

# Implementing hybrid cloud automation to optimize IT costs while reducing compliance concerns

Cloud architectures allow automated, on-demand delivery of applications and services, flexibly deployed across large, cost-effective resource pools, whether on-premises or from service providers. The automation and delivery of on-demand services is driving previously unimagined business agility and a new generation of business applications and revenue opportunities. Organizations must often weigh the trade-offs of additional complexity and overhead of an on-premises private cloud, with the limited controls and compliance risks inherent with public cloud providers.

Hybrid cloud is rapidly becoming the optimal solution for most enterprises. It delivers cost-effective shared services between a private cloud and public cloud provider—Virtual Private Cloud (VPC) such as Amazon Web Services (AWS), Microsoft Azure Cloud, or Google Cloud Platform (GCP). In its simplest form, a hybrid cloud seamlessly connects on-premises private cloud infrastructure to a public cloud provider, allowing the exchange of data and applications between locations. Bridging an application network, such as a three-tier web application, across multiple sites and providers, with the appropriate network and security policies, and the same ease of orchestration as if the entire app was running on-site, can be a complex challenge to overcome. There are many reasons and use cases for why an enterprise would adopt a hybrid cloud model:

- **Cloud bursting or application elasticity** – Many enterprises provision their on-premises application workloads for baseline or median capacity to reduce public cloud outsourcing costs, and to keep local resources fully utilized.

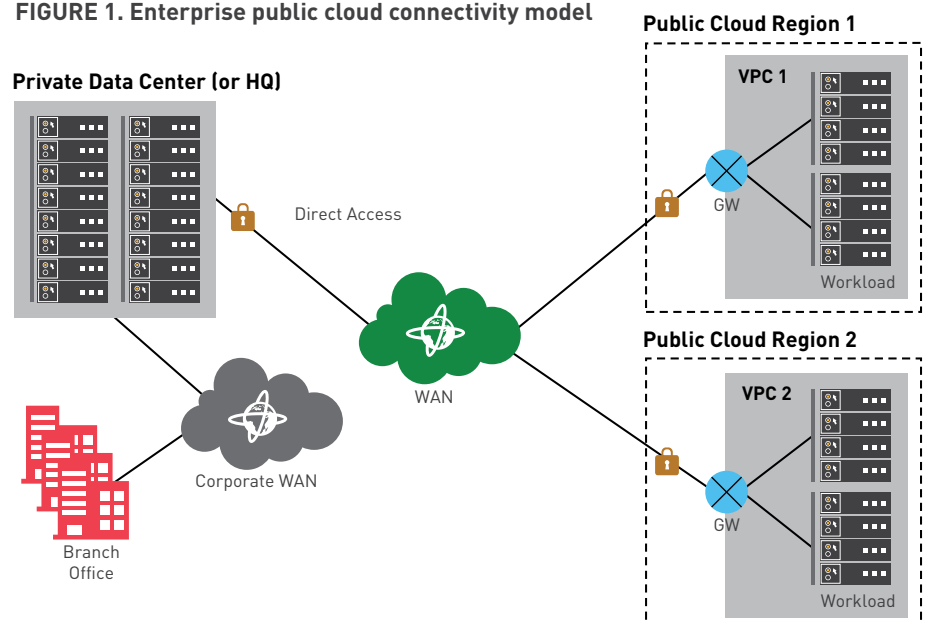
During peak times (e.g. holiday season, special events, promotional windows), this median capacity won't deliver optimal performance. In order to address this peak load, many enterprises burst excess capacity to the public cloud to limit additional IT spending to precisely when it is needed.

- **Architectural flexibility** – Enterprises frequently split their applications into two or more components and host some on-premises for data privacy and others in the public cloud VPC. Hybrid cloud can also be used for new application development, where only temporary compute resources are needed while new applications are being developed.
- **Workload localization** – Hybrid cloud may be used when enterprises are required to bring the application close to end users due to local laws or simply to improve the end-user experience. In this case workloads may be distributed across multiple cloud providers in multiple geographies.

- **High availability and resilience** – Enterprises need to design for the worst-case scenario. A public cloud option provides them backup for their on-premises datacenter. Rather than waiting for disaster to strike, a certain amount of live workloads and capacity, along with mission-critical data is usually running in parallel to assume capacity without interruption.

There are a few common ways in which enterprises connect their on-premises datacenter and a public cloud provider. The most common way is a VPN connection between the private datacenter and the cloud provider. The public cloud provider has a VPN gateway where the enterprise terminates the IPSec tunnel from their datacenter or branch offices (WAN). For software-defined networking (SDN) automation and cloud orchestration, the hybrid cloud link is usually a VXLAN overlay virtual network, making it transparent to the application workloads whether they are running remotely or on adjacent CPUs.

**FIGURE 1. Enterprise public cloud connectivity model**



## Challenges with hybrid cloud connectivity and automation

Providing such a seamless level of integration across virtual networks and sites, with transparency that avoids application redesign and allows for full flexibility, does present some challenges:

- **Scalability** – A typical enterprise may have dozens or hundreds of virtual application networks. As the number of VPCs grows, it creates challenges for enterprises to maintain and manage a large number of secure IPsec tunnels to the various VPCs.
- **Security and segmentation** – An enterprise typically has many internal business groups with various policies. This requires a strict segmentation of the workloads, or logical isolation across various hybrid cloud networks. Public clouds require additional capability to enforce these policies compared to private cloud architectures.
- **High availability** – Continuous availability of workloads under all conditions and scenarios is frequently a mission-critical business requirement. The connectivity to the public cloud workloads also needs to be considered due to possible failures.
- **Application visibility** – Visibility to application performance and potential security anomalies is required for optimal service delivery. A frequent challenge is how to get the insight into the application workloads coming in and out of a public cloud as easily as ones on-premises.
- **Centralized policy and management** – A typical large enterprise uses multiple cloud providers and the connectivity and management of applications, services and workloads are likely different for each provider, adding additional complexity and orchestration concerns.

## The Nuage Networks hybrid cloud solution

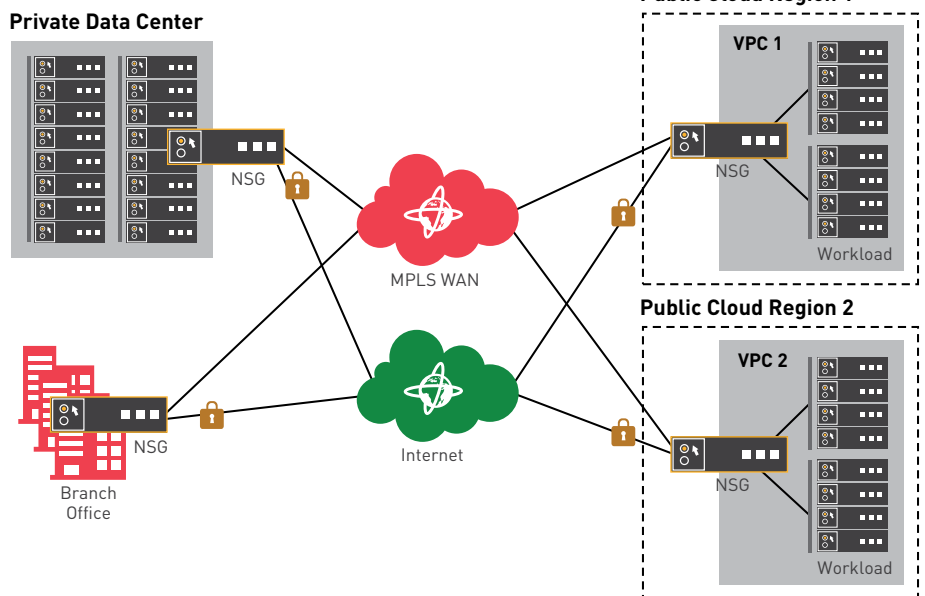
Nuage Networks has developed a comprehensive virtual networking and SDN platform—the Virtualized Services Platform (VSP)—for enterprises looking at hybrid cloud architectures. It provides a public cloud gateway image, for example a Network Services Gateway – Amazon Machine Image (NSG-AMI) for connectivity to a VPC. Using the NSG public cloud gateway, Nuage Networks treats the VPC as a logical extension of the enterprise network, making it a software-defined wide area network (SD-WAN).

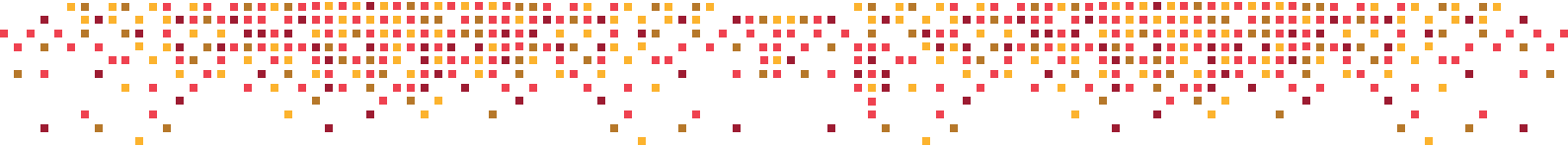
The Nuage Networks solution enables:

- **Unified policies** – Using an NSG public cloud image, the Enterprise network is extended to the VPC in the public cloud. This means the Nuage Networks Virtualized Services Directory (VSD) can now apply the same user and application policies to the public cloud instances as it applies to on-premises infrastructure and remote offices.

- **Scalable networking** – With direct connectivity to a VPC from remote WAN sites over the internet, Nuage Networks removes the need to have traffic “hairpin” through the on-premises datacenter before routing to the VPC. As the number of VPCs grows, there is no need to maintain multiple IPsec connections, increasing scalability of the overall hybrid cloud network.
- **Resiliency** – Most cloud providers offer multiple gateways for connectivity. For example, AWS provides iGW (via the internet) and vGW (from an MPLS direct connection). For the enterprise sites with multiple transports available (both internet and MPLS VPN), the Nuage Networks solution enables the same hybrid WAN principles for the VPC as well. This means applications can utilize the best available path considering both cost and performance requirements to optimize network access and WAN costs.

FIGURE 2. Nuage Networks hybrid cloud solution





- **Context-aware security** – Nuage Networks Virtualized Security Services (VSS) provides contextual flow visualization and application flow mapping of all traffic coming in and out of the VPC to visualize and detect traffic anomalies and provide more effective remediation. This can help provide the same degree of security policy automation, along with virtualized security appliances, as has traditionally been found only in on-premises deployments.

- **Application Aware Networking** – Using the Nuage Networks Application Aware Routing (AAR) feature, enterprises can utilize all available WAN access links to the hybrid cloud provider, and based on the application policies and service level agreement can always provide the most cost-effective path.
- **Operational efficiency** – Nuage Networks VSD provides a single pane of glass for all application workloads (on-premises and public cloud) as well as remote sites and users. It also provides centralized configuration and automation of all network-wide security policies and audits. The same degree of SDN automation that was previously only available for private clouds can now easily be extended to multiple hybrid cloud deployments.

For more information: <http://www.nuagenetworks.net/products/virtualized-network-services/>