Simplify and Automate Connectivity to AWS with Prisma SD-WAN

We live in an age of cloud and digital transformation. Cloud adoption is skyrocketing. Public cloud adoption among organizations has grown to 91%,[1] and companies now run the majority of their workloads in the cloud, often with multiple cloud providers. Users and applications are moving outside the traditional network perimeter and accessing an ever-increasing number of public cloud applications.

With applications distributed across many virtual private clouds (VPCs), organizations are often challenged with the high cost and complexities of building and managing the transport infrastructure to connect their locations and users with cloud resources.

1. "The 2019 RightScale State of the Cloud Report from Flexera," Flexera, February 2019, https://www.flexera.com/about-us/press-center/rightscale-2019-state-of-the-cloud-report-from-flexera-identifies-cloud-adoption-trends.html.

To achieve successful digital transformation and realize the full benefit of their cloud investments, organizations must transform their existing networking infrastructure. This transformation requires a solution that makes it easy to connect branch locations to the cloud while meeting performance needs and keeping costs in check.

Challenges with Legacy Network Infrastructure

While the cloud's value proposition is compelling, it is only after making a cloud deployment decision that many organizations realize the many complexities of planning the integration with their existing enterprise network. Many organizations are still using traditional wide area network (WAN) designs that were not designed with the cloud in mind. They face the following challenges:

- **Cloud application performance for remote users:** Traditional WAN designs backhaul application traffic from remote offices through the data center before going to the cloud, which adds latency and bandwidth strain, affecting performance for remote office users.
- **Troubleshooting performance issues:** With applications hosted in public cloud environments, lack of visibility means most organizations find it difficult to identify and remedy the source of application performance issues.
- **Ensuring high availability for remote office users:** Most remote offices have a single private multiprotocol label switching (MPLS) WAN link to the data center, meaning productivity ceases when the WAN is down. Even in ideal conditions, this architecture puts a heavy load on the MPLS lines and adds latency to the cloud connections, negatively impacting the end user experience.
- **VPC routing management issues:** Complexity increases with scale. As organizations deploy more VPCs for various application and business needs, the complexity and operational burden of connecting on-premises users with each VPC can increase significantly. Since separate routing tables must be maintained within each VPC, separate network gateways should be used to connect to on-site locations, and various VPC peering relationships should be established.

The heavy overhead in network management and operations, in addition to the poor traffic performance, negatively impacts the overall cloud adoption experience.

Prisma SD-WAN Overview

Prisma® SD-WAN enables organizations to transform their networks and reduce WAN costs with the industry's only application-defined, autonomous SD-WAN solution. It leverages machine learning and automation to simplify management, enables policy defined by applications to improve the end user experience, and secures your cloud-delivered branch.

Prisma SD-WAN allows you to combine disparate networks, including MPLS, internet, and cellular, into a highly available, high-performance, and secure application fabric. Prisma SD-WAN Instant-On Network (ION) devices deployed in your network actively analyze each application flow to ensure policies for performance, compliance, and security are maintained and that the most appropriate network connections are used for each flow.

AWS Transit Gateway

Amazon Web Services (AWS®) introduced AWS Transit Gateway in 2018 to help solve the problem of maintaining multiple routing tables, network gateways, and VPC peering relationships. AWS Transit Gateway acts as a cloud router that connects VPCs and on-premises networks through a central hub. Two network attachments types are supported:

- **VPC attachment** supports only static routing without equal-cost multipath (ECMP) routing. This attachment type is used to connect VPCs to the transit gateway.
- **VPN attachment** supports only static routing using IPsec VPN tunneling without ECMP. This attachment type is used to connect third-party devices (e.g., SD-WAN virtual appliances) to the transit gateway.

Introducing AWS Transit Gateway Connect

To enable advanced connectivity requirements as well as support dynamic routing, higher bandwidth connections, and greater visibility, AWS introduced AWS Transit Gateway Connect.

AWS Transit Gateway Connect provides tighter native integration with the SD-WAN gateway appliance to allow for more natively consolidated edge connectivity to AWS. It can:

- Dynamically route through a single ingress/egress point.
- Provide higher bandwidth interconnects, enabling it to scale beyond the 1.25 Gbps bandwidth using IPsec VPN connections to up to 5 Gbps connections.
- Enable increased scalability and performance.
- Simplify route management.
- Provide advanced visibility into performance and telemetry data.

To facilitate these capabilities, the AWS Transit Gateway now provides a new network attachment, a "connect attachment," that supports dynamic routing with Border Gateway Protocol (BGP) and Generic Routing Encapsulation (GRE) tunneling for third-party devices, such as SD-WAN networks. This attachment runs on top of the existing VPC attachments.

A New Approach to Cloud Connectivity: Prisma SD-WAN Integrated with AWS Transit Gateway Connect

Prisma SD-WAN dramatically reduces the operational complexity of managing your WAN by simplifying site-to-site connectivity, eliminating complex routing configurations, and reducing the hardware footprint at remote offices. Prisma SD-WAN does this not only for sites you own and manage, but also for virtual sites you manage in the cloud.

To ensure that connecting the cloud to the networks is simple regardless of the WAN design, Prisma SD-WAN now integrates with AWS Transit Gateway Connect. This integration puts an end to the manual, time-consuming, step-by-step configuration and connectivity of individual sites with local AWS points of presence.

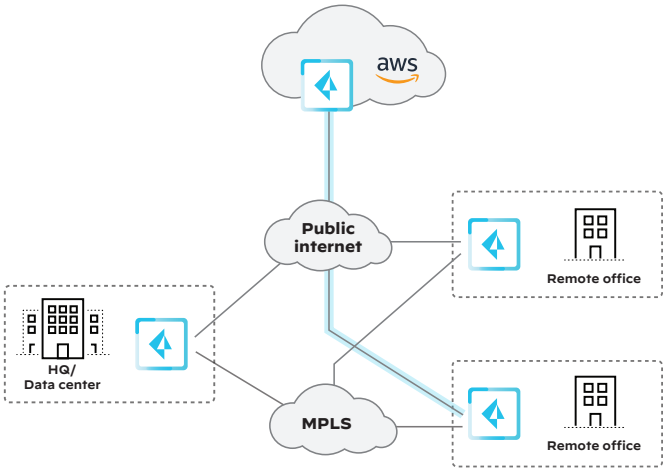

Figure 1: Prisma SD-WAN integrated into AWS Transit Gateway Connect with CloudBlades

This integration is made possible thanks to Prisma SD-WAN CloudBlades, a platform on the Prisma SD-WAN controller that translates business intent into an underlying configuration. It is an API abstraction layer that uses the built-in software development kits in Prisma SD-WAN to integrate with third-party applications and services like AWS.

The CloudBlades platform is built independently of the device and the controller, so any current or future third-party integrations need no software upgrades, either on the device or the controller side. For the AWS integration, a new "AWS Transit Gateway Connect CloudBlade" automates the entire process of connection between Prisma SD-WAN and AWS.

Automated Branch Connectivity to AWS

The process to connect branches to AWS is simple and automated: the network administrator only needs to introduce the required parameters in the AWS Transit Connect CloudBlade at the Prisma SD-WAN UI. These parameters include AWS account details—access key ID, AWS Transit Gateway regions to attach to, and the associated transit gateway ID—as well as the IP address for the VPC creation, GRE tunnel, and iBGP peering. Afterward, the AWS Transit Gateway Connect CloudBlade automatically enables connectivity from any branch or Prisma SD-WAN site to AWS host VPCs through the AWS Transit Gateway by automatically performing the following steps:

1. The CloudBlade connects to AWS using standard APIs. It creates Prisma SD-WAN Connect VPCs in the associated regions on the AWS side with the associated subnet information provided by the network administrator.
2. Using CloudFormation templates, the CloudBlades platform deploys two vION virtual machines in separate availability zones in the Prisma SD-WAN Connect VPC. Prisma SD-WAN has a CloudFormation template-based marketplace listing on AWS, which makes deploying into existing or new VPCs easy.
3. The Prisma SD-WAN Connect VPCs are attached/connected to the AWS Transit Gateway using the VPC attachment (see figure 2).
4. A new site is created on the Prisma SD-WAN side as a data center site type, and the AWS vIONs will be associated/claimed in that site. This site characterization is important as a Prisma SD-WAN data center site type ensures by default that all Prisma SD-WAN branch sites build zero-touch secure fabric links (VPN tunnels) to the IONs in AWS.
5. Once the vIONs are up, the CloudBlades platform configures the "connect attachment" from the vIONs to the AWS Transit Gateway. The "connect attachment" establishes point-to-point GRE tunnels from the vIONs to the AWS Transit Gateway along with iBGP peering for dynamic routing. The IP address provided by the administrator is used for this peering (see figure 3).

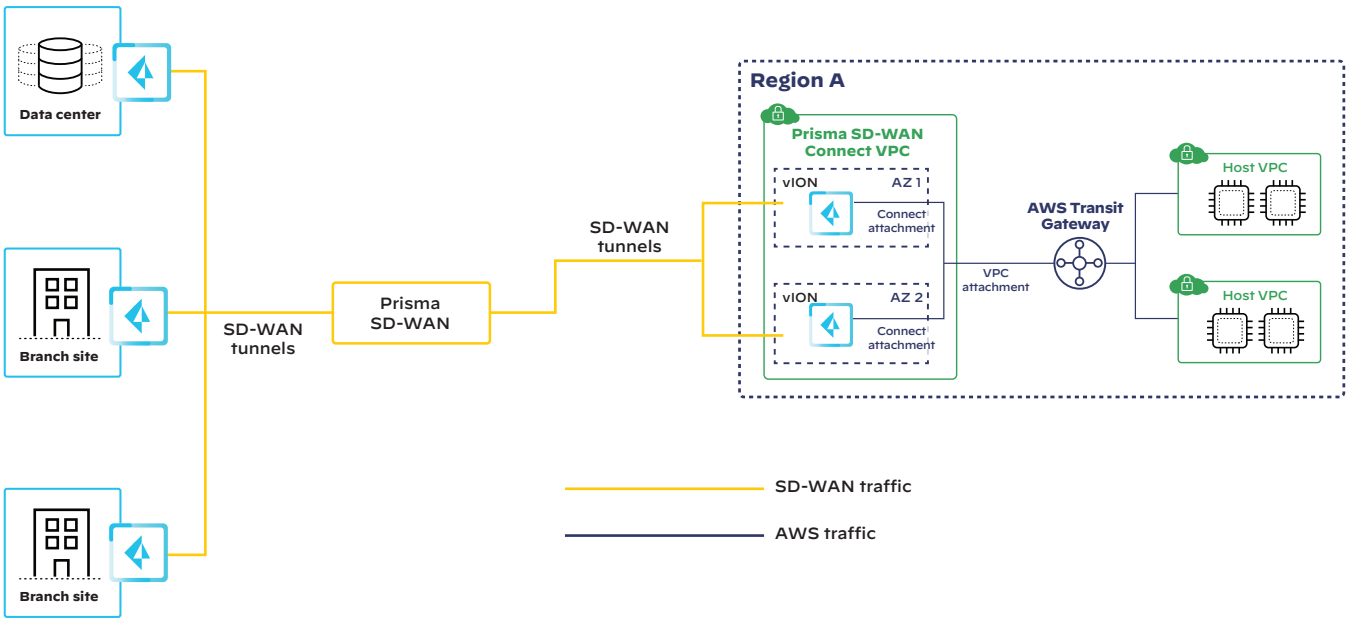

Figure 2: End-to-end connectivity from branch sites to AWS

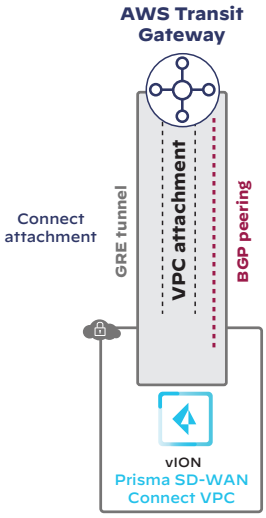

Figure 3: AWS Transit Gateway Connect attachment from a single vION to AWS Transit Gateway

Benefits of the Integrated Prisma SD-WAN and AWS Transit Gateway Connect

This integrated solution automates branch connectivity to the AWS cloud and reduces the branch cloud onboarding time from days or hours to a few minutes per site. Administrators can automatically connect new branch offices to AWS cloud infrastructure and avoid the tedious, repetitive, and manual process of configuring each connection. Adding automation to the overall process also significantly reduces management and operational cost.

By extending Prisma SD-WAN from your WAN into the AWS cloud with Transit Gateway Connect, your organization will realize the following benefits:

- **Secure and flexible branch-to-cloud connectivity:** A single console offers ease and flexibility in enabling automated deployment of secure tunnels from branches and data centers to multi-cloud workloads. Strict use of private IP addresses for connectivity and reachability fully addresses compliance and security.
- **Automated routing optimization:** Eliminating complex peering relationships lets you optimize and simplify routing management within the AWS global network, speeding up access to cloud resources around the globe. Dynamic routing removes the complexity of static routing configuration and allows for high-bandwidth tunnel attachment, enabling you to rapidly add traffic capacity and scale to accommodate future growth while saving operational and management overhead.
- **Global network visibility:** You can visualize and monitor the network from a single dashboard with access to multiple views, including list view, logical view, and map view of network resources and connectivity. Additionally, you can receive notifications related to performance metrics and telemetry data (e.g., unhealthy connections, availability changes) across AWS regions and on-premises sites.
- **Consolidated and centralized network management:** Through a single pane of glass on the Prisma SD-WAN orchestration platform, you can perform end-to-end management of your organization's global branch network and AWS cloud networks, from onboarding a new branch to updating the route table affecting intelligent routing decisions. Prisma SD-WAN uses AWS Transit Gateway Connect APIs to provide automation that speeds up and simplifies network deployments of any size.

Summary

Prisma SD-WAN simplifies WAN management by automatically establishing secure network paths between your locations, and it continually monitors application flows to ensure your WAN is highly available and policy objectives are met. With Prisma SD-WAN, connecting the cloud to your network is simple regardless of your WAN design.

Prisma SD-WAN integration with AWS Transit Gateway Connect further integrates your cloud resources into your IT architecture without compromise while simplifying network management, improving performance and visibility, and reducing cost. Ultimately, the integration delivers operational efficiency and automation that enable your organization to be more agile as you move to the cloud.

Rather than depending on costly models that involve deploying your own hardware in cloud providers' locations merely to realize consistent performance and manageability, you can take advantage of even better performance and superior manageability using Prisma SD-WAN.

For more information on how Prisma SD-WAN enables the cloud-delivered branch, please visit us online.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com