Cisco Secure WAN

Cisco SD-WAN: Enhancing Network Performance and Security

Ben Craig
Solutions Engineer
becraig@cisco.com

Agenda

- Solution Overview
- Application Experience
- Cloud On Ramp
- Security
- Unified SD-WAN
- Demo

cisco *Connect*

Solution Overview

cisco *Connect*

Cisco Catalyst SD-WAN is uniquely positioned to transform your WAN

Key focus areas for
Cisco Catalyst SD-WAN

Connect

Multicloud access
To connect a hybrid
workforce to
apps anywhere

Predictable
app experience

Secure

Secure SD-WAN
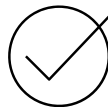To secure access
to apps and data
from everywhere

Right security,
right place

Automate and Observe

Analytics
To deliver end-to-end
visibility for
actionable insights

Always on,
easily available

CISCO Connect

Cisco Catalyst SD-WAN Architecture

Orchestration Plane

First point of authentication
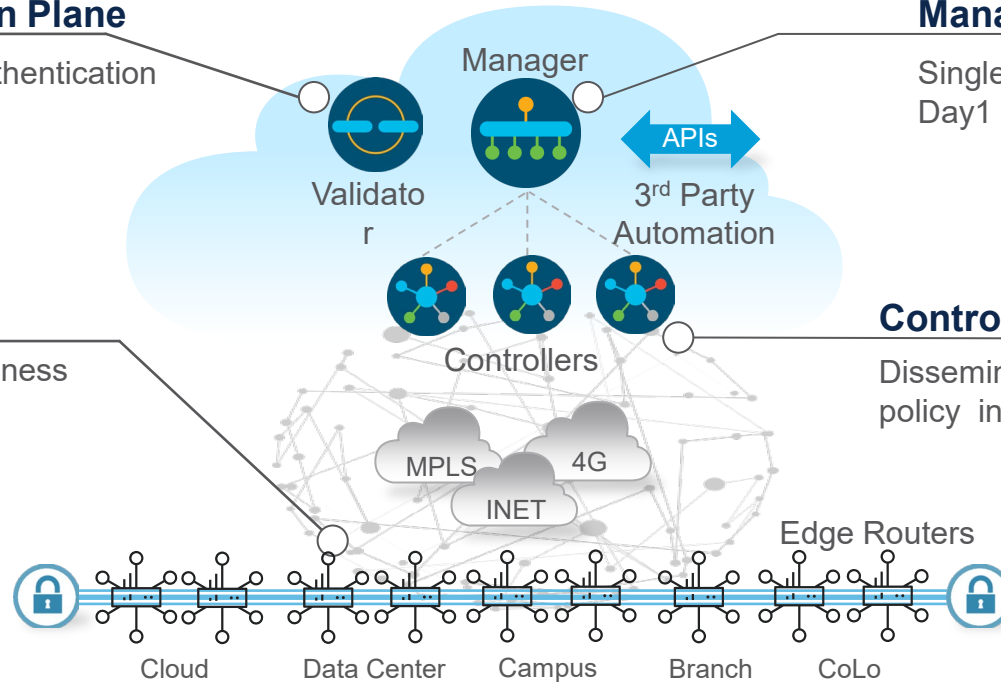
Management Plane

Single pane of glass for Day0, Day1 and Day2 operations

Data Plane

Implements business intent policies

Control Plane

Disseminates control plane and policy information between Edges

Manager

Validator

APIs

3rd Party Automation

Controllers

MPLS

4G

INET

Edge Routers

Cloud   Data Center   Campus   Branch   CoLo

Cisco Catalyst SD-WAN Fabric Deployment Models

Reduce operational burden of customers →

Customer Hosted

Customer Data Center

MSP Data Center

Cisco Hosted
(AWS & Azure)

Standard Environment
(Shared and Dedicated)

Certified Environment
(PCI, SOC2, ISO, C5, etc.)

Gov. Cloud
(FedRAMP)

Cloud-delivered

- Life Cycle Management of SD-WAN Fabric
- Agile and scalable service access
- Operational simplicity
- Rich analytics providing actionable insights

Flexible deployment models aligned to your business needs

cisco Connect

SD-WAN platforms for any deployment

Virtual

Cloud

Branch

Core

CSP 5000

ENCS 5000

SD-WAN and routing devices

Catalyst 8000 Edge platforms family

ASR 1000

Catalyst 8000V

Catalyst 8200 uCPE

ISR 1000

ISR 4000

Catalyst 8200, 8200L

Catalyst 8300

Catalyst 8500, 8500L

Hybrid / Remote

Catalyst Wireless Gateway CG113

Catalyst Cellular Gateway CG418-E, 522-E

Industrial IoT Edge
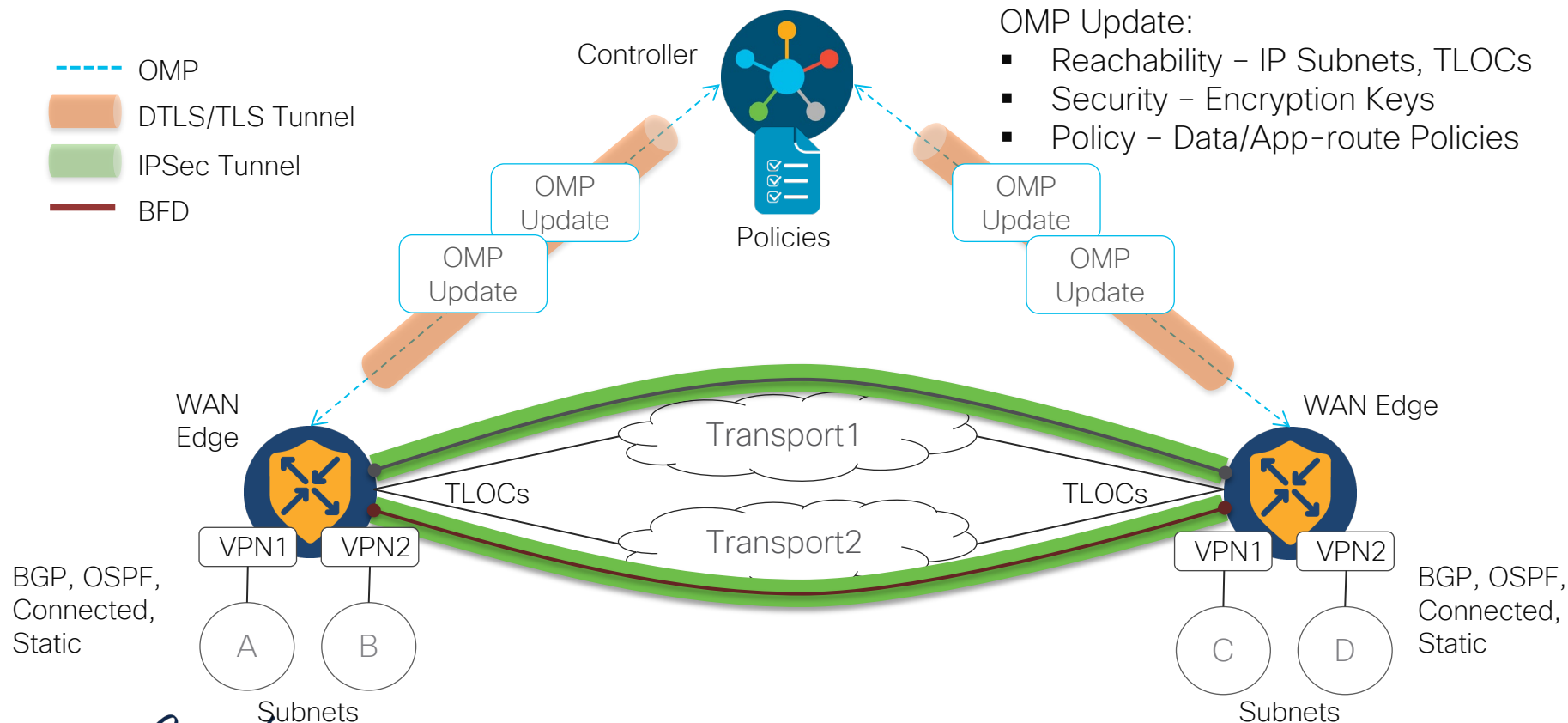
Catalyst IR1100
Catalyst IR1101

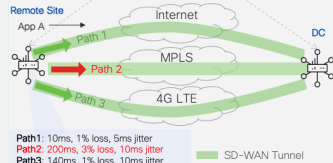Catalyst IR1800

Catalyst IR8100

Catalyst IR8300

CISCO Connect

#CiscoConnect

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Operation Walk-Through

OMP Update:
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies

OMP
DTLS/TLS Tunnel
IPSec Tunnel
BFD

Controller

OMP Update
OMP Update
OMP Update
OMP Update

Policies

WAN Edge
WAN Edge

Transport1
Transport2

TLOCs
TLOCs

VPN1 VPN2
VPN1 VPN2

BGP, OSPF, Connected, Static

BGP, OSPF, Connected, Static

A   B
C   D

Subnets
Subnets

Application Experience
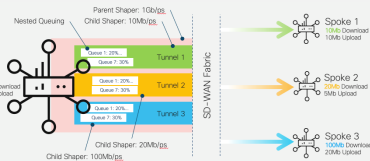
Application Experience

Application Aware routing

- Detects brownout conditions in overlay path.
- SLA based traffic steering
- Automatic failover to secondary path if primary path fails.

Remote Site
App A
Path 1
Internet
DC
MPLS
Path 2
Path 3
4G LTE

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

SD-WAN Tunnel

Packet Duplication

- Send duplicate packets over alternate path
- Mitigate packet loss for critical voice or video traffic
- Enhances Application quality of experience

110 110
1011 1011
010 010

110 110
1011 1011
010 010

Quality of Service (QOS)

- Manage and avoid network congestion
- Guaranteed Bandwidth
- Traffic queueing and shaping
- Prioritize critical application traffic over other traffic.

TCP optimization

- BBR2 Congestion control algorithm
- Window scaling
- Large Initial windows
- Selective acknowledgement
- Helps in reducing latency and increase throughput

Forward Error Correction

- Protects against packet loss
- Protocol agnostic (TCP/UDP)
- Enhances Application quality of experience
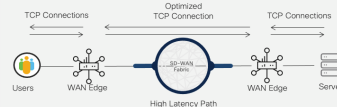
DRE, LZW

- Traffic optimization techniques
- Byte level caching & Data compression
- Protocol agnostic

DRE Signature Database

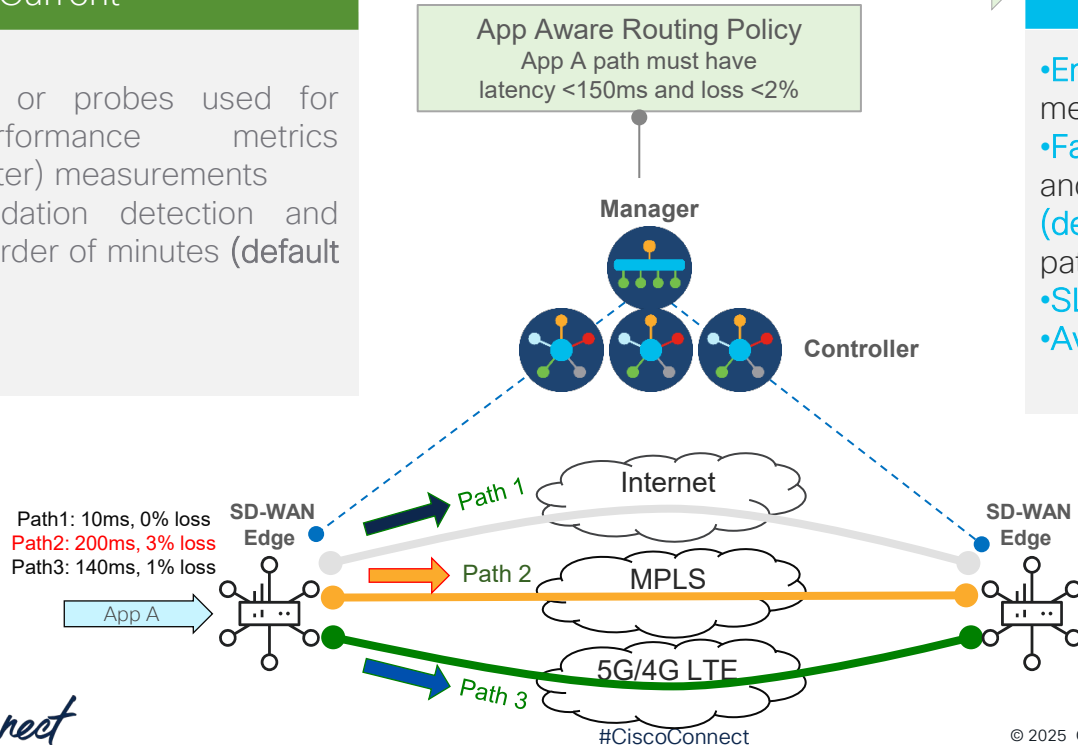# Enhanced Application-Aware Routing (EAAR)
Improved Application Performance Experience (from **mins to sec**)

Current

- BFD packets or probes used for tunnel performance metrics (loss/latency/jitter) measurements
- Tunnel degradation detection and failover in the order of minutes (default 10min)

App Aware Routing Policy
App A path must have latency <150ms and loss <2%
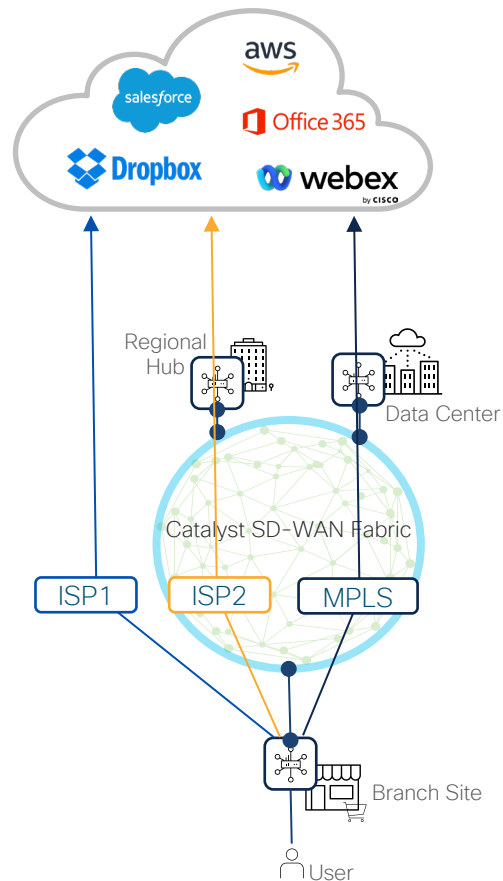
Manager

Controller

Improvements

- Enhanced tunnel performance metrics measurements by using inline data
- Faster tunnel degradation detection and switchover in the order of seconds (default minimum 10sec) to another path when SLA not met
- SLA Dampening
- Available from 20.12/17.12

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

App A

SD-WAN Edge

Path 1 — Internet

Path 2 — MPLS

Path 3 — 5G/4G LTE

SD-WAN Edge

#CiscoConnect

CISCO Connect
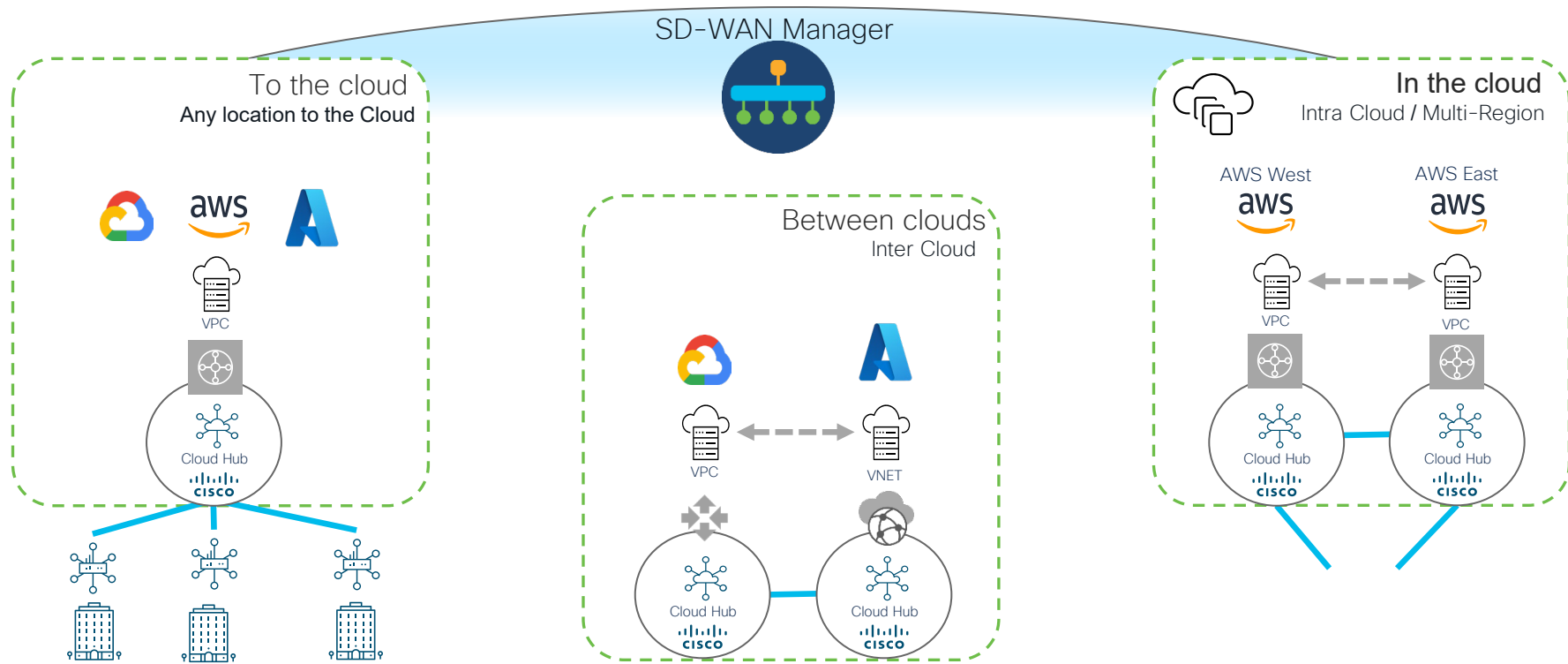
SaaS Optimization

The Challenges

- What path to use for SaaS app?
  - Direct Internet Access
  - Regional Breakout
  - Data Center Backhaul

- Which path is having better SLA for a given SaaS app, How to get performance visibility for each path?

- When specific path is having performance issues, How to automatically steer traffic ?

Cloud OnRamp

Cloud OnRamp for Multicloud

Legend: Cloud-Native Connections · SD-WAN Tunnel

SD-WAN Manager

To the cloud
Any location to the Cloud

In the cloud
Intra Cloud / Multi-Region

AWS West · AWS East

VPC · Cloud Hub · CISCO

Between clouds
Inter Cloud

VPC · VNET · Cloud Hub · CISCO

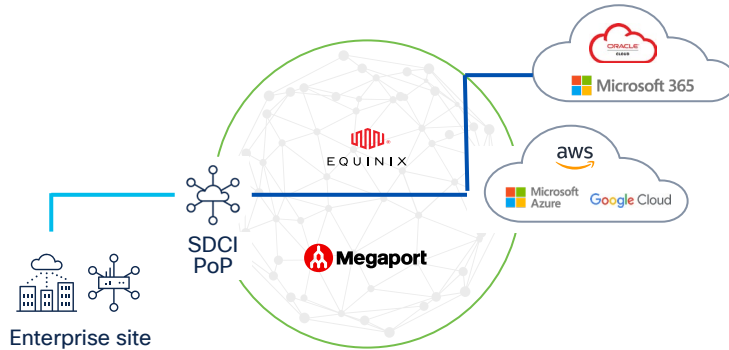| Automation	Ease of Management	Normalization	Security
Automate SD-WAN extension to the cloud	Single dashboard for SD-WAN and Cloud	Consistent UI and workflow for all cloud	Extend segmentation policy into the cloud

cisco Connect

Cloud Interconnect

= Cisco SD-WAN router hosted at Megaport or Equinix
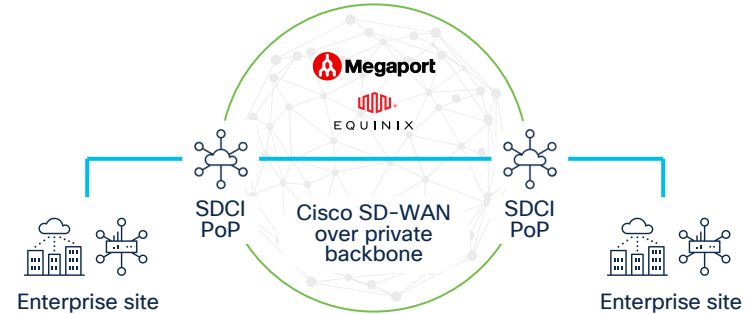
Site-to-Multicloud

ORACLE CLOUD

Microsoft 365

EQUINIX

aws

Microsoft Azure   Google Cloud

Megaport

SDCI PoP

Enterprise site

| Simple | Automated | Secure |

Site-to-site

Megaport

EQUINIX

SDCI PoP

Cisco SD-WAN over private backbone

SDCI PoP

Enterprise site

Enterprise site

| On-demand | High performance | Global connectivity |

Automated with SD-WAN Manager

Security

Flexible Deployment Options

SD-WAN w/ On-Prem Security

Internet / Private Application
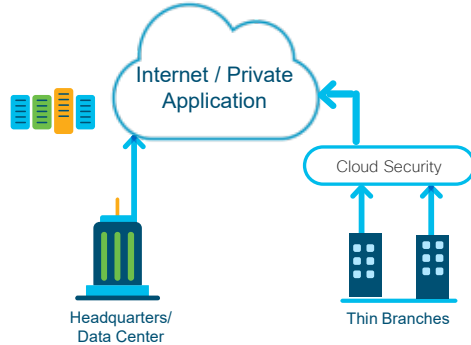
Headquarters/ Data Center

Branch Office
Integrated Security Enabled
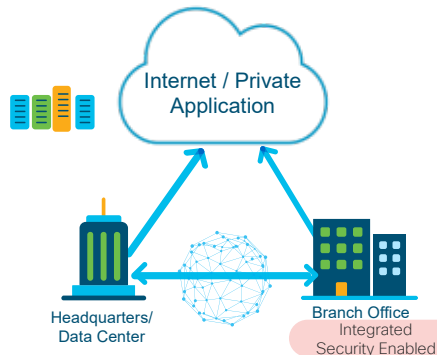
Integrated Security

SD-branch model
Thick branch with routing and security

SD-WAN w/ SSE Integration and Hybrid Security

Internet / Private Application

Cloud Security

Headquarters/ Data Center

Thin Branches

SD-WAN with SSE/SIG integration

Hybrid model
Thin branch with cloud security
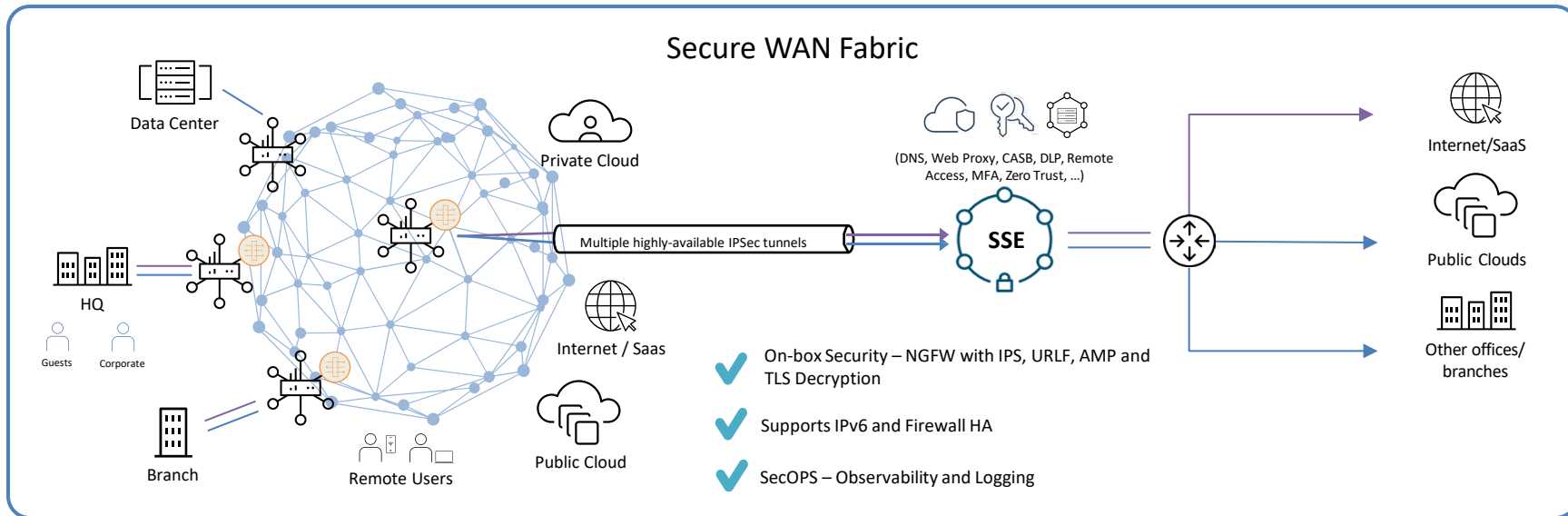Thick branch with routing and security

SD-WAN w/ Colo Security

Internet / Private Application

colocation

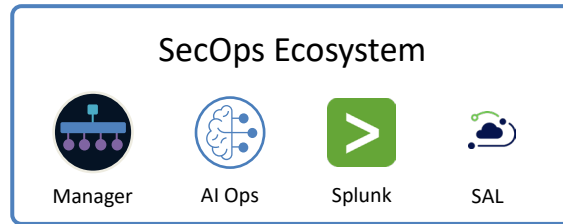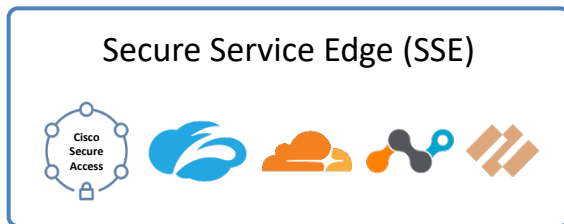Headquarters/ Data Center

Branch Office
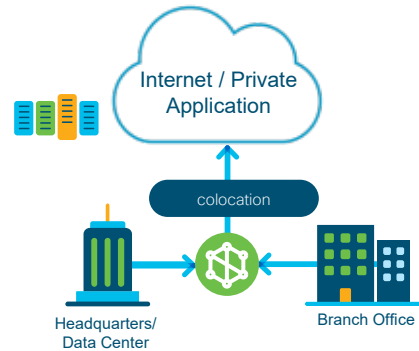
Service Insertion at Colo

SD-branch model
Thick branch with routing & Security Services as VNF at Regional Colocation Hub

Feature Richness with Operational simplicity

cisco Connect

#CiscoConnect

Cisco Secure WAN – Cloud Security

Policies
- Manager
- Controller
- ISE
- Security Cloud Control

Secure Service Edge (SSE)
Cisco Secure Access

SecOps Ecosystem
- Manager
- AI Ops
- Splunk
- SAL

Secure WAN Fabric

Data Center
Private Cloud
HQ
Guests
Corporate
Internet / Saas
Branch
Remote Users
Public Cloud

Multiple highly-available IPSec tunnels

(DNS, Web Proxy, CASB, DLP, Remote Access, MFA, Zero Trust, …)

SSE

Internet/SaaS
Public Clouds
Other offices/ branches

- On-box Security – NGFW with IPS, URLF, AMP and TLS Decryption
- Supports IPv6 and Firewall HA
- SecOPS – Observability and Logging

cisco Connect

Core Capabilities

SD-WAN Manager

Monitoring Ecosystem

Splunk

Next Generation Firewall

| L3 – L7 + Identity FW | IPS/IDPS | AMP | Sandboxing | URL-F | TLS Decryption |

+

SASE Ecosystem

| Auto Tunnel + HA | Traffic Steering | CASB | FWaaS | DLP | DNS/SWG |

#CiscoConnect

cisco Connect

Cisco Secure WAN – Granular End-to-End Segmentation

Macro Segmentation

SD-WAN Overlay
- VPN 1 (IT)
- VPN 2 (FIN)
- VPN 3 (Partner)
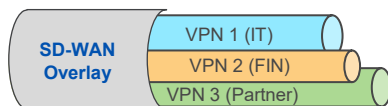
VPN Level Segmentation
- IT VPN
- Finance VPN
- Partner VPN

Micro Segmentation

SD-WAN Overlay

VPN1 (IT)
- Employee
- App Server
- Shared Resource
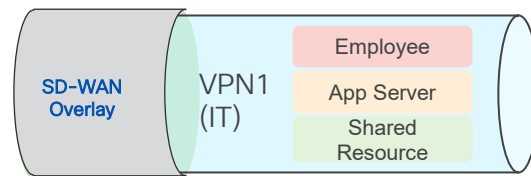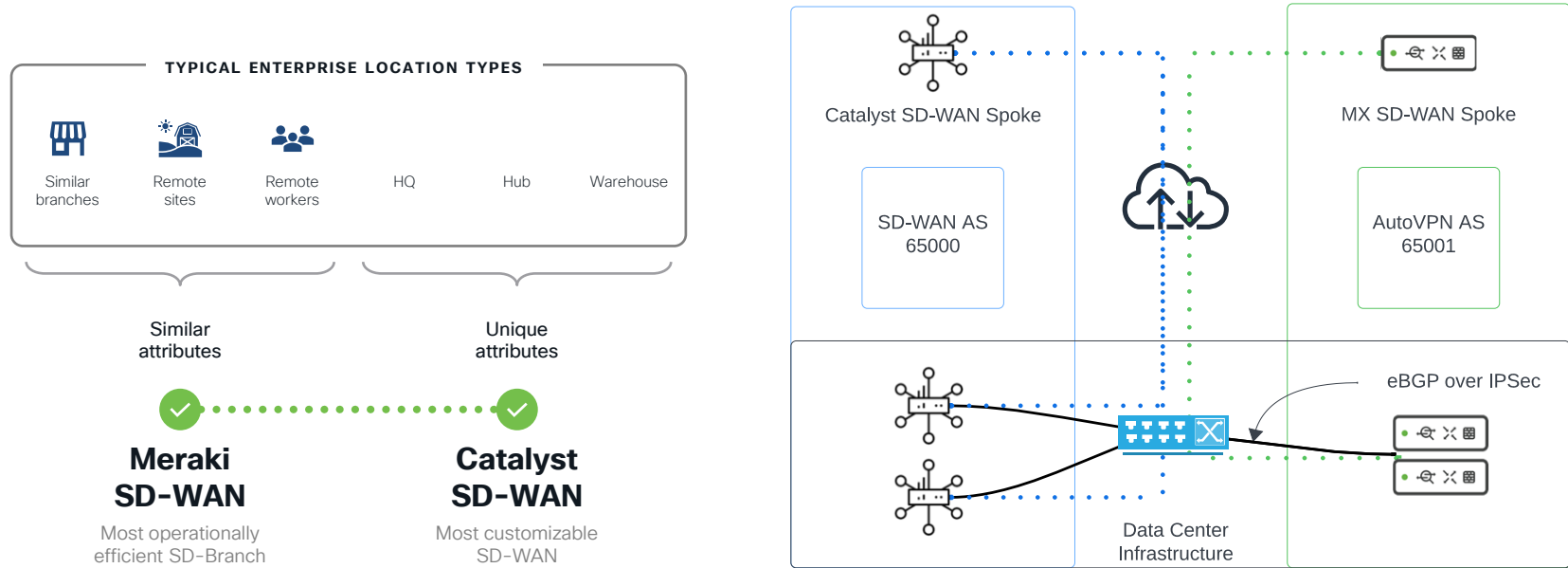
Group Level Segmentation
Example: IT VPN
- Employee
- App Servers
- Printers

Unified SD-WAN

Custom-fit SD-WAN for disparate location types

Natively interconnect Meraki and Catalyst SD-WAN

TYPICAL ENTERPRISE LOCATION TYPES

Similar branches | Remote sites | Remote workers | HQ | Hub | Warehouse

Similar attributes

Unique attributes

Meraki SD-WAN

Most operationally efficient SD-Branch

Catalyst SD-WAN

Most customizable SD-WAN

Catalyst SD-WAN Spoke

SD-WAN AS 65000

MX SD-WAN Spoke

AutoVPN AS 65001

eBGP over IPSec

Data Center Infrastructure

Choose the best-fit SD-WAN for every location and streamline management

Demo

Thank you