Versa SASE and Google Network Connectivity Center

Accelerating Cloud Workloads and Branch Communications

Part of Versa SASE, industry-leading Versa Secure SD-WAN is now also available with Google Cloud Network Connectivity Center (NCC). This collaboration extends the benefits of Versa Secure SD-WAN for customers connecting their on-premises data centers and branch offices to Google Cloud. Versa and Google provide a network architecture which improves the application experience for both branch and remote users. Customers can expect a simplified solution to their WAN network by leverage Google's global backbone infrastructure to accelerate communication between the branch sites. Google's private infrastructure is a great alternative to the internet because it allows for accelerated private access to geographically distributed cloud workloads from on-premises branch offices and data centers, reducing costs and simplifying network deployments.

The Enterprise Network is Evolving

Enterprises today are looking for innovative ways to offer unparalleled speed and security for their users by adopting a network architecture that is more internet-centric to provide better ways for their employees and customers to interact with their business. This adoption is driven by two fundamental changes:

- Rise of remote work: By 2025, 36.2 million Americans will be working remotely, an 87% increase from pre-pandemic levels.*
- Adoption of Cloud platforms: Organizations are expected to be running up to 75% of their workload on cloud platforms by 2022.**

Over the past few years, SD-WAN has become the de-facto technology to connect enterprise branches with applications and services hosted in private or public cloud environments. SD-WAN delivers top application performance and seamless user experience by ensuring quick response times. With Layer 7/Application-centric policies, SD-WAN technology ensures that the business applications are given appropriate priority and network treatment depending on the business criticality and performance requirements of the applications. SD-WAN technology relies on application-aware traffic engineering and application acceleration techniques to overcome any last mile network performance degradation, delivering the best end user experience and cost savings.

Enterprise workloads are moving to the cloud at a faster pace than ever, as 'work-from-Anywhere' is becoming the new normal. Organizations need to embrace the cloud so that they can offer flexible, elastic, and lower cost business continuity. These trends are encouraging enterprises to leverage internet access (broadband, 5G/4G, business-grade internet) as the de-facto connectivity choice for their branch sites and data centers.

In the new Internet-centric network, enterprises need to also consider options that provide reliable and cost-effective mechanisms to connect to on-premises and cloud workloads. Organization looking to simplify management and optimize costs need to direct traffic through different routes dynamically depending on data criticality. The key consideration in all of this is how to offer the most simplified way for administrators to manage, monitor, and scale network connectivity.

To address these challenges with network simplification and cost savings, the partnership between Versa Secure SD-WAN and Google Cloud Network Connectivity Center delivers dynamic, secure branch-to-branch and branch-to-Google hub connectivity with Versa's industry-leading SASE services. Versa SASE powered by Google Infrastructure result in a reliable and automated private connection to cloud and datacenter workloads: providing a dynamic, intelligent solution to network optimization.

Versa SASE for Google Network Connectivity Center

Versa SASE's industry-leading SD-WAN delivers enterprise-grade networking, security, visibility, automation, and performance capabilities all in a single software, and single management interface. With this platform, enterprises can reap the benefits of fast, scalable, and secure IT deployment which results in better application performance, excellent user experience, smaller attack surfaces, and lower total cost of ownership. Built from the ground-up, Versa Secure SD-WAN helps organizations of all sizes overcome the challenges and complexities of brownfield environments.

Google Cloud Network Connectivity Center (NCC) simplifies deployment, configuration, and management of on-premises networks and cloud connectivity. By leveraging Google's global infrastructure, Google Cloud NCC provides a centralized

*Workforce Pulse Report, 2020 **Forrester, The Public Cloud Outlook, 2019

management model, allowing connectivity between physical locations to application workloads hosted on-premises or in Google Cloud, while using connectivity types such as a cloud VPN, cloud Interconnects, and third-party router appliances. Google NCC and Versa Secure SD-WAN together help reduce operational burden and costs with automation and by always finding the most dynamic, cost efficient path.

For Versa Secure SD-WAN current and potential customers, the SD-WAN Overlay provides the last mile connectivity to the Google cloud environment – a key component to reducing costs . In the Google NCC architecture, a Secure SD-WAN Branch appears as a SD-WAN Spoke. Logically, a customer-instantiated hub in Google Cloud would become a SD-WAN Spoke Hub (see Figure 1).

In the Google Network Connectivity Center architecture, the Versa Operating System (VOS) instances in Google VPC are attached as NCC Spokes to the Network Connectivity Center Hub. The VOS instances establish BGP sessions with the cloud routers (in each region) to dynamically exchange network reachability information. With BGP-based dynamic information sharing, users in Branch Office 1 in figure 1 can leverage the Google Backbone to reach applications in Branch Office 2, located across the globe.

Versa Secure SD-WAN integrated with the Google Cloud Network Connectivity Center delivers an end-to-end network architecture that is access independent, leverages multiple accesses at the branch, and is application aware – leading to low latency and reliable connectivity. Additionally, Versa Secure SD-WAN blends in Zero Trust capabilities to ensure the user is who they say they are and the devices they are accessing from are not compromised.Versa Secure SD-WAN provides the contextual intelligence to enable reliable connectivity over a variety of access links on the edge. Google NCC leverages a global backbone for providing reliable connectivity between Google NCC Hubs and cloud workloads. Together, Versa and Google provide a cost effective, reliable, and operationally simple solution to connect branches, data centers, and cloud workloads around the globe.
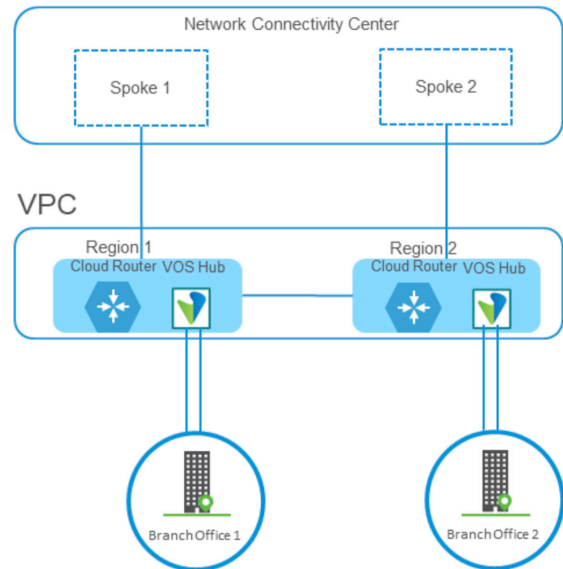

Figure 1: VOS integrated in Google Cloud NCC

Enterprise-Grade Connectivity for Branch Users to On-Premises Workloads

Consider a globally distributed workforce needing VoIP, video conferencing, and other high bandwidth communication tools to effectively conduct day to day business. The branches across the globe are connected using the best local connectivity i.e., connectivity from local Internet Service Providers (ISPs) with wired and/or wireless technologies.

The challenge in this globally distributed workforce is the ability to deliver optimal user and application experience, irrespective of whether this communication is between branch offices or between multi-cloud.
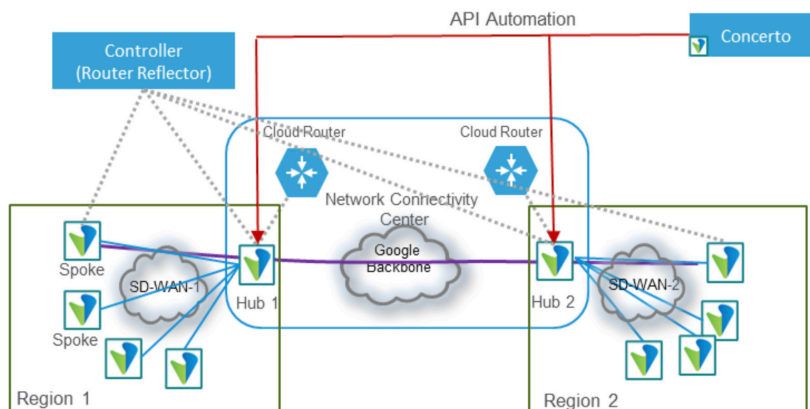

Figure 2: Enterprise leveraging Versa Secure SD-WAN and Google NCC for branch transit

To offer optimal experience, Versa Secure SD-WAN needs to be deployed at branch sites. At one end: Versa SD-WAN CPEs terminate on local WAN links and at the other end: Versa SD-WAN needs to be deployed within a Google VPC. In order to overcome challenges where the last mile connectivity to the sites is less reliable and thus not meeting corporate SLA requirements, Versa SD-WAN solution can auto-identify these applications and steer the application traffic over to the best possible path – reducing costs and increasing performance (See Figure 2).

Versa Secure SD-WAN makes use of industry-leading network SLA monitoring, deep packet inspection, video and voice performance monitoring, and application acceleration techniques like Forward Error Correction to overcome the underperforming local links and provide a better user experience end to end.

While Versa Secure SD-WAN ensures optimal user experience from local branch to the closest Google cloud hub over local ISP, Google's global backbone provides ultra-reliable connectivity between the Google NCC spoke hubs (which run VOS).

The integrated solution between Versa and Google offer optimal and intelligent end-to-end connectivity that reduces total costs and complexity.
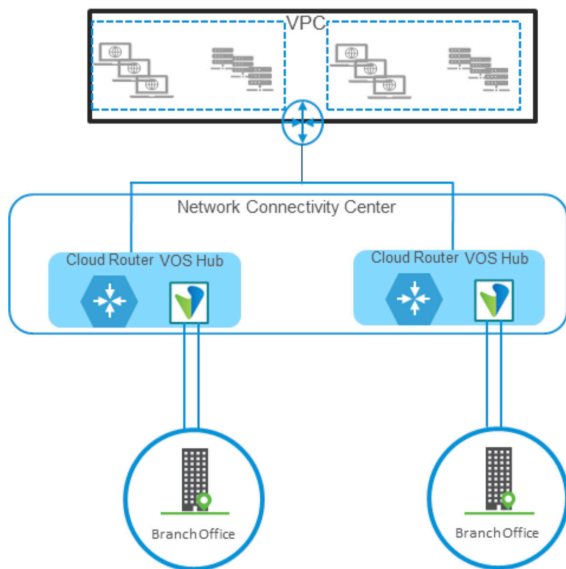
Reliable Connectivity from Branch Users to Cloud Services

Now consider a global workforce accessing cloud hosted workloads that are not centrally managed. The workloads are distributed globally to scale in and out elastically based on the resource requirements, and spanning to different regions and availability zones based on geo-redundancy requirements. Branches are connected to cloud workloads using a diverse set of internet links both wired and wireless.

The challenge many enterprises face is to provide reliable connectivity from the branch site to cloud workloads. Any inefficiency in application access spirals immediately into loss of business continuity and employee productivity.

In order to maintain business continuity, Versa Secure SD-WAN provides connectivity from the branch to Google NCC Hubs over an SD-WAN overlay (see Figure 3). The Secure SD-WAN solution applies deep packet inspection and role-based access control to prioritize and accelerate certain types of traffic.

Figure 3: Architecture for reliable connectivity to cloud workloads.

Once the traffic enters the Google NCC domain, the traffic takes advantage of highly reliable and scalable Google infrastructure to reach the intended destination.

Automated Integration with a Single Click

Enterprise networks today are complex and require global scale. The enterprise workloads are distributed across public clouds, private clouds, and SaaS clouds. Organizations leverage hundreds, if not thousands of applications, all of which have different networking and security requirements.   Compounded by the shortage of technical staff, it is mission critical for organizations to offload manual configuration and deployment with easy-to-use, automated processes. Technology integrations require REST APIs to provide the best automation workflows.

Versa's orchestration system integrates with Google NCC in a single click. The Versa Secure SD-WAN overlay network easily integrates into the Google NCC solution with developer-friendly REST APIs. Once integrated, Versa offers an intuitive single-pane-of-management that simplifies networking while abstracting out the complexity of applications, networks, and traffic.

Benefit from the Versa and Google partnership:

Cloud-Agnostic Security :

- Versa brings in comprehensive SASE security blended with robust routing and SD-WAN.

- Some of the security services include: PS, IDP, DNS protection, DLP, URL Filtering, SSL proxy, Captive Portal and Zero Trust Network Access to protect against unauthorized access, malware, and ransomware.

- Versa delivers a secure gateway in the cloud for traffic originating anywhere in the world to be secured and encrypted.

Operational Simplicity:

- Single pane-of-management for end-to-end integration and visibility with Google NCC.

- Simplified orchestration that allows network professionals a simplified and easy configuration with Google NCC connections, Google APIs, and network monitoring.

- Full traffic visibility across Google NCC domains and beyond – multi-cloud, on-premises, private cloud, and the edge.

Genuine Multi-tenancy:

- Versa in conjunction with Google NCC provides true multi-tenancy by enabling organizations to achieve management plane, data plane, and control plane multi-tenancy at the cloud, headend, data center, branch, and edge device locations.

Seamless User Experience:

- Versa leverages inbuilt end to-end SLA and performance metrics driven by application factors such as bandwidth, latency, jitter, circuit utilization, MOS score, and more. All of these factors are calculated dynamically to make intelligent traffic steering decisions in real-time.

- Versa identifies over 3800+ applications, 190+ CODECs, and offers granular policies to leverage optimal steering across multi-cloud, on-premises sites, and the edge network.

- Versa uniquely eliminates middle-mile complexity through intelligent multi-cloud traffic steering by leveraging real-time propagation of the transport path from end to end.

- Versa delivers consistent and optimal end user experience through its dynamic traffic intelligence – offering industry lowest latency and best application performance.

About Versa Networks

Versa Networks, the leader in SASE, combines extensive security, advanced networking, full-featured SD-WAN, genuine multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers, and via the simplified Versa Titan cloud service designed for Lean IT. Thousands of customers globally with hundreds of thousands of sites trust Versa with their networks, security, and clouds. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, Liberty Global Ventures, Princeville Global Fund and RPS Ventures.

For more information, visit https://www.versa-networks.com or follow Versa Networks on Twitter @versanetworks.