VxCloud ZSCALER SD-WAN Security

Demand for bandwidth in enterprise branch offices is increasing with the increased use of cloud applications, collaboration tools, and video. Because MPLS is so expensive, enterprises that require additional bandwidth need to leverage the Internet where possible without backhauling to a centralized peering point and gateways.

Distributed enterprises are undergoing dramatic changes, driven by the adoption of mobility, direct Internet access, public cloud applications, and the Internet of Things (IoT). This has resulted in an exponential increase in devices, users, bandwidth, and transactions flooding their networks through the cloud applications. Modern attack surfaces are growing, the more connected and flexible enterprises become, the more opportunities it creates for cybercriminals to exploit new technologies and services that haven't yet been fully secured.

Distributed enterprises face several challenges in deploying and managing their networks:

Complexity: Deploying branch WAN edge services, configuring the WAN to access multiple destinations to increase performance and availability. Multiple paths not only increases the robustness of the infrastructure, but also results in significant increase in complexity.

Application Performance: IT departments are under increasing pressure to address the constraints on bandwidth and redundancy which impact application performance and/or usage. This also increases expenses through OPEX and CAPEX.

Cloud Migration: Traditional WAN architectures don't always provide wireline-type integrity to multiple, dynamic cloud destinations, whether they be SaaS, IaaS (Infrastructure as a Service), or cloud network services.

Security Vulnerability: Direct internet access by leveraging the public Internet instead of MPLS increases vulnerability of branch offices to security threats. Traditional security architectures are not agile enough to support local access security, nor do they easily support zero-touch deployments to ease OPEX issues with support.

To address the challenges of maintaining inter-site connectivity and quality of service without over-reliance on expensive circuits such as MPLS, the router or firewall responsible for WAN connectivity needs to intelligently balance internet and intranet traffic across the available WAN services.

VxCloud Cloud SD-WAN is an effective solution to this challenge, capable of providing per packet link steering at an application level and at the same time addresses needs of distributed enterprises who want to avoid deployment complexity and expensive backhaul and application performance penalties associated with conventional solutions.

Security is a key consideration in distributed deployments. Attempting to secure the modern distributed enterprise with a traditional centralized security approach is like trying to keep rain off a football game using umbrellas. What's needed is a new distributed security architecture that mirrors and complements the new distributed enterprise – an architecture in which the entire network infrastructure is protected through a common, integral security fabric.

This, in a nutshell, is the essence of Fortinet's Distributed Enterprise Firewall (DEFW) – one of the available Deployment modes for Fortinet's Enterprise Firewall. With Fortinet's DEFW, every remote site of the network, regardless of size, is protected under a common, scalable security fabric, the Fortinet Security Fabric. As the network expands, through new sites added to the network or through new wired or wireless connections, the fabric extends automatically, securing each new site and connection.

The Fortinet and VxCloud Secure Software-defined WAN (SD-WAN) solution leverages Fortinet's Distributed Enterprise Firewall (DEFW) and VxCloud's zero-touch deployment, one-click service insertion, single-pane management and assured application performance to provide a comprehensive, cloud-delivered secure SD-WAN solution for distributed enterprises.

The Fortinet and VxCloud secure SD-WAN Solution consists of the Fortinet enterprise firewall platform integrated with an overlay network of VxCloud Edges in distributed sites and data centres, as well as South African cloud-hosted VxCloud Gateways and VxCloud Orchestrator. The overlay deployment is a physical transport layer that is secure and provides unified, automated orchestration, control and visibility, as well as business-level abstraction and incremental migration.