Cloud Security with SD-WAN, Case Studies and Best Practices

David Klebanov
Director, Technical Marketing | Viptela

Sri Subramanian
Sr. Director, Product Management | Zscaler
Customer Ask

- Eliminate dependency on MPLS traffic backhaul
- Improve cloud applications performance for corporate users
- Offload guest WiFi traffic
- Streamline remote office infrastructure
- Establish strong security posture
- Lower costs
- Simplify operations

Solution:
By the end of 2019, **30% of enterprises** will have deployed SD-WAN technology in their branches, up from less than 1% today.

Spending on software-defined WAN products will rise from $129 million in 2016 to **$1.24 billion** in 2020.

Enterprise spending on SD-WAN growing at a compound annual growth rate (CAGR) of **76.2%** from 2016 through 2020.

By 2020, **more than 50% of WAN edge infrastructure refresh initiatives** will be based on SD-WAN versus traditional routers (up from less than 2% today).

Source: Gartner Predicts 2016: Enterprise Networks and Network Services, Dec 2015
Today’s WAN Challenges

- Insufficient Bandwidth
- Limited Application Awareness
- Applications Downtime
- Limited Scale
- Fragmented Security
- No Cloud Apps Readiness
- Complex Operations
- High Cost

Is Your WAN Business Ready?
Viptela SD-WAN Solution Philosophy

Application Policies
- Application SLA
- Traffic Engineering
- Per-Segment Topologies
- Secure Perimeter
- Cloud Path
- Cloud Accel
- Transport Hub

Delivery Platform
- Routing
- Security
- Segmentation
- QoS
- Multicast
- Svc Insertion
- Survivability

Transport Independent Fabric
- Broadband
- MPLS
- Cellular

Analytics
- Monitoring
- Operations

FutureWAN 2017 SD-WAN Virtual Summit
Viptela Solution Elements

- Network Security
- QoS
- Services
- OPS

- GUI
- APIs

Private/Viptela/Managed Cloud

Secure Control Plane

Ubiquitous Data Plane

Cloud Data Center

Data Center

vEdge Route
Delivering Cloud Enabled Enterprise

IaaS

SaaS

Security

Security
Zscaler Cloud Security Platform
Gartner Research

30 percent of the world’s largest 100 vendors are expected to shift their software investments from a “cloud-only” to “cloud-first” policy by 2019.

Gartner Webinar: Clouds are Secure. How Secure are you?

Through 2020, 95 percent of cloud security failures will be the customer’s fault.

By 2018, the 60 percent of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

Through 2020, 99 percent of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Source: Gartner Top Ten Predictions for 2016 and Beyond, Oct 2016
Source: Gartner Market Insight: Cloud Computing’s Drive to Digital Business Creates Opportunities for Providers

Despite large investments in data center security appliances, all these brands got compromised.
Attacks have shifted from servers to users – weakest link

Protecting the user is critical to protecting the enterprise

- Hacker infects a trusted site
- C&C accesses company data
- User visits the trusted site and becomes infected with a botnet
- Botnets
- C&C accesses company data
- Trusted user machine connects to the corporate network and steals IP

www.facebook.com
Can you trust a reputable web site?

Appliances don’t have the capacity to inspect all objects and traffic

Total object requests: 167

Personalized content delivered from multiple sources

Traffic: SSL

CDN: Akamai

Page objects loaded: JavaScript, CSS, images

Potential threats: 167
You need to adopt a zero-trust strategy

60% of the top 100 sites have malware

40% of Internet traffic crosses CDNs and goes uninspected.

54% of advanced threats hide behind SSL.

Inspecting all traffic can require 8X more security appliances

Gartner

Virtual Networking Index, Cisco

ThreatLabz Research, Zscaler
Mission: Secure your Internet Experience

Zscaler sits between your users and devices and the Internet to make sure nothing bad comes in and nothing good leaves.

- 100+ Data centers worldwide
- 25B+ transactions processed every day
- 125M+ threats blocked every day
- 120K+ security updates every day

All Locations

Any Device
Zscaler stands for Zenith of Scalability

All users – All traffic
5K+ Enterprises
15M+ Users
Cloud-effect = better threat intelligence

How often are your security appliances updated?

- 25B+ transactions from 15M users across 185 countries
- Detected once and immediately propagated to all 100 data centers
- 120K security updates per day: immediate, every 15, 30, and 60 minutes
Purpose-Built Multi-tenant, Modular Architecture

1. Brain/Nervous system, Policy, Real-time threat updates
2. Onramp to Internet, Executes policy
3. Policy follows the user to the nearest ZEN
4. Logs consolidated & correlated in real-time

Same policy & protection, near-zero latency for a user anywhere
World Class Cloud Infrastructure

- **World-Class Data Centers**
  - Zscaler Owned Dedicated Systems - No Amazon, RackSpace, etc.
  - Tier III and Tier IV Datacenters
  - Certified (SAS 70, ISO 27001, etc.)
  - Strict Security Controls

- **Lightning-fast Network Performance**
  - Carrier Class and Carrier Neutral Design
  - Fiber-Based 10GE Connectivity, Multiple Tier 1 transit provider
  - Strategically Located at Major Internet Routing Centers (NAPs)
  - Access to Diverse Peering Arrangements For Performance, Resiliency, and Flexibility
Ease of Deployment for a Uniform User Experience

**Easy Connection:**
- PAC Files
- Agent
- GRE Tunnels
- VPN Tunnels
  - No new HW

**Simplify IT**
- Policy-follows-the-user everywhere
- No traffic backhauling; No VPN to HQ
- Transparent user experience

**Enforce policy bi-directionally**

ID Federation with SAML 2.0
- Single-Sign On
- Active Directory Federation

Logs are always written to disk only in the region of choice.

"Zscaler enables us to very effortlessly manage policy across 100 locations."
Leading industry analysts agree...

“Zscaler is a very strong choice for any organization interested in a cloud gateway.”

“…on-premises web content security can’t protect digital business…”
Why Zscaler?

**Reduced Risk**  
CISO  
- Unmatched security - all users, branches, devices  
- Consistent policy & protection  
- Always up-to-date

**IT Simplification**  
CTO / IT Head  
- Consolidate point products & simplify IT  
- Cloud-enabled network  
- Rapid deployment

**Impressive Value**  
CIO / CFO  
- No Capex, elastic subscription fee  
- Reduced Opex - no box management  
- Reduced MPLS costs

**Productivity**  
End-users  
- Fast response time – local breakouts  
- Localized content  
- Empowers users to leverage cloud apps

A Trusted & Reliable Partner  
Commitment to Quality & Customer Success  
Technology Innovator - Market Leader - Financially Strong
Joint Solution and Customer Success Story
Cloud Enabled Enterprise With Viptela SD-WAN & Zscaler

- Regional Cloud Path
- Application Visibility
- Advance Security
Cloud Enabled Enterprise With Viptela SD-WAN & Zscaler

- Direct Cloud Path
- Application Visibility
- Advance Security
Zero Trust Security

- Zone-based network segmentation
- SD-WAN polices for user traffic steering
- Cloud security polices for user traffic inspection
Service High Availability and Redundancy

Data Center

- Core Router
- Core Router
- OSPF/BGP
- Tunnel
- SD-WAN Fabric

Large Campus

- Core Router
- Tunnel
- SD-WAN Fabric
- VRRP

Remote Location

- Retail Location, Bank Branch, Oil Rig
- Core Router
- Tunnel
- SD-WAN Fabric

FutureWAN 2017 SD-WAN Virtual Summit
Customer Case Study

Fortune-500 Healthcare Equipment

- Locations: Over 100 locations worldwide
- Employees: 12,000 global employees
- Market size: $45B
- FY15 revenue: US $4.04B

Customer Requirements

- SD-WAN with MPLS & Broadband
- Split tunnel for Internet bound traffic
- Centralized security and WAN management
- FW / IPS / URL Filtering / Behavior Analysis

- DPI based SD-WAN policies
- Entirely cloud controlled
- Optimal SaaS access
- Dual redundancy

FutureWAN 2017 SD-WAN Virtual Summit