Possibilities

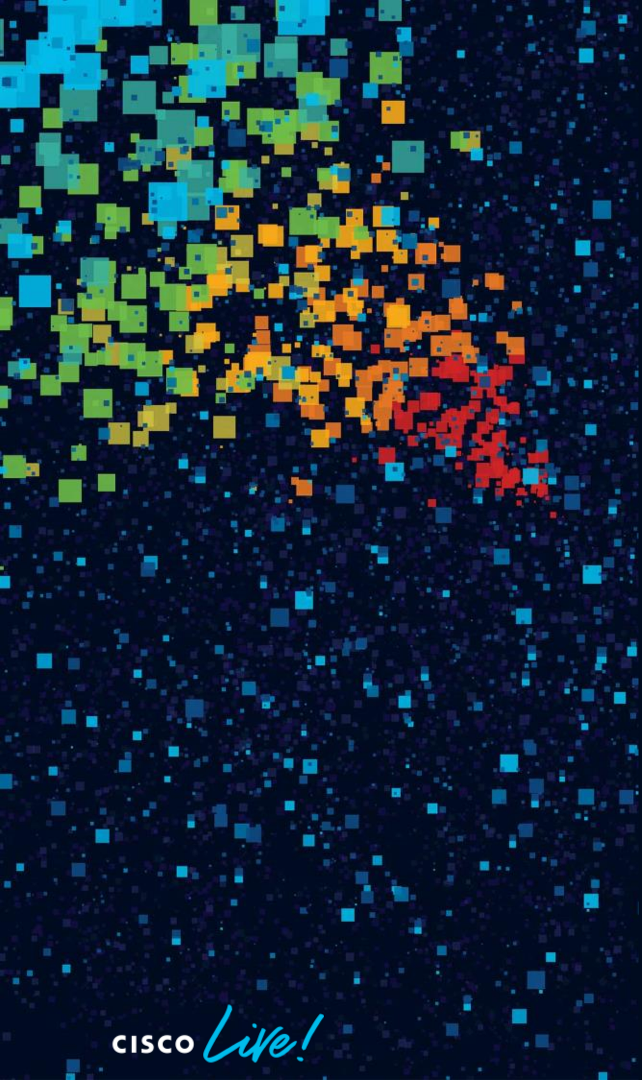
#CiscoLive

Outsmarting SD-WAN Threats

Securing the cloud edge with Intent-Based networking

Tom Kunath, Solutions Architect, CCIE 1679 @KNc11T

DGTL-PSOCX-2463



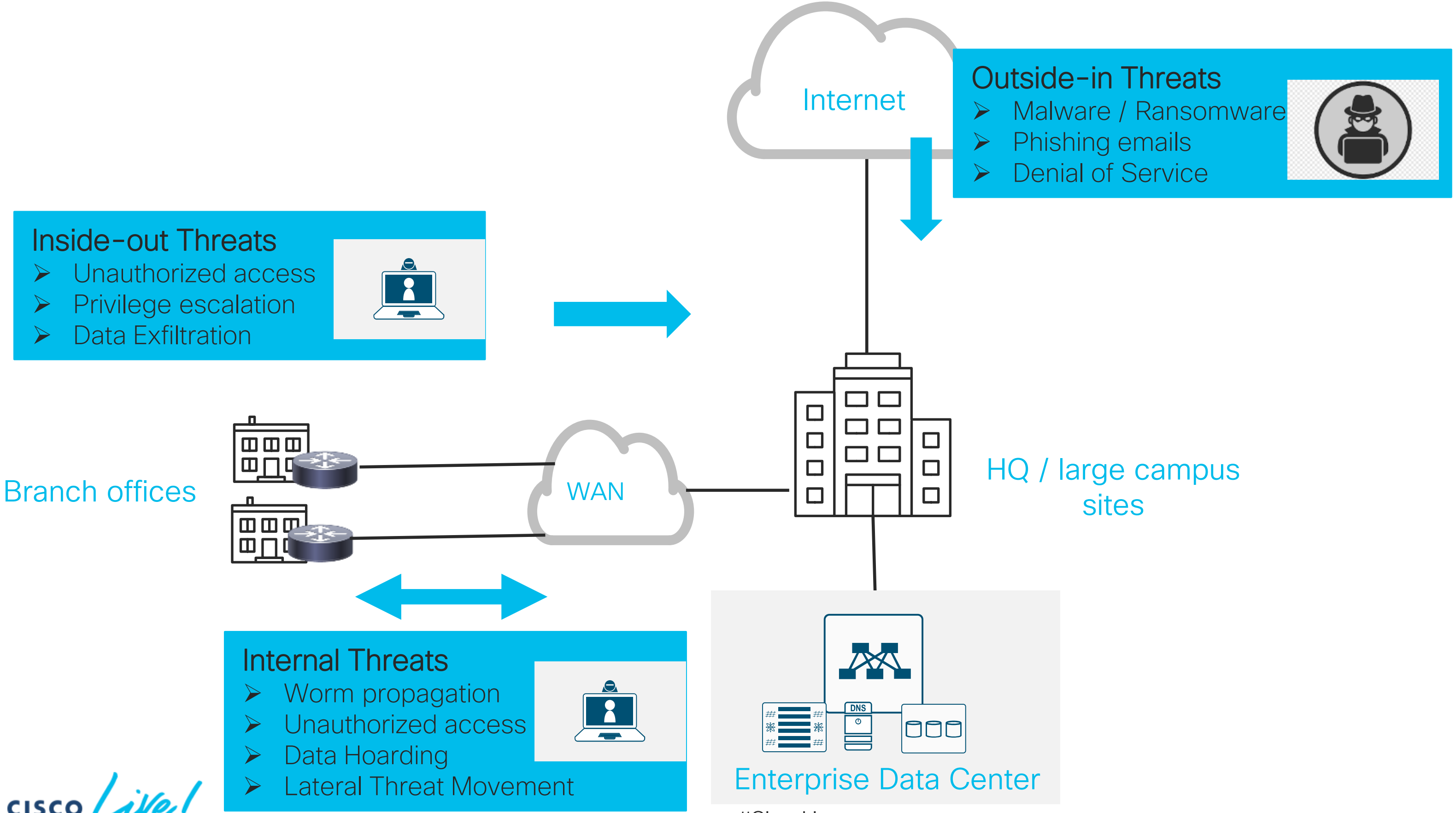
Agenda

- Introduction
- Evolution of the Enterprise WAN
- Integrating Security into SD-WAN design
- Demo
- Conclusion

Introduction

Cybersecurity threats to the enterprise WAN

Top 3 Threat Types



Outside-in Threats

- Malware / Ransomware
- Phishing emails
- Denial of Service

Inside-out Threats

- Unauthorized access
- Privilege escalation
- Data Exfiltration

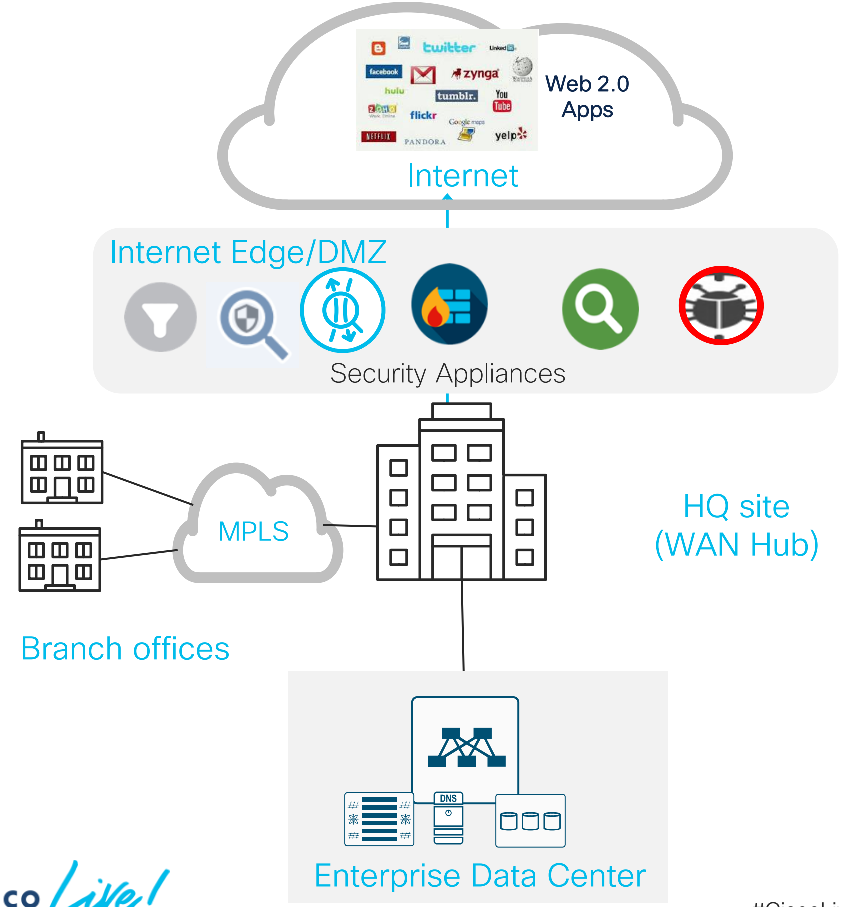
Internal Threats

- Worm propagation
- Unauthorized access
- Data Hoarding
- Lateral Threat Movement

Evolution of the Enterprise WAN

Classic WAN Design with Centralized DMZ

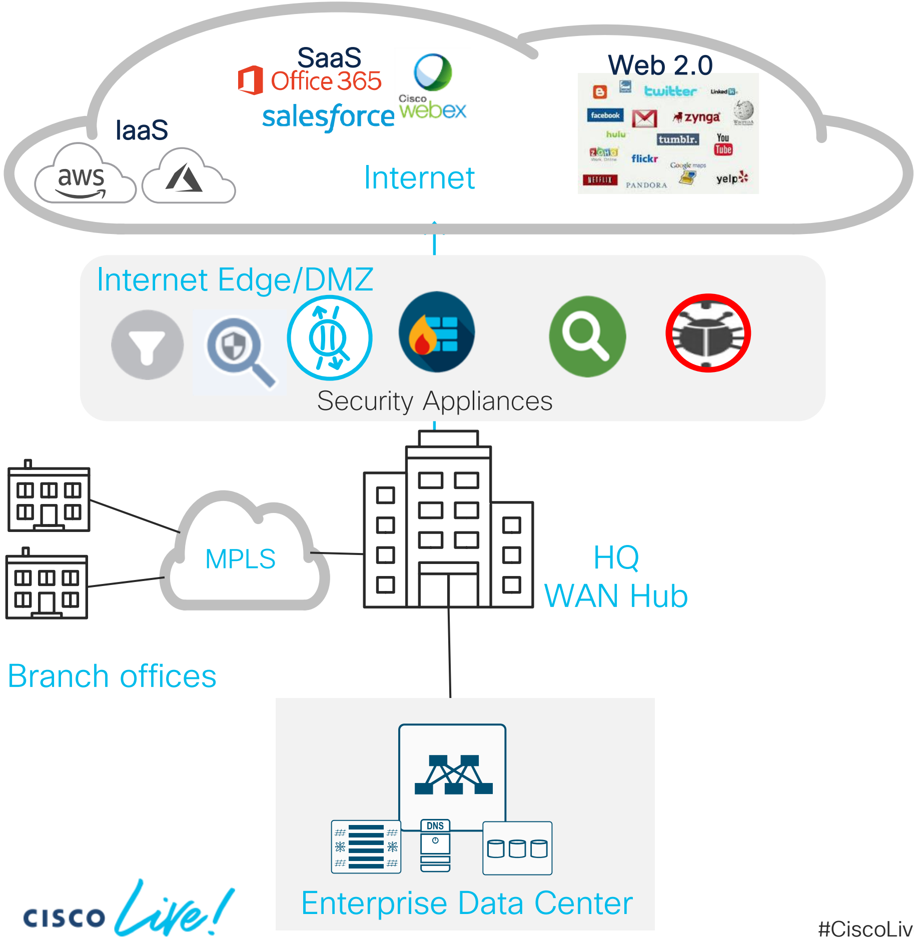
Internet backhaul through centralized Internet Edge Security Stack



- MPLS / IP VPN services ubiquitous and generally accepted as “secure” for site-to-site VPN
- Business critical applications hosted in Enterprise Data Center(s)
- Traditional design leverages centralized DMZ(s) as aggregation point for Internet access and edge security
  - FW, IPS, AMP, SWG, Analytics

Disruption: Enterprise Cloud Adoption

Business critical applications moving to SaaS/IaaS Cloud providers



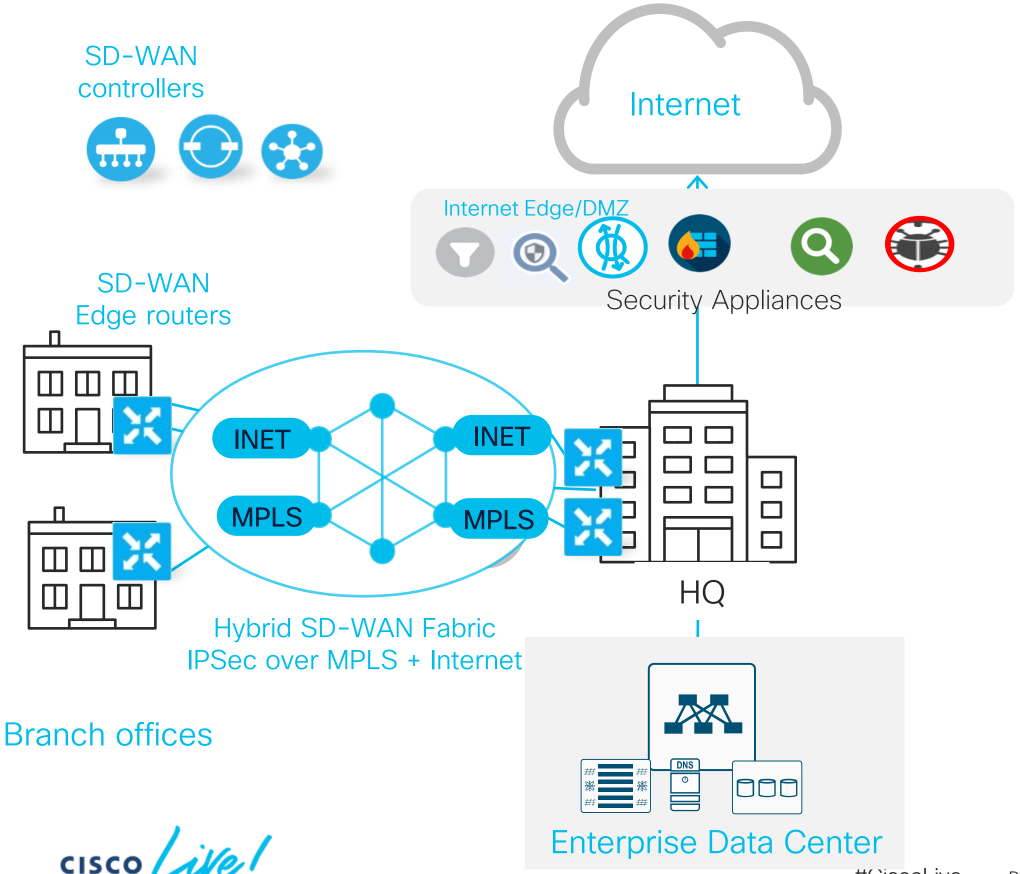
- Enterprises migrating apps from private DC to IaaS providers and transitioning to SaaS applications for common business functions

- Concerns with cloud app performance when backhauling cloud traffic through centralized DMZ
  - Congestion and latency

- Traditional security appliances not cloud centric

Disruption: Hybrid SD-WAN

Secure fabric overlay with MPLS + Internet as WAN transports

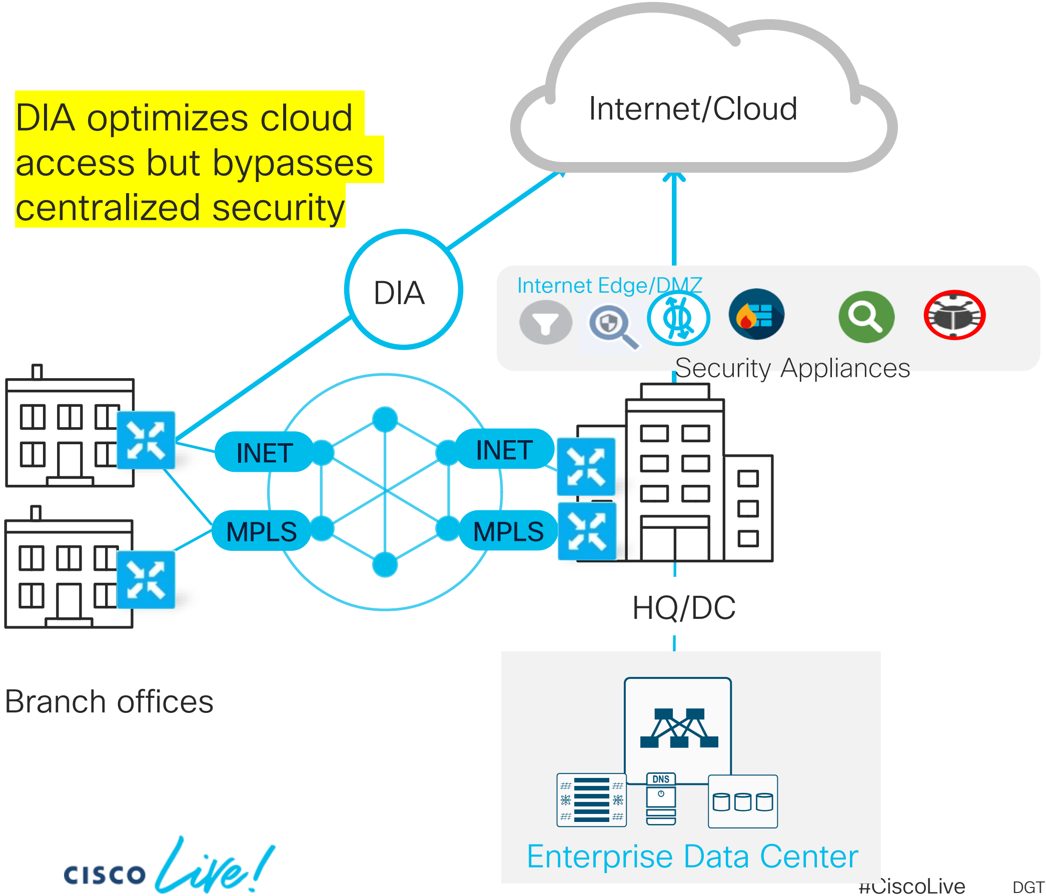


- Lowers WAN CAPEX and OPEX
- Robust edge-to-edge security with zero-trust model
- Business intent enforced with application visibility and path control
- Zero touch provisioning of WAN edge routers speeds deployments
- Single Pane of glass for configuration and management

SD-WAN with Direct Internet Access (DIA)

Optimizing branch access to Internet and Cloud

DIA optimizes cloud access but bypasses centralized security



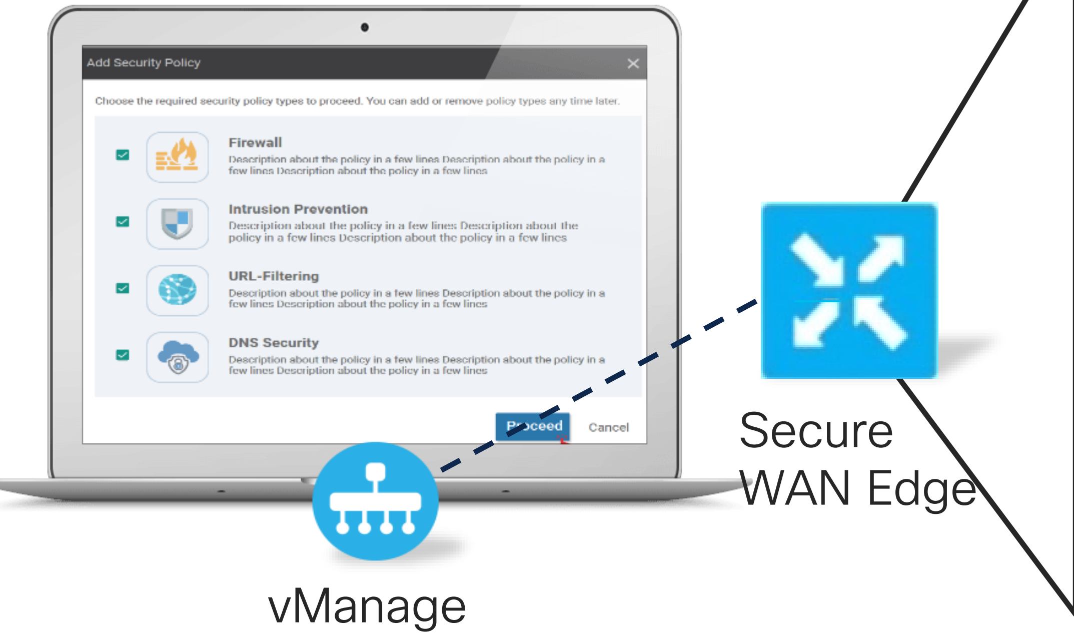
- Local Internet exit created at branch leveraging existing ISP circuit used for SD–WAN overlay
- Eliminates backhaul latency to Internet/Cloud and reduces traffic across WAN fabric
- Local DIA bypasses centralized security, opening branch to Internet threats

Integrating Security into Cisco SD-WAN design

An intent-based approach

Cisco SD-WAN edge security stack

Integrated on-prem and cloud security



Add Security Policy ✕

Choose the required security policy types to proceed. You can add or remove policy types any time later.

☑ **Firewall**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **Intrusion Prevention**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **URL-Filtering**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

☑ **DNS Security**
Description about the policy in a few lines Description about the policy in a few lines Description about the policy in a few lines

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)

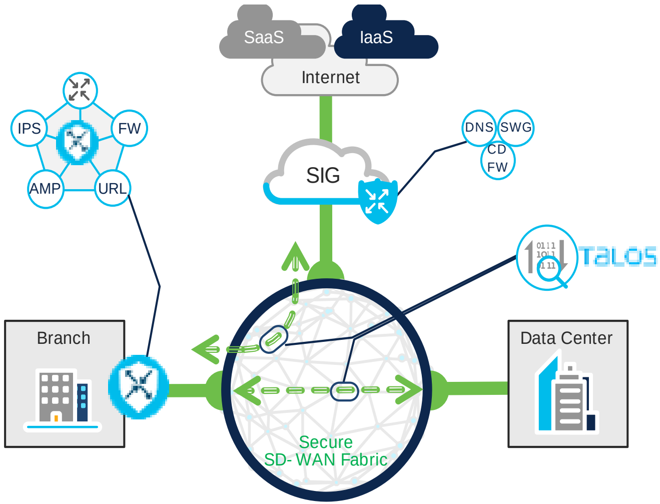
TLS/SSL Proxy
Threat Inspection for Encrypted Traffic

Secure Internet Gateway
DNS Security/Cloud FW with Cisco Umbrella

Intent based Networking deployments in hours vs weeks or months

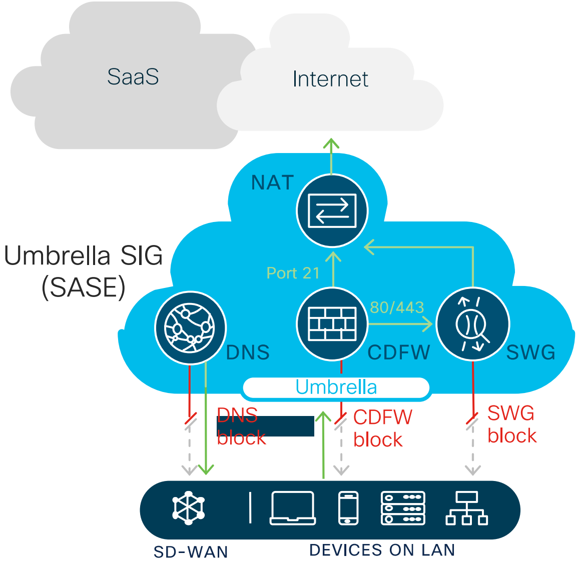
Cisco SD-WAN Security Delivery Options

Embedded Security



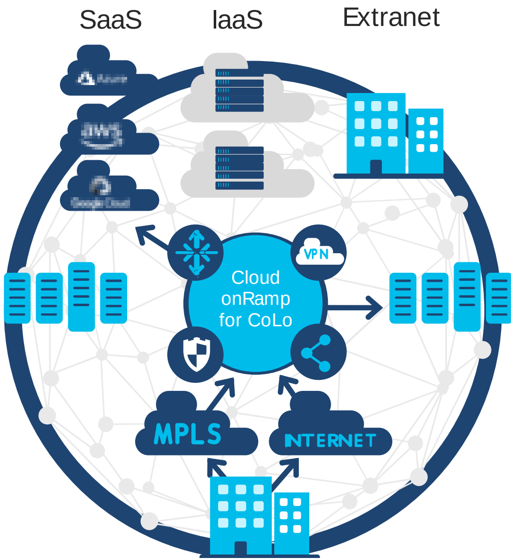
- ❖ Single Platform for Routing and Security

Cloud Security



- ❖ Lean Branch w/Security in the Cloud

Regional Colocation



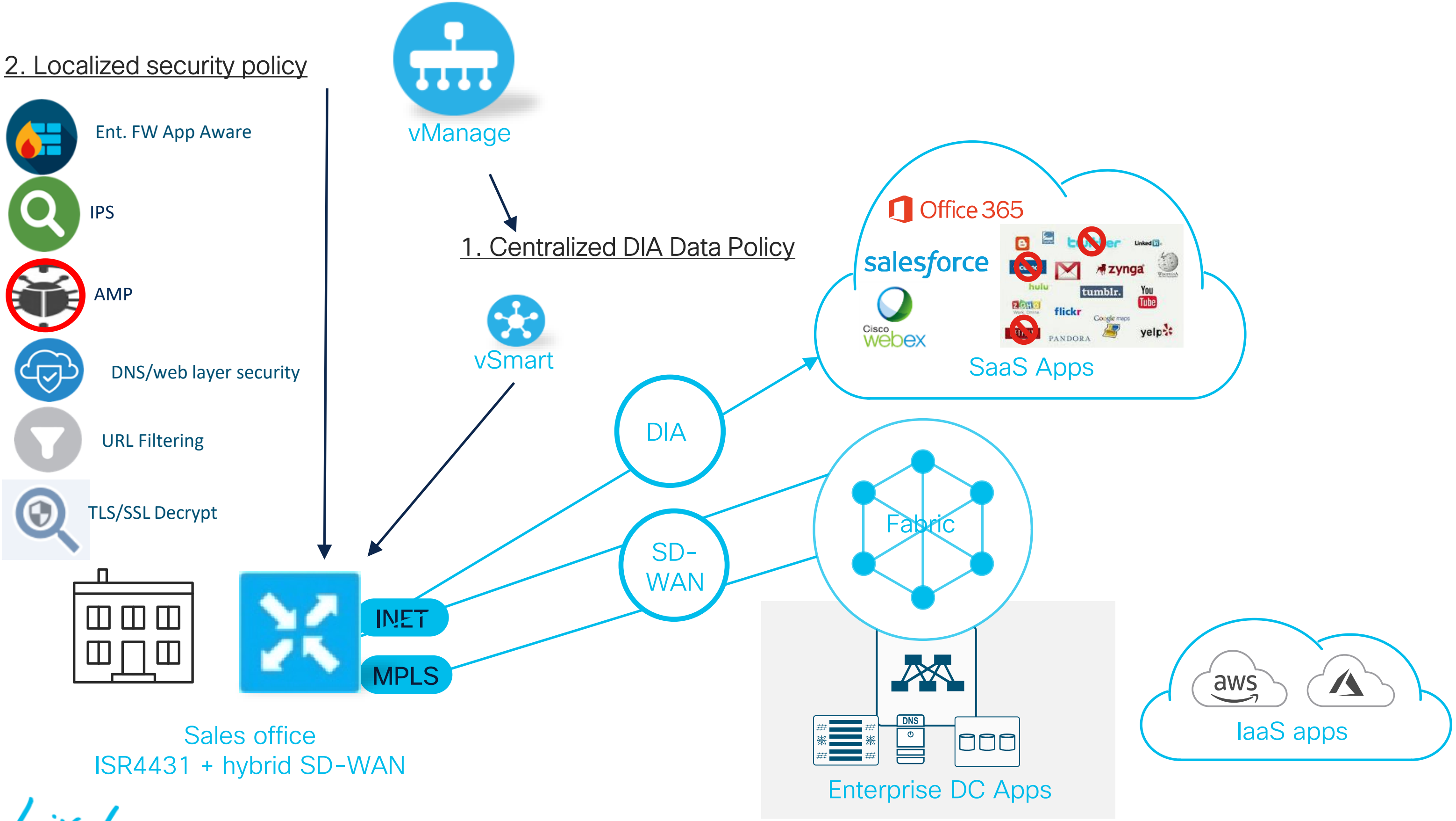
- ❖ Security Services as VNF

Demo: Secure Direct Internet Access (DIA)

Intent-based networking deployment with vManage

Securing Direct Internet Access

Intent: Provide optimal access to SaaS and select Internet 2.0 apps for all Sales Offices



Conclusion

Conclusion

Outsmarting SD-WAN Threats

- Cisco SD-WAN includes a robust set of use cases to solve a wide range of branch networking business needs
- Cisco Security features are available to mitigate a wide array of Internet threats
  - Inside-out, outside-in, internal threats
- The integration of security features into the SD-WAN solution allows users to take an intent based approach to simplify deploying secure SD-WAN use cases

Cisco
Customer Experience | Let’s Go

https://www.cisco.com/go/cxen

Where the energy from Cisco Live continues
and a collaborative journey begins.

Plan. Explore. Connect. Let’s go.

Cisco
Customer Experience

Continue your Pathway to Success

Visit CX On Demand beginning June 4

Cisco Live Day 2 Keynote

Alvio Barrios

Liz Centoni

Todd Nightingale

CX Demos

CX Cloud

CX Cloud for Partners

Business Critical Services

Innovation Channel

Innovation Talk
Collaborative Intelligence + Future Innovations: How Cisco CX Accelerates Customer Success
Tony Colon, Pat Tittiranonda

Product & Strategy Overview
How CX Uses ML/AI to Reduce Your Operational Risk
Chris Rittler

Product or Strategy Overview Sessions

Managed Services

- Accelerate Transformation with Cisco Managed Services

Support Services

- Leverage Cisco Support Services for Business Continuity

Cloud

- Optimizing the Application Experience in a Cloud Native World

IoT

- Best Practices for Deploying Large Scale IoT Devices

Enterprise

- ITSM OS Update - Closed Loop Between Cisco DNA Center and Service Now
- Accelerate and Prepare the Groundwork for Your Cisco DNA Center Implementation
- Outsmarting SD-WAN Threats

Security

- How to Adapt Your Workforce Needs During Changing Times

Service Provider

- Virtualization in Mobility

Thank you

Possibilities

#CiscoLive