Využití technologie Cisco SD-WAN pro budování moderních pobočkových sítí

Miroslav Brzek
Previously, Connecting Users to Data Center was the Priority
Today, things have changed completely
Cisco SD-WAN Architecture
Flexible yet simple at Cloud-scale

Management & Analytics
On-premise | Cloud | Multi-tenant
Automation | Network Insights | Machine Learning | AI
Open | Programmable | Scalable

Any Deployment

Any Service
Branch Security | Cloud Security | Application Quality of Experience | Voice and Collaboration | Optimization for SaaS/IaaS

Any Transport
Satellite | Internet | MPLS | 5G/LTE

Any Location
Branch | Colocation | Cloud | AWS
Introducing Cisco Secure Cloud-Scale SD-WAN
Differentiated Innovations

Summary of Basic SD-WAN Capabilities*
- Circuit Load Balancing
- Direct Internet Access
- Centralized Management & Orchestration
- Circuit Cost Savings

Cisco SD-WAN extended capabilities
- Multi-layered Security
  - Branch Security & Segmentation
  - Cloud Security
- Application Optimization
  - Voice Optimization
  - SaaS/IaaS Optimization
  - App Aware Dynamic Routing
- Enterprise Grade
  - Open and Programmable
  - Multi-Domain IBN Policy
  - Analytics & Visibility

*Gartner Critical Capabilities for WAN Edge Infrastructure, December 2020
Cisco SD-WAN Interconnects Multi-Domain Networks

- Users (Consumers)
- Applications (Providers)

End-to-end Experiences
- Automation and Policy
- Telemetry, Analytics and Assurance
- Security and Segmentation
- Normalized APIs

Vertically Integrated Solutions

Pervasive Security

API Integration
- Cisco DNA Center
- vManage
- APIC

SD-Access
SD-WAN
ACI
Business Value of Cisco SD-WAN

- 38% Lower five-year cost of WAN operations
- 58% Faster to implement policy/configuration changes
- 94% Less unplanned downtime

Full IDC report available on www.cisco.com/go/sdwan
Cisco SD-WAN solution overview
Cisco SD-WAN Solution Overview
Applying SDN Principles To The Wide Area Network

- Orchestration Plane
- Management Plane (Multi-tenant or Dedicated)
- Control Plane (Containers or VMs)
- Data Plane (Physical or Virtual)

Orchestration Plane
Management Plane (Multi-tenant or Dedicated)
Control Plane (Containers or VMs)
Data Plane (Physical or Virtual)

© 2020 Cisco and/or its affiliates. All rights reserved.
Orchestration Plane
vBond Orchestrator

- Orchestrates control and management plane
- First point of authentication
- Distributes list of vSmarts/vManage to all SD-WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address [could sit behind 1:1 NAT]
- Highly resilient
- Multitenant or single tenant
Management Plane

vManage

Main Characteristics

- Single pane of glass for Day0, Day1 and Day2 operations
- Centralized provisioning
- Multitenant or single tenant
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC
- Programmatic interfaces (REST, NETCONF)
- Highly resilient
Control Plane

vSmart Controller

- Facilitates fabric discovery
- Disseminates control plane information between vEdges
- Distributes data plane and app-aware routing policies to the SD-WAN Edge routers
- Implements control plane policies
- Dramatically reduces control plane complexity
- Highly resilient
Data Plane
SD-WAN Edge Router

Main Characteristics

- WAN edge router
- Provides secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP and VRRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb, 20Gb+)
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

© 2020 Cisco and/or its affiliates. All rights reserved.
Cisco SD-WAN: Zero Trust Architecture

WAN Edge and Controllers White-List

Certificate Based Mutual Trust

Signed WAN Edge List
Administrator Defined Controllers
### SD-WAN Edge Portfolio with Cisco XE SD-WAN

#### Branch

<table>
<thead>
<tr>
<th>Model</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR 1000</td>
<td>• Integrated wired and wireless access&lt;br&gt;• LTE Advanced Pro&lt;br&gt;• VDSL2,ADSL2/2+</td>
</tr>
<tr>
<td>ISR120 / 1160</td>
<td>• Smallest form-factor&lt;br&gt;• WWAN pluggable flexibility&lt;br&gt;• PiM: 4G LTE CAT4/6/18</td>
</tr>
<tr>
<td>ISR 4000</td>
<td>• WAN and voice module flexibility&lt;br&gt;• Compute with UCS E&lt;br&gt;• Container Architecture&lt;br&gt;• Slot Modularity, RPS&lt;br&gt;• 1GE, 10GE options</td>
</tr>
<tr>
<td>ASR 1000</td>
<td>• High-performance service with hardware assist&lt;br&gt;• Modular ASR 1K is not supported</td>
</tr>
</tbody>
</table>

#### Aggregation

<table>
<thead>
<tr>
<th>Model</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 1000</td>
<td>• High-performance service with hardware assist&lt;br&gt;• Modular ASR 1K is not supported</td>
</tr>
</tbody>
</table>

#### Viptela OS

<table>
<thead>
<tr>
<th>Model</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR1100-4G</td>
<td>• 4 GE WAN ports</td>
</tr>
<tr>
<td>ISR1100-4LTE</td>
<td>• 4G LTE (CAT4)</td>
</tr>
<tr>
<td>ISR1100-6G</td>
<td>• 6 WAN ports (4GE and 2 SFP)</td>
</tr>
<tr>
<td>vEdge 2000</td>
<td>• RPS, PiM options</td>
</tr>
<tr>
<td>vEdge5000</td>
<td>• Modularity, RPS</td>
</tr>
</tbody>
</table>

#### Virtualized

<table>
<thead>
<tr>
<th>Model</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>vEdge Cloud</td>
<td>• Software Router Platform&lt;br&gt;• Can be deployed in private, public, and hybrid cloud</td>
</tr>
<tr>
<td>Cisco ENCS</td>
<td>• Service chaining virtual functions&lt;br&gt;• Options for WAN connectivity&lt;br&gt;• Open for 3rd party services &amp; apps&lt;br&gt;• NFVIS Hypervisor</td>
</tr>
<tr>
<td>CSR 1000V</td>
<td>• Extend Enterprise routing, security &amp; management to Cloud&lt;br&gt;• Cisco DNA virtualization</td>
</tr>
</tbody>
</table>

© 2020 Cisco and/or its affiliates. All rights reserved.
Cisco SD-WAN Licensing Model

The Cisco SD-WAN licensing model consists of two components

1. Subscription license (3YR and 5YR) for software charged per SDWAN Edge router. This cost is dependent on two factors:
   - Service bandwidth
   - Features

2. Perpetual cost of SDWAN Edge router.
## Cisco DNA SD-WAN Licensing
### Capability Based Packaging

<table>
<thead>
<tr>
<th><strong>Cisco DNA Essentials</strong></th>
<th><strong>Cisco DNA Advantage</strong></th>
<th><strong>Cisco DNA Premier</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplified management &amp; security protection for the cost-conscious customer</td>
<td>Advanced SD-WAN with enhanced security for feature-rich &amp; valued branch deployment models</td>
<td>Advanced SD-WAN security will mitigate the most sophisticated threats to your business</td>
</tr>
<tr>
<td>Enterprise firewall with Talos-powered IPS and app controls Cisco Umbrella DNS Monitoring</td>
<td>Cisco AMP with SSL proxy URL filtering Cisco Umbrella app discovery</td>
<td>Cisco Umbrella Insights® Cisco Threat Grid®</td>
</tr>
<tr>
<td>Application-based SLA Basic WAN &amp; path optimizations</td>
<td>Cloud OnRamp for IaaS, SaaS, and Colo AppQoE &amp; WAAS RTU</td>
<td></td>
</tr>
<tr>
<td>Single centralized management console in the cloud or on-prem</td>
<td>Integrated border plus orchestration for campus, branch &amp; DC</td>
<td></td>
</tr>
<tr>
<td>Forward Error Correction (FEC) Packet duplication</td>
<td>Integrated voice/UC gateways</td>
<td></td>
</tr>
<tr>
<td>Flexible topology &amp; dynamic routing (hub/spoke, partial/full mesh)</td>
<td>vAnalytics</td>
<td></td>
</tr>
<tr>
<td>Up to 50 Device Overlay</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 Cisco and/or its affiliates. All rights reserved.
Cisco SD-WAN Fabric
**Overlay Management Protocol (OMP)**

**Unified Control Plane**

- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
  - Inside authenticated TLS/DTLS connections
- Advertises control plane context and policies
  - Reachability – IP Subnets
  - Security – Encryption Keys
  - Policy – Data/App-route Policies
- Dramatically lowers control plane complexity and raises overall solution scale

**Note:** SDWAN Edge routers need not connect to all vSmart Controllers

---

**SD-WAN**

- O(n) Control Complexity

**Traditional**

- O(n^2) Control Complexity
OMP Update:
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies

Data Plane Establishment

vSmart

OMP Update

Policies

OMP Update

VPN1

VPN2

A

B

C

D

BGP, OSPF, Connected, Static

SDWAN Edge

BGP, OSPF, Connected, Static

Subnets

Transport1

TLOCs

Transport2

TLOCs

BFD

DTLS/TLS Tunnel

IPSec Tunnel

OMP

© 2020 Cisco and/or its affiliates. All rights reserved.
Each Edge advertises its local IPsec encryption keys
- Encryption key is per-transport
- Keys are rotated frequently through OMP

Symmetric encryption keys used asymmetrically

- Traffic Encrypted with Keys 1' / 2'
- Traffic Encrypted with Keys 1 / 2
End-to-End Secure Segmentation

- Segment connectivity across fabric w/o reliance on underlay transport
- Edge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup
- Interfaces and sub-interfaces (802.1Q tags) or a mix of both are mapped into VPNs
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 SDWAN Edge 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-WAN Edge, per-color
Common Data Plane Communication

Per-Session Load Sharing
Active/Active

Per-Session Weighted
Active/Active

Application Pinning
Active/Standby

Application Aware Routing
SLA Compliant

Default
Device Configurable
Policy Enforced
Policy Enforced
Common Enterprise Deployment Use Cases
Common Enterprise SD-WAN Deployment Use Cases

- Centralized configuration management and application visibility
- Critical Application SLA
- Secure Branch
- MultiCloud onRamp for SaaS and IaaS
Centralized configuration management and application visibility

vManage

- Intuitive GUI driven operations - Management, monitoring and troubleshooting
- Cloud Delivered - Private, hosted or managed
- Single or Multi-tenant
- Role-based Access Control
- Clustered for scale and high availability
- REST APIs based
Centralized Device Configuration Enforcement

Building the template
Application and Flow Visibility

- Application and flow visibility for each WAN Edge router
  - DPI/NBAR2 need to be enabled for application visibility
  - Flow data can be exported from WAN Edge to external collector

- Realtime views or custom timeline views granularity

- Views can be zoomed into
Visualizing Application Paths
Checking Transport Quality
Troubleshooting

• Basic connectivity troubleshooting with ping and traceroute from any vEdge in the topology to any destination

• Advance troubleshooting with real-time queries against vEdge routers

• Expert troubleshooting with full featured CLI and Linux bash shell

• Traffic analysis with synthetic traffic generation to test policies
Common Enterprise SD-WAN Deployment Use Cases

- Centralized configuration management and application visibility
- Critical Application SLA
- Secure Branch
- MultiCloud onRamp for SaaS and IaaS
Critical Applications SLA

- WAN Edge Routers continuously perform path liveliness and quality measurements.

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

**Paths**
- **Path 1**: 10ms, 0% loss, 5ms jitter
- **Path 2**: 200ms, 3% loss, 10ms jitter
- **Path 3**: 140ms, 1% loss, 10ms jitter
Common Enterprise SD-WAN Deployment Use Cases

- Centralized configuration management and application visibility
- Critical Application SLA
- Secure Branch
- MultiCloud onRamp for SaaS and IaaS
Secure Branch - Segmentation

[Diagram showing network segmentation with SD-WAN, VPNs, and VPCs for Finance, HR, and UC]
Secure Branch – Segmentation

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

Per-VPN Topology

Full-Mesh

Hub-and-Spoke

Partial Mesh

Point-to-Point
Secure Branch – SD-WAN Security

Use Case:
Direct Internet Access
- Firewall
- IPS
- AMP+TG
- URL Filtering
- Cisco Umbrella

Use Case:
Guest Services
- Firewall
- URL Filtering

Use Case:
Industry Compliance
- Firewall
- IPS
- AMP+TG

Internet
- Applications

Direct Internet Access

SD-WAN

Data Center
- Applications

vManage

Internet
- Applications

Employees

Contractors

Guests

VPN1

VPN2

VPN3
Common Enterprise SD-WAN Deployment Use Cases

- Centralized configuration management and application visibility
- Critical Application SLA
- Secure Branch
- MultiCloud onRamp for SaaS and IaaS
Traditional Cloud Applications Access

- Data Center backhaul
- Increased application latency
- Unpredictable user experience

![Diagram showing data flow from users to remote site, through wide area network, to data center and SDWAN edge router.](image)
Cloud onRamp for SaaS
Direct Internet Access and Gateways

- One of the recommended designs, for SaaS deployments
- Cloud On-ramp continuously monitors the edge to SaaS performance on both DIA path and the back-haul path
- SDWAN Edge router picks the best performing path based on the performance metrics (loss & delay)
  - Per-Application, Per-VPN
- Automatic failover in case of performance degradation
- Fully automated

© 2020 Cisco and/or its affiliates. All rights reserved.
SaaS applications & vQoE scores

• The vQoE value ranges from 0 to 10, with 0 being the worst quality and 10 being the best.

• vQoE = desired metrics / actual metrics * 10

• vQoE score is computed for each remote site application and per path

<table>
<thead>
<tr>
<th>SaaS Application</th>
<th>Path 1 - vQoE on ISP1 DIA</th>
<th>Path 2 - vQoE on Gateway 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>O365</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Sales force</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Box</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Dropbox</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Google Apps</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>Goto Meeting</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Intuit</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Oracle</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>SugarCRM</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>ZenDesk</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Zoho CRM</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>
Traditional IaaS Access

- No Direct to Cloud access
- Limited segmentation and QoS
- Dependent on underlying technology
Cloud onRamp for IaaS
End-to-End SD-WAN

- SDWAN Edge cloud routers are instantiated in every VPC/VNET - Marketplace
- End-to-end SD-WAN fabric between sites and public cloud - Multipathing, QoS and segmentation
- Shortest-path to Public Cloud
Cisco SD-WAN Security
How SD-WAN exposes new security challenges

**Internal & External Threats**

**External**
- Exposure to malware & phishing due to direct internet and cloud access
- Data breaches
- Guest access liability

**Internal**
- Untrusted access (malicious insider)
- Compliance (PCI, HIPPA, GDPR)
- Lateral movements (breach propagation)
Benefits with integrated security everywhere

<table>
<thead>
<tr>
<th>PRO</th>
<th>CON</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONLY Cloud Security</td>
<td>Consistent user and device protection in all locations and scales on-demand</td>
</tr>
<tr>
<td>Lacks visibility and control over internal traffic and threats</td>
<td></td>
</tr>
<tr>
<td>ONLY On-Prem Security</td>
<td>Visibility into all traffic and protects against internal and external threats</td>
</tr>
<tr>
<td>Decrypting traffic for malware detection increases edge device footprint</td>
<td></td>
</tr>
<tr>
<td>On-Prem and Cloud Security</td>
<td>Best balance of security and user experience for direct internet access</td>
</tr>
<tr>
<td>Cisco integrated solution eliminates these cons</td>
<td></td>
</tr>
</tbody>
</table>
Combining Best of Breed in Security and SD-WAN

Cisco Security

- Enterprise Firewall
  +1400 layer 7 apps classified
- Intrusion Prevention System
  Most widely deployed IPS engine in the world
- URL-Filtering
  Web reputation score using 82+ web categories
- Adv. Malware Protection
  With File Reputation and Sandboxing (TG)
- Secure Internet Gateway
  DNS Security/Cloud FW with Cisco Umbrella

Cisco SD-WAN

Hours instead of weeks and months

© 2020 Cisco and/or its affiliates. All rights reserved.
Conclusion
Differentiators For Cisco Secure Cloud Scale SD-WAN

- **Multi-Layer Security**
  - Segmentation across the entire network stack
  - App FW, IPS, URL-Filtering; AMP and Secure Internet Gateway with Cisco Umbrella
  - Cisco Umbrella

- **Multi-Cloud Application Optimization**
  - Voice Optimization for Collab Applications
  - Multi-Cloud OnRamp for IaaS, SaaS and Colo
  - Office 365

- **Multi-Domain IBN**
  - End-to-End policy from Campus/Branch to DC/Cloud

One user interface across Branch, Cloud and Colocation