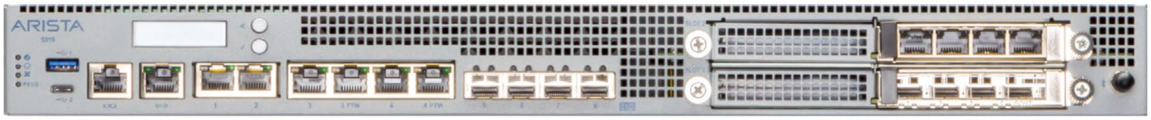


Figure 3: Arista 5310 WAN Routing System

Arista 5510 WAN Routing System (Figure 4), provides up to 50Gbps IPsec encrypted throughput, with 16 x 1/10G SFP+ Ports, and four expansion slots.

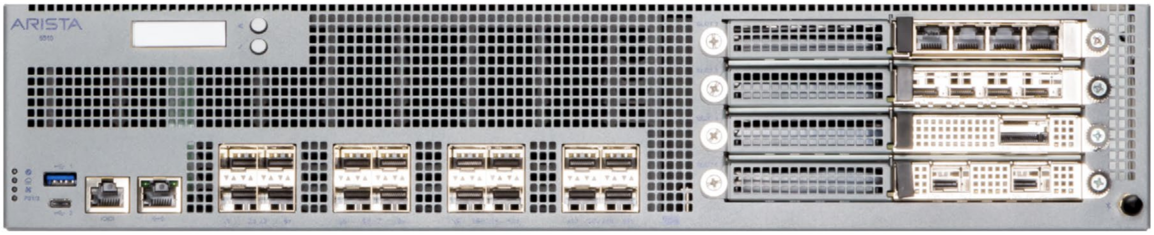


Figure 4: Arista 5510 WAN Routing System

The Arista 5000 Series WAN Systems are suited for deployments in critical sites requiring high availability and service resilience, across multiple different WAN service providers.

In addition, Arista CloudEOS Router (Figure 5) is offered in public cloud providers like AWS, Azure, GCP, and Equinix platform, as well as private VM deployment with the support of VMware ESXi and Linux KVM.

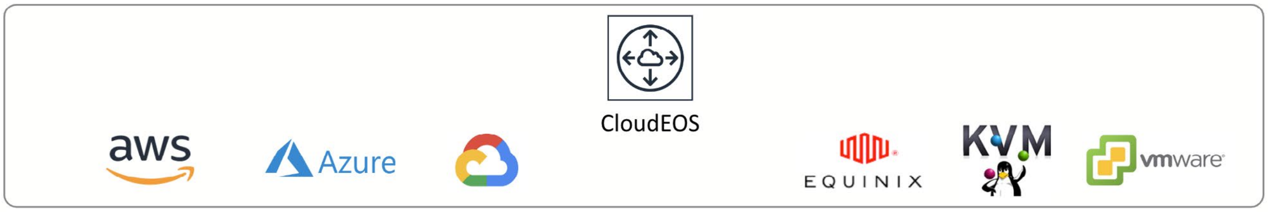


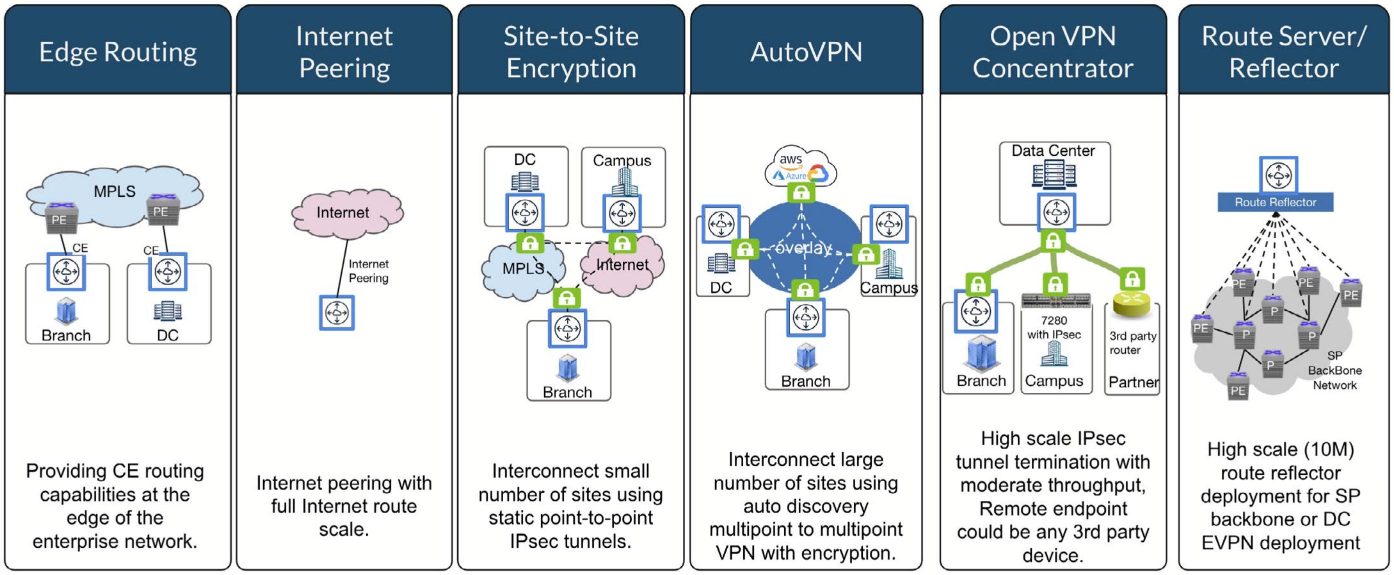
Figure 5: Arista CloudEOS Router for Cloud and Virtual Deployment

Use Cases

The dual modality of the Arista WAN Routing System provides flexibility to deploy the solution for different use cases:

Traditional WAN Services

In enterprise WAN networks today, traditional WAN services are still being delivered on routed WAN networks, based on traditional federated routing protocols and usually manually configured via the CLI. Arista WAN Routing Systems can be deployed as a standalone system to meet these well-known and established requirements, but with a more modern automated approach (Figure 6).



Edge Routing: Providing CE routing capabilities at the edge of the enterprise network.

Internet Peering: Internet peering with full Internet route scale.

Site-to-Site Encryption: Interconnect small number of sites using static point-to-point IPsec tunnels.

AutoVPN: Interconnect large number of sites using auto discovery multipoint to multipoint VPN with encryption.

Open VPN Concentrator: High scale IPsec tunnel termination with moderate throughput, Remote endpoint could be any 3rd party device.

Route Server/ Reflector: High scale (10M) route reflector deployment for SP backbone or DC EVPN deployment

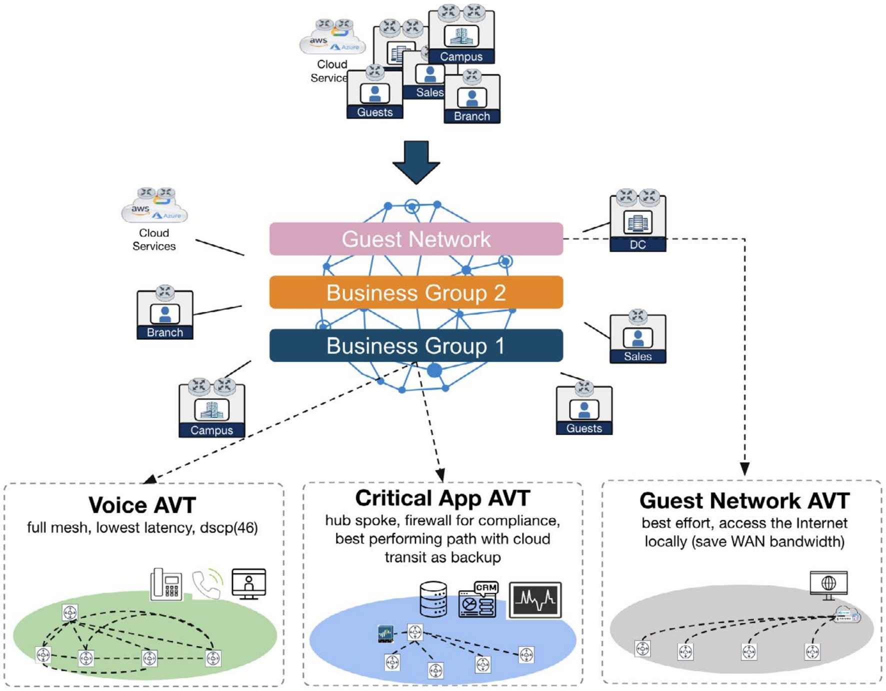
Figure 6: Traditional WAN Services - Use Cases

Modern WAN Services

The evolution of applications from residing solely within enterprise data centers to a modern hybrid environment with distributed systems across campus, branch, edge, cloud, SaaS, and data centers has been the primary driver of new WAN architectures. The Arista WAN Routing System enabled by CloudVision Pathfinder Service, allows enterprise customers to modernize their WAN infrastructure and deliver a reliable and secure WAN service at the SLA that each application and user needs.

Delivering Network Services on a Shared infrastructure

Providing network services to internal and external customers over a complex WAN environment is always a challenge for IT organizations. The Arista CloudVision Pathfinder solution (Figure 7) allows customers to create different tenants for multiple business groups and separate out network resources across a shared WAN infrastructure. Within a tenant, Adaptive Virtual Topologies (AVTs) are used to further define the network policies for different users and applications.



aws
Azure
Cloud Service
Campus
Sales
Guests
Branch
Cloud Services
Guest Network
Business Group 2
Business Group 1
DC
Branch
Sales
Campus
Guests
Voice AVT
full mesh, lowest latency, dscp(46)
Critical App AVT
hub spoke, firewall for compliance, best performing path with cloud transit as backup
CRM
Guest Network AVT
best effort, access the Internet locally (save WAN bandwidth)

Figure 7: Delivering Network Services on a Shared infrastructure

Optimizing User and Application Experience with Transit Hubs

With an ever-changing WAN environment, link failure or performance and quality degradation can happen at any time. The CloudVision Pathfinder Service (Figure 8) continuously monitors all available WAN links in real-time and finds the lowest latency and optimal link that will deliver the best operator and client experience for their critical applications. If there is a network outage or performance degradation, traffic will be rerouted for a better experience.

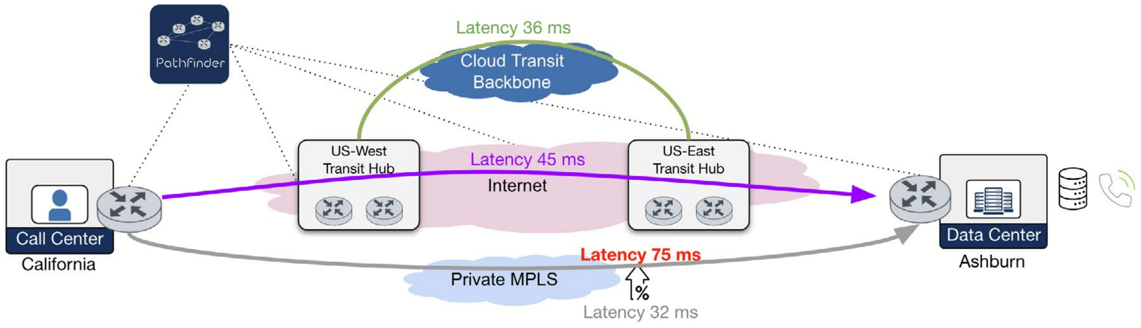


Figure 8: Optimizing User and Application Experience with Transit Hubs

Hybrid Cloud and Multi-Cloud

Consistent and secure connectivity for hybrid-cloud and multi-cloud requirements are a top priority. With Arista CloudEOS deployed at the edge of the public clouds (Figure 9), integrating with cloud-native services like AWS Transit Gateway, enterprise customers seamlessly connect their existing on-premises environments into the public clouds. This provides IPSec encryption for all data in transit, and network segmentation and enables direct edge-to-cloud access to avoid backhauling traffic through their data center or core network.

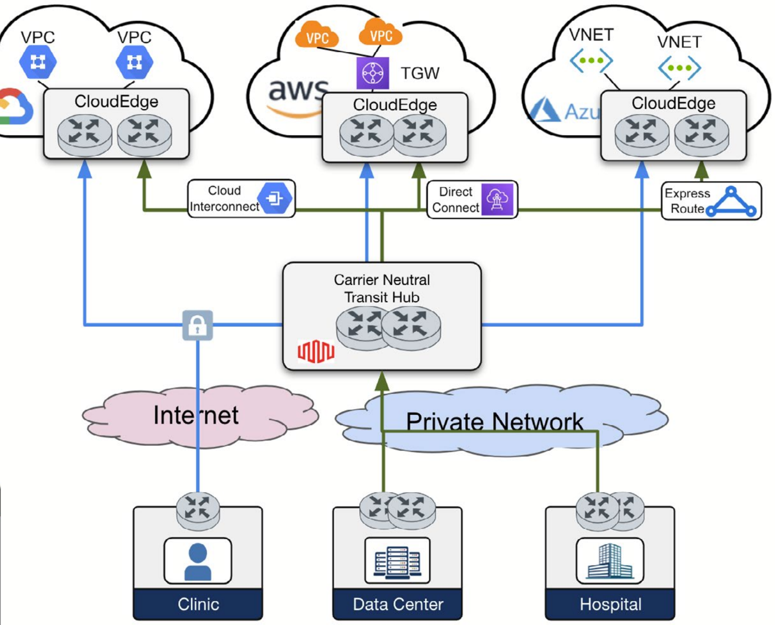


Figure 9: Multi-Cloud Connectivity

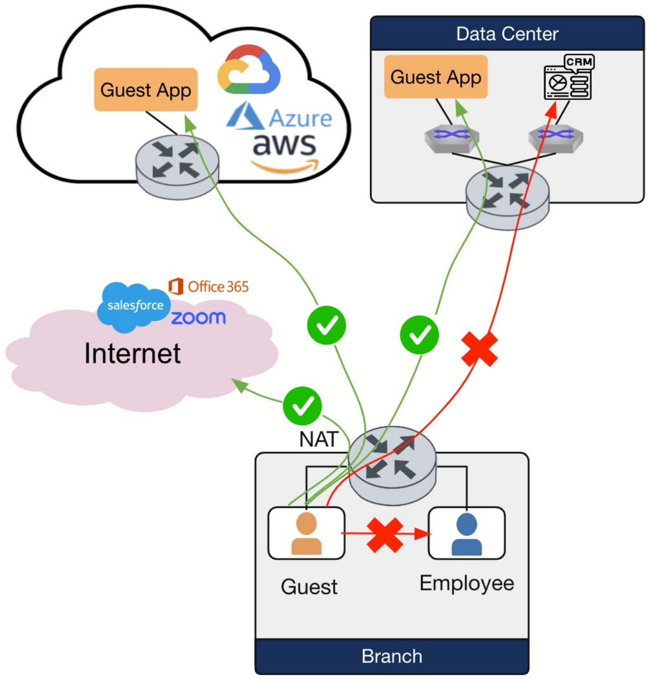


Figure 10: Providing Guest Network Access

Guest Network Access

Providing network access for guests, contractors, and partners to the existing WAN infrastructure is a key requirement for modern WAN architecture. The Arista CloudVision Pathfinder solution protects corporate resources and assets from being accessed by external users (Figure 10).

Internet Access

Within an enterprise WAN environment, employees, guests, vendors, and enterprise applications need access to the Internet securely. The Arista CloudVision Pathfinder solution is designed to provide a flexible Internet access path for different groups and applications based on their requirements and the security policies of the organization.

In the following diagram (Figure 11), different Internet access policies are applied within an organization for

- Applications: Internet traffic needs to be inspected by an on-premises firewall because of compliance reasons
- Employees: the employee to Internet traffic needs to go through a cloud security provider or via a pair of firewalls
- Guests: the guest can access the Internet directly from the branch

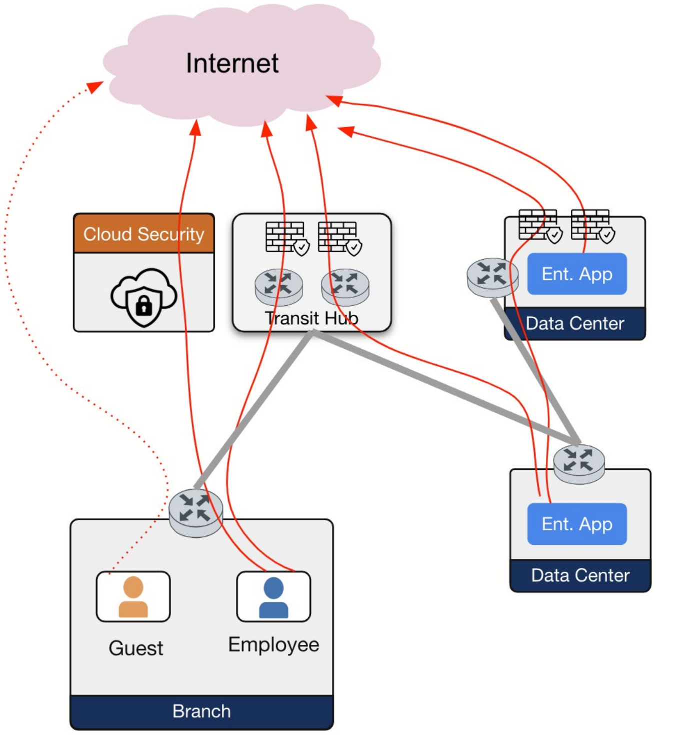


Figure 11: Providing Flexible Internet Access Options

Summary

With the Arista WAN Routing System, enterprise customers can interconnect data centers, campuses, branches, remote sites, cloud resources, and transit hubs over any transport with automated deployment, provisioning, cryptographic management, application traffic engineering provided by the CloudVision Pathfinder Service to deliver the user and application experience in a modern WAN architecture.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989