HughesON™

SIMPLIFYING HYBRID CLOUD CONNECTIVITY

INTRODUCTION

The massive shift to Cloud-based services and infrastructure increases a network's complexity—especially for the distributed enterprise. Here we explore how connectivity can be simplified to overcome challenges, optimize performance, and improve the user experience.

No matter how you approach your network and digital infrastructure, it's nearly impossible to do business without the Cloud. With that shift comes increased network complexity and challenges. Legacy applications, those running on timeworn networks and hardware, are usually less effective and secure than emerging solutions. They may also be unreliable and no longer supported by the original vendor or manufacturer. As many network servers, equipment, applications, databases, and business critical software and hardware get closer to their "end of life," we are seeing enterprises move these elements from on-premises data center solutions to the Cloud.

Depending upon the type of application or service, the shift to Software as a Service (SaaS) applications makes sense given they are feature-rich, widely available, generally cost advantageous, and come with significantly cheaper compute and storage solutions. However, while SaaS is useful for driving business productivity, exponential growth in these SaaS and private Cloud applications bring security concerns that are like those associated with the traditional on premises network infrastructure.

Public and private Cloud services, such as Infrastructure as a Service (IaaS) as well as SaaS, are also gaining traction as enterprises trade capital expenses for operating expenses (CAPEX for OPEX). These services offer flexibility and scalability.

Today, a hybrid Cloud solution—with applications deployed both on premises and multiple private Clouds—is now the most popular approach for enterprises.

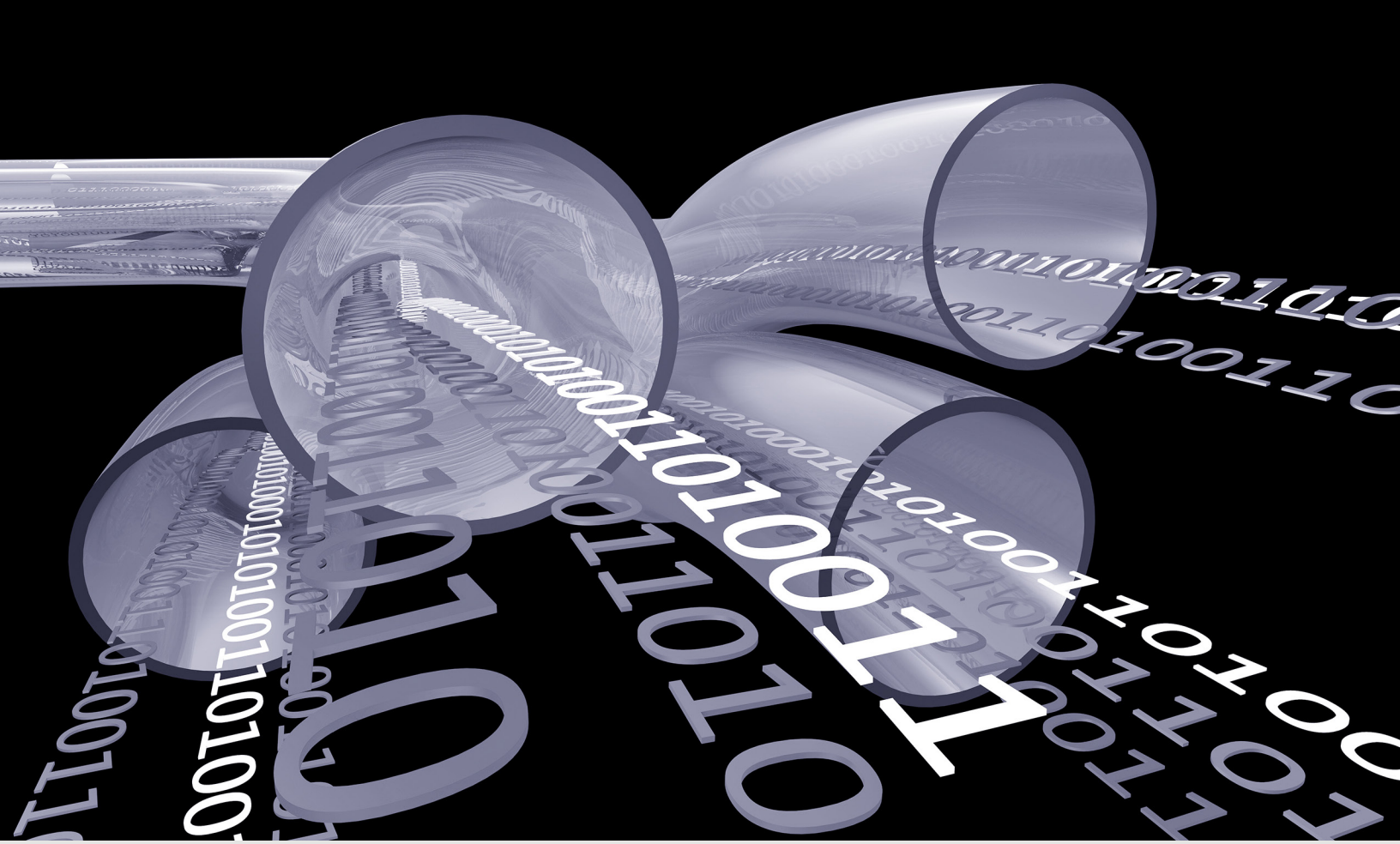
Unfortunately, hybrid deployments result in inefficient routing practices, such as hairpinning all traffic through a corporate data center which causes network delays. This is due the conventional router on a Wide Area Network (WAN) being designed to support creation of a Virtual Private Network (VPN) within the data center architecture, rather than being built to support native Cloud or hybrid architectures. The delay caused by hairpinning traffic via backhaul impairs application performance, and results in poor user experiences and lower productivity.

The Hybrid Model and a Distributed Network

Enterprises encounter big challenges when they operate in a distributed network environment and attempt to move to a hybrid Cloud architecture across multiple WAN branches. They also struggle when it comes to protecting their IaaS/SaaS traffic over the public Internet.

The only way to deploy a hybrid model with a distributed network and overcome these challenges is with a Software Defined Wide Area Network (SD-WAN). SD-WAN intelligently and dynamically routes traffic based on protocols defined by service type and application priority. That means SD-WAN can choose the best path in real time for mission critical traffic, while less critical traffic travels a different path. With SD-WAN's ability to manage branch-to-Cloud and branch-to-HQ connectivity, the hairpinning of traffic through a data center is eliminated.

In the case of SaaS applications (e.g., Office 365, Salesforce, Atlassian, RingCentral), Direct-to-Internet (DIA) access often wreaks havoc with traditional WAN transport. This is seen in packet loss, high jitter, latency, and varying bandwidth availability. Depending on the type of application, these impairments affect not only application performance, but also productivity and potentially revenue. Figuring out connectivity to the branches to support robust use of Cloud services therefore becomes essential.



Tunneling to the Cloud

Tunneling is a method of transporting data across a network using protocols. It is often used with VPN. Let's look at a real-world example of a traditional router scenario, using AWS products. (Similar options are available from other Cloud providers like Azure. The table provides the product name equivalent.)

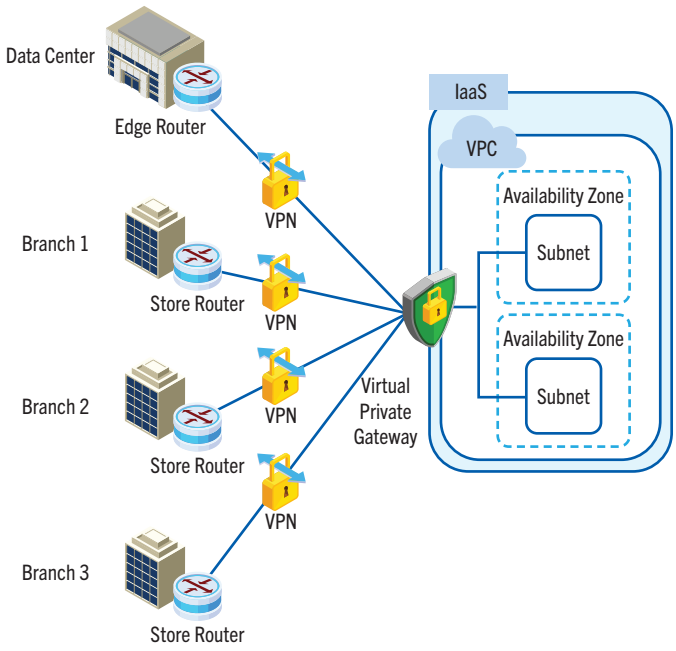
Amazon Web Services	Azure
Virtual Private Cloud	Virtual Network
AWS Direct Connect	Azure Express Route
Transit Gateway	Virtual WAN
Virtual Private Gateway	Virtual Private Network Gateway

One way to extend your branch LAN to the public Cloud is to build an IPsec tunnel from your branch router. IPsec tunnels are used between two dedicated routers, with each router acting as one end of a virtual "tunnel" through a public network.

Typically, there are two popular options:

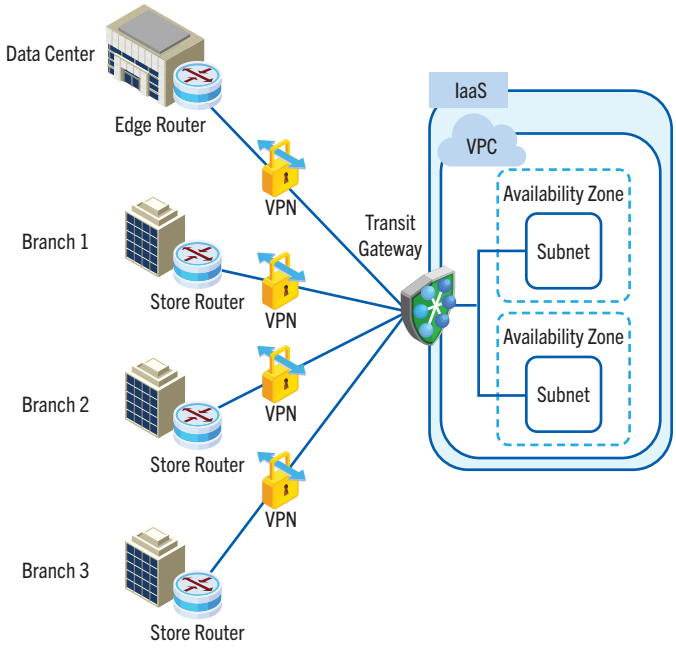
1. Building IPsec Tunnels Between Branches and a Virtual Private Gateway

You can attach a VPG to a Virtual Private Cloud (VPC) and configure multiple site-to-site VPN connections to data centers and branches. You would configure routing so that any traffic bound to the VPC will route to the VPN tunnel; and any traffic to your branch network will route to a VPG (as illustrated).



2.Building IPsec Tunnels to a Transit Gateway

You can attach a TGW to a VPC and configure multiple site-to-site VPN connections to individual branches. You would configure routing so that any traffic bound to the VPC will route to the VPN tunnel; and any traffic to your branch network will route to the TGW, as shown. This approach requires network engineers to configure branch routers and set up the VPN. Depending on the vendor and type of router, this might be a manual process (although some engineers may develop an automated script). Regardless, as the number of branches increases, the process gets complicated and harder to maintain.



Without a controlled overlay, the visibility into application performance is also limited. Static IPsec tunnels mean your applications are at the mercy of the transport's performance. Traditional IPsec will often expose an impaired WAN when application performance degrades and causes reduced productivity or lost revenue.

Investing in SD-WAN

Both scenarios can benefit from an investment in SD-WAN that simplifies Cloud connectivity. One approach is to build geographically distributed Internet breakpoints and optimize traffic until it reaches these Internet Points of Presence (PoPs). Historically, most WAN impairments occur at the last mile of connectivity. By building a tunnel to local Internet PoPs and exchanges, SD WAN protection extends throughout the network. This strategy prevents hairpinning of traffic and added latency.

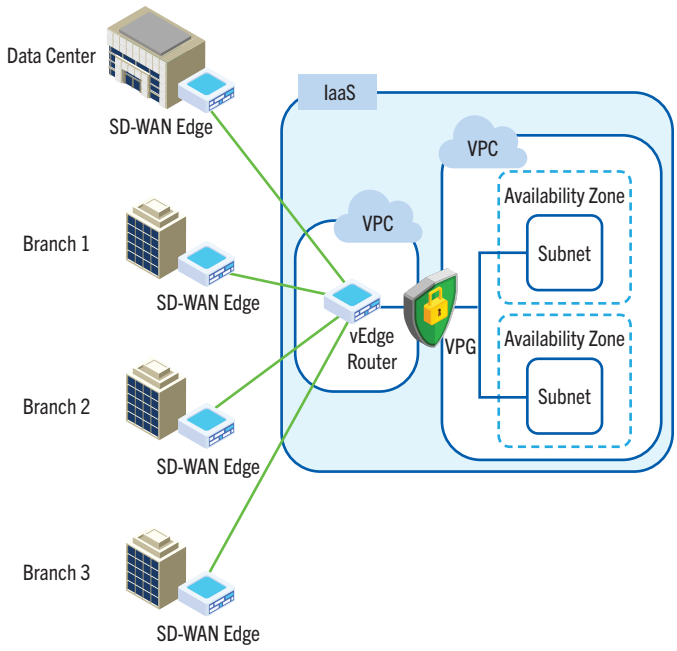
Most advanced SD-WAN platforms also support dynamic multi-tunneling to virtual instances on a private Cloud to ensure protection and security. Additionally, SD-WAN securely connects enterprise branch sites over any transport, including by Multi Protocol Label Switching (MPLS), Internet, or LTE. Centralized orchestration systems enable enterprises to extend their branch WAN to Cloud services without any major architectural redesigning.

Most SD-WAN vendors have virtual instances of their edge devices available on public Cloud marketplaces. By installing an SD-WAN appliance in the VPC, you can add your Cloud environment as an endpoint in your SD-WAN network. Then, with SD-WAN orchestration, you can treat your public Cloud as any other data center. The branch SD-WAN edges can build tunnels directly to the Cloud endpoint and reach applications quickly. The SD-WAN overlay reduces the need for router configurations and provides application enhancements.

Similar to traditional routing, SD-WAN allows you to integrate the network into the public Cloud in multiple ways. The two most popular ways are to:

1. Install an SD-WAN Appliance on the VPC

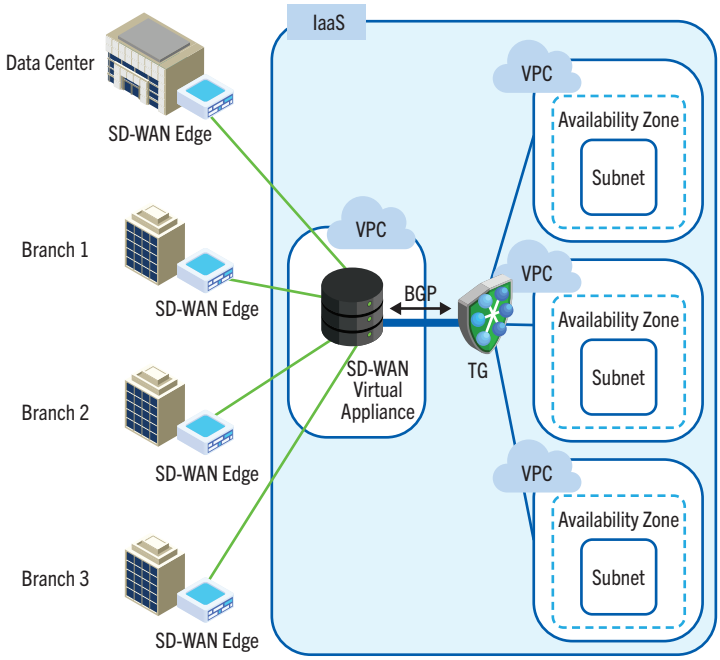
In this deployment, a virtual instance of an SD-WAN edge (or vEdge) can be deployed in a VPC, which then learns from other peer vEdges. The branch vEdge will automatically discover your Cloud routes and build dynamic or static tunnels to reach applications. Since overlay tunnels are established between branch SD-WAN edge and the public Cloud, you have visibility into the network, and gain SD-WAN enhancements and Quality of Service (QoS) end-to-end. Depending on SD-WAN capabilities, you can also extend your branch operations like Payment Card Industry (PCI) systems, back office applications, and guest Wi-Fi to your public Cloud.



2. Connect to a Third-party Virtual SD-WAN Appliance on a Transit Gateway

You can now natively connect your network to a TGW without configuring complex IPsec VPN connections. Dynamic routing capability further simplifies route management across hybrid Cloud environments. In addition, you no longer need to manage and operate multiple IPsec VPN connections between third-party appliances and the TGW to support higher bandwidth.

Many SD-WAN vendors have developed virtual appliance integration with various TGWs. Branch SD-WAN edges build overlay to the virtual appliance in a public Cloud and hand off traffic to the TGW for routing. The TGW simplifies routing within the public Cloud when applications reside in multiple VPCs.



Powering and Simplifying the Network You Depend On

No matter how you approach your network and digital infrastructure, it's nearly impossible to do business without the Cloud. Progressive SD-WAN vendors, like Hughes, work closely with Cloud providers to reduce the resulting network complexity and improve performance. If you already have SD-WAN at your branches, there are a host of ways to optimize connectivity to the public Cloud. If you don't yet have SD-WAN, Hughes can help you to explore how to move to or operate in a hybrid model. With the right SD-WAN solution, you can both power and simplify the network you depend on and make the most out of your investments.

About the Author

Pranav Kondala is a Solutions Architect at Hughes who loves to help customers solve complex networking problems. Follow Pranav on LinkedIn and Twitter @PranavKondala

For additional information, please call 1-888-440-7126 or visit business.hughes.com.

HUGHES
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

business.hughes.com