CLOUDGENIX
NETWORKS WITHOUT NETWORKING

WHITE PAPER

CloudGenix Application-Defined Fabric

Application-Defined Fabric Allows Enterprises to Deploy Apps Anywhere Based on App-SLA; Virtualizes Remote Office; Introduces Defense-In-Depth Security Model for Direct Cloud Access

Introduction

The emergence of modern application delivery models using cloud, SaaS and virtualized data centers, and the availability of Internet broadband connectivity as a viable business class transport are driving a fundamental change in the design and economics of the enterprise WAN. Software-defined WAN (SD-WAN) solutions make it easier for customers to implement hybrid WAN technologies, enabling reduced telecom spend. Virtualization technologies coupled with Moore's Law and x86 performance improvements can make it easier to deploy SD-WAN (and other) branch functions on commodity x86 servers, reducing costs even further. However, these technologies in isolation do not address the most challenging burden on IT teams — driving performance, security and compliance SLAs for modern applications when these applications can be delivered from a heterogeneous hosting locations and over varying transport. Legacy networking-centric mechanisms for application controls were designed for data center-hosted applications delivered over MPLS networks. For IT to realize the benefits of modern application delivery, CloudGenix introduces the application-defined WAN fabric.

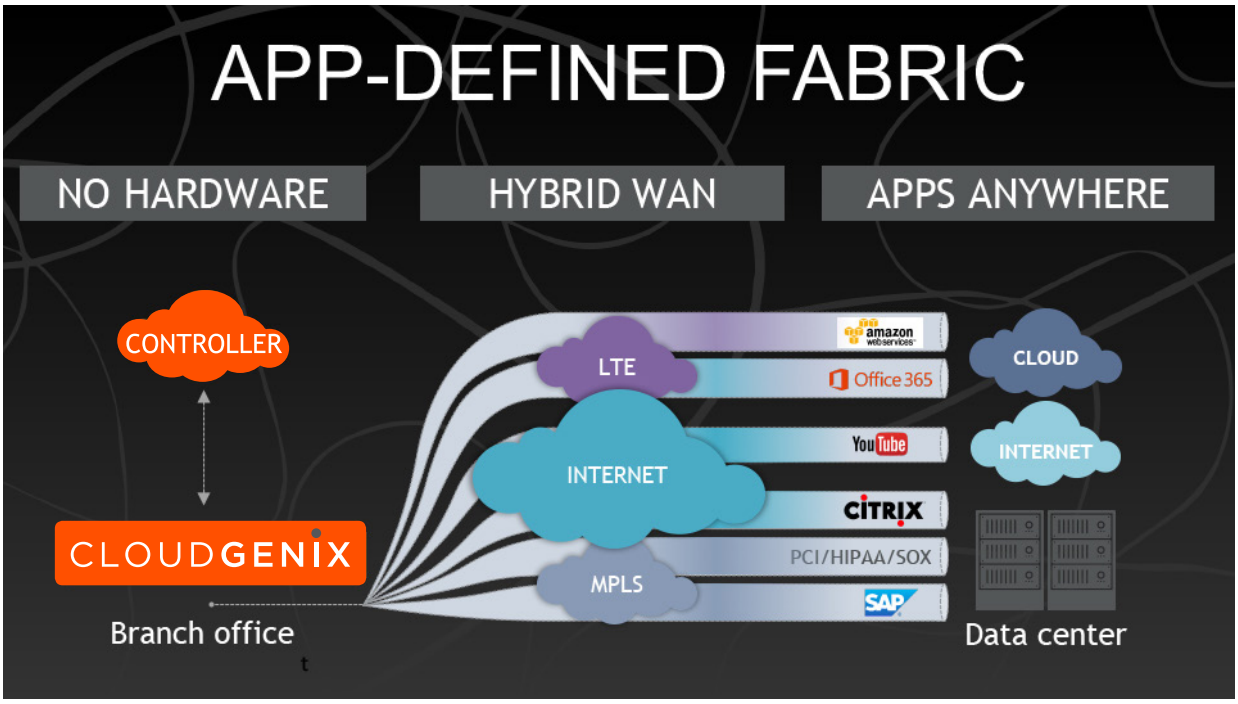

Figure 1: CloudGenix App-Defined Fabric

As the name suggests, an application-defined WAN fabric allows enterprises to logically define and re-structure their WANs around individual application-specific attributes and requirements. Traditional "routed" SD-WAN fabric centers on network and link-level attributes such as network uptime (aka "five 9s" of reliability) and path selection based upon link latency, jitter and packet loss. Application-defined fabrics, however, allow customers to define and dynamically instantiate application-specific policies around application health and application performance (application SLAs), security and segmentation (security SLAs), and basic path selection. This app-defined fabric can also be extended to include direct Internet-reachable SaaS applications without sacrificing application or security SLAs. In fact, an app-defined fabric dynamically creates a secondary application-level security perimeter with full whitelist/blacklist and stateful firewalling capabilities.

An application-defined fabric allows easy and reliable WAN programming around the needs and control requirements of specific applications, including allowable path (direct Internet, direct MPLS, VPN, satellite, LTE, etc.), application performance, security and WAN segmentation. The app-defined fabric can also monitor compliance to application performance and security SLAs — specifically, application health; application transaction-level performance and security policy violations.

Customer Drivers for an Application-Defined Fabric

The need for an app-defined fabric is driven by numerous factors, both internal and external to an IT organization. Some of these factors, in addition to cost savings and operational simplification, are as follow.

Application performance: SLAs provide competitive advantages

Organizations rightly focus on voice and video performance since they are critical to effective collaboration internally as well as with partners and customers. Transactional applications are often equally as critical to an organization as voice, but there have historically been no networking tools available to measure and control application health for business applications, such as credit card clearinghouses, ERP applications for traditional enterprises, or CAD applications for engineering organizations.

Application rollouts, including SaaS, are increasingly being driven by line of business

When LOBs find a SaaS application to be important to their business, they increasingly fund application rollouts aligning deployment schedules to business milestones, rather than traditional network upgrade and refresh cycles. The WAN must be more flexible and agile to support rapid deployment of these applications.

Modern applications are multifaceted and adaptive

Historically, enterprise applications were unencrypted and could be reliably and readily identified by the classic network "tuple" and DSCP marking. Today's applications are increasingly encrypted and have multiple different subapplications. As an example, Google apps and Office365 comprise email, chat and file-sharing apps, among others. These subapplications share a common IP and wildcard cert and are encrypted. End users expect the network to properly detect these subapplications and apply appropriate application performance controls.

Ever-increasing focus on compliance and security

Historically, the requirements of security and applications have been, at best, orthogonal, and more realistically,

in direct conflict. For instance, SaaS applications often perform best when accessed directly over the Internet instead of being backhauled to a data center or regional services hub. When security and application performance are viewed independently, they are often in conflict. By embedding security into the fabric, it is possible to have the best of both worlds providing strong application-level firewalling and secure segmentation while improving application performance.

The Solution

CloudGenix instant on network (ION) nodes are built on top of commodity off-the-shelf x86 compute platforms, and are deployed at each remote site, data enters, and IaaS clouds. The IONs automatically authenticate with each other, and establish encrypted tunnels to secure the transport. Based on the application-SLA defined by the administrator, the IONs create a secure application-defined fabric that enforces performance, security and compliance policies over any underlying transport for all applications.

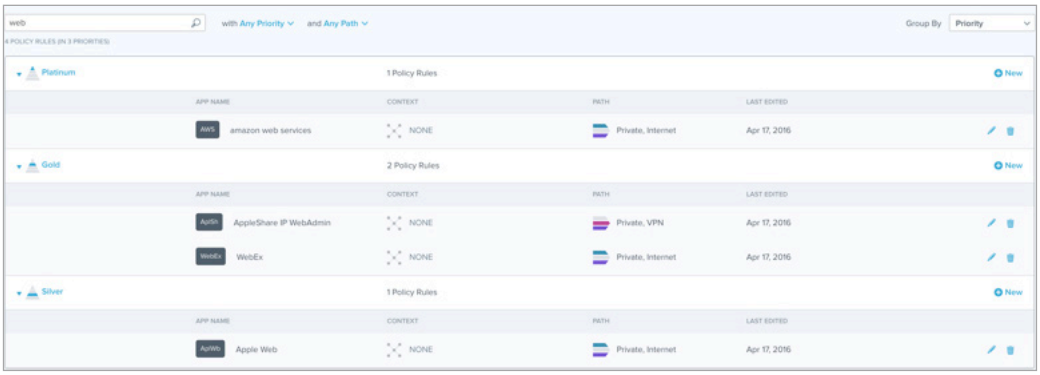

Figure 2: CloudGenix App-SLA definition

Each branch ION end point has a zone-based stateful application firewall, automatically creating a defense-in-depth model that extends a secondary perimeter to the branch. This secondary perimeter enables whitelisting and blacklisting of internal and external applications, as well as traffic segmentation and isolation for security and compliance requirements.

Unlike traditional routed SD-WAN solutions, which operate at the packet level, the unit of operation of the CloudGenix ION end points is each individual application session. By operating at the session level, the CloudGenix fabric is able to:

- Identify individual subapplications for traditional, modern and SaaS applications, even if they are encrypted
- Directly measure application transaction performance attributes, including transaction error rates, MOS score for voice, application health, application transaction time and server response time
- Make path selection decisions based on policy and measured application health and performance, rather than link-specific attributes
- Detect changes in behavior of modern application sessions and re-queue as appropriate to provide optimal performance

The ION-fabric paths and firewall functions are tightly aligned to specific applications via an application policy model. The policy model is expressed in terms of application names, allowed path, and performance SLA and security SLA requirements instead of networking tuples and routing protocols used in traditional routed SD-WANs. This ensures that the business intent underlying the application and security policies is directly programmed into the WAN fabric, ensuring there is no gap between policy and intent and simplifying audit.

Next Steps

With CloudGenix, you can deploy modern cloud and data center applications fluidly, combine economic transport like Internet broadband as part of your WAN strategy, and virtualize your remote office infrastructure. Using the CloudGenix app-defined fabric, the need for hardware routers is eliminated, and foundational hybrid WAN cost savings and carrier independence are gained. As cloud-based applications become part of your enterprise IT, you can enhance the security of the WAN, and enforce application performance and security SLAs for enterprise- and cloud-hosted applications. Please contact CloudGenix or an authorized CloudGenix partner for a no-obligation SD-WAN and cloud readiness assessment customized to your environment.