Global vision.
Local knowledge.

Cisco Connect Dubrovnik
Croatia • 28.03.2019
Cisco SD-WAN
Delivering Cisco Next Generation SD-WAN with Viptela

Vedran Franjić
System Engineer Sales
28.03.2019
Agenda

• Introduction
• SD-WAN architecture
• SD-WAN fabric
• Deployment options
• Use Cases
• Licensing
Introduction
The WAN Has Changed

Users → Branch → WAN → Data Center → Internet

Users, Devices, Things → Branch → WAN → Internet → Multi-Cloud → SaaS → Internet
Traditional and Legacy Architectures
Cannot Scale to Address Changing Needs

EXPENSIVE

POORLY INTEGRATED
Conflicting policies and configurations
Risk from accidental interactions and vulnerabilities

DIFFICULT TO SUPPORT
Device-by-device configurations
Complex management silos
Require slow truck rolls for changes

CONNECTIVITY-CENTRIC
Incomplete user experience
Not application-centric

INFLEXIBLE
Static network
SD-WAN Architecture
Cisco SD-WAN Architecture Overview

Orchestration = vBond

Management = vManage
(Multi-tenant or Dedicated)

Control Plane = vSmart
(Containers or VMs)

Data Plane = Edge
(vEdge, Cisco ISR/ASR/ENCS, Whitebox)

APIs

Orchestrator

PnP

vManage

vSmart

WAN Edge

Data Analytics

PnP APIs

vBond

vManage

vSmart

WAN Edge

Data Center

Campus

Branch

SOHO

Cloud
vBond is SD-WAN Orchestrator

- Orchestrates connectivity between management, control and data plane
- Serves as the first point of authentication
- Requires public IP Address, provides NAT-T
- All other components need to know the vBond IP or FQDN
- Authorizes all control connections (white-list model)
vManage is NMS for SD-WAN

- Single-tenant or Multitenant
- Single pane of glass for Day 0, Day 1 and Day 2 operations
- Enables centralized provisioning and simplifies changes
- Supports REST API, CLI, Syslog, SNMP, NETCONF
- Provides real time alerting
- Role Based Access Control
vSmart is Centralized Control Plane

- Implements control plane policies, such as service chaining, traffic engineering and per-VPN topology
- Reduces complexity of the entire network
- Establishes peering with all WAN Edges, distributes connectivity and security context
WAN Edge is your SD-WAN Data Plane

- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with vSmart controllers
- Implements data plane and application aware routing policies
- Exports performance statistics
- Physical or Virtual form factor
Operations
Simplicity and Visibility

vManage

Single Pane Of Glass Operations

- Cloud-first management and orchestration
- Zero-touch provisioning

vAnalytics

Rich Analytics

- Troubleshooting with simplified workflows
- Advanced analytics and assurance
SD-WAN Fabric
Unified Control Plane

- Overlay Management Protocol (OMP)
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
- Dramatically lowers control plane complexity and raises overall solution scale

Note: WAN Edge routers need not connect to all vSmart Controllers

SD-WAN vs. Traditional:

- SD-WAN: O(n) Control Complexity
- Traditional: O(n^2) Control Complexity
Data Plane Establishment

SD-WAN fabric between tunnel endpoints
- IPsec
- IPsec
- IPsec

vSmarts advertise routes and encryption keys to WAN Edges in OMP updates.

Routes and encryption keys are advertised to vSmarts in OMP updates.

Local Routes
- Local prefixes (OSPF/BGP)
- SD-WAN tunnel endpoints (TLOCs)

Security Context
- IPSec Encryption Keys

Fabric Routing:
<prefix> via
- Transport Locator (TLOC)
- OMP
- IPSec Tunnel
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 WAN Edge routers in the topology
  - Inside SD-WAN tunnels
  - Across all transports
  - Operates in echo mode
  - Automatically invoked at SD-WAN tunnel establishment
  - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
  - Fully customizable per-WAN Edge, per-transport
Common Data Plane Communication

- **Per-Session Load Sharing**
  - Active/Active
  - Default

- **Per-Session Weighted**
  - Active/Active
  - Device Configurable

- **Application Pinning**
  - Active/Standby
  - Policy Enforced

- **Application Aware Routing**
  - SLA Compliant
  - Policy Enforced
**SD-AVC**

- **vManage**
- **SD-AVC Controller**:
  - Application Signatures updates
  - Connectors to external service (O365)
  - Custom-app definition

---

**Diagram**

- **Office 365**
- **SD-AVC**
- **vManage**
- **NBAR2 Agent**
- **cEdge**
- **Microsoft Azure**
  - Learn O365 IP Networks
  - SD-AVC Controller
  - vManage
  - Cloud onRamp for SaaS
  - First-packet match O365
  - First-packet steer O365
  - Distribute O365 IP Networks
  - Branch
Deployment options
Controllers’ Deployment Models

Cisco Cloud Ops
- vManage
- vSmart
- vBond
- Cisco Cloud

MSP Ops Team
- vManage
- vSmart
- vBond
- MSP Cloud

Enterprise IT
- vManage
- vSmart
- vBond
- Private Cloud
Deploying Controllers – Options

On-Premise/SP Hosted

- vBond
- vManage
- vSmart
- vSmart

ESXi or KVM

Physical Server

VM

Container

Cloud Hosted

- vBond
- vManage
- vSmart
- vSmart

AWS or Azure

VM

Container
Controller Scale

**vManage:**
- Validated Scale: 2,000 Devices per-single instance
- Max Production Deployment: 6 vManage instances in a cluster

**vSmart:**
- Validated Scale: 5,400 Connections per-single vSmart
- Max Production Deployment: 20 vSmarts

**vBond:**
- Validated Scale: 1,500 Connections per-single vBond
- Max Production Deployment: 6 vBonds
SD-WAN Transition Strategy
High Availability and Redundancy

Site Redundancy

- VRRP
- OSPF/BGP

Transport Redundancy

- MPLS
- INET

Network/Headend Redundancy

- Data Center
- MPLS
- INET

Control Redundancy

- vSmart Controllers
- Control
- Data
- MPLS
- INET
Cisco SD-WAN Platform Options

**SD-WAN with Services**
- **ISR 1000**: Next-gen Performance Flexibility
- **ISR 4000**: Modular Integrated services
- **ASR 1000**: High-performance with redundancy

**Pureplay SD-WAN**
- **vEdge 100**: 100 Mbps
  - 4G LTE & WiFi
- **vEdge 1000**: 1 Gbps
  - Fixed
- **vEdge 2000**: 10 Gbps
  - Modular
- **vEdge 5000**: 20+ Gbps, Modular

**Virtualization**
- **ENCS 5100**
- **ENCS 5400**

**Public and Private Clouds**
- Amazon Web Services
- KVM
- VMware
- Microsoft Azure
Use Cases
Common Enterprise Deployment Use Cases

- Critical Application SLA
- MultiCloud onRamp for IaaS and SaaS
- SD-WAN Security
- Zero Touch Provisioning
- Regional Deployment
Critical Applications SLA

Application Aware Routing

Forward Error Correction (FEC)

- Protects against packet loss
- Protocol (TCP/UDP) agnostic
- Supports multiple transports
- Can be invoked dynamically

Packet Duplication

- Protects against packet loss
- Protocol (TCP/UDP) agnostic
- Operates over multiple transports

SD-WAN Tunnel

FEC Header
MultiCloud onRamp for IaaS

Using Marketplace (DIY)

- Compute VPC/VNET
- SD-WAN Fabric
- Cloud Data Center
- Branch
- Campus

Fully Automated

- Compute VPCs/VNETs
- Gateway
- VPC/VNET
- Cloud Data Center
- Branch
- Campus

Remote Site
MultiCloud onRamp for SaaS
Secure Branch – Firewall

Unified Access Security

Branch/Campus

SD-WAN and APP Firewall/IPS/URL Filtering

Cisco Umbrella

Secure Internet GW

Data Center/Private Cloud

Internet/SaaS

IaaS
Secure Segmentation

- Security Zoning
- Compliance
- Guest Wi-Fi
- Multi-Tenancy
- Extranet

SD-WAN IPSec Tunnel

WAN Edge

VPN 1
VPN 2
VPN 3

WAN Edge

Per-VPN Topology

Full-Mesh
Hub-and-Spoke
Partial Mesh
Point-to-Point
Branch – SD-WAN Security

vManage

Use case: Cloud and DIA
- Firewall
- DNS/web layer security
- IPS

Use Case: Industry Compliance
- Firewall
- IPS

Use Case: Guest Services
- Firewall
- URL Filtering

AMP in 2019

Cloud Applications

Direct Cloud Access

SD-WAN

Data Center Applications

VPN1

Employee

VPN2

Guest
Assumption:
- DHCP on Transport Side (WAN)
- DNS to resolve devicehelper.cisco.com*

* Factory default config
Regional deployment

- **Split**: Full/Partial mesh
- **Zagreb**: Hub and spoke
- **Osijek**: Full/Partial mesh
Licensing
Cisco DNA Premier

Cisco DNA Advantage

Cisco DNA Essentials

1. Identify license tier
2. Select bandwidth
3. Pick license term
4. Choose on premises or cloud managed
5. Determine platform for future scale
Delivering Cisco Next Generation SD-WAN with Viptela