ARUBA + ZSCALER
Better Together Network Transformation

Raja Sundarrajan
Systems Engineer
Aruba

Bil Harmer CISSP, CISM, CIPP
Americas CISO
Zscaler
Who are we?

Raja Sundarrajan
Systems Engineer
Aruba
@RajaSundarrajan

Bil Harmer
Americas CISO
Zscaler
@wilharm3
How, when, and where we work is changing
Are you ready for the Millennials?
35% of Workforce and Growing Quickly

Source: Mary Meeker Internet Trends 2017 – Code Conference
Technology is no longer the sole domain of technologists.
Cloud Transformation

• By 2020 “Cloud Shift” will affect $1 Trillion in IT spend

• 81% of companies with 1000+ employees are using, testing or investigating AWS

• AWS active users exceed 1,000,000 users

• 320% increase in the adoption of O365
State of the art in 2010

**Challenges**

- Single-tenant systems
- Separate control, enforcement and logging
- No single policy object to share context
- Expensive to deploy and scale
- Poor user experience
In 2018: We Virtualized Everything!

Solves
- Horizontal scaling
- Hardware headaches

Remaining Challenges
- Single-tenant systems
- Separate control, enforcement and logging
- No single policy object to share context
- Poor user experience
A simple web request takes 28 hops

Despite this massive investment, breaches are on the rise.

Securing your cloud transformation
Yet We Still Rely on Datacenters That Break Cloud Services

Bring users onto the corporate network to provide remote access to apps

**Internal apps on public cloud (Azure, AWS)**

- Traffic backhauled to gateway
- Traverses site-to-site tunnels
- Hairpins back to user location
- May require new appliances

**Internal apps in data center**

- Poor user experience with remote access VPN
- Traffic backhauled to static remote access VPN gateway
- Network is exposed to the user
How our Users Feel
Organizations are turning to SD-WAN

SD-WAN simplifies the branch and makes local internet breakouts easy

<table>
<thead>
<tr>
<th>Reduce Costs</th>
<th>Agility</th>
<th>Simplify IT</th>
<th>Fast Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduces MPLS dependency/cost with comparable reliability</td>
<td>• Support evolving business needs</td>
<td>• Reduce branch hardware</td>
<td>• Direct to cloud connections</td>
</tr>
<tr>
<td></td>
<td>• Add/removeSCALE branches easily</td>
<td>• Granular visibility and control</td>
<td>• Fast user experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rapidly deploy and provision connections</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
TODAY’S BRANCH COMPLEXITIES

INCREASED CLOUD ADOPTION
85%
of IT will commit to multi-cloud architecture by 2020

INCREASED SECURITY RISK
20B+
IoT devices will be deployed by 2020

SaaS applications are backhauled to the data center

HR Systems  PBX  Apps

Dedicated links are up to 10x the cost

Private WAN is complex and expensive

Device sprawl, operations in silo, and static configuration

INCREASED SECURITY RISK

85% of IT will commit to multi-cloud architecture by 2020

INCREASED CLOUD ADOPTION

20B+
IoT devices will be deployed by 2020

INCREASED SECURITY RISK

85% of IT will commit to multi-cloud architecture by 2020

INCREASED CLOUD ADOPTION

20B+
IoT devices will be deployed by 2020

INCREASED SECURITY RISK
ARUBA’S SOFTWARE DEFINED BRANCH

SD-WAN + SD-LAN

Security

Access Points

Aruba Central

Switches

Branch Gateways

Virtual and Headend Gateways
REDEFINING THE BRANCH INFRASTRUCTURE

TRADITIONAL BRANCH
DISPARATE DEVICES WITH SEPARATE MANAGEMENT

ARUBA SOFTWARE DEFINED BRANCH
COMBINES LAN AND SD-WAN SERVICES WITH SECURITY
THE POWER OF ARUBA’S SD-BRANCH SOLUTION

Simplicity at Enterprise Scale
Optimized Branch Experience
Integrated, Best-in-class Security
SIMPLECTITY AT ENTERPRISE SCALE

- Single pane of glass for WLAN, LAN, and SD-WAN provisioning and management for thousands of sites
- Simple onboarding with Installer app
- Single point of policy enforcement with Branch Gateways
DYNAMIC SEGMENTATION, BRANCH-WIDE

PORT-BASED
- Manual configuration of ACLs, VLANs, QoS
- PCI-compliant
- Static

Hard to scale for device type and quantity across multiple sites

ROLE-BASED
- Automate configurations with context
- Dynamic

Flutter configurations at high scale based on user, device, app

- PoS port
- Camera port
- Printer port

Manual configuration of ACLs, VLANs, QoS

Automate configurations with context
OPTIMIZED BRANCH EXPERIENCE

Meet or exceed SLAs with fine-grained context awareness

Real-time insight into application responsiveness

DPS provides intelligent path selection and automatic failover

Contextual Policy for LAN and WAN

Users

Device

Applications

Location

Real-Time Dynamic Path Steering
INTEGRATED, BEST-IN-CLASS SECURITY

- Application and user aware firewall
- Web content filtering
- Dynamic Segmentation
- Unified WAN and LAN policy architecture

Branch Gateways

Single Point of Policy Enforcement

140+ ecosystem partnerships
Summary of Operations

All this is great... But how does it help my day to day ops?

1. Create job
2. Installer scans devices
3. Devices geotagged Branch view created
4. Auto SW upgrade Hierarchical config pushed
5. Proactive alerting/reporting on a site/group basis
More than just monitoring…

- Reports
- Remote Console
- Software Management
- API for all platform interactions
- Webhooks for outbound notifications
ACCELERATE BRANCH DEPLOYMENTS AND REDUCE COSTS

BEFORE
IT must perform time-consuming truck rolls to deploy branch services
Impact: Can take months or years to roll out new services to all branches and cost thousands per site

AFTER
IT improves operations with centralized management of branch services
Impact: IT can roll out new services and changes quickly with limited staff
ENTERPRISES NEED TO IMPROVE USER EXPERIENCE

**BEFORE**
IT must troubleshoot problems without visibility into root causes

*Impact: Problems may go unresolved for days*

**AFTER**
IT can deploy onsite sensors that keep track of branch health

*Impact: IT can identify potential problems before they impact users*
REGULATE IOT WORKFLOWS ACROSS ALL SITES

**BEFORE**
IT manually configures static rules per port for specific devices at each site

**Impact:** Security is deployed inconsistently and prone to misconfiguration

**AFTER**
Use Dynamic Segmentation enforced by the branch gateway

**Impact:** Vendors can remotely access specific IoT devices at each site, but not the network
But how do you consistently secure internet connections across all your locations without adding complexity?
Can you do network security in the world of cloud?

How do you secure a network you don’t control?

Can’t build a ‘moat’ around it with firewalls and proxies

How do you protect your users and apps?

A new approach to security is needed

Agnostic
Cloud
Network
Device

Securing your cloud transformation
Securing direct-to-internet connections
Reduce deployment time and TCO with flexibility, scalability, and centralized management

You probably can’t replicate the HQ security stack in all branch locations

- High cost and complexity of branch security appliances
- Appliance or VNF sprawl
- Negative performance impact
- Compromises in branch security

But you can enable internet breakouts with cloud-delivered security

- Reduces costs, eliminates branch security appliances
- Delivers a fast and secure user experience
- Simplifies branch IT operations
- Provides identical protection wherever users connect

Securing your cloud transformation
Fast, secure, and reliable access to the internet and SaaS
The best approach for Secure SD-WAN and Office 365

Platform Services

Access control
- Cloud firewall
- URL filtering
- Bandwidth control
- DNS resolution

Threat prevention
- Cloud sandbox
- DNS security
- Proxy (Native SSL)
- Advanced threat protection

Data protection
- Data loss protection
- Exact data match
- CASB
- File type controls

Security and Policy Enforcement

Unprecedented Visibility
Logs only written in memory and forwarded to a logging cluster in a geography of your choice
Log streaming to your SIEM / SOC

Security and Policy Enforcement

3rd Party Auth

Unprecedented Visibility

Security and Policy Enforcement

3rd Party Auth
The New Reality

There is only one network in the world
……you can’t control it
……services are consumed on it at will
……you can’t secure it

Security requires an architecture transformation
Focus on high impact risk…trying to protect everything protects nothing
Don’t confuse security with compliance

Question everyone and everything!
Accept nothing at face value.

Speed is the new currency
Thank You
Patch Your @*#&$ Systems!!!

njRat  #WannaCry  Bad Rabbit

Meltdown  Spectre  Ransomeware