Architecting a Business-driven SD-WAN with Enterprise-grade Security
Agenda

- SD-WAN Use Cases Driving Tangible Business Outcomes
- Best Practices Updated – Can I Really Replace My Branch Routers and Firewalls?
- Silver Peak SD-WAN and Zscaler → 1 + 1 = 3
- Summary
- Q&A
WHY CUSTOMERS ARE ACCELERATING SD-WAN ADOPTION
Use cases driving tangible business outcomes

Top SD-WAN Use Cases

Router replacement and WAN simplification
Increase application performance
Improve security across the enterprise
Increase agility in bringing new sites online quickly
Increase agility in deploying new applications quickly
Utilize multiple transport technologies

Source: 2019 SD-WAN Growth Outlook, Futuriom, June 2019
SD-WAN IN 2019
Rethinking the WAN in a cloud-first world

- Can I retire routers and firewalls at my branch sites?
- Can I move from hub and spoke to local internet breakout?
- Can I retire MPLS in favor of internet services?
- Can I go “all in” on SD-WAN and cloud-hosted security?
CLOUD BREAKS LEGACY NETWORKS AND SECURITY

Cloud-first enterprises are rethinking WAN and security infrastructure

**Slow, Unpredictable Performance**
- Impaired application performance
- Inability to achieve SLAs
- Poor visibility increases MTTR

**Incompatible Security**
- Larger attack surface
- Inconsistent security between data center and branch
- Inability to scale perimeter security for distributed enterprises

**Higher Costs**
- Infrastructure
- Network
- Administration overhead
WHY SD-WAN AND CLOUD-HOSTED SECURITY

Secure local internet breakout delivers highest quality of experience with reduced risk

Improved Application Performance
• Quality of experience
• Business productivity
• Customer satisfaction

Consistent Security Policies
• Full security stack
• Consistent protection
• Eliminates security and performance tradeoffs

Reduced Risk and Cost
• Always up-to-date
• Optimizes MPLS spend
• Simplifies WAN infrastructure

Granular Internet Breakout by First-packet iQ™

Branch Office

Legacy Corporate Apps

HQ / Hub / Data Center

Custom Apps

10,000+ Apps 300 Million+ Web Domains

Customer-specified Whitelist

All Other Web and Cloud Traffic
SILVER PEAK ZSCALE AUTOMATED SECURITY ONBOARDING

- Establish tunnels to primary and secondary Zscaler ZEN PoPs
- Forward all branch traffic to the primary ZEN PoP
- Create additional tunnel pairs to the same ZEN pairs for branch locations served by multiple ISP’s
- EdgeConnect SD-WAN monitors transport service health to the ZENs and controls tunnel fail-over
- Support GRE tunnels for high-bandwidth locations and IPSec tunnels for dynamic IP locations
- Comply with Zscaler IPSec and GRE tunnel best practices

Best practice results in 2, 4 (or more) tunnels per branch
ZSCALER SD-WAN API INTEGRATION WORKFLOW

Integration automates the complexity of IPSec tunnel configuration

1. Start Zero-touch provisioning
2. Select Zscaler Primary & Secondary Data Center VIPs based on geo-location
3. Prepare tunnel configuration elements
4. Authenticate to Zscaler API
5. Create new **VPN Credential** object in Zscaler
6. Create new **Location** object in Zscaler, associated with VPN Credential
7. Active configuration
8. Establish IPSec VPN Tunnels

**Configuration Elements**

- **Unity EdgeConnect™**
- **Unity Orchestrator™**
- **Zscaler API**

**Zscaler API**

1. GET
   - Datacenter IPs JSON

2. POST /api/v1/authenticatedSession
   - Session Cookie

3. POST /api/v1/vpnCredentials
   - 200 OK with vpnCredential ID

4. POST /api/v1/Locations
   - 200 OK with Location ID

5. POST /api/v1/status/activate
   - 200 OK Status: ACTIVE

**Identify nearest Zscaler PoPs**

**Set up Shared Credentials**

**Add Branch Locations in Zscaler**

**Start ZTP**

**Send Device Config to Load**

**Confirm Device Config Loaded**
Thank You