Cisco SD-WAN Application Acceleration

Sukruth Srikantha, Technical Marketing Engineer
Hamzah Kardame, Technical Marketing Engineer
Atif Khan, Sr. Director Enterprise Routing
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKRST-2514
Agenda

- Introduction
- SD-WAN Introduction and Architecture
- SD-WAN Application Acceleration
- Next-Gen WAAS Application Optimization
- SD-WAN WAAS Deployment
- Demo
- Conclusion
Introduction
Current WAN Challenges

Is Your WAN Business Ready?

- Insufficient Bandwidth
- Limited Application Awareness
- Applications Downtime
- Fragmented Security
- Limited Scale
- No Cloud Apps Readiness
- Complex Operations
- High Cost
Why SD-WAN in Enterprise?

- 50% of Apps accessed via Internet
- 70% have either 2 or 3 WAN connections/branch
- 32.4% cite management of connectivity at branch as a challenge
- 48.6% cite poor application performance and latency as corporate WAN concern
SD-WAN Introduction and Architecture
Cisco SD-WAN Solution Pillars

- Agile Operations
- Cloud-Delivered Architecture
- Application Quality of Experience
- Comprehensive Security
Cisco SD-WAN Secure Extensible Network

Orchestration Plane

Management Plane
(Multi-tenant or Dedicated)

Control Plane
(Containers or VMs)

Data Plane
(Physical or Virtual)

vManage
vSmart
vBond
vEdge

vOrchestrator

MANAGEMENT
ANALYTICS
ORCHESTRATION
CONTROL
INTERNET
MPLS
4G

Data Center
Campus
Branch
Home Office
SD-WAN Application Acceleration
Application Performance Influencers

- Bandwidth
- High Latency
- User Experience
- Brownouts
- Lossy Links
- Chatty Apps
- Cloud Adoption

All of them contribute to bad Application Performance
Application Acceleration Techniques

- App-Aware Routing
- TCP Optimization
- Cloud OnRamp
- QoS
- SD-WAN Native
- SD-WAN WAAS
- Caching
- Deduplication
- Compression
- Protocol Specific
Application Visibility and Recognition

- App Firewall
- Traffic prioritization
- Transport selection
Data Plane Liveliness and Quality

- Bidirectional Forwarding Detection (BFD)
- Path liveliness and quality measurement
  - Up/Down, loss/latency/jitter, IPSec tunnel MTU
- Runs between all vEdge and vEdge Cloud routers in the topology
  - Inside IPSec tunnels
  - Operates in echo mode
  - Automatically invoked at IPSec tunnel establishment
  - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
  - Fully customizable per-vEdge, per-color
Critical Applications SLA

- vEdge Routers continuously perform path liveliness and quality measurements

App Aware Routing Policy

App A path must have:
- Latency < 150ms
- Loss < 2%
- Jitter < 10ms

Path1: 10ms, 0% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

Internet
MPLS
4G LTE
IPSec Tunnel
TCP Optimization

- High latency path between users and applications, i.e. geo-distances
- vEdge routers terminate TCP sessions and provide local acknowledgements
  - Hosts don’t have to wait for end-to-end TCP ACKs and pause TCP transmission
- Optimized TCP connection uses selective acknowledgement to prevent unnecessary retransmissions and large initial TCP window size to maximize throughput
- Hosts using older TCP/IP stacks will see the most benefit
Bandwidth Augmentation

- Augment MPLS with Internet bandwidth
- Create traffic engineering policy to steer application traffic
  - Active/Active if no policy

Traffic Engineering Policy (data policy)
App A -> MPLS TLOC
App B -> Internet TLOC
Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
- Per-VPN behavior enforcement

VPN default route for all traffic DIA or data policy for selective traffic DIA

Network Address Translation (NAT) on the vEdge router only allows response traffic back
- Any unsolicited Internet traffic will be blocked by IP table filters

For performance based routing toward SaaS applications use Cloud onRamp
Cloud onRamp for SaaS - DIA

- vEdge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
  - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated
Cloud onRamp for SaaS - Gateway

- vEdge routers at the remote site and regional hub perform quality probing for selected SaaS applications across their local Internet exits
  - Simulate client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
  - HTTP ping for local DIA and App-Route+HTTP ping for regional Internet exit
- Internet exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated
Quality of Experience Score

• Every site where SaaS application is enabled, is classified as performing Good, Average or Bad

• Sites are color coded based on the performance
vEdge Router Device QoS Overview

Data Policy
Classification of application traffic into QoS forwarding classes (queues)

Ingress Interface
- vManage
- Map into QoS forwarding classes
  - FC

Egress Interface
- QoS Scheduler
  - Q

QoS Overview
- QoS forwarding classes
- Map into FCs
- Map into Egress Queue
- Policing
- Rewrite inner DSCP
- Rewrite outer DSCP
- Shaping
- Bandwidth % Buffer % Scheduling Priority Drop
- Out
Next-Gen WAAS Application Optimization
Building Blocks of WAAS

Bandwidth

Object Cache

DRE

LZ

Latency

TCP Flow Optimization

Application Behavior

AO

AO

AO

Akamai

Application Behavior
## Transparent Caching: with four (4) different mode settings

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BASIC</strong></td>
<td>- Follows IETF HTTP 1.1 guidelines for standard object caching</td>
</tr>
<tr>
<td></td>
<td>- Only caches responses marked explicitly as cacheable</td>
</tr>
<tr>
<td><strong>STANDARD</strong></td>
<td>- Default mode</td>
</tr>
<tr>
<td></td>
<td>- Also caches objects with no explicit cache marker</td>
</tr>
<tr>
<td></td>
<td>- And with a last-modified date. It ignores “reload” headers from clients</td>
</tr>
<tr>
<td><strong>ADVANCED</strong></td>
<td>- Caches media files more aggressively, and all object types for longer times (when there is no explicit expiration time)</td>
</tr>
<tr>
<td><strong>BYPASS</strong></td>
<td>- Turns off caching for a configured site(s)</td>
</tr>
</tbody>
</table>

### 2. Connected Cache (CC):
Retrieves content from Akamai’s Intelligent Platform

### 3. Over-the-Top Caching (OTT):
Caching content of 3rd party Web sites using a predefined configuration

### 4. Cache Warming or Prepositioning: Scheduled fetch and cache of content from a Web site
Use Case: Accelerate Live Video

Challenges
• Delivering corporate live video over the enterprise network - serving 70K+ end users across 250 branches globally
• End-users in South America and Asia suffer from WAN congestion and video quality issues with frequent re-buffering and slow load times

Benefits
• Cisco WAAS with Akamai Connect caches live and on-demand HTTP video fragments
• Resulted in significant WAN offload while improving video quality & end-user experiences
• Reduced IT tickets related to corporate video webcast quality/performance issues
Use Case: Software Download

Software updates keep growing and consuming more enterprise network bandwidth
iOS 8 Update = ~1.1MB; iOS 9 Update = ~1.2GB

Akamai Connect can help by caching iOS and OS X updates locally in the branch
Improving performance
Offloading the enterprise network

Updating 3 iPads resulted in 2.67GB of WAN offload
Cloud and SaaS
WAAS 6.4: Dual-Sided and Smart SSL

Ability to cache both HTTP and SSL in DIA scenario
Dual-Sided SSL Optimization Solution

- **SSL Handshake**: Client to Core WAE
- **SSL Session**: Client to Core WAE
- **SSL Session**: Core WAE to SSL Server

**Transparent Secure Channel**

**Send Session Key**

**Original Data** - Encrypted

**Optimized & Encrypted**
AppNav Redirection
AppNav Solution

Data Center

- Optimization
- Load Distribution
- Redirection
- Interception
- Asymmetric Traffic and H.A.

Data Center

- AppNav
- AppNav-XE

Interception

Load Distribution

Optimization

Asymmetric Traffic and H.A.
AppNav Affinity Features

- AppNav’s powerful policy engine allows for easy separation of branch traffic
- No knowledge of IP addresses or ACLs required
- Split traffic into separate application clusters
- Allows WAAS to easily adapt to application traffic increases and changes.
NG-WAAS
Cisco Application Optimization Form Factors

**WAAS Appliance**
- Application acceleration
- Scalable platforms for range of deployments
- 200 – 150,000 optimized flows

**Next-Gen WAAS Appliance**
- Application acceleration
- Improved HW and performance
- 200 – 6000 optimized flows

**Virtual WAAS in the cloud**
- For public cloud and SaaS acceleration
- 200 – 12,000 Connections
- Hourly based/BYOL
- Solution template for ease of deployment

**ISR-WAAS on ISR4K**
- Identical features and management as other WAAS options
- Simple installation has you up and running in 7 minutes
- Included in Cisco One Foundation and AX

**WAAS NFV on ENCS**
- Scale as you grow
- WAAS 200 Conn- 750 conn
- Interop/Service Chaining with other NFVs
- Included in WAN Foundation

**Virtual WAAS on UCS-E**
- Ideal for hosting on UCS-E on ISR 4K with other apps
- No forklift upgrade
- Included with Cisco and AX on ISR4K router

BRKRST-2514 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
What’s new with WAAS?

• On September 30th 2017, End-of-Sale and End-of-Life was announced for the Cisco WAVE x94, 7541, 7571 and 8541 platforms as well as the AppNav IOM cards.

• Replacement solutions will be released in phases, starting with branch-side WAVE replacements by Jan 2018.

• At a high-level the current replacement offerings are as follows:
  • For DC-side WAVE (8541/7571/7541), move to BYOH model and run vWAAS (150K*/50K/12K)
  • For branch-side WAVE (694/594/294), move to new WAAS HW platform (ENCS-W)
  • For AppNav IOM, move to AppNav-XE which is a software feature available on CSR/ISR4K/ASR platforms.
SD-WAN WAAS Deployment
SD-WAN WAAS Inline

LAN

DC/Remote Office

SD-WAN Fabric

MPLS

Internet

OMP-to-BGP/OSPF
BGP/OSPF-to-OMP

vEdge

Local prefixes (OSPF/BGP)

(WAAS, UC, Akamai Connect)

LAN

SD-WAN Traffic
SD-WAN WAAS Offpath
**SD-WAN WAAS Redirection**

**DATA POLICY ON VSMART**
- policy data-policy WAAS-REDIRECT
- vpn-list VPN-1
  - sequence 10
  - match
    - protocol 6
  - action
    - set next-hop 10.1.2.2
  - default-action accept
- apply-policy site-list Branches
- data-policy WAAS-REDIRECT from-tunnel

**POLICY ON VEDGE**
- policy access-list WAAS-REDIRECT
  - sequence 10
  - match
    - protocol 6
  - action
    - set next-hop 10.1.2.2
  - default-action accept
- int ge0/1
- access-list WAAS-REDIRECT in

**CONTROL POLICY ON VSMART**
- policy control-policy WAAS-EXTRANET
  - sequence 10
  - match route
    - vpn-list VPN1
  - action accept
  - export-to
    - vpn-list VPN2
  - sequence 20
  - match route
    - vpn-list VPN2
  - action accept
  - export-to
    - vpn-list VPN1
  - default-action accept
- apply-policy site-list Branches
- control-policy WAAS-EXTRANET in
Demo
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKRST-2514
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions