SOLUTION OVERVIEW

Direct branch to multi-cloud connectivity

BACKGROUND

Geographically distributed enterprises with many branch office locations and multi-cloud instances typically backhaul cloud-destined traffic to the data center at headquarters or to a regional hub site for advanced security inspection. The aggregated traffic is then directed to cloud Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS) providers using a private high-speed link on the backend such as Microsoft Azure ExpressRoute and Amazon AWS Direct Connect for IaaS services and MPLS or business-grade broadband for SaaS, as shown in Figure 1.

Increasingly, enterprises are adopting multi-cloud strategies to leverage multiple cloud platforms to support a range of SaaS and corporate workloads, each with varying software application requirements. A multi-cloud strategy can be implemented with a mix of public, private, hybrid and SaaS clouds to support the specific objectives of an enterprise.

The reasons for implementing a multi-cloud strategy can include:

- Reducing spend on IT infrastructure
- Accelerating the onboarding and delivery of applications to enterprise users
- Improving application performance and the end user quality of experience
- Shifting networking expense from CAPEX to OPEX budgets

Perhaps the most attractive benefit of a multi-cloud strategy for some enterprises is the ability to avoid vendor lock-in. A multi-cloud strategy provides enterprises with an advantage, rather than the cloud provider, providing IT organizations with the flexibility to use a combination of cloud (IaaS or SaaS) providers to meet specific workload requirements.

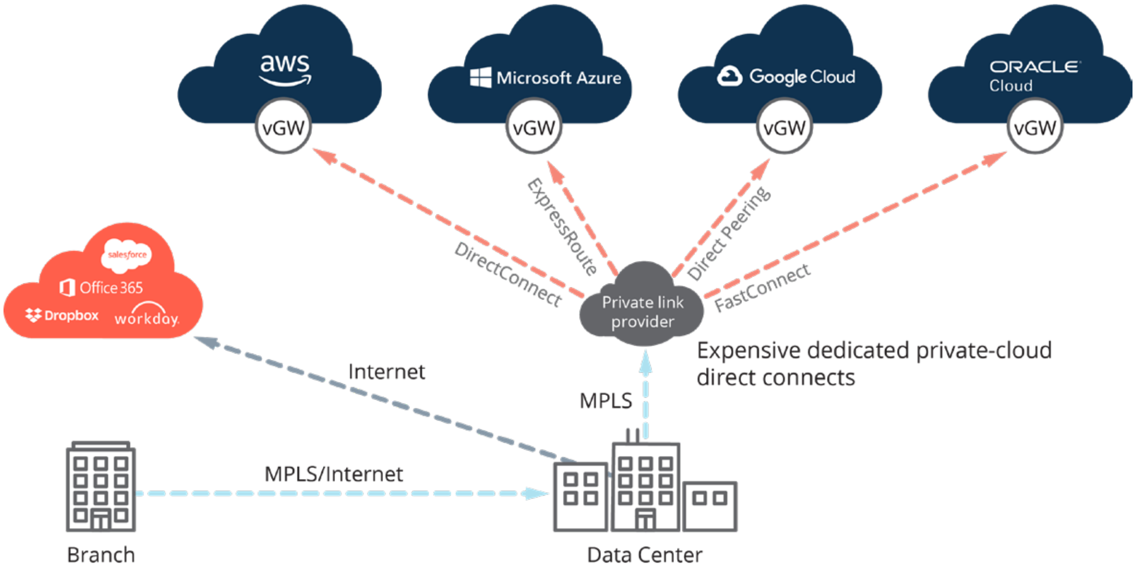


Figure 1: Cloud-destined traffic backhauled from branch site to the data center

CHALLENGES

As enterprises migrate more workloads to public cloud infrastructure and also migrate more applications to SaaS, they must address the complexities associated with managing multi-cloud connectivity requirements for IaaS, SaaS and private cloud-hosted applications. To summarize, key enterprise challenges can include:

- Resolving poor end user quality of experience and impaired application performance resulting from increased latency due to backhauling cloud-destined application traffic to a data center for security inspection
- Added costs from relying on expensive, dedicated high bandwidth private MPLS circuits from data centers to virtual private clouds to support application traffic and the transfer of large files between on-premise data centers and IaaS providers
- Increased risk from managing and optimizing the use of multiple cloud providers. If one web service host fails, a business can continue to operate with other platforms in a multi-cloud environment versus storing all data in one place
- Exposing the organization to potential security threats by leveraging the internet itself, policing for personal applications (e.g. Facebook, Instagram, Netflix) and any unsanctioned "Shadow IT" cloud environments

SOLUTION

The Aruba EdgeConnect SD-WAN edge platform addresses the challenges associated with backhauling cloud-destined traffic to the data center, thereby reducing the cost of bandwidth connectivity from the data center to cloud providers, as shown in Figure 2, in the following ways:

1. Aruba EdgeConnect virtual instances can be easily deployed within all of four of the major public cloud providers, Amazon AWS, Google Cloud, Microsoft Azure and Oracle Cloud Infrastructure, via their respective marketplaces.
2. Aruba EdgeConnect First-packet iQ application classification technology identifies applications on the first packet to enable granular traffic steering and secure local internet breakout of trusted SaaS application traffic directly from branch locations. Directly sending SaaS traffic to SaaS providers avoids backhaul to the data center, delivering the highest quality of experience to application users. This also eliminates the potential for wasted bandwidth, increased latency and performance bottlenecks for trusted SaaS and web traffic. Untrusted cloud traffic can be automatically directed to more robust security services in the cloud or back at headquarters in accordance with corporate security policies.

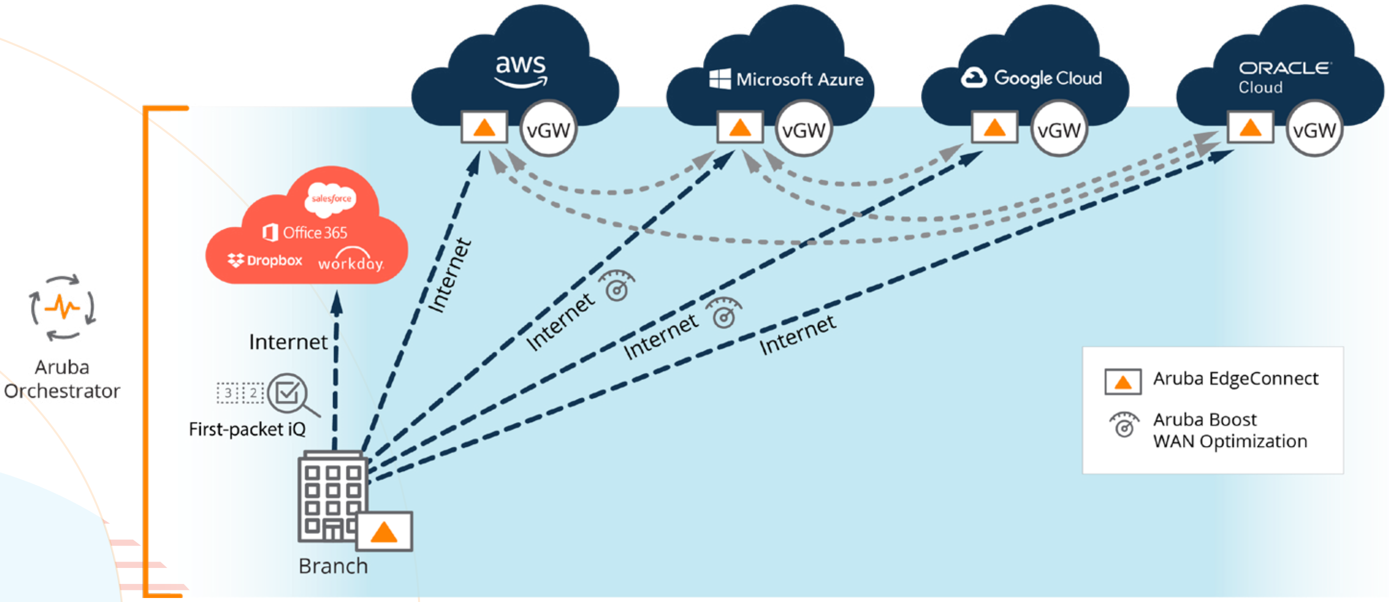


Figure 2: SaaS application traffic breaks out locally at branch site. Aruba Boost WAN optimization accelerates applications and compresses data sets thereby reducing bandwidth costs.

3. Centralized orchestration of any IaaS and SaaS connectivity policies and services via Aruba Orchestrator, simplifies secure connectivity and configuration policies to cloud providers. From a single pane-of-glass, IT can manage on-going operations of Aruba EdgeConnect network functions. Centralized orchestration ensures that consistent policies are enforced across the enterprise.
4. Aruba EdgeConnect includes an optional unified WAN optimization software performance pack, Aruba Boost, that accelerates applications and compresses data sets. Boost mitigates the effects of latency by accelerating TCP and other protocols, thus improving application response times across the WAN. Furthermore, deploying Aruba EdgeConnect with Aruba Boost for high bandwidth private direct connections between the data center and to IaaS providers, improves the performance for replication and backup applications by overcoming distance limitations and poor network quality when impairments occur. Data reduction techniques can be applied to all inbound and outbound WAN traffic in real-time, storing a single local instance of data on each Aruba EdgeConnect appliance.

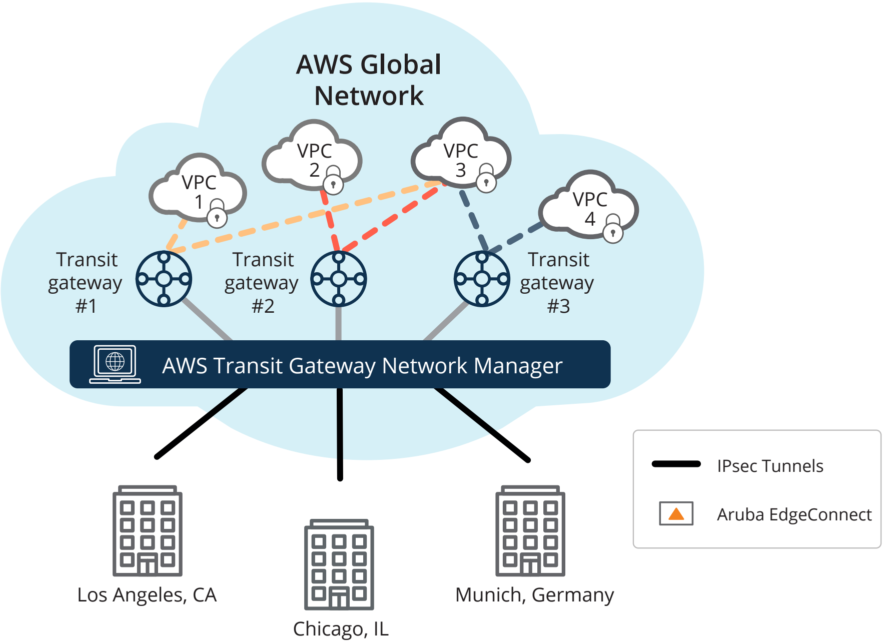
INTEGRATION WITH AWS TRANSIT GATEWAY NETWORK MANAGER AND AZURE VIRTUAL WAN

Global enterprise networks tend to be hybrid in nature and include applications and workloads hosted in on-premise data centers as well as in the cloud. To avoid increased costs resulting from missed insights into their respective networks, enterprises need real-time monitoring of their entire global network. Both AWS and Azure offer solutions that provide enterprises with greater visibility into all of their workloads whether hosted on-prem or in the cloud. This helps avoid increased costs resulting from missed insights into the global enterprise networks. However, to leverage the benefits of using AWS or Azure networks, enterprises need a solution that fully integrates with cloud provider network such that manual tasks are automated. Aruba EdgeConnect automates IPsec tunnel connectivity to Azure Virtual WAN (vWAN) and AWS transit gateway network manager (TGNM) from branch locations using API integration. This integration allows enterprises to seamlessly connect their branch sites to the cloud providers global network to make the most of the high-speed connectivity and rich analytics offered for a better network experience.

With the Aruba EdgeConnect integration with AWS TGNM or Azure vWAN, enterprises looking to connect to public cloud platforms no longer need to backhaul all IaaS cloud-destined traffic from branch sites back to the data center. Instead, customers can breakout IaaS traffic locally from the branch. This results in better application performance as latency is minimized. As a result, the branch-to-cloud connectivity is greatly simplified. Branch-to-branch or branch-to-data center connectivity is optimized as enterprises can utilize the global cloud network infrastructure of either Amazon or Microsoft for reach and connectivity. Enterprise customers can use the Aruba EdgeConnect to automate the onboarding of new locations to the AWS or Azure cloud while using any combination of underlying WAN transport including MPLS, broadband internet or 4G/LTE connectivity. This results in operational efficiencies and faster time-to-market, all without compromising security. The solution enables customers to optimize routing within the global AWS or Azure network, speeding up access to cloud resources across the globe.

Aruba Orchestrator uses the AWS TGNM or Azure vWAN API to target the branches in the network and associate them to a transit gateway or a hub, configuring both ends of the tunnel endpoints for each branch as shown below in Figures 3 and 4. The Aruba EdgeConnect appliance in the branch then establishes primary and secondary standards-based IPSec tunnels that terminate at the head-end gateway or hub in AWS or Azure. Aruba Orchestrator continuously monitors the status of the connections and redirects traffic to alternate gateways or hubs as needed.

Figure 3: Branch-to-cloud and branch-to-branch connectivity using AWS TGNM.



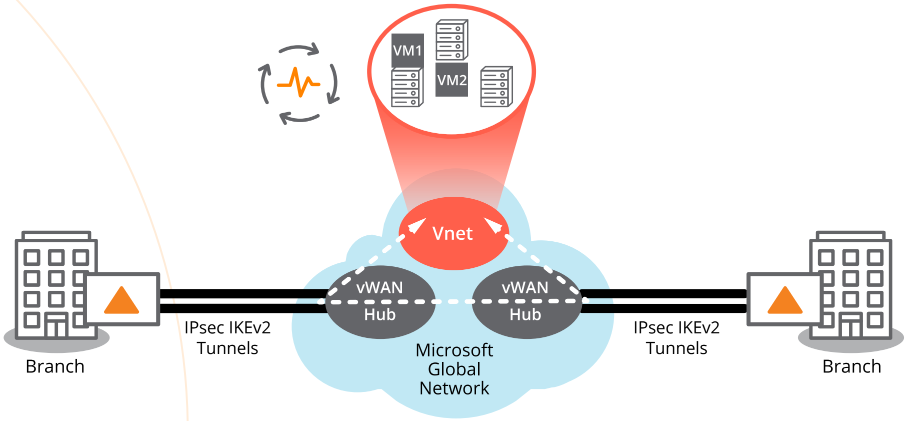
Branch-to-cloud and branch-to-branch connectivity using AWS TGNM

MICROSOFT OFFICE 365 REST API INTEGRATION

To deliver the highest quality of experience for Office 365, Microsoft recommends that organizations enable secure local internet breakout for their Office 365 application traffic directly from their branch offices. To connect users to Office 365 applications, IT organizations must direct their traffic to the Microsoft Global Network. The Microsoft Global Network supports several hundred points of presence (PoPs) around the globe. Within the Microsoft Global Network are interconnected data centers where customers' Office 365 data is stored and replicated. Customers connect users to these global data centers via the Microsoft Global Network PoPs in order to access their respective Office 365 applications and data.

Enterprise customers can deliver unprecedented Office 365 application performance with Aruba EdgeConnect. With First-packet iQ application classification and automated integration with the new Microsoft Office 365 REST API, Aruba EdgeConnect enables secure internet breakout directly from the branch office to the nearest Office 365 entry point using the latest Office 365 endpoint data.

Figure 4: Branch-to-Cloud and Branch-to-Branch Connectivity using AWS TGNM and Azure vWAN.



Branch-to-cloud and branch-to-branch connectivity using Azure vWAN

Office 365 endpoint data is a global list of IP addresses and fully qualified domain names (FQDN) that is continuously updated and made available on a regular basis through the Office 365 REST API. With Office 365 REST API integration, Aruba continuously learns and discovers new Office 365 end points and/or IP addresses and automatically re-configures Aruba EdgeConnect if a new, closer Office 365 end point becomes available. By doing so, users can always connect and always realize optimal Office 365 connectivity and performance by reducing the round-trip time (RTT).

The Aruba EdgeConnect SD-WAN edge platform has been independently tested and certified to support the Microsoft Office 365 Connectivity Principles to provide reliable connections directly from branch office locations to the nearest Office 365 entry point (see Figure 5). As a result of the independent testing, the Aruba EdgeConnect platform has been inducted into the Microsoft Office 365 Networking Partner Program and has been given the official "Works with Office 365" designation.

Direct branch-to-multi-cloud connectivity with the Aruba EdgeConnect SD-WAN edge platform enables organizations to securely connect users directly from branch offices to cloud-hosted services, simplify how IT deploys new hosted applications, optimize direct connect bandwidth and optimize Office 365 performance all while driving a better user experience and cost savings for the business.

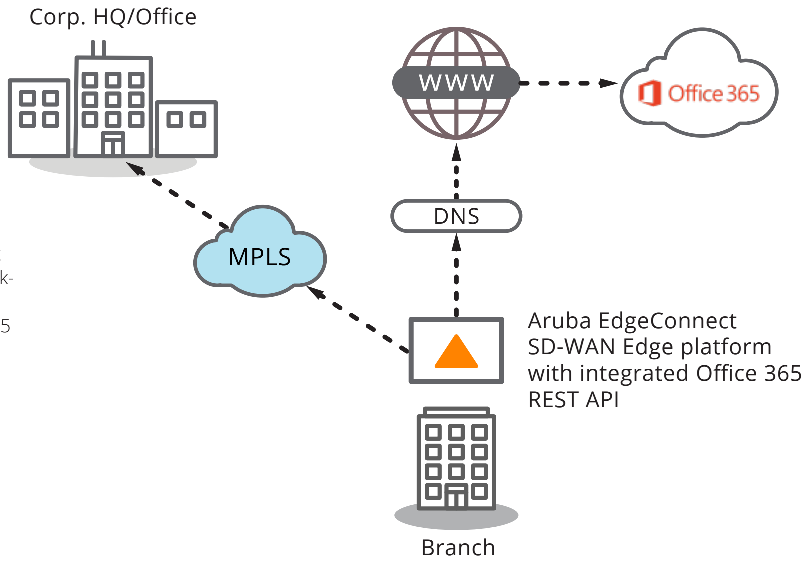

Corp. HQ/Office
WWW
Office 365
DNS
MPLS
Aruba EdgeConnect SD-WAN Edge platform with integrated Office 365 REST API
Branch

Figure 5: Aruba EdgeConnect enables secure internet break-out directly from the branch office to the closest Office 365 entry point using the latest Office 365 endpoint data.

aruba
a Hewlett Packard Enterprise company

Contact Us Share