You make **possible**

SD-WAN Security

Kureli Sankar – Manager, Technical Marketing
Kural Arangasamy – Technical Marketing Engineer

BRKRST-2377

Barcelona | January 27-31, 2020

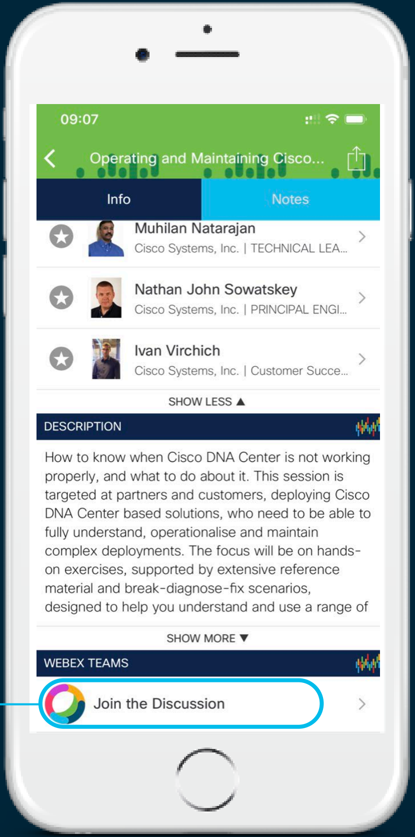
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click "Join the Discussion"
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

About Kureli Sankar

Distinguished Speaker Ciscolive!

BS in Electrical and Electronics Engineering

2006 – 2013 TAC Engineer

- CCIE Security #35505

2013 – 2018 TME

2019 – Present TME Manager

Areas of expertise

- IOS and IOS-XE security features
- SD-WAN Security solutions

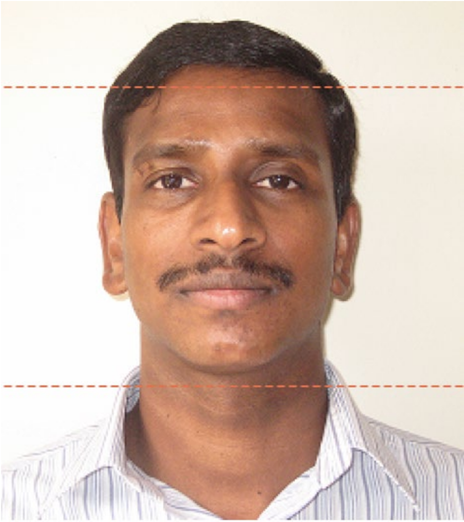
2018 - Distinguished Speaker Cisco Live (EUR and ANZ)

NITT

CISCO CERTIFIED CCIE SECURITY

# 35505

About Kural Arangasamy



Family : Wife & 2 kids

Work History : 20+ years in IT Field

Cisco : 14+ years

Cisco Experience : Switching, Routing & Security Solutions Team

Previous : As a Consultant in NYC & NJ Area: Cabletron, Nortel, Bear Stearns, Goldman Sachs, Merrill Lynch: Designing & Architecting MAN

Ambition : Security Researcher & Educate the World about Security Threats!

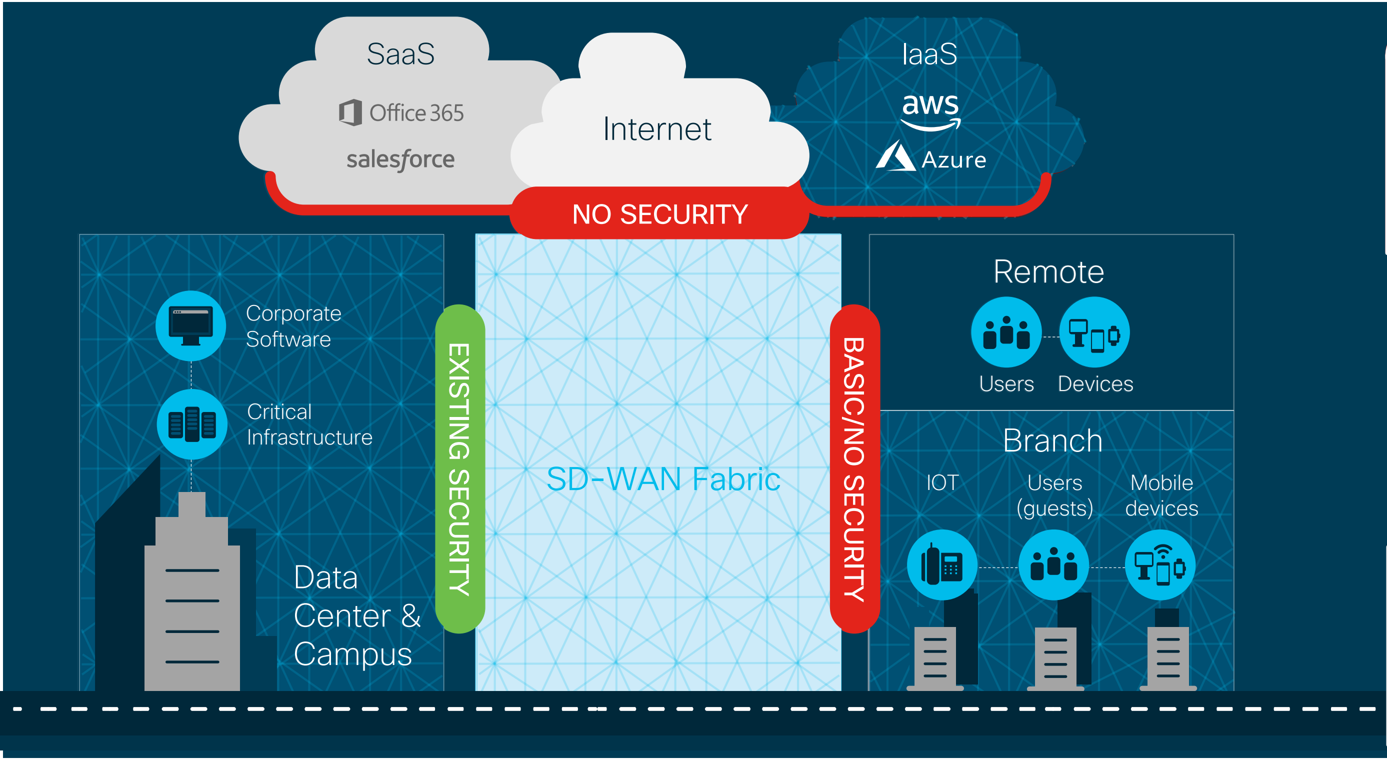
Social Network : @kuralvanan in Kural Arangasamy

Agenda

- Introduction
- Secure Infrastructure
  - Device Identity
  - Secure Control Plane
  - Secure Data Plane
- Secure Branch
  - Ent Firewall App Aware
  - Intrusion Prevention
  - URL - Filtering
  - DNS/Web-layer Security
  - Advanced Malware Protection + Threat Grid
- Secure Management
- Demo

Introduction

SD-WAN exposes new security challenges



SaaS

Office 365

salesforce

Internet

IaaS

aws

Azure

NO SECURITY

Corporate Software

Critical Infrastructure

Data Center & Campus

EXISTING SECURITY

SD-WAN Fabric

BASIC/NO SECURITY

Remote

Users

Devices

Branch

IOT

Users (guests)

Mobile devices

Outside-in threats

- Exposed ingress points as traffic is no longer backhauled to the data center

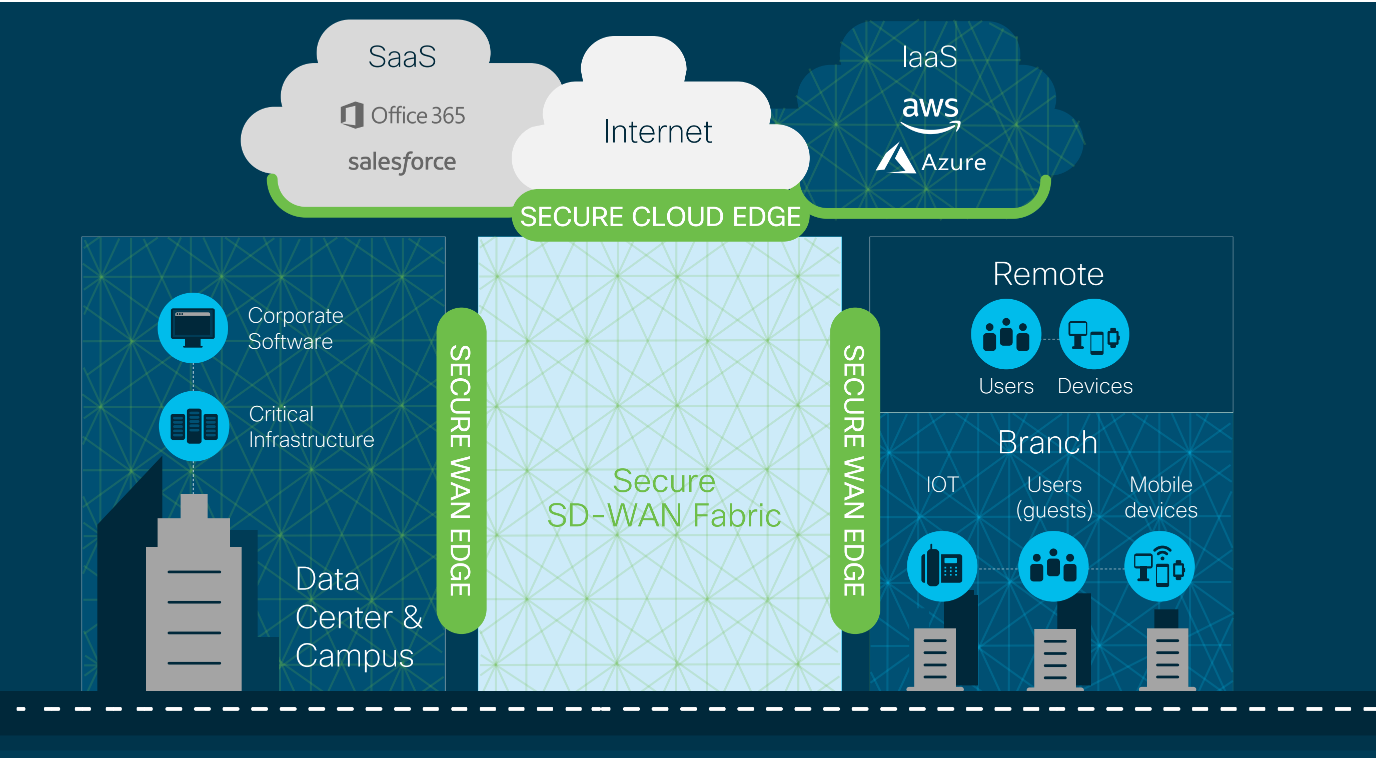
Inside-out threats

- Users and devices request access to infrastructure and applications

Internal threats

- Traffic must be encrypted and access must be segmented end to end

Comprehensive SD-WAN security



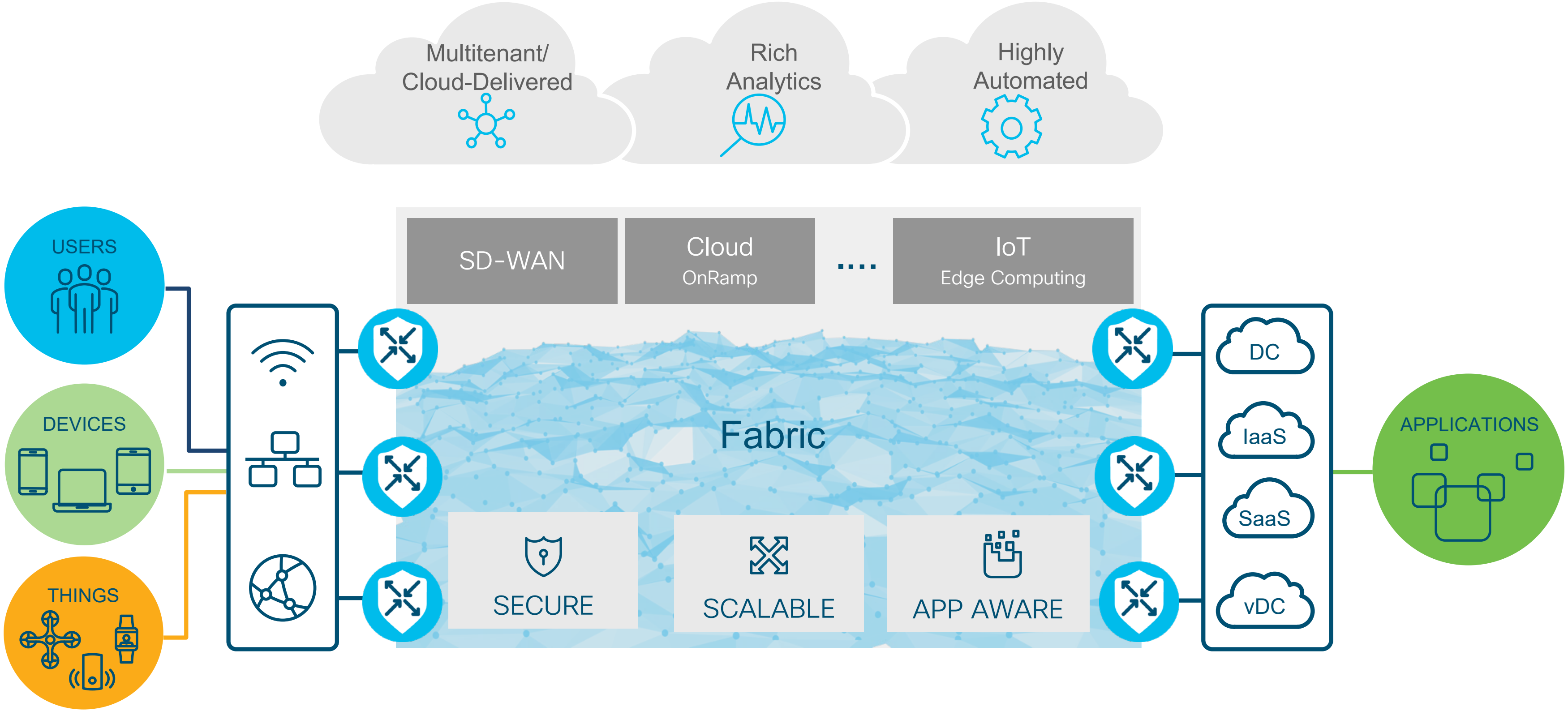
Full edge security stack

- Mitigate external security risks with integrated threat defense from the WAN to cloud edge

Thin, rich or full-stack router

- Mitigate internal security risks with a secure SD-WAN fabric with simple or flexible routing configurations

Cisco SD-WAN Holistic Approach



cisco Live!

Secure Infrastructure

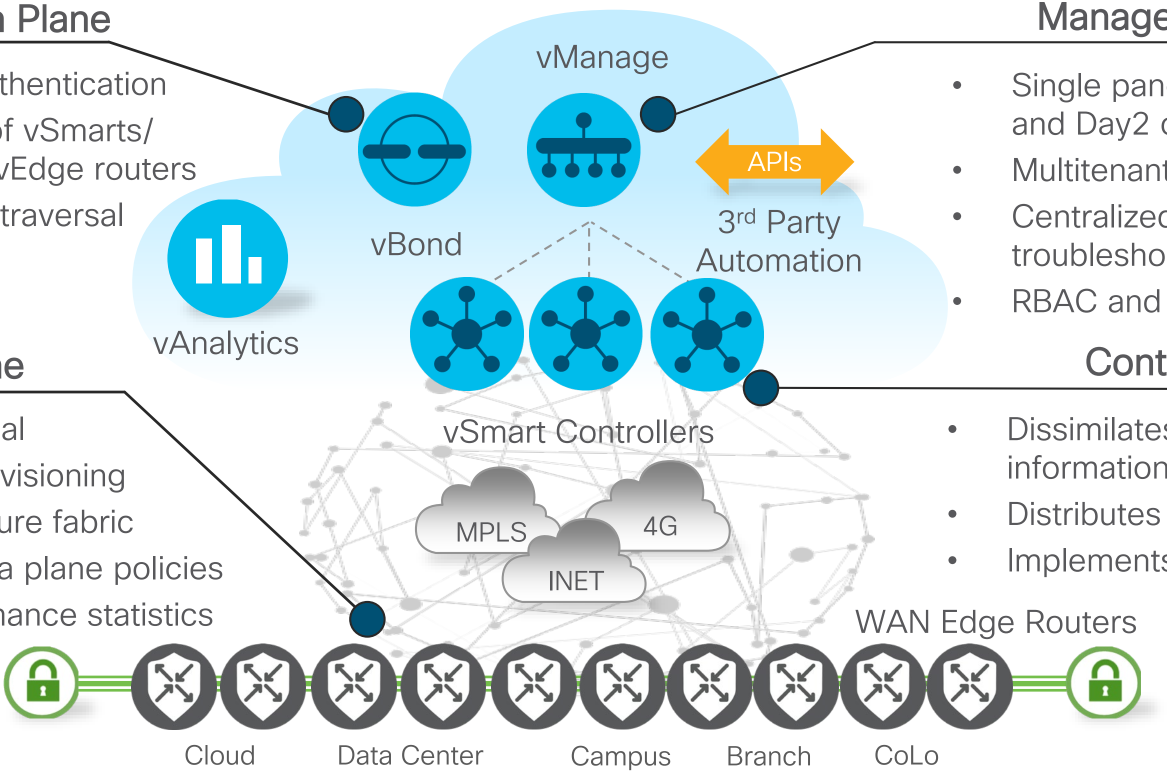
Cisco SD-WAN Architecture

Orchestration Plane

- First point of authentication
- Distributes list of vSmarts/ vManage to all vEdge routers
- Facilitates NAT traversal

Management Plane

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant or single-tenant
- Centralized provisioning, troubleshooting and monitoring
- RBAC and APIs



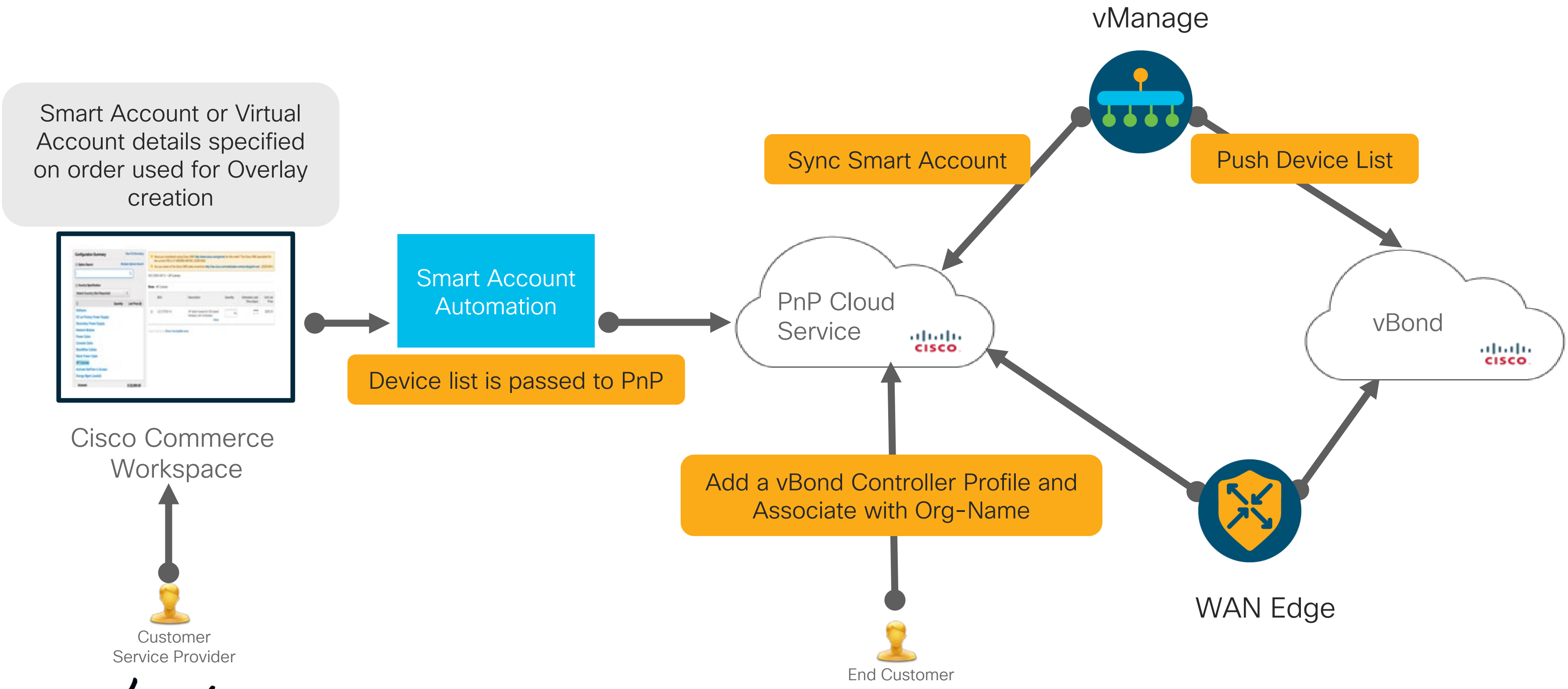
Data Plane

- Physical or virtual
- Zero Touch Provisioning
- Establishes secure fabric
- Implements data plane policies
- Exports performance statistics

Control Plane

- Dissimilates control plane information between vEdges
- Distributes data plane policies
- Implements control plane policies

High level view of ordering and on-boarding



Smart Account or Virtual Account details specified on order used for Overlay creation

Cisco Commerce Workspace

Customer Service Provider

Smart Account Automation

Device list is passed to PnP

PnP Cloud Service

vManage

Sync Smart Account

Push Device List

vBond

Add a vBond Controller Profile and Associate with Org-Name

End Customer

WAN Edge

Device identity and Integrity

History of Malware Found on Cisco IOS Devices

	Incident 0	Incident 1	Incident 2	Incident 3	Incident 4	Incident 5 "SYNful Knock"
Date Discovered	2011	2012	2013	2013	2014	2015
Device(s) Affected	Cisco 2800 and 3800 Families	Cisco 2800 and 3800 Families	Cisco 7600 IOS & line cards	Cisco 7600 IOS & line cards	Cisco 1800,3800, 7200 IOS & ROMMON	Cisco 1841, 2811, 3825
Infection Method	Modifications to IOS binary	Modifications to IOS binary	Modification of in-memory IOS	Modification of in-memory IOS	Modification to both ROMMON, and in-memory code	Modifications to IOS binary
Remote Detectability	Via crypto analysis	Via crypto analysis	C2 protocol	C2 protocol	Not Directly	Yes
Preventions To Be Taken	Trust Anchor Technology, Secure Boot, & Image Signing	Trust Anchor Technology, Secure Boot, & Image Signing	Strong admin credentials & authorization	Strong admin credentials & authorization	Secure Boot, Trust Anchor Technologies + Image Signing	Strong admin credentials, Secure Boot, Image Signing
Complexity Level	Low	Low	Medium	Medium	High	Low

Image Signing

Image Signing

Runtime Defenses

Runtime Defenses

Secure Boot

Secure Boot

Key Trustworthy Technologies

Secure Boot of Signed Images

- Prevents malicious code from booting on a Cisco platform
- Automated integrity checks
- Monitors startup process and shuts down if compromised
- Faster identification of threats

Trust Anchor module (TAm)

- Tamper-resistant chip with X.509 cert installed at manufacturing
- Provides unique device identity and anti-counterfeit protections
- Secure, non-volatile on-board storage and RNG/crypto services
- Enables zero-touch provisioning and minimizes deployment costs

Runtime Defenses (RTD)

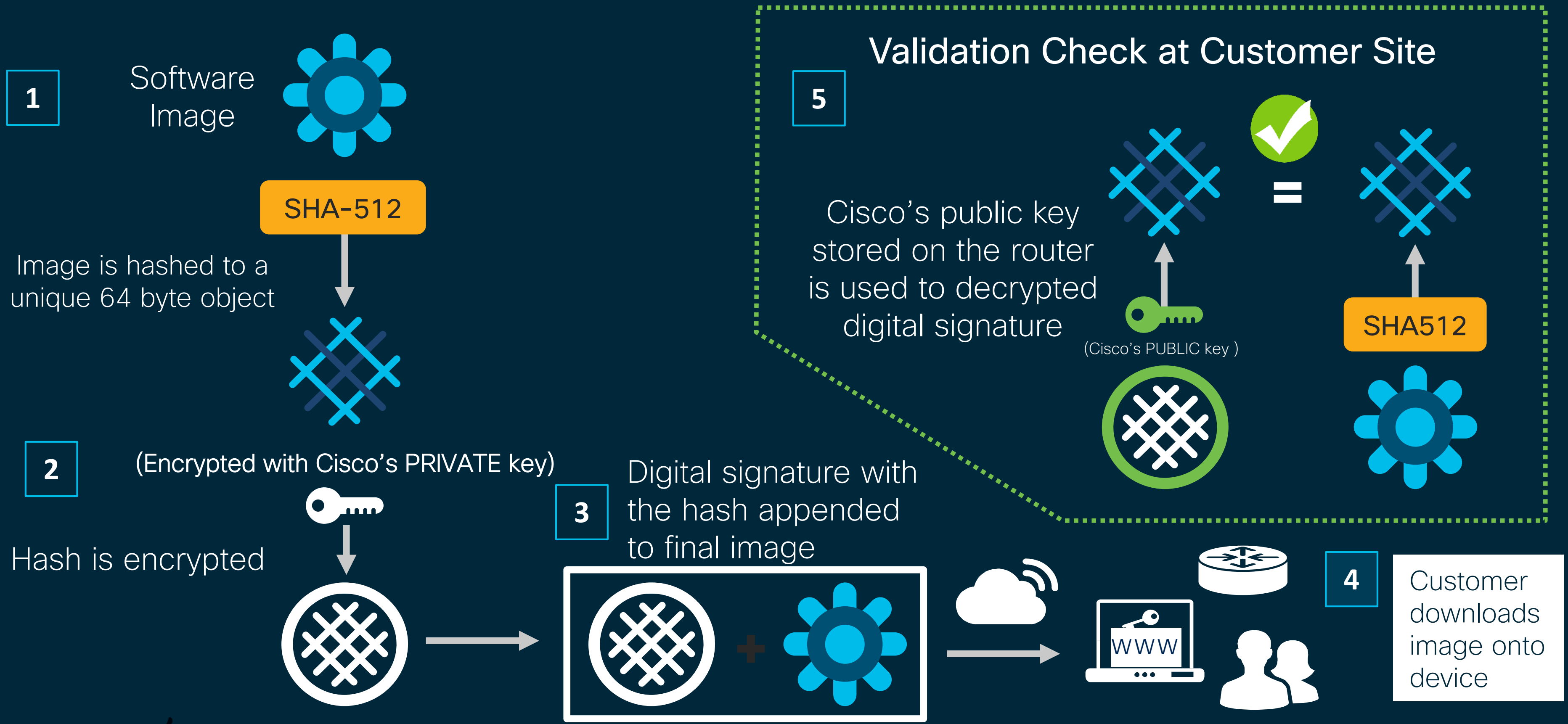
- Protects against injection of malicious code into running software
- Makes it harder for attackers to exploit vulnerabilities in running software
- Runtime technologies include ASLR, BOSC, and X-Space

Trustworthy technologies enhance the security and resilience of Cisco solutions

Secure Unique Device Identification (Secure – UDI)

- Tamperproof ID for the device
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate PID during manufacturing
- Connections with the device can be authenticated by the SUDI credential
- IEEE 802.1AR Compliant

Image Signing: Integrity & Non Repudiation



1 Software Image

SHA-512

Image is hashed to a unique 64 byte object

2 (Encrypted with Cisco's PRIVATE key)

Hash is encrypted

3 Digital signature with the hash appended to final image

4 Customer downloads image onto device

Validation Check at Customer Site

5 Cisco's public key stored on the router is used to decrypted digital signature

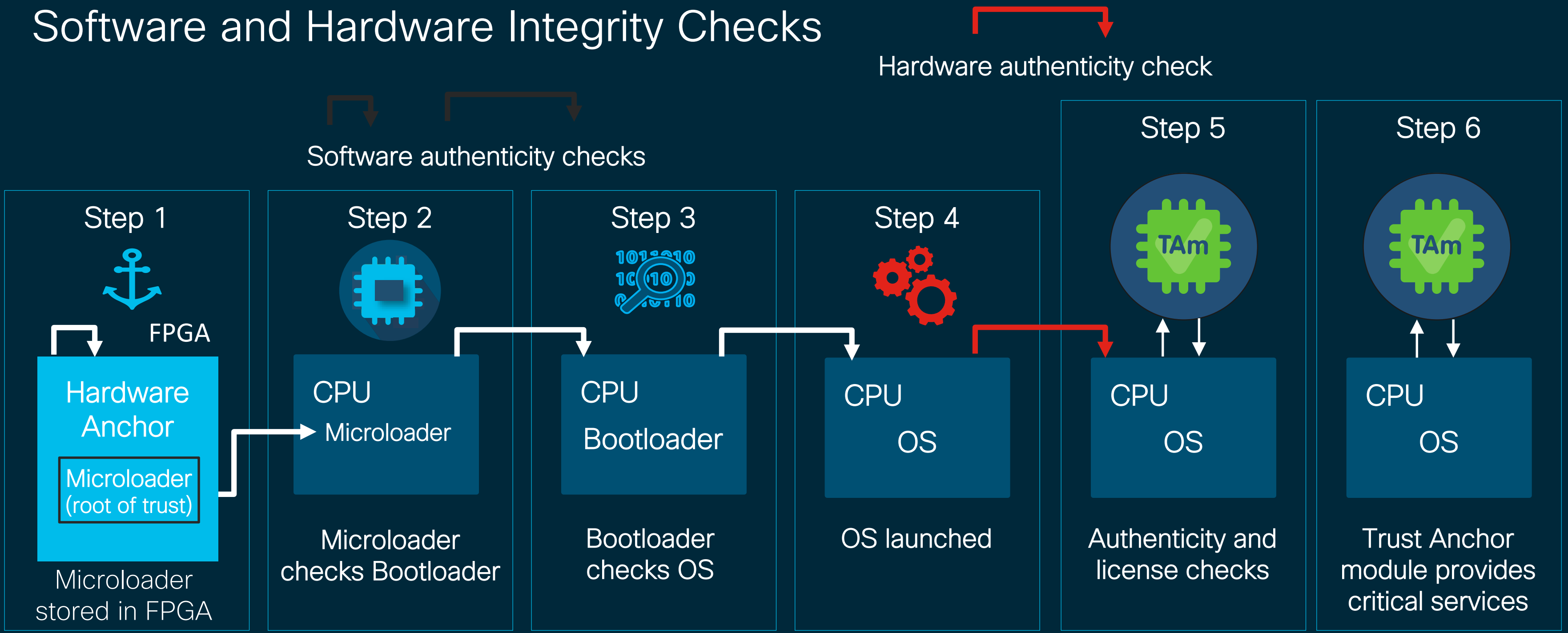
(Cisco's PUBLIC key)

SHA512

cisco Live!

Cisco Secure Boot

Software and Hardware Integrity Checks



Hardware authenticity check

Software authenticity checks

Step 1

FPGA

Hardware Anchor

Microloader (root of trust)

Microloader stored in FPGA

Step 2

CPU

Microloader

Microloader checks Bootloader

Step 3

CPU

Bootloader

Bootloader checks OS

Step 4

CPU

OS

OS launched

Step 5

TAm

CPU

OS

Authenticity and license checks

Step 6

TAm

CPU

OS

Trust Anchor module provides critical services

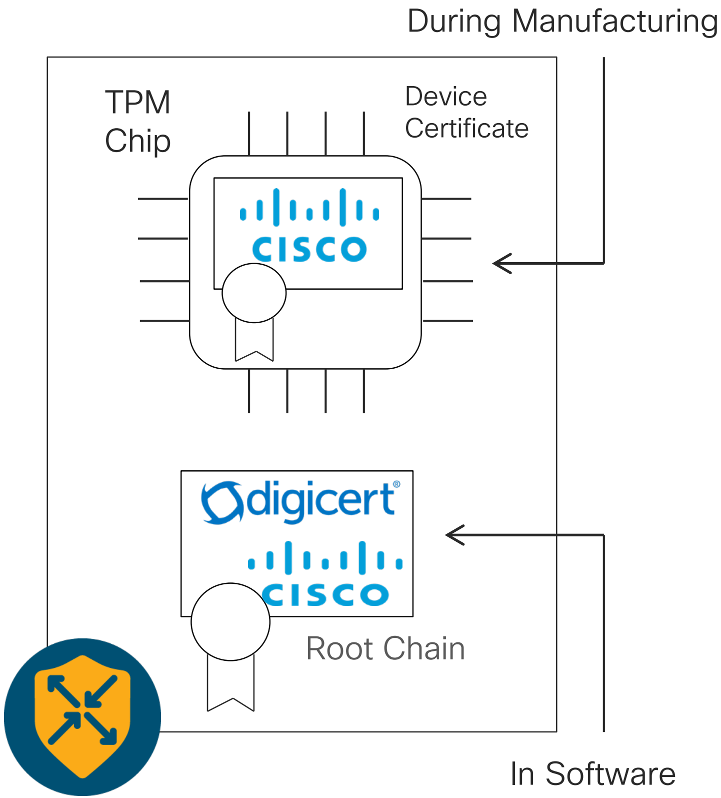
First instructions run on CPU stored in tamper-resistant hardware

TAm = Trust Anchor module

Secure boot checks images and verifies that software is authentic and unmodified before it is allowed to boot

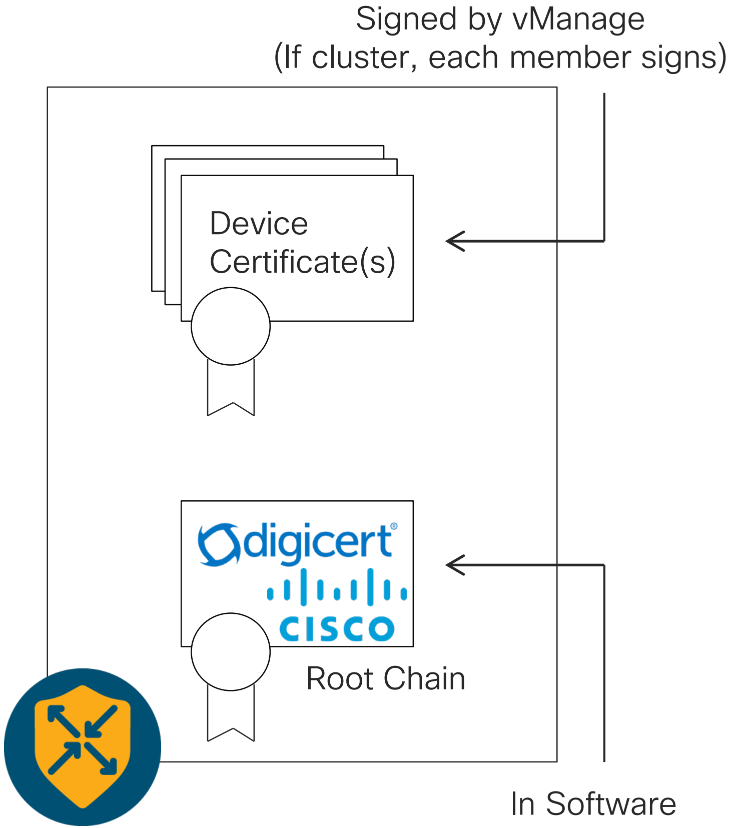
cisco Live!

Cisco Router Identity



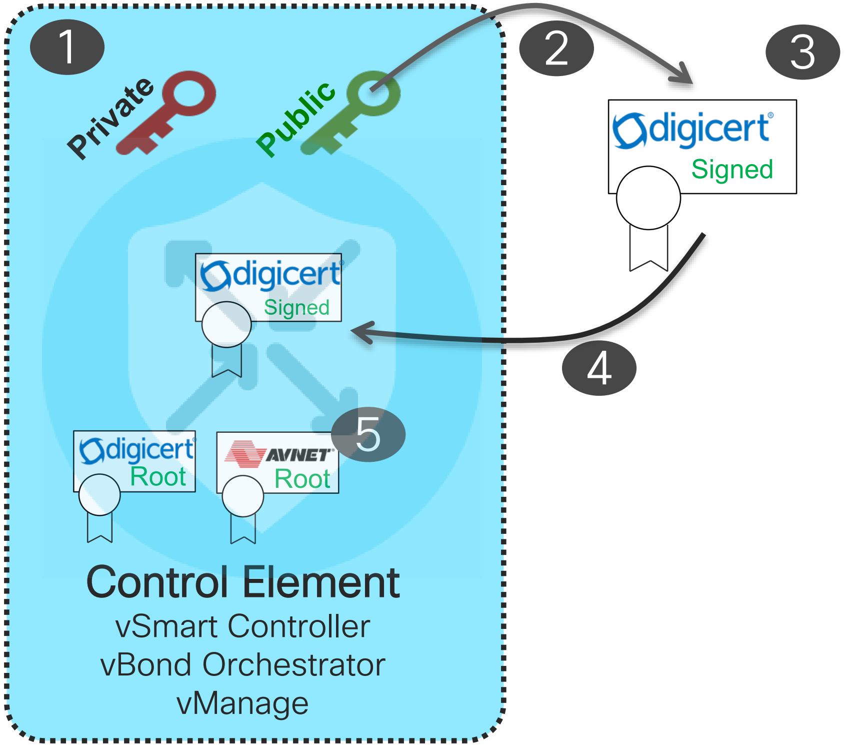
- Each physical router is uniquely identified by the chassis ID and certificate serial number
- Certificate is stored in on-board Tamper Proof Module (TPM)
  - Installed during manufacturing process
- Enterprise cert can also be used to authenticate the WAN Edge
- DigiCert or Cisco root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be automatically installed during ZTP

Cloud (Virtual) Router Identity



- OTP/Token is generated by vManage
  - One per-(chassis ID, serial number) in the uploaded WAN Edge list
- OTP/Token is supplied to Cloud router in Cloud-Init during the VM deployment
  - Can activate from CLI post VM deployment
- vManage signs certificate(s) for the Cloud router post OTP/Token validation
  - If vManage cluster, each member signs
  - vManage removes OTP to prevent reuse
- DigiCert or Cisco root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be provided in Cloud-Init

Establishing Control Elements Identity



1. Private and public keys are generated on the control element
2. Certificate Signing Request is generated
3. Certificate is signed by Digicert/Cisco
4. Certificate is installed into the control element
5. Control element has a built-in root CA trust chain for Avnet, Digicert and Cisco. To Validate other controllers and WAN Edge routers.

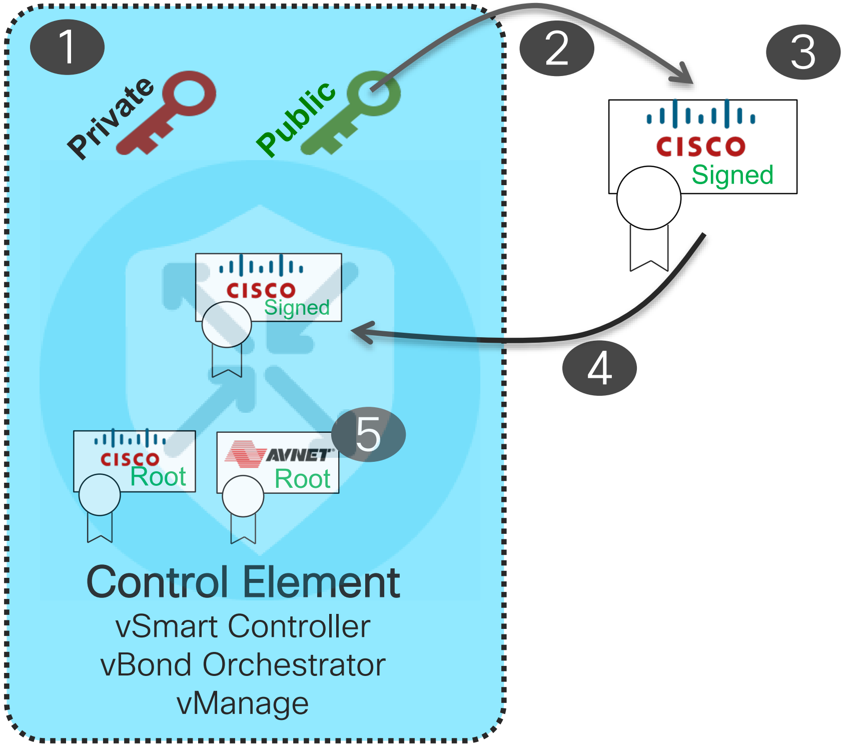
6. This process is fully automated within vManage.

?

Q: Can I Use Enterprise CA?
A: Yes!

Establishing Control Elements Identity – Cisco PKI

19.1

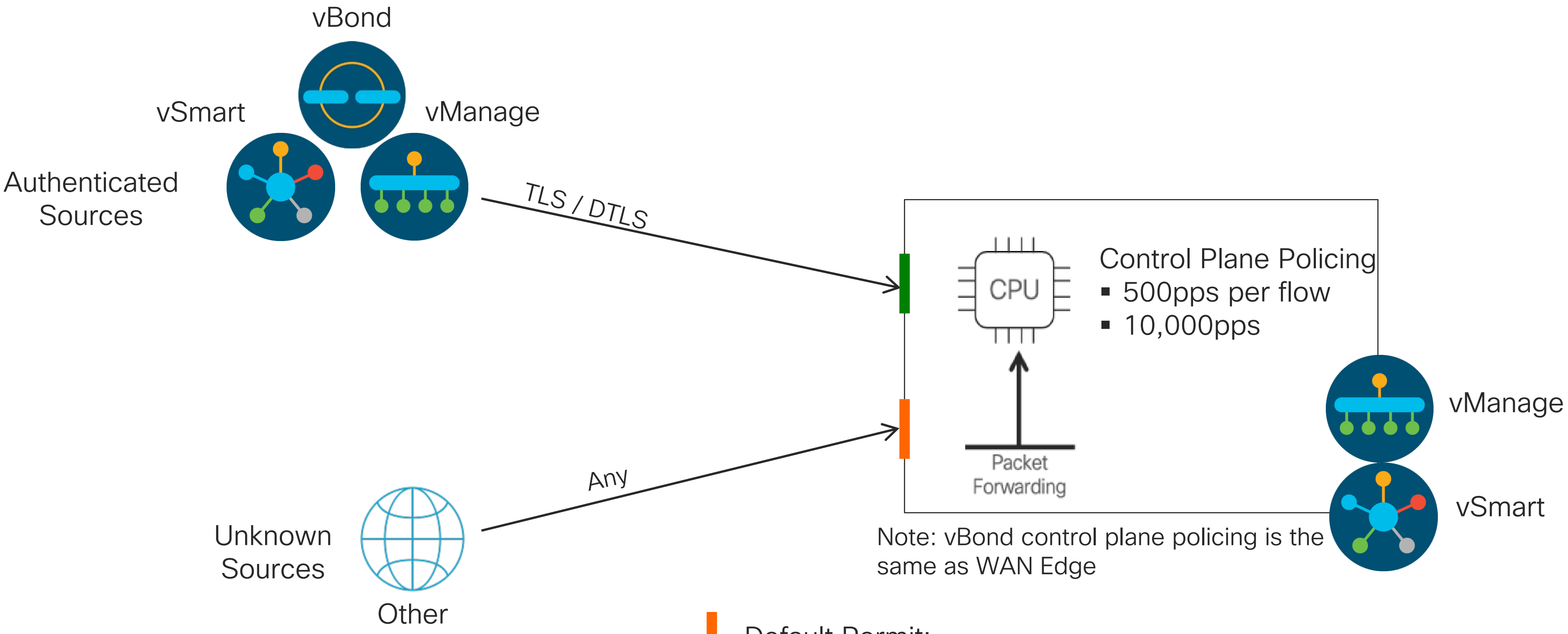


1. Private and public keys are generated on the control element
2. Certificate Signing Request is generated
3. Certificate automatically signed by Cisco PnP linked to your Smart Account (when Cisco signing is selected in vManage)
4. Certificate is installed into the control element
5. Control element will have a built-in root CA trust chain for Cisco and Avnet, to Validate other controllers and WAN Edges
6. This process is fully automated within vManage.

?

Q: Can I Use Enterprise CA?
A: Yes!

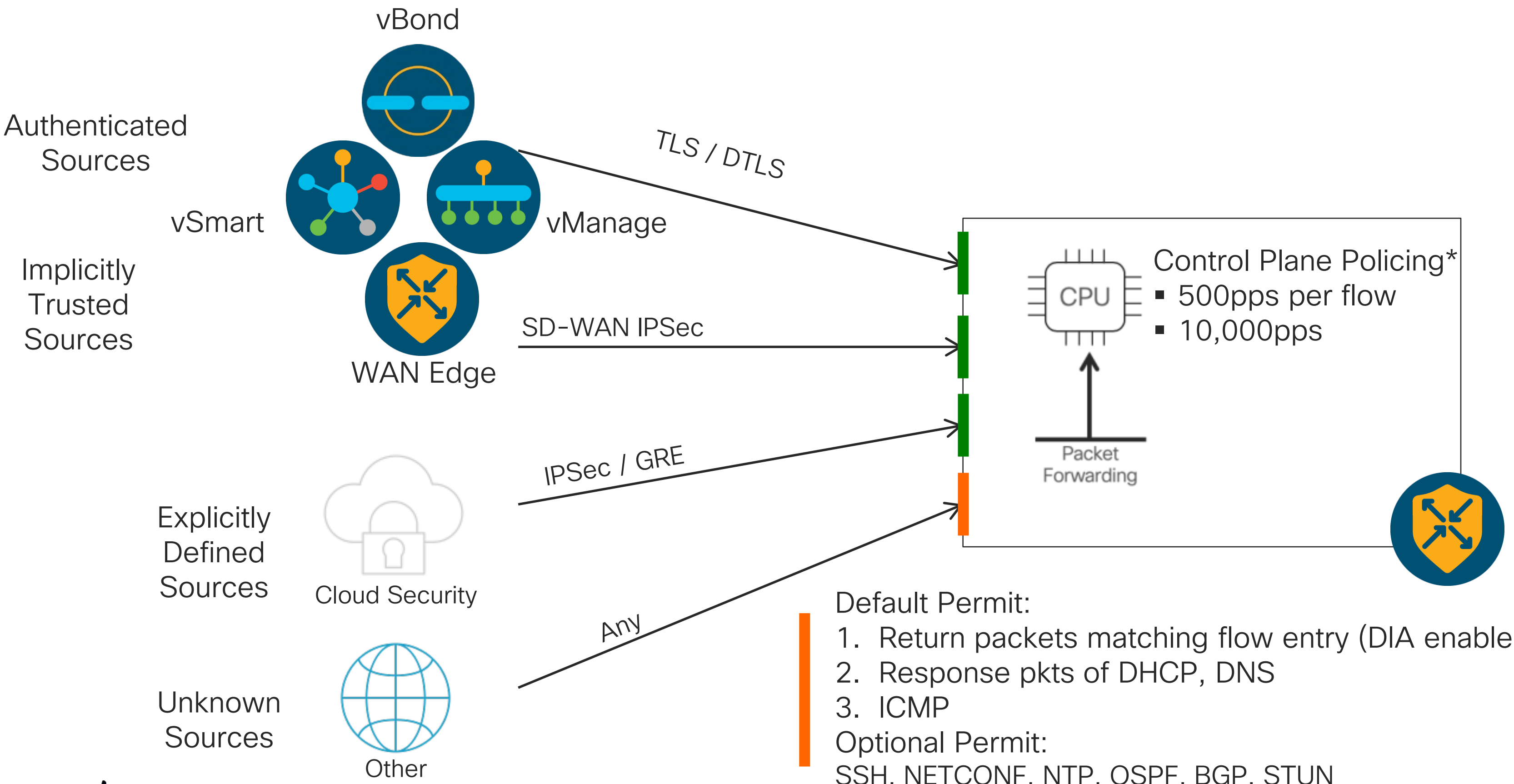
DDoS Protection for Controllers



Note: vBond control plane policing is the same as WAN Edge

Default Permit:
DHCP, DNS, ICMP, NETCONF
Optional Permit:
SSH, NTP, STUN, HTTPS (vManage)

DDoS Protection for SD-WAN Edge Routers



Control Plane Policing*
- 500pps per flow
- 10,000pps

Default Permit:

1. Return packets matching flow entry (DIA enabled)
2. Response pkts of DHCP, DNS
3. ICMP

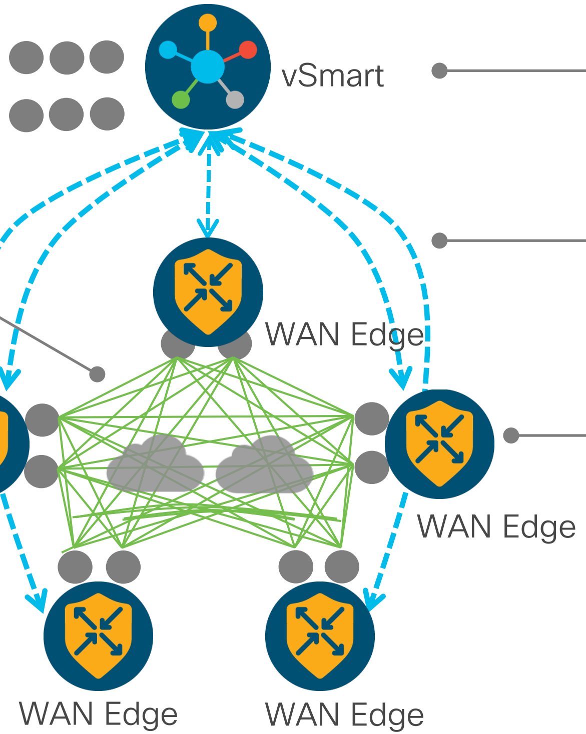
Optional Permit:

SSH, NETCONF, NTP, OSPF, BGP, STUN

* Only on vEdges

Secure Control Plane

Transport Locators (TLOCs)



vSmarts advertise TLOCs to all WAN Edges* (Default)

TLOCs advertised to vSmarts

Local TLOCs
(System IP, Color, Encap)

Full Mesh
SD-WAN Fabric
(Default)

● Transport Locator (TLOC) — OMP — IPSec Tunnel

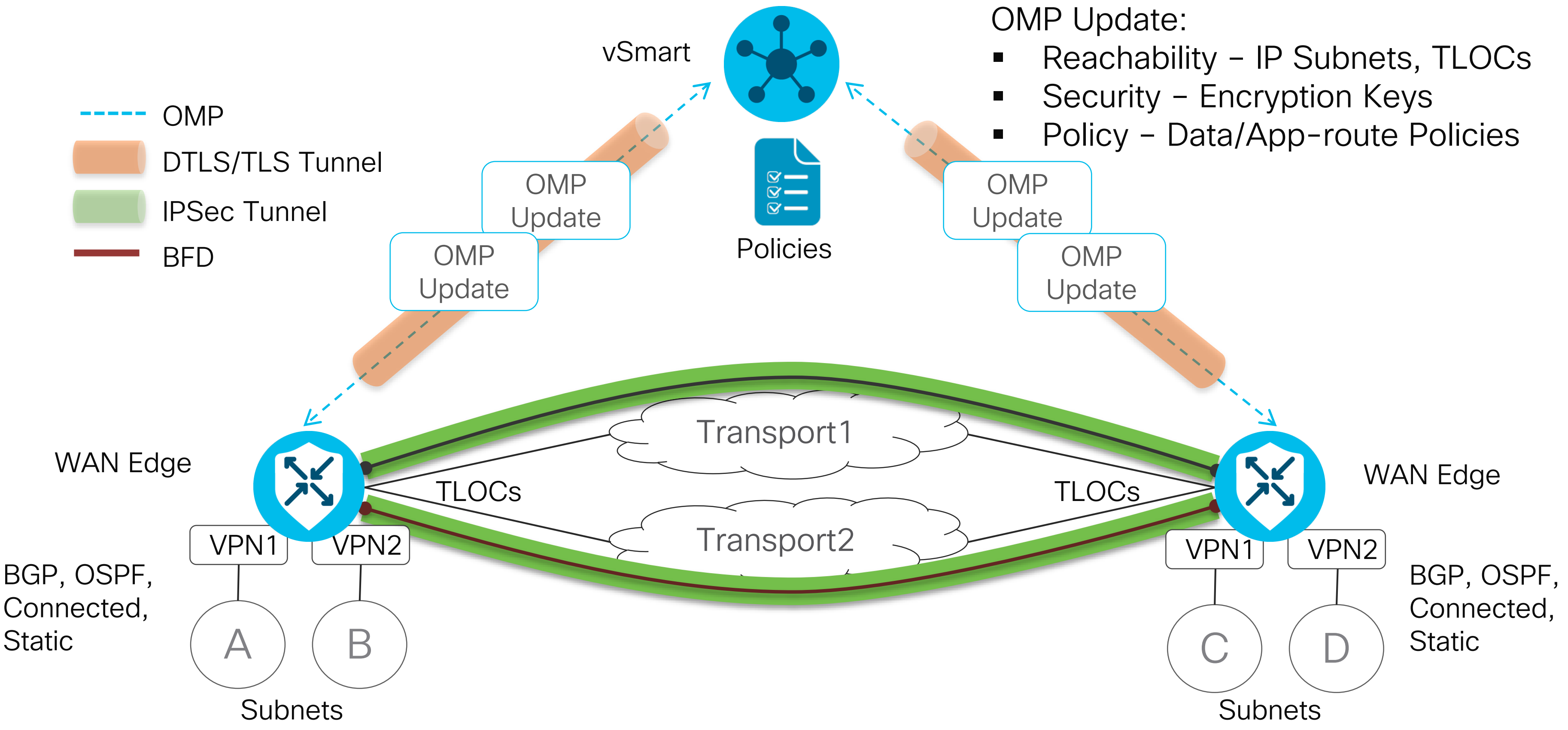
* Can be influenced by the control policies

Secure Data Plane

SD-WAN Fabric Operation Walk-Through

OMP Update:

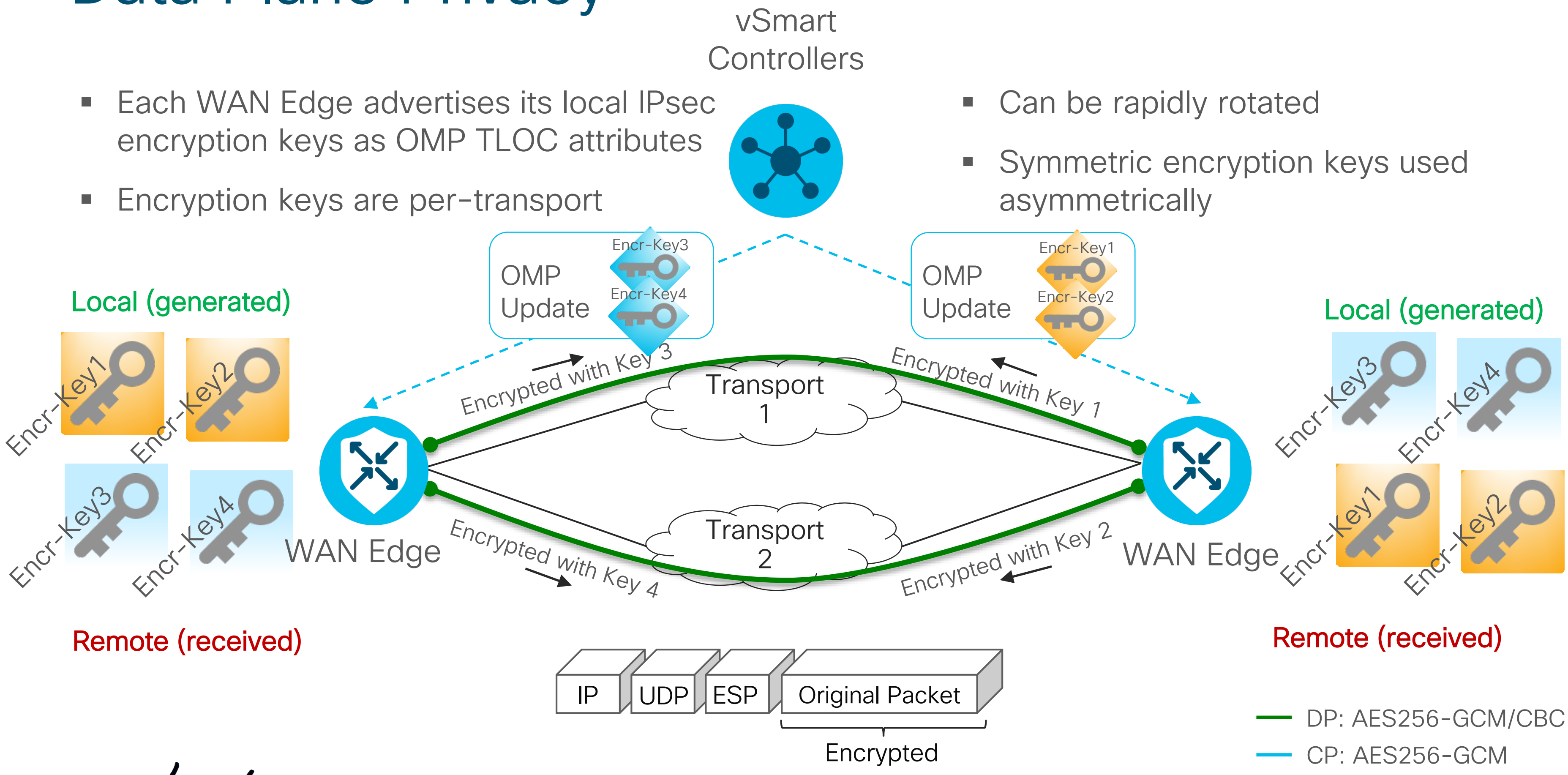
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies



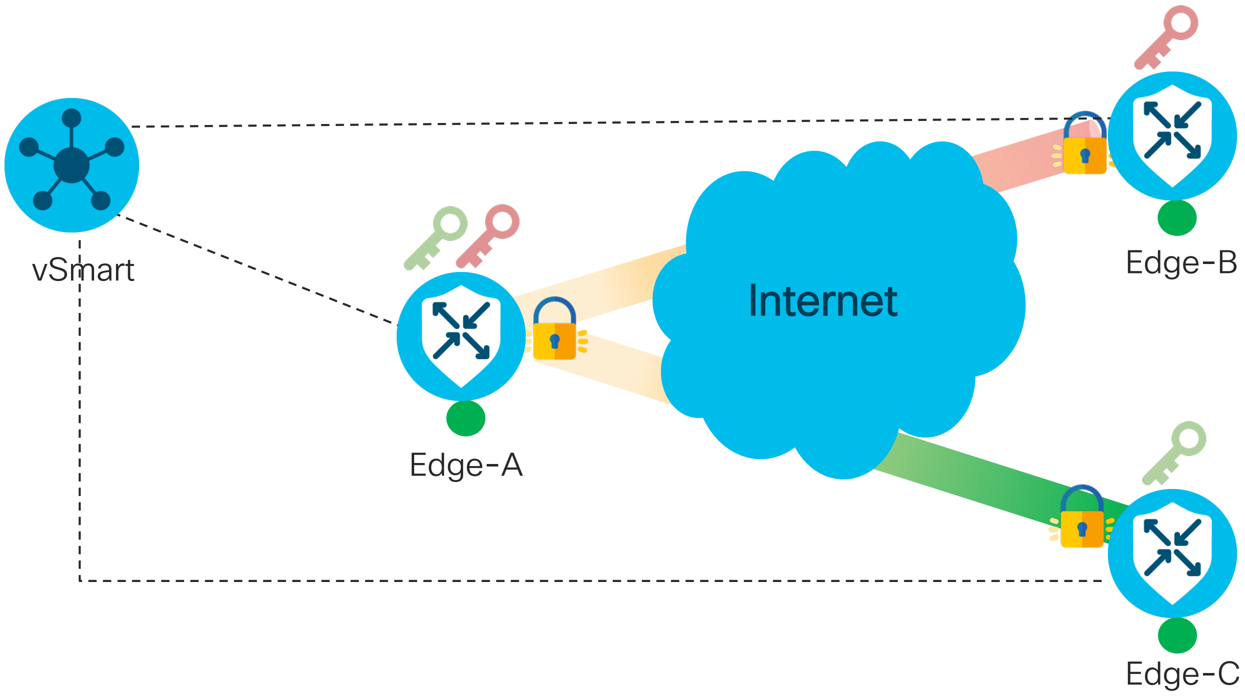
Data Plane Privacy

- Each WAN Edge advertises its local IPsec encryption keys as OMP TLOC attributes
- Encryption keys are per-transport

- Can be rapidly rotated
- Symmetric encryption keys used asymmetrically



Pairwise IPSec Keys for SA



● LAN

IPSec/GRE

--------- DTLS

A's Encryption Key for B

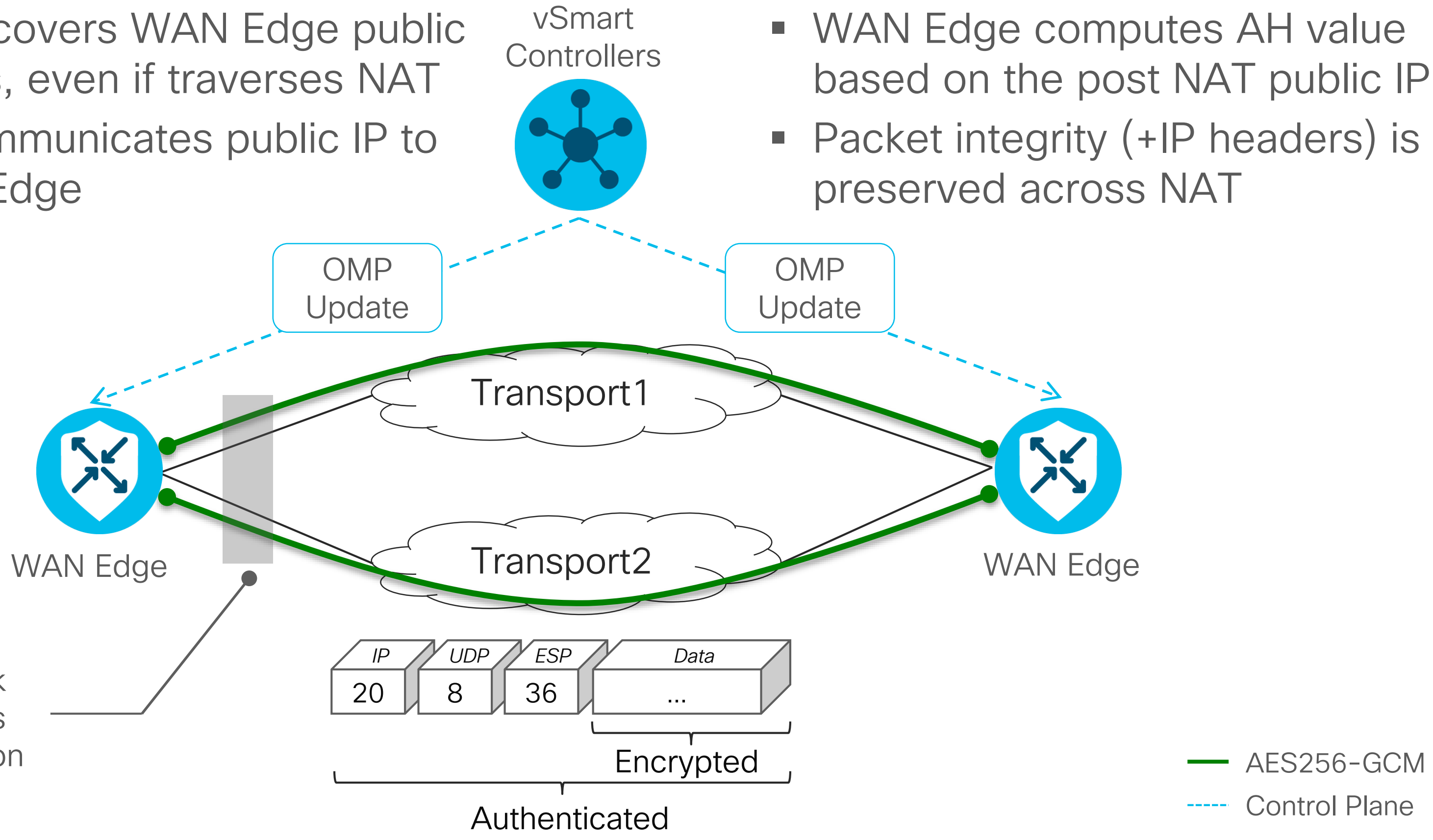
A's Encryption Key for C

cisco Live!

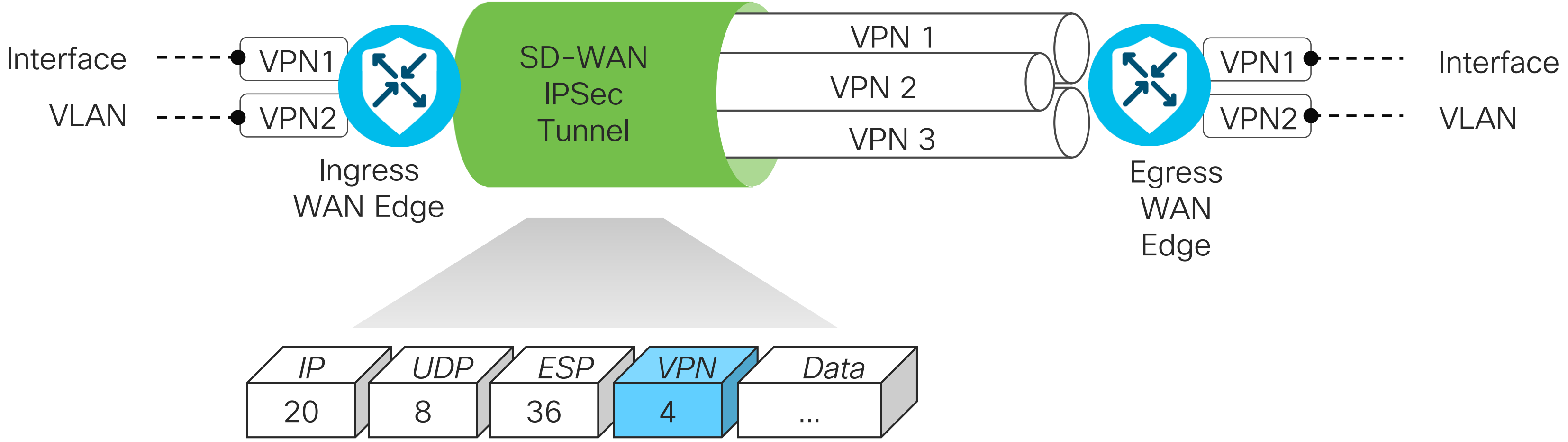
Data Plane Integrity

- vBond discovers WAN Edge public IP address, even if traverses NAT
- vBond communicates public IP to the WAN Edge

- WAN Edge computes AH value based on the post NAT public IP
- Packet integrity (+IP headers) is preserved across NAT

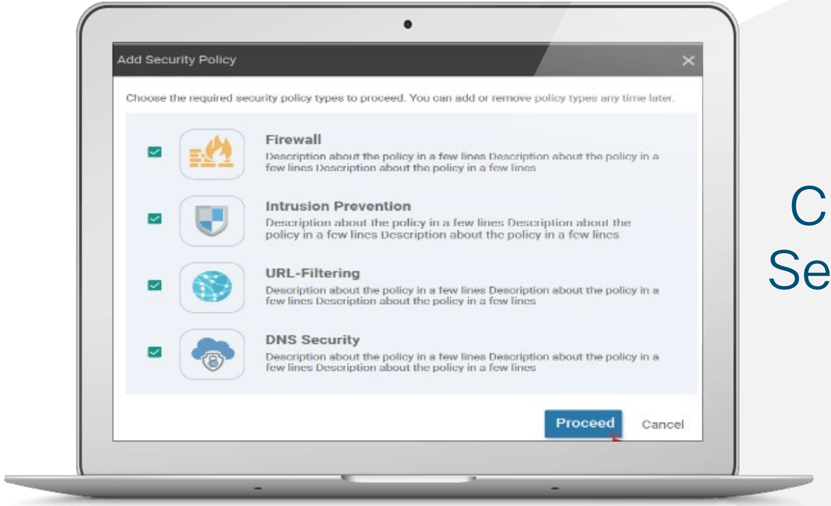


End-to-End Segmentation



- Segment connectivity across fabric w/o reliance on underlay transport
- WAN Edge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup (rfc 4023)
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs

Combining Best of Breed in Security and SD-WAN



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

Cisco SD-WAN

Cisco Security

Enterprise Firewall
+1400 layer 7 apps classified

Intrusion Protection 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

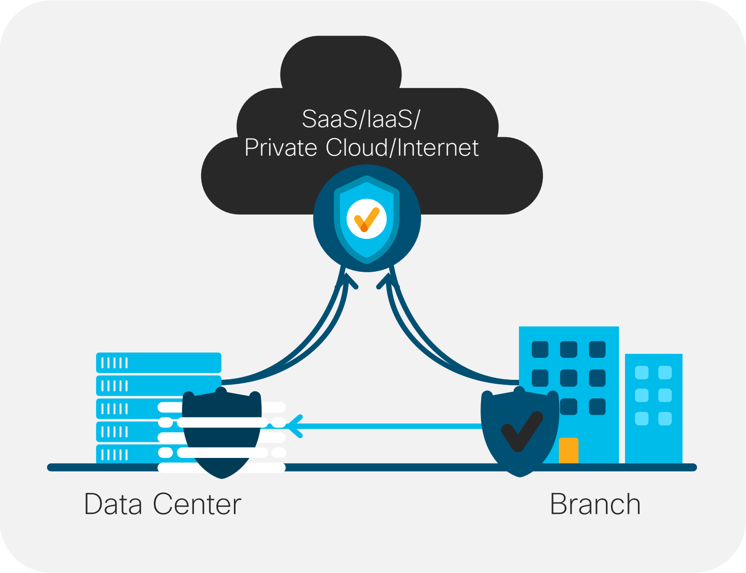
COMING SOON!

TLS/SSL Proxy
Detect Threats in Encrypted Traffic

Hours instead of weeks and months

Secure Branch

Why SD-WAN Branch Security?



Cloud Security
Firewall/IPS
Branch Security

1. Avoid Backhauling

Benefit: Better use of WAN bandwidth

2. Benefit Regional SaaS PoP

Benefit: Improves application performance

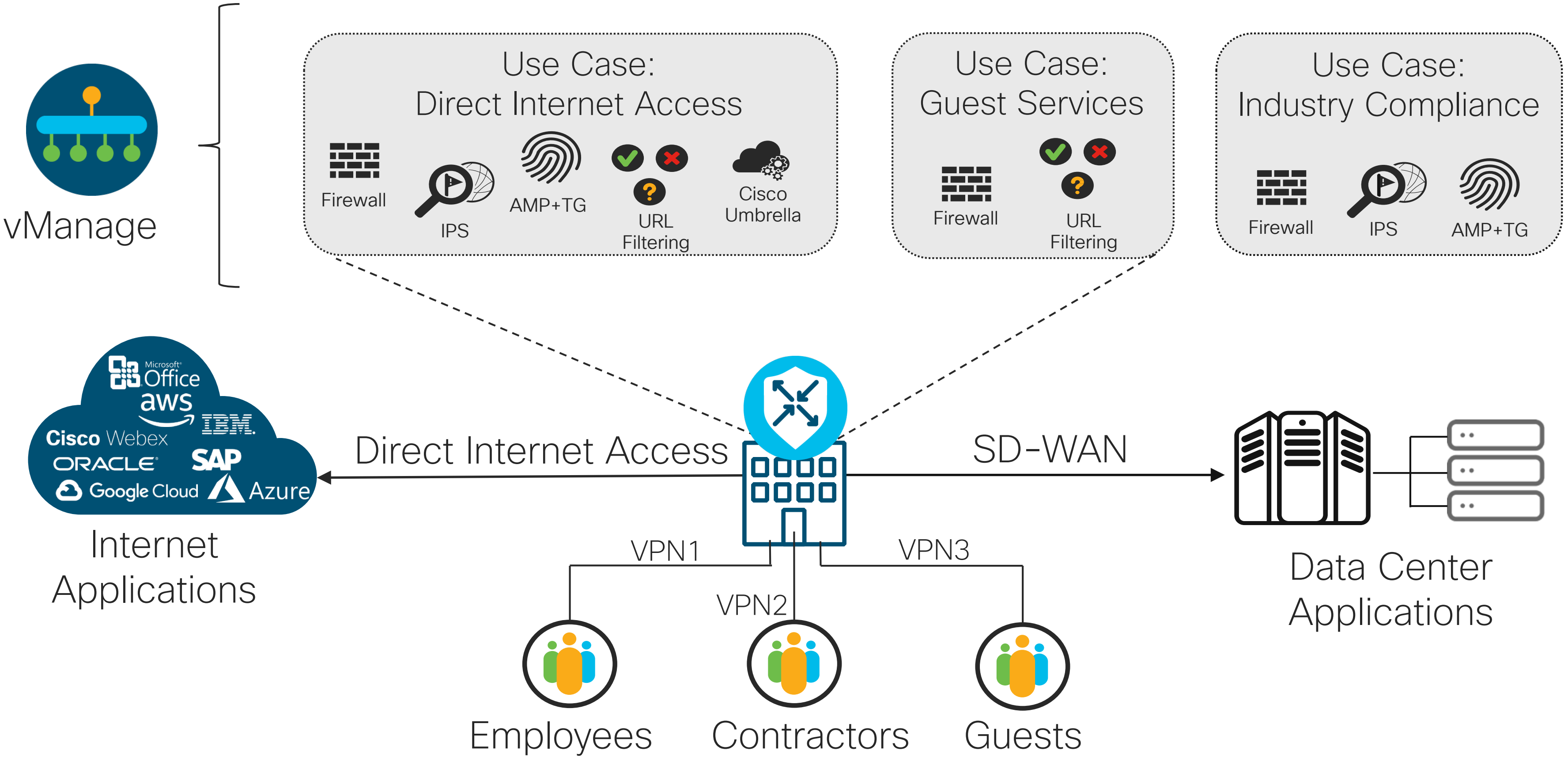
3. Enable DIA

Benefit: Improves user experience

4. Centralized Policy/Monitoring

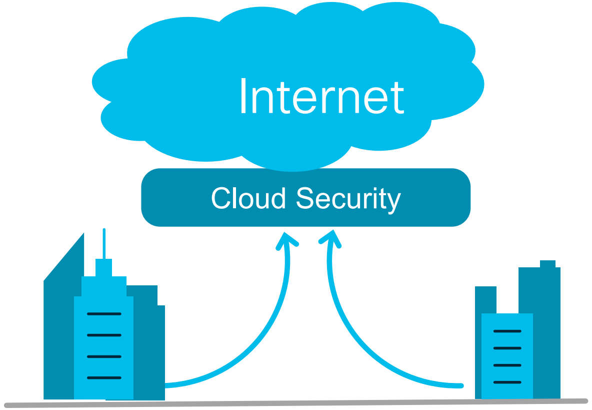
Benefit: Consistent Security Policy & monitoring

SD-WAN Security Use Cases



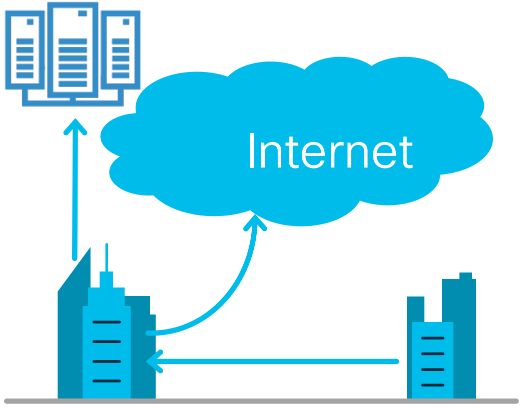
Security Deployment models

Flexible Security based on customer needs



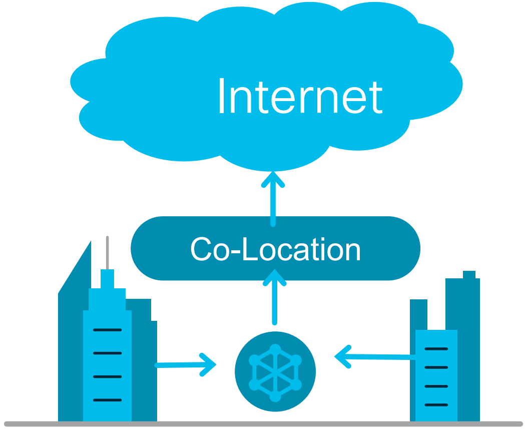
Cloud Security

- Lean Branch with Security in the cloud



Integrated Security

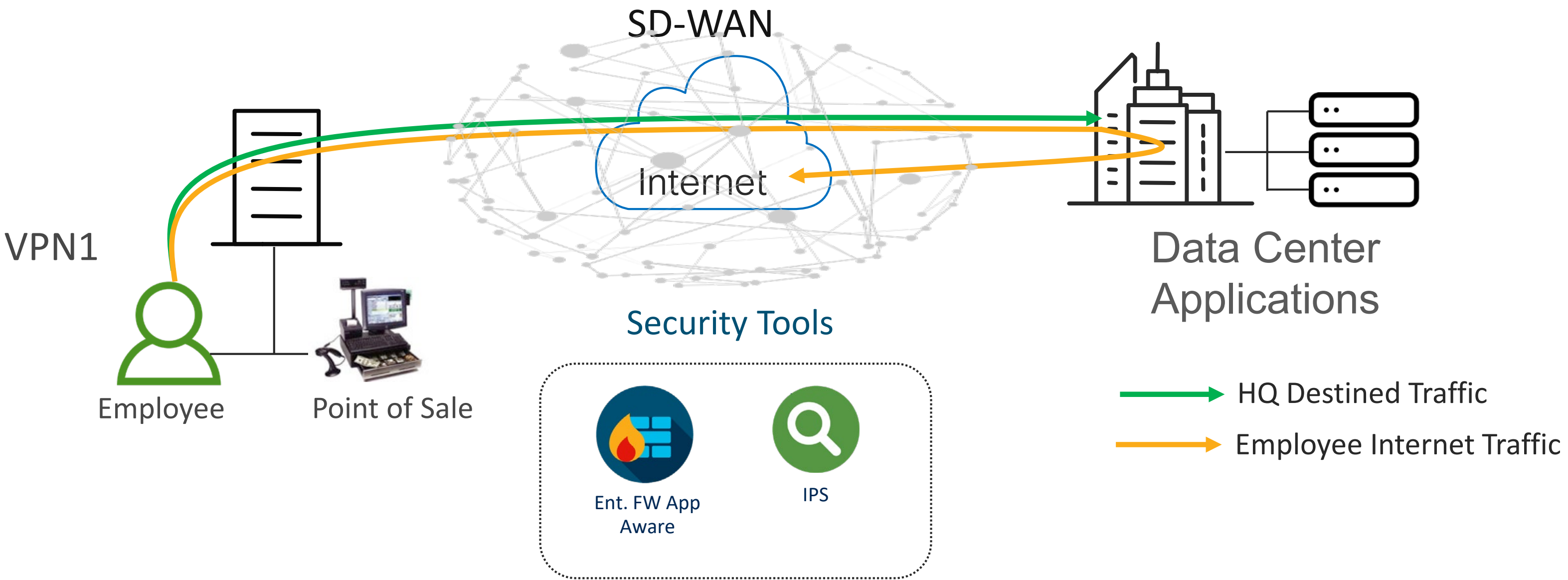
- Single platform for Routing and Branch Security at the Branch



@Regional Hub

- Security Services as VNF at Regional Colocation Hub

Use Case 1: PCI Compliance



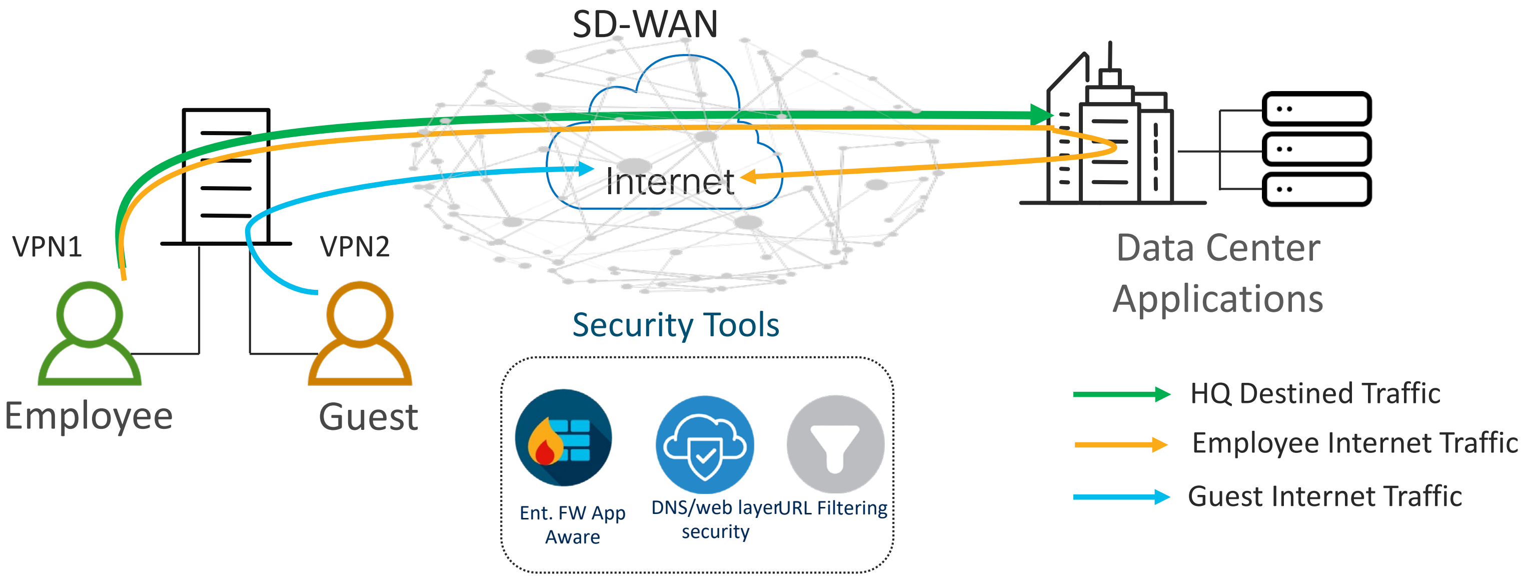
Use Cases

- PCI-DSS - Retail stores
- HIPAA - Hospitals/Clinics
- FERPA – Schools/Colleges/Universities

Requirements

- Segmentation
- Perimeter Control
- Intrusion Prevention

Use Case 2: Guest Access



SD-WAN

Internet

VPN1

VPN2

Employee

Guest

Data Center Applications

Security Tools

Ent. FW App Aware

DNS/web layer security

URL Filtering

→ HQ Destined Traffic

→ Employee Internet Traffic

→ Guest Internet Traffic

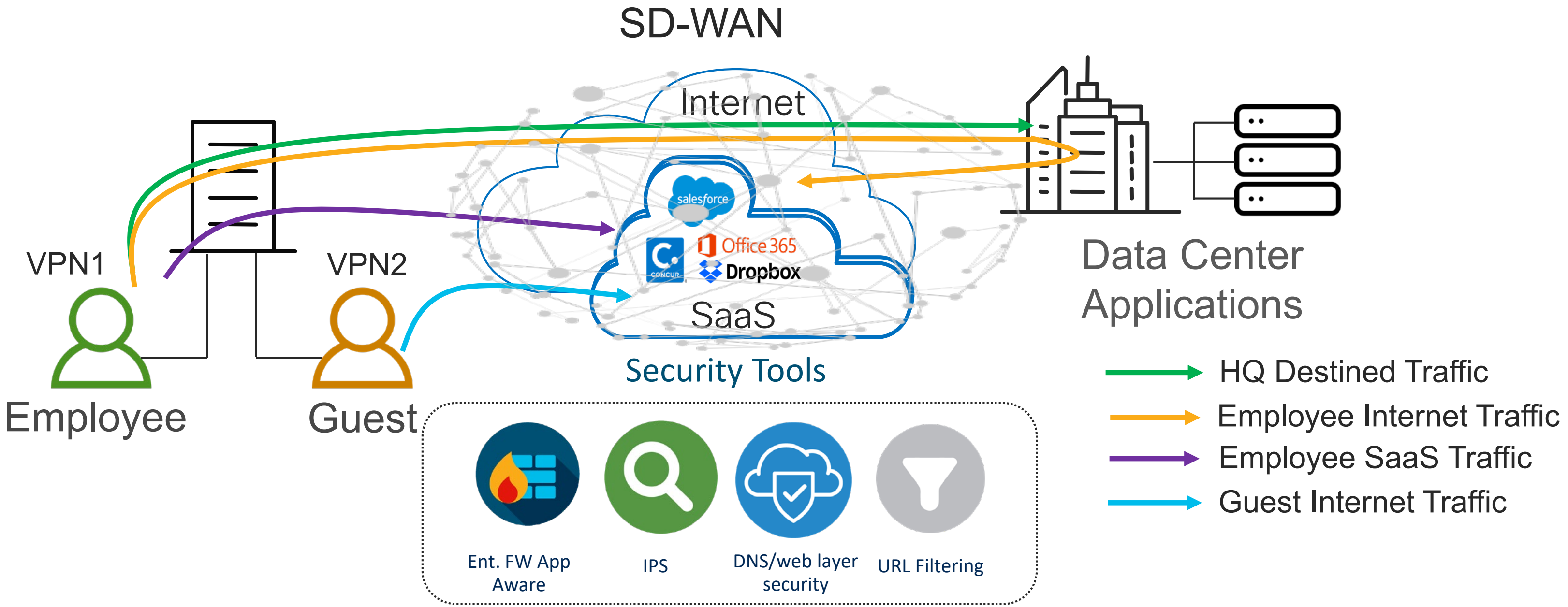
Use Cases

- Retail stores
- Hospitals/Clinics
- Schools/Colleges/Universities

Requirements

- Segmentation
- Application Control
- Liability Protection

Use Case 3: Direct Cloud Access



SD-WAN

Internet

SaaS

VPN1

VPN2

Employee

Guest

Data Center Applications

→ HQ Destined Traffic

→ Employee Internet Traffic

→ Employee SaaS Traffic

→ Guest Internet Traffic

Security Tools

Ent. FW App Aware

IPS

DNS/web layer security

URL Filtering

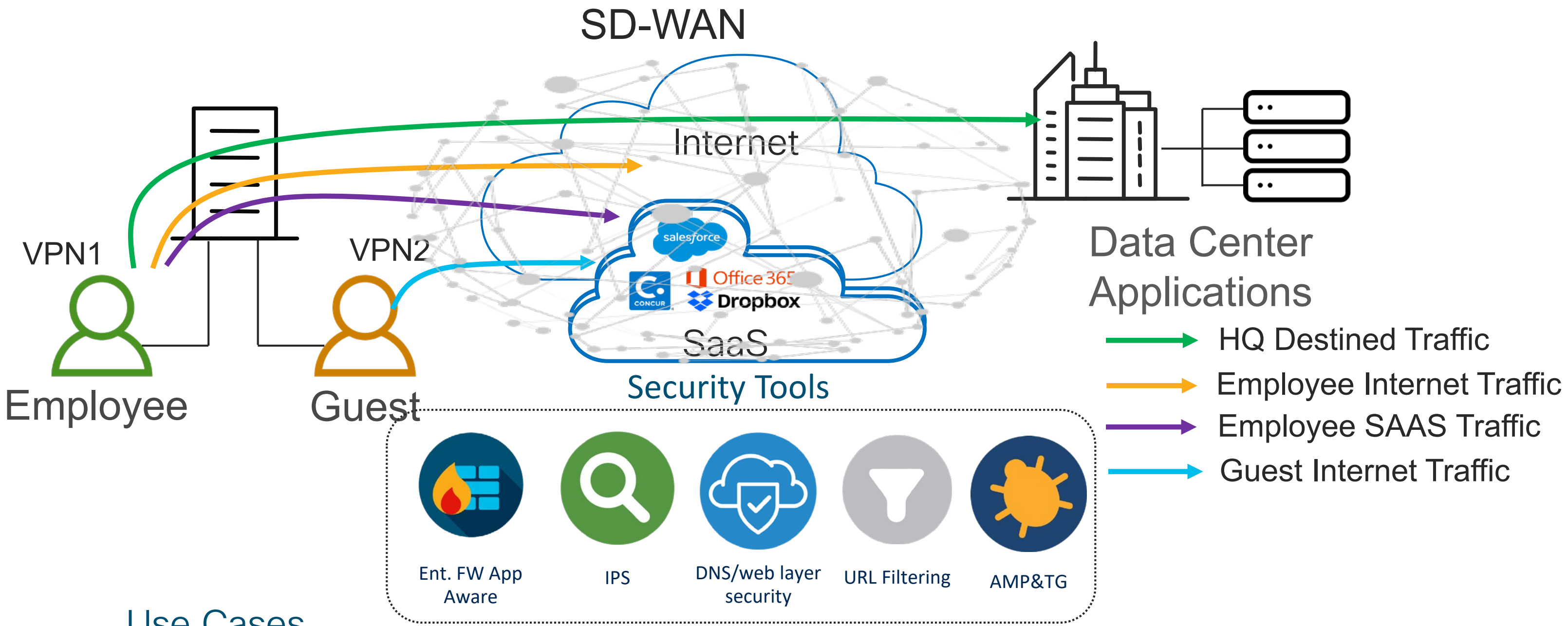
Use Cases

- SaaS applications
- Applications in IaaS: AWS/Azure
- Extranet or partner cloud applications
- Partner Applications

Requirements

- Controlled Redirection
- Application Control
- Intrusion Prevention
- Malware Prevention

Use Case 4: Direct Internet Access



Use Cases

- SaaS applications
- Applications in IaaS: AWS/Azure
- Web Conferencing / Social Media
- Video Streaming Applications

Requirements

- Application Control
- Intrusion Prevention
- Malware Prevention
- Web Content Filtering

Why Multi-Layered Security and How it Works?

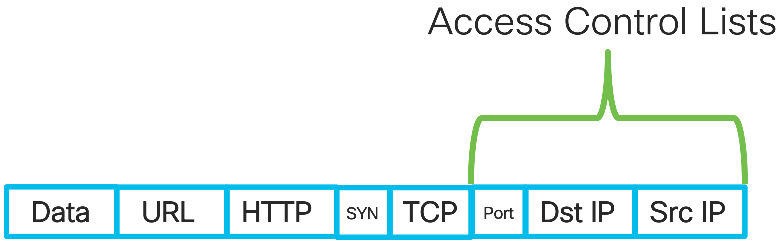
Multi-layer Security

- Access Control Lists (Network Access Control)
- Stateful Firewall (Layer 4 inspection)
- Application Control (Layer 7 inspection)
- IPS (Signature Detection)
- DNS/Web/Content Filtering (Application inspection)
- IP Reputation (Block known bad IPs)
- File Reputation (Block known bad Files)
- Anti-Malware / Anti-Virus (Signature / Heuristic Detection)
- Sandboxing Capabilities (Zero-day threats)
- CASB (Cloud Access Security Broker) (Cloud Applications)
- TLS/SSL Decryption (Man in the Middle (MiTM)) (Encrypted Applications)

Access Control Lists

Access Control Lists

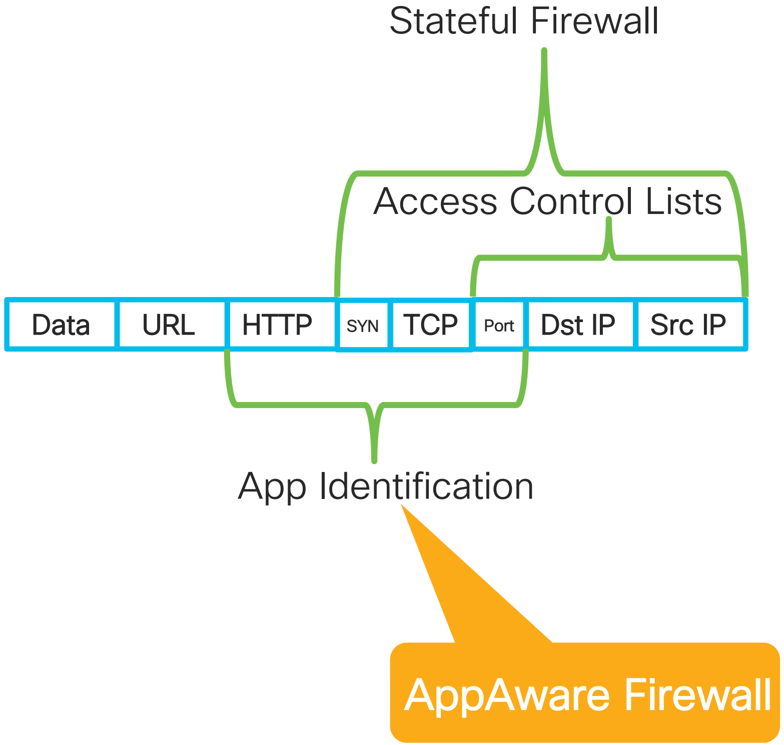
- Network Access Control
- Prevent Unauthorized access
- IP or Protocol Port level
- No Directional Control



Stateful Firewall

Firewall

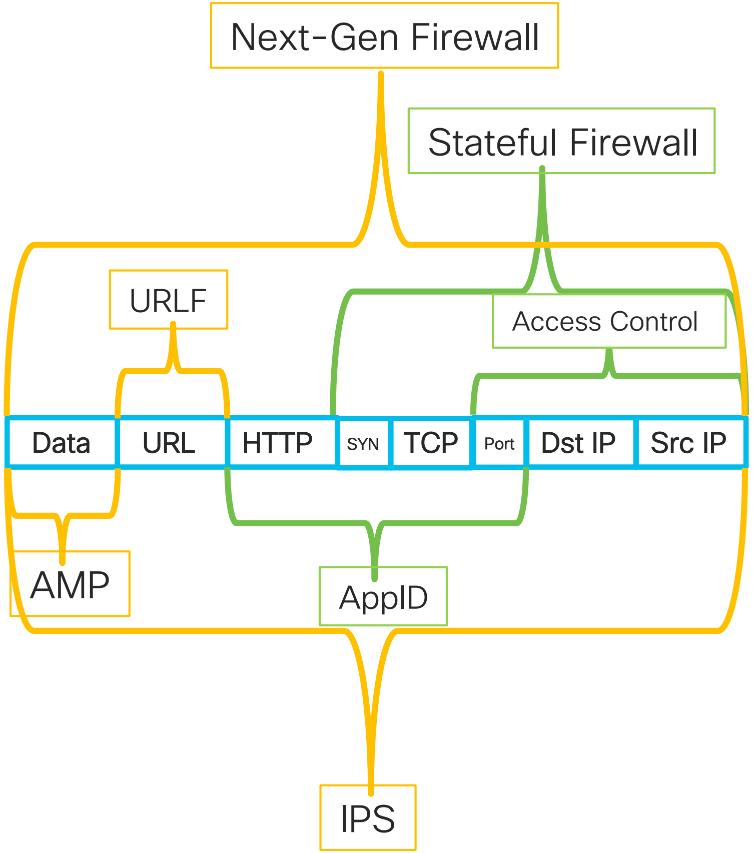
- Deep inspection
- Session Tracking
- Stateful inspection
- Application Layer Gateway
- Protocol Misbehaviors
- Directional Control
- Stricter Layer 4 Control



Firewall vs Next-Gen Firewall - What's the difference?

Firewall

- Deep inspection
- Stateful inspection
- Protocol Misbehaviors
- Directional Control
- Stricter Layer 4 Control

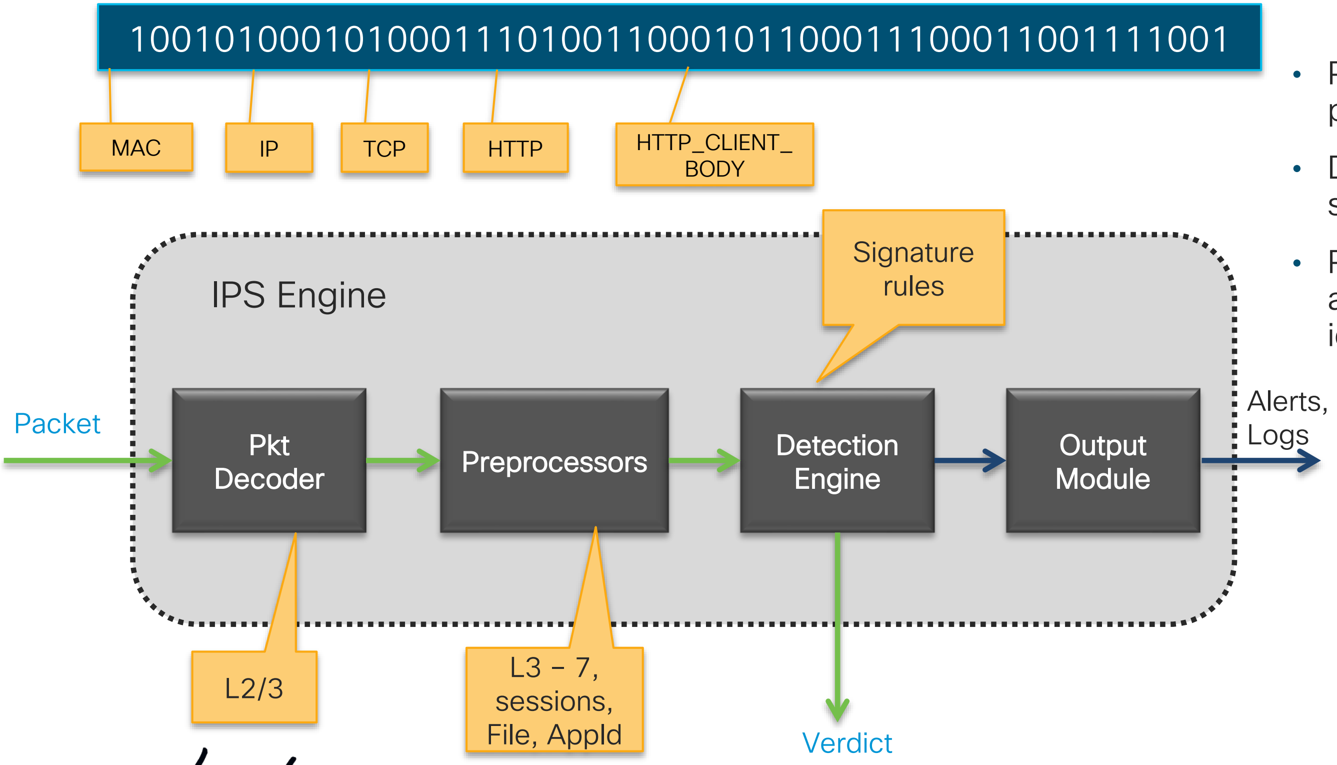


Next-Gen Firewall

- Deep inspection
- Stateful inspection
- Application identification by L7 inspection
- Directional control
- User Id / Context based policy
- Intrusion Prevention
- URL/DNS/Web Content Filtering
- Anti-Malware / Anti-Virus
- Advanced logging / alerting
- SIEM Integration
- TLS/SSL Inspection
- Threat Intel Integration

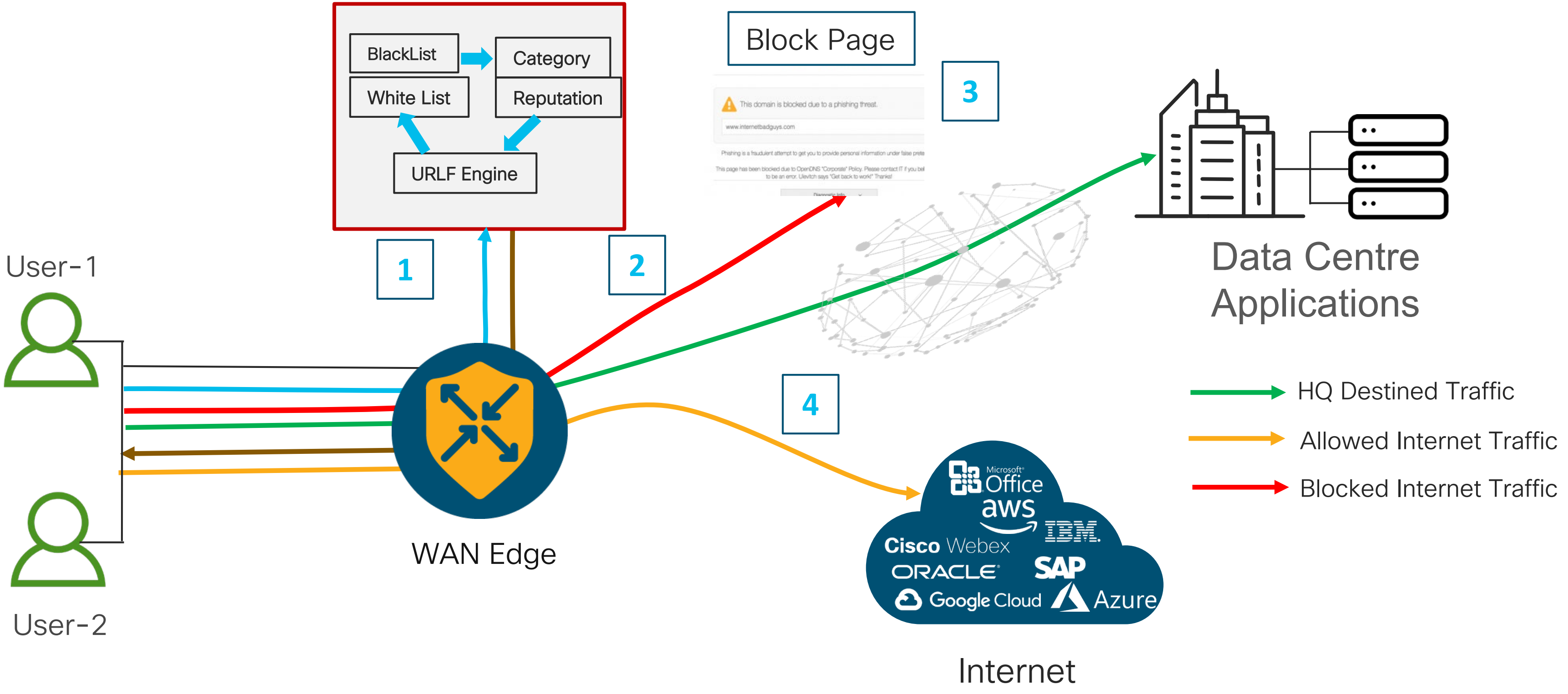
Intrusion Detection/Prevention System (IDS/IPS)

```
drop tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC User-Agent known malicious user agent - SAH Agent";
flow:to_server,established; content:"User-Agent|3A| SAH Agent"; fast_pattern:only; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy
security-ips drop, service http; classtype:misc-activity; sid:5808; rev:10;)
```



- Protocol engines check for protocol level misbehaviours
- Detection engine matches attack signatures
- Rules (Signatures) are updated as and when new attacks are identified

URL-Filtering Solution Overview



This domain is blocked due to a phishing threat.

www.internetbadguys.com

Phishing is a fraudulent attempt to get you to provide personal information under false prete

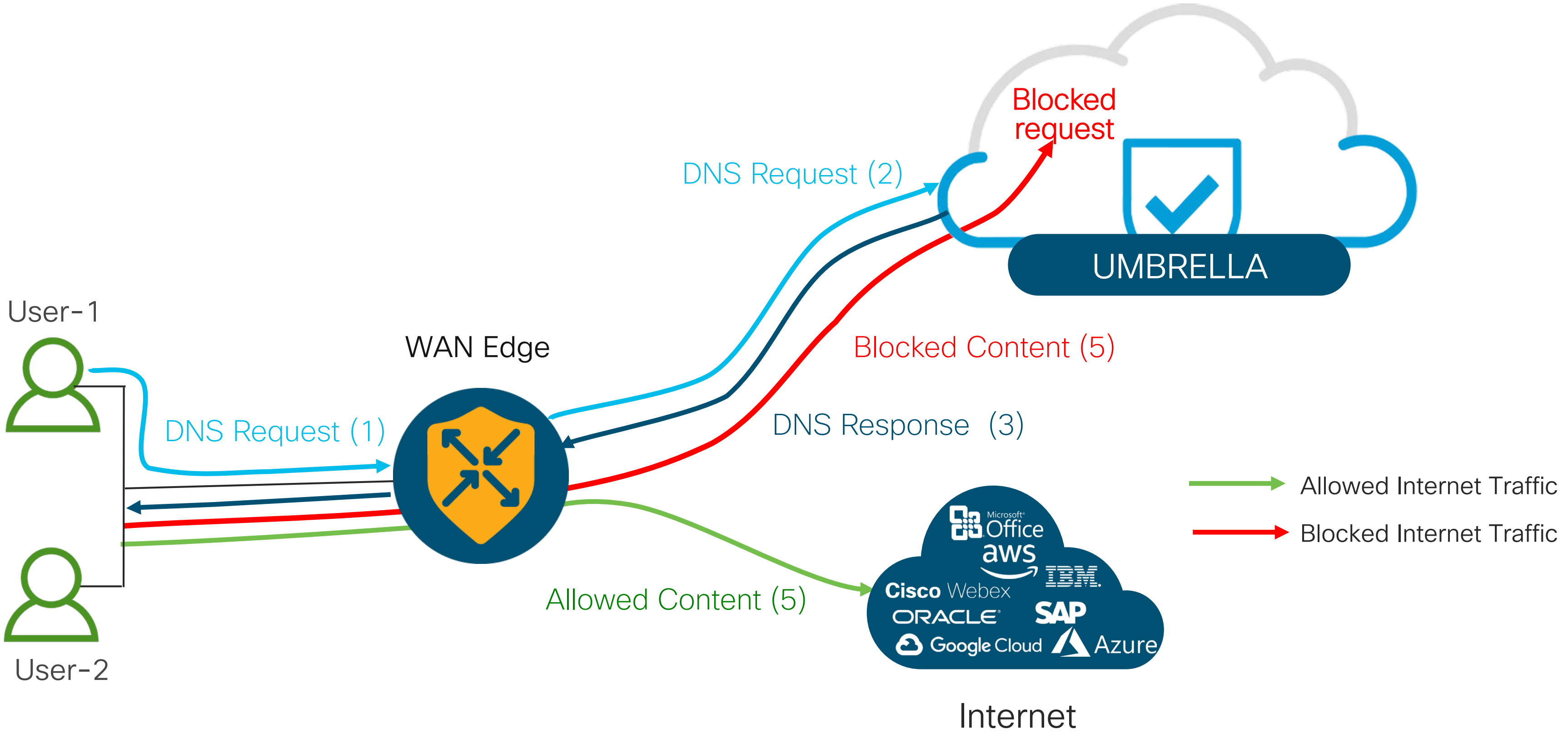
This page has been blocked due to OpenDNS "Corporate" Policy. Please contact IT if you bel
to be an error. Ulevitch says "Get back to work!" Thanks!

HQ Destined Traffic

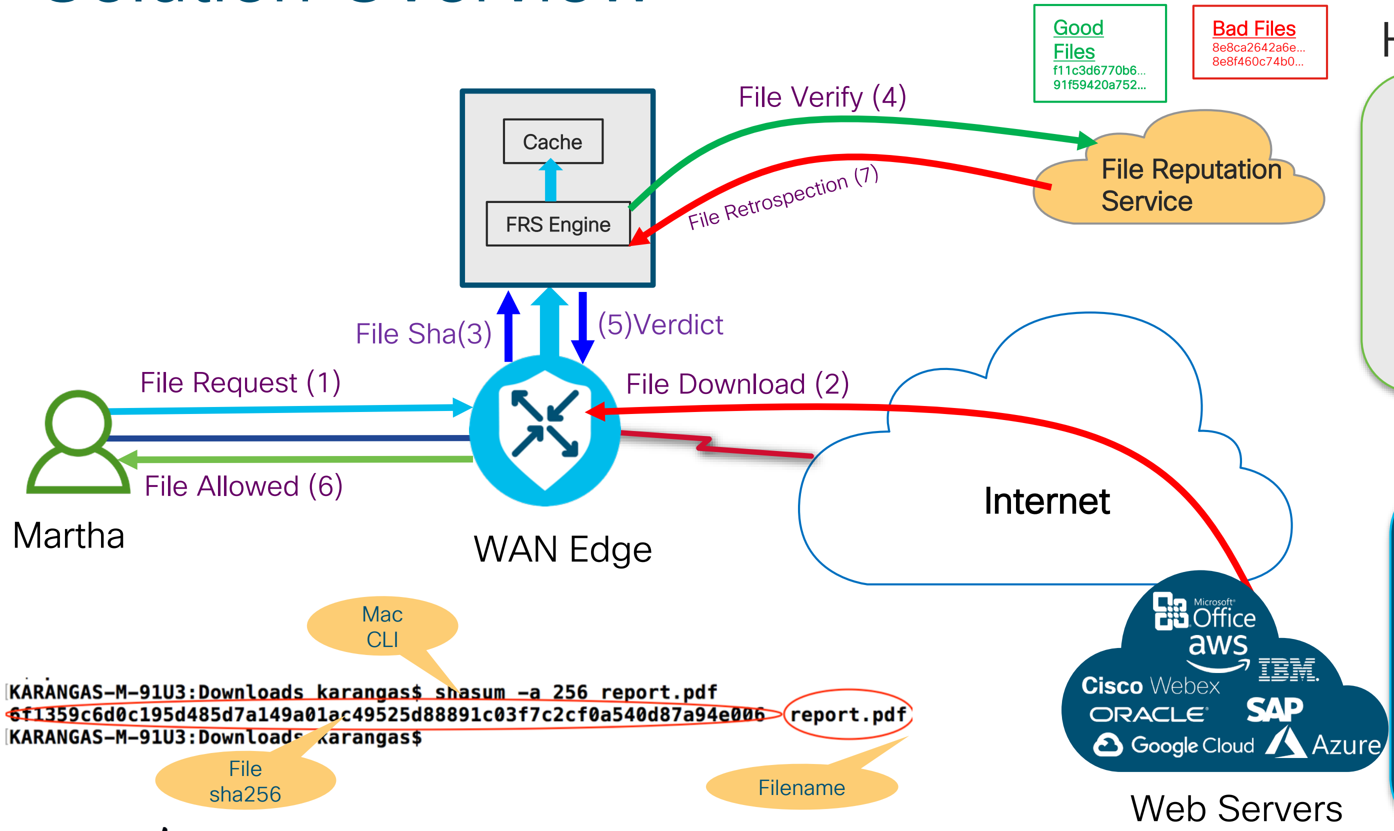
Allowed Internet Traffic

Blocked Internet Traffic

DNS-Filtering Solution Overview



File Reputation & Retrospection Service – Solution Overview



```
KARANGAS-M-91U3:Downloads karangas$ shasum -a 256 report.pdf
6f1359c6d0c195d485d7a149a01ac49525d88891c03f7c2cf0a540d87a94e006  report.pdf
KARANGAS-M-91U3:Downloads karangas$
```

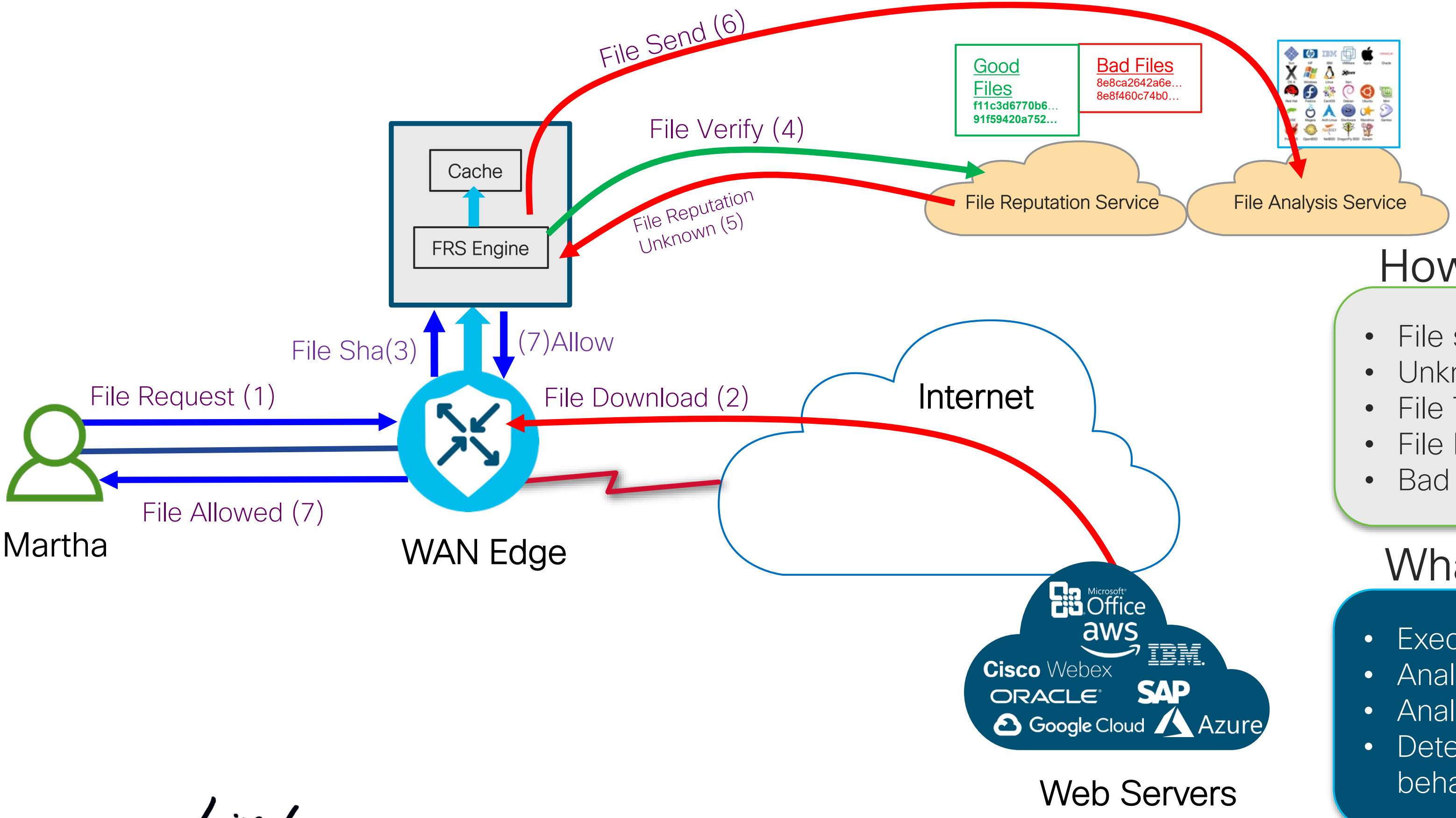
How it works?

- File download intercepted
- File sha calculate
- Reputation lookup
- File released or blocked
- Local or Cloud Database

What it does?

- File Sha match
- Good or Bad Files Database
- Known bad files blocked
- File Database updated frequently
- File Retrospection

File Analysis (Sandbox) – Solution Overview



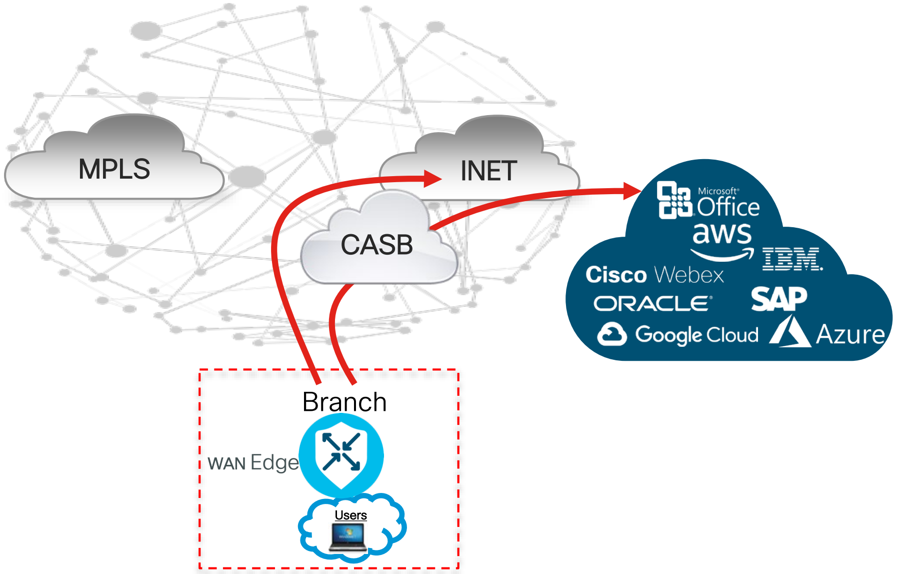
How it works?

- File sha lookup
- Unknown Reputation
- File Transfer to FAS
- File Runs in a virtual env.
- Bad files blocked

What it does?

- Execute file in a VM
- Analyze file execution
- Analyze file content
- Detect Malicious behavior

Cloud Access Security Broker (CASB) – Solution Overview



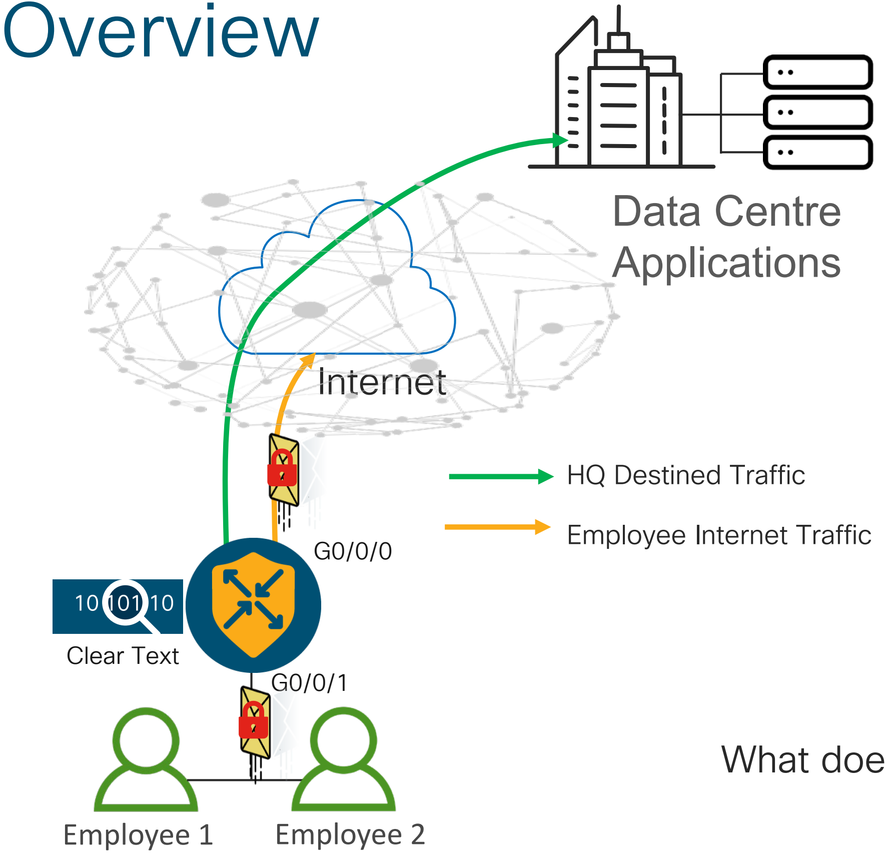
How it works?

- Forward Proxy
- Reverse Proxy
- API Node

What it does?

- Visibility
- Policy Compliance
- Security
  - Authentication
  - Authorization
  - Device Profiling
  - Encryption
  - Data Loss Prevention
- Malware Prevention

TLS/SSL Decryption (MiTM Proxy)– Solution Overview



Why do you need it ?

- More Apps/Data-cloud hosted
- Internet going dark
- >80% Internet traffic encrypted
- Lack of security control
- Malwares hidden in encrypted traffic

How does it work?

- URL request intercepted
- Server certificate checked
- Proxy resigns server Certificate
- User traffic redirected via proxy
- Decrypt and inspect
- Re-encrypt and send

What does it do?

- Proxy runs a cert signing authority
- Re-signs server certificate
- Redirects traffic through security stack
- Enforce security control
- Inspect for malware

Manage in Cloud or On-Prem

Single Pane of Glass

- Provision
- Manage
- Monitor
- Report
- Troubleshoot

Full Edge Security

Embedded

- Ent. Firewall App Aware
- IPS
- URL-Filtering
- AMP and Threat Grid

Cloud

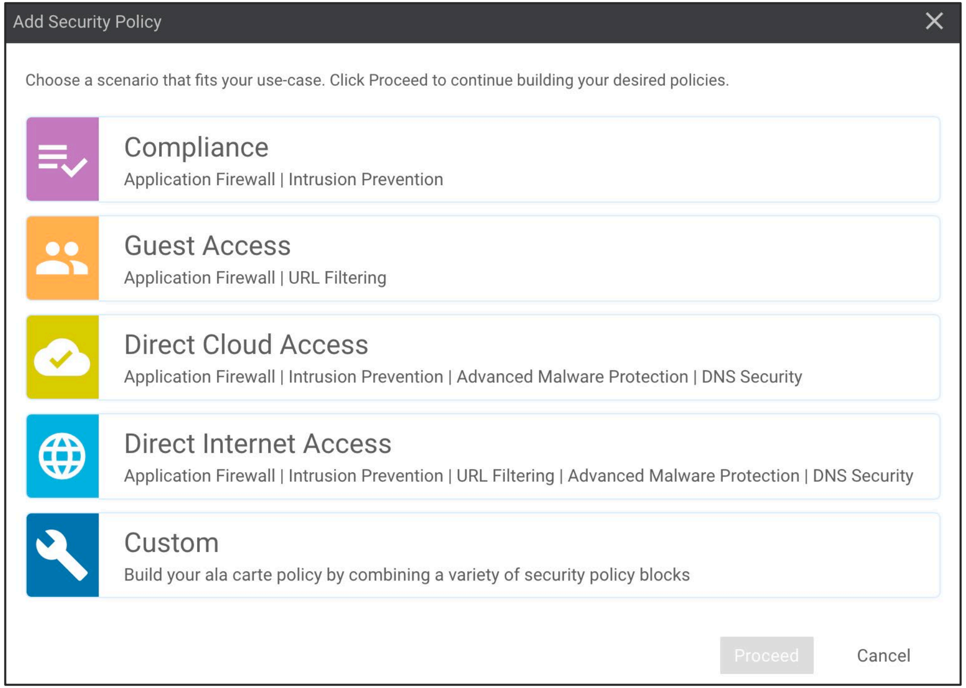
- DNS/web-layer Security
- Secure Internet Gateway

Edge Router Flexibility

Platforms

- ISR 1K
- ISR 4K
- ENCS (ISRv)
- CSR
- ASR 1K (Ent FW App Aware and DNS/web-layer security)
- vEdges (FW and DNS/web-layer security)

SD-WAN Security: vManage Provisioning Wizard



Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- **Compliance**
  Application Firewall | Intrusion Prevention
- **Guest Access**
  Application Firewall | URL Filtering
- **Direct Cloud Access**
  Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security
- **Direct Internet Access**
  Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security
- **Custom**
  Build your ala carte policy by combining a variety of security policy blocks

Proceed Cancel

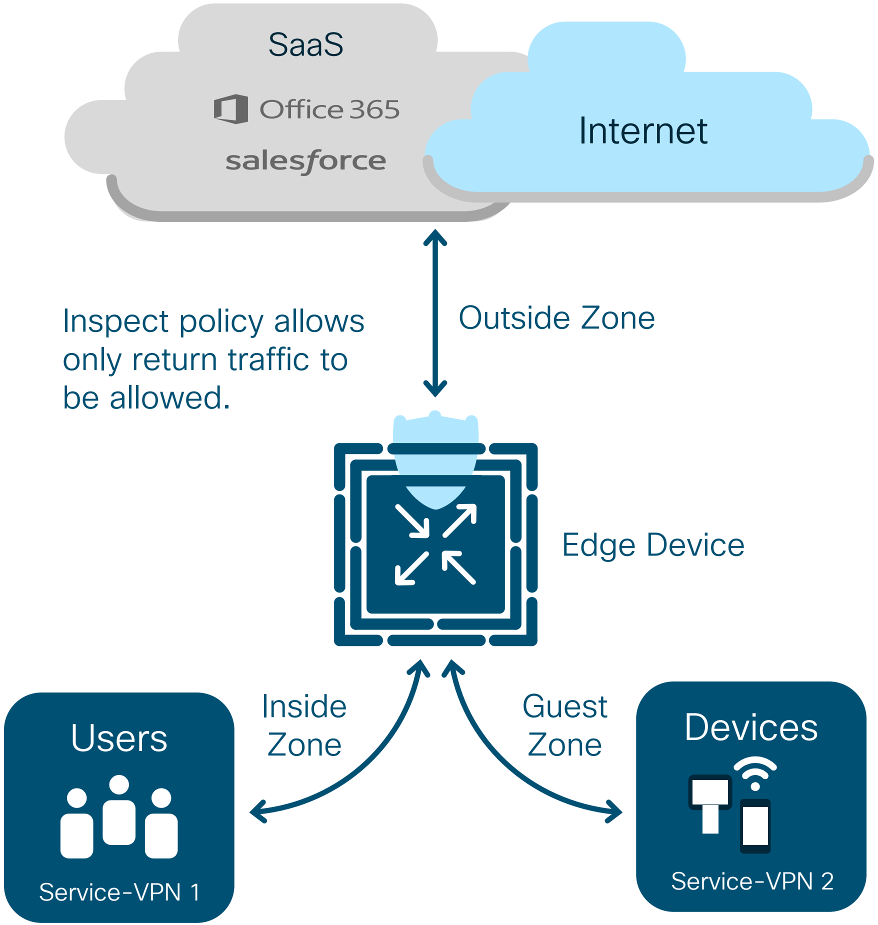
Configuration > Security

⊕ Add Security Policy

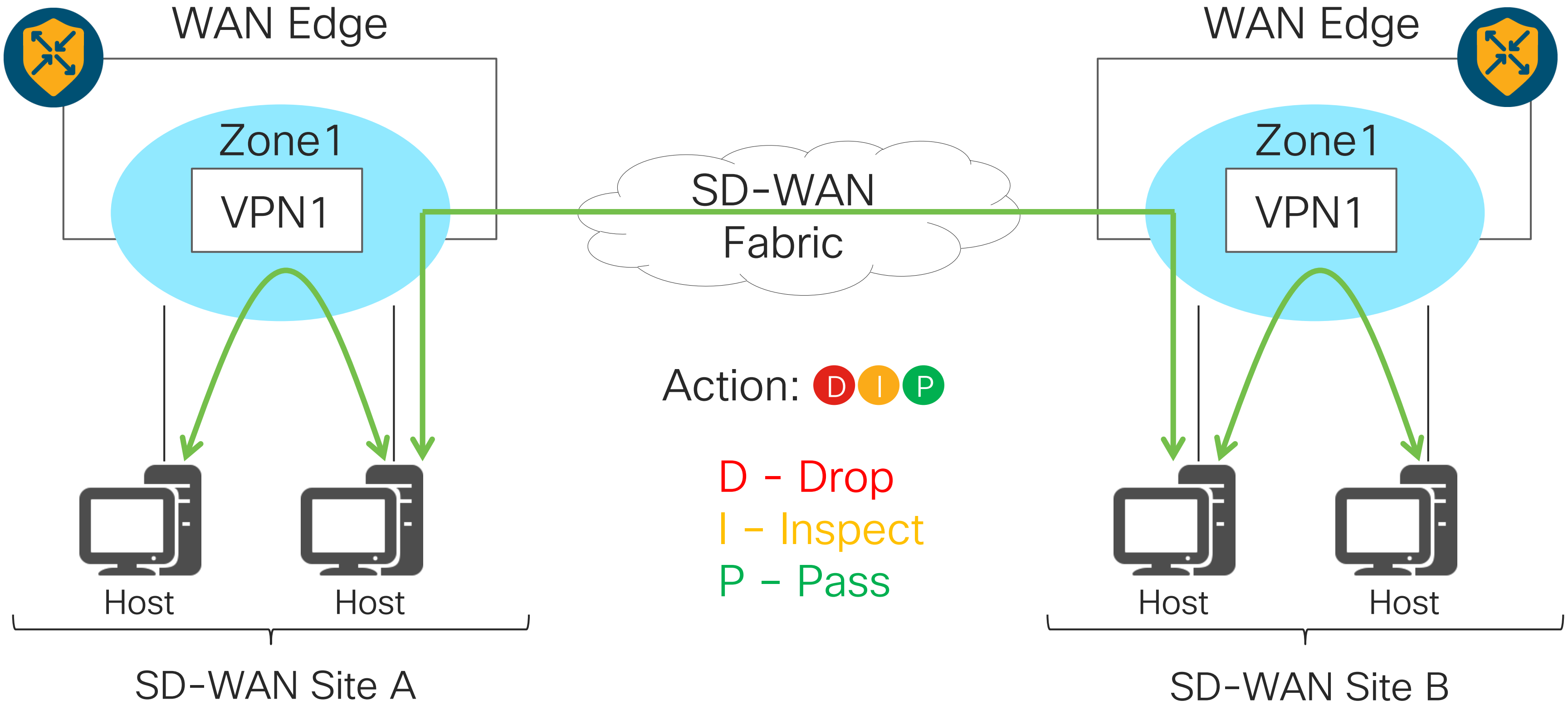
Enterprise App Aware Firewall

Enterprise App Firewall

- Stateful Firewall, Zone Policies
- Application Visibility and Granular control
- 1400+ layer 7 applications classified
- Drop traffic by application category or specific application
- Segmentation
- PCI compliance
- HSL Logging
- Self Zone Policy



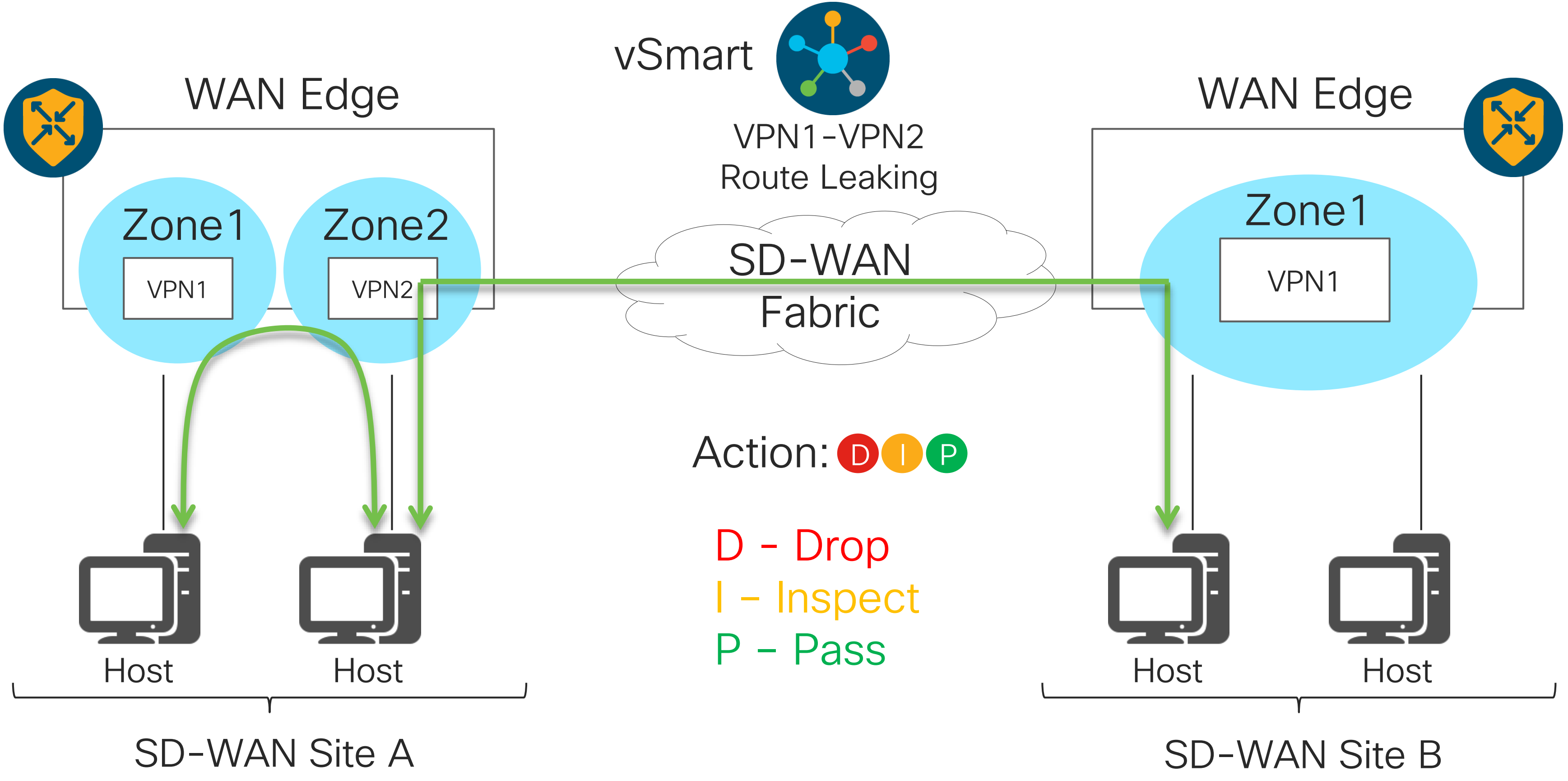
Ent. Firewall App Aware: Intra-Zone Security



Action: D I P

D - Drop
I - Inspect
P - Pass

Ent. Firewall App Aware : Inter-Zone Security



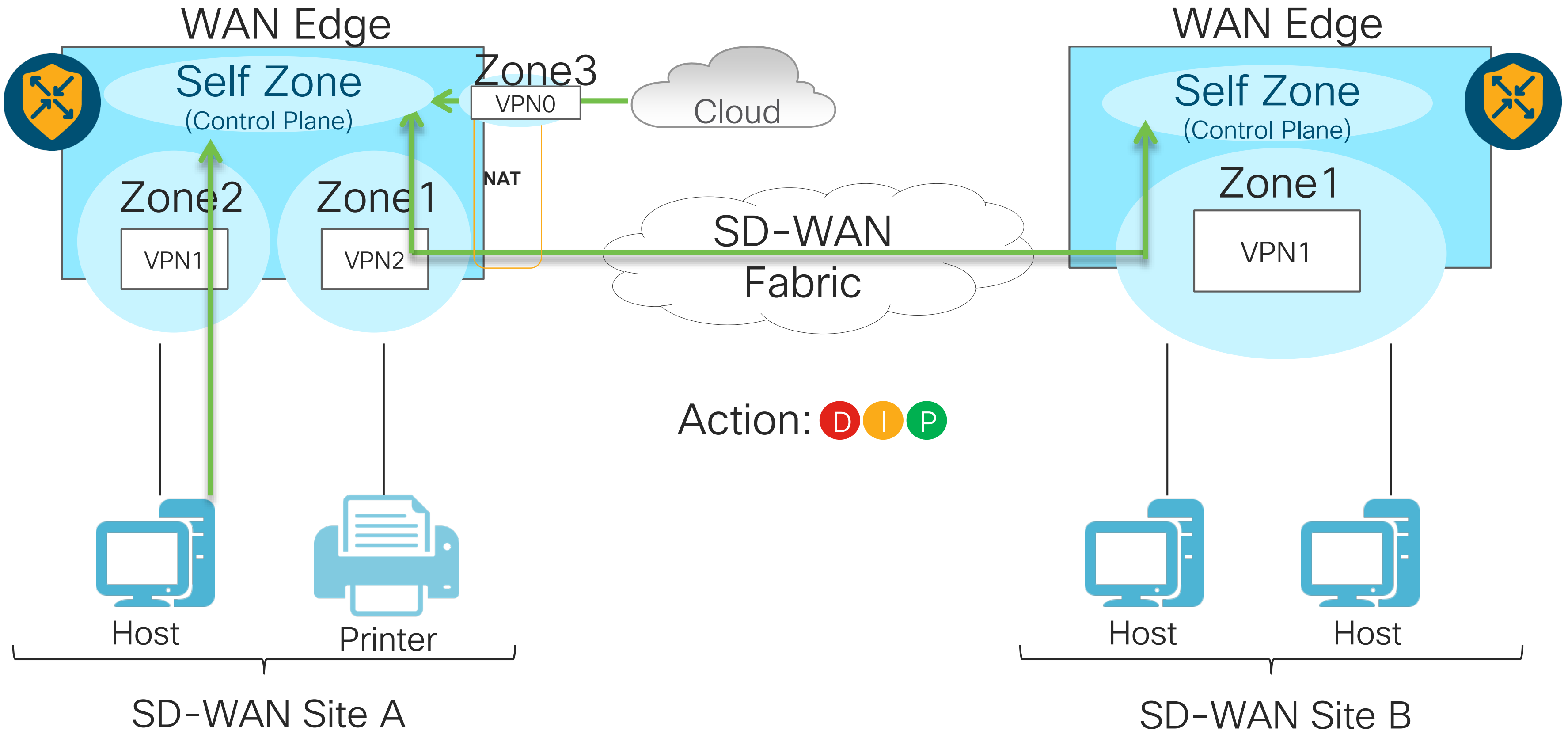
Action: D I P

D - Drop

I - Inspect

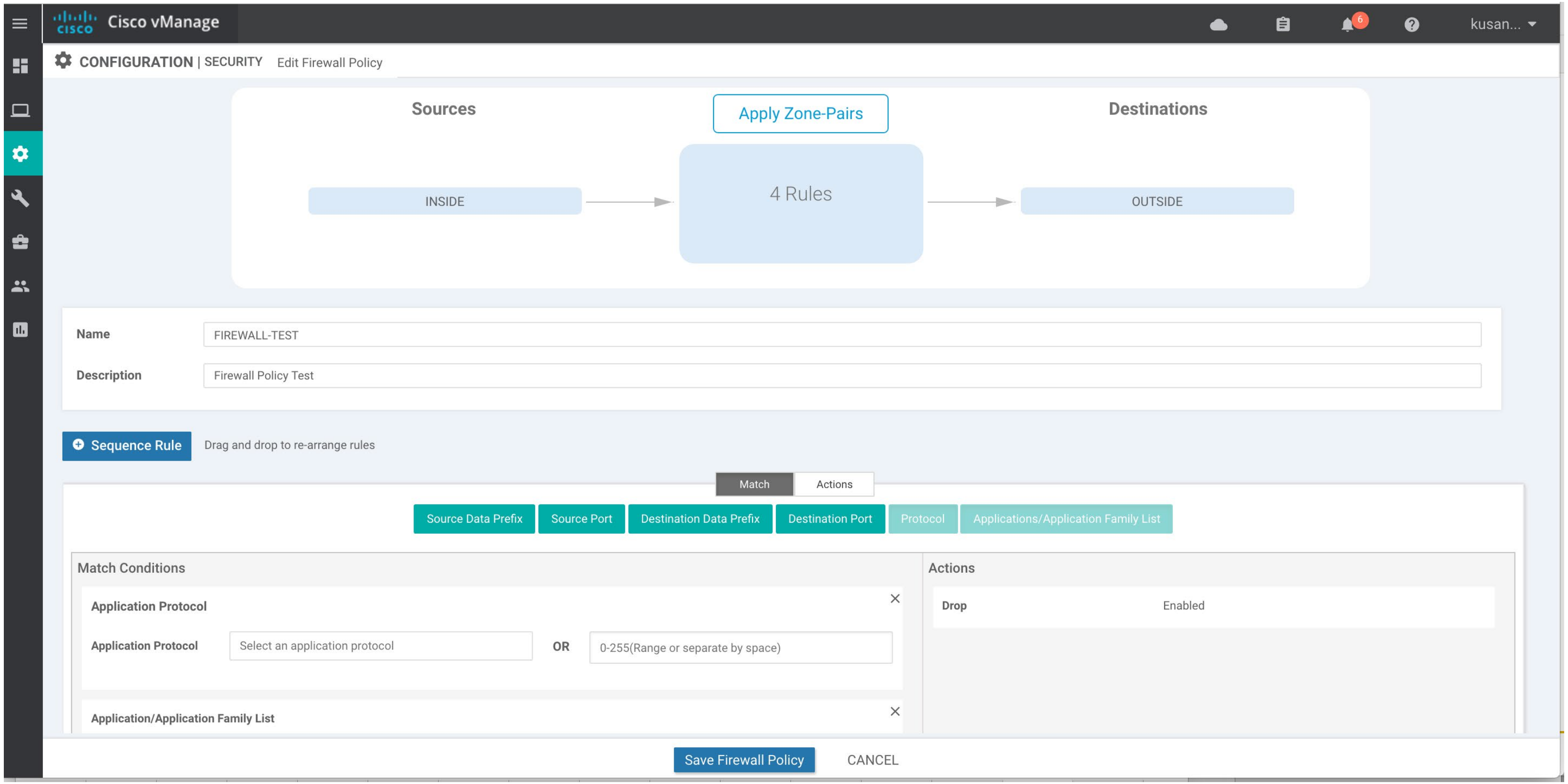
P - Pass

Ent. Firewall App Aware : Self-Zone Security



vManage - Ent FW App Aware - Configuration

For Your Reference



Name: FIREWALL-TEST

Description: Firewall Policy Test

Match Conditions

Application Protocol

Application Protocol: Select an application protocol OR 0-255(Range or separate by space)

Application/Application Family List

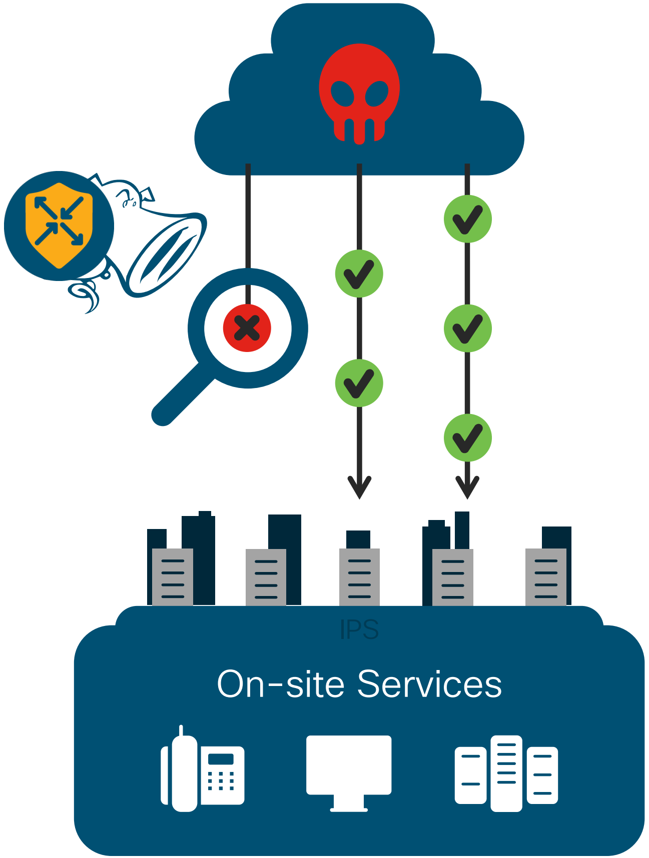
Actions

Drop: Enabled

Intrusion Prevention

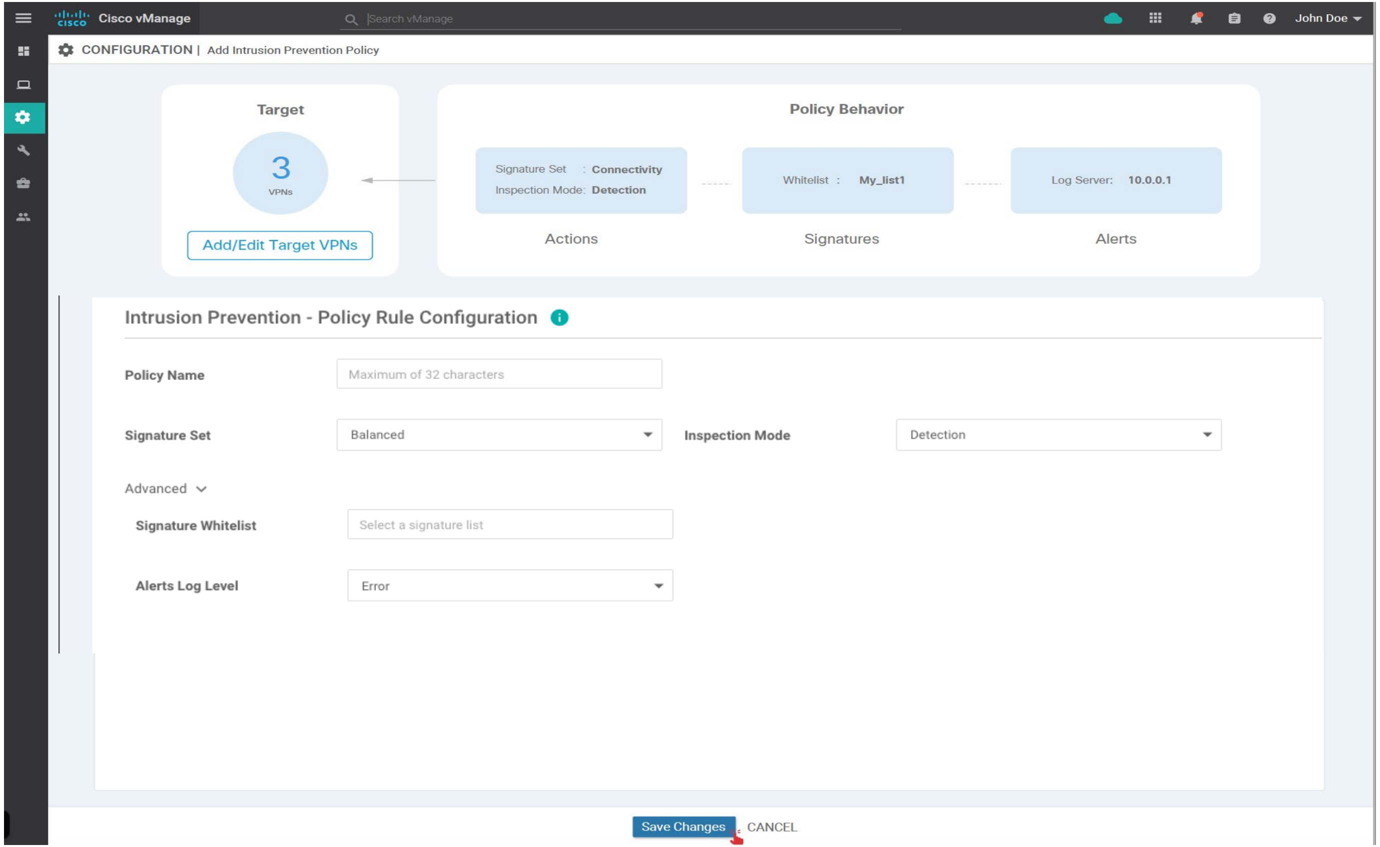
Intrusion Prevention

- Snort is the most widely deployed
- Intrusion Prevention solution in the world
- Backed by global threat intelligence (TALOS), signature update is automated
- Signature whitelist support
- Real-time traffic analysis
- PCI compliance



vManage - Intrusion Prevention

For Your Reference



CONFIGURATION | Add Intrusion Prevention Policy

Target

3 VPNs

Policy Behavior

Signature Set : Connectivity
Inspection Mode: Detection

Whitelist : My_list1

Log Server: 10.0.0.1

Actions

Signatures

Alerts

Intrusion Prevention - Policy Rule Configuration

Policy Name: Maximum of 32 characters

Signature Set: Balanced

Inspection Mode: Detection

Advanced

Signature Whitelist: Select a signature list

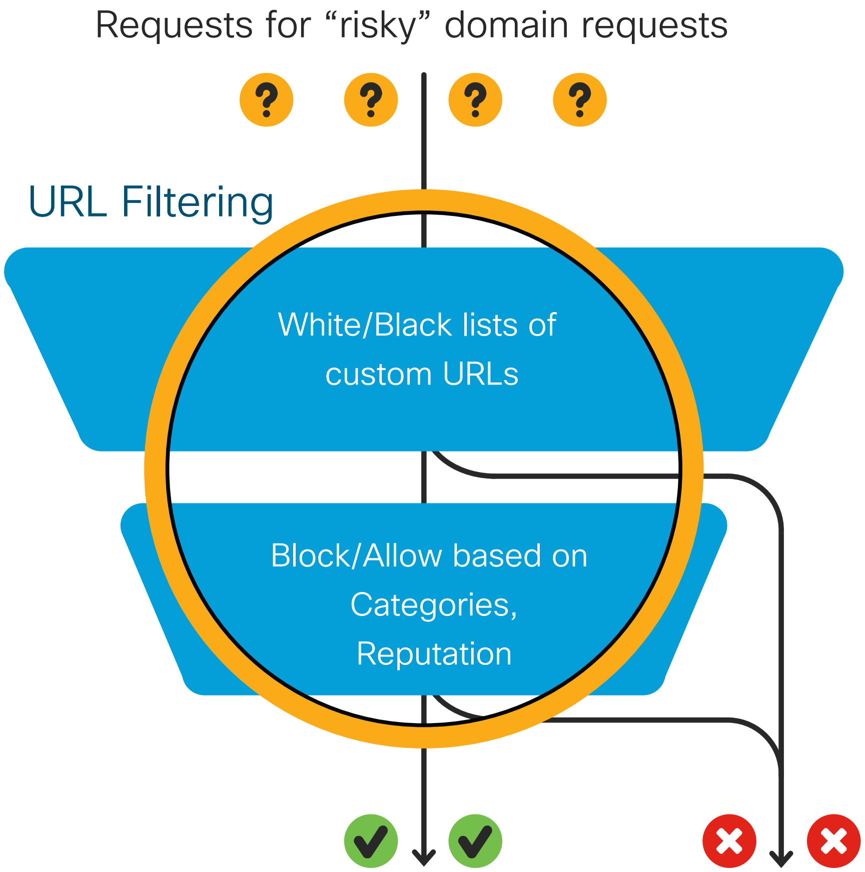
Alerts Log Level: Error

cisco Live!

URL Filtering

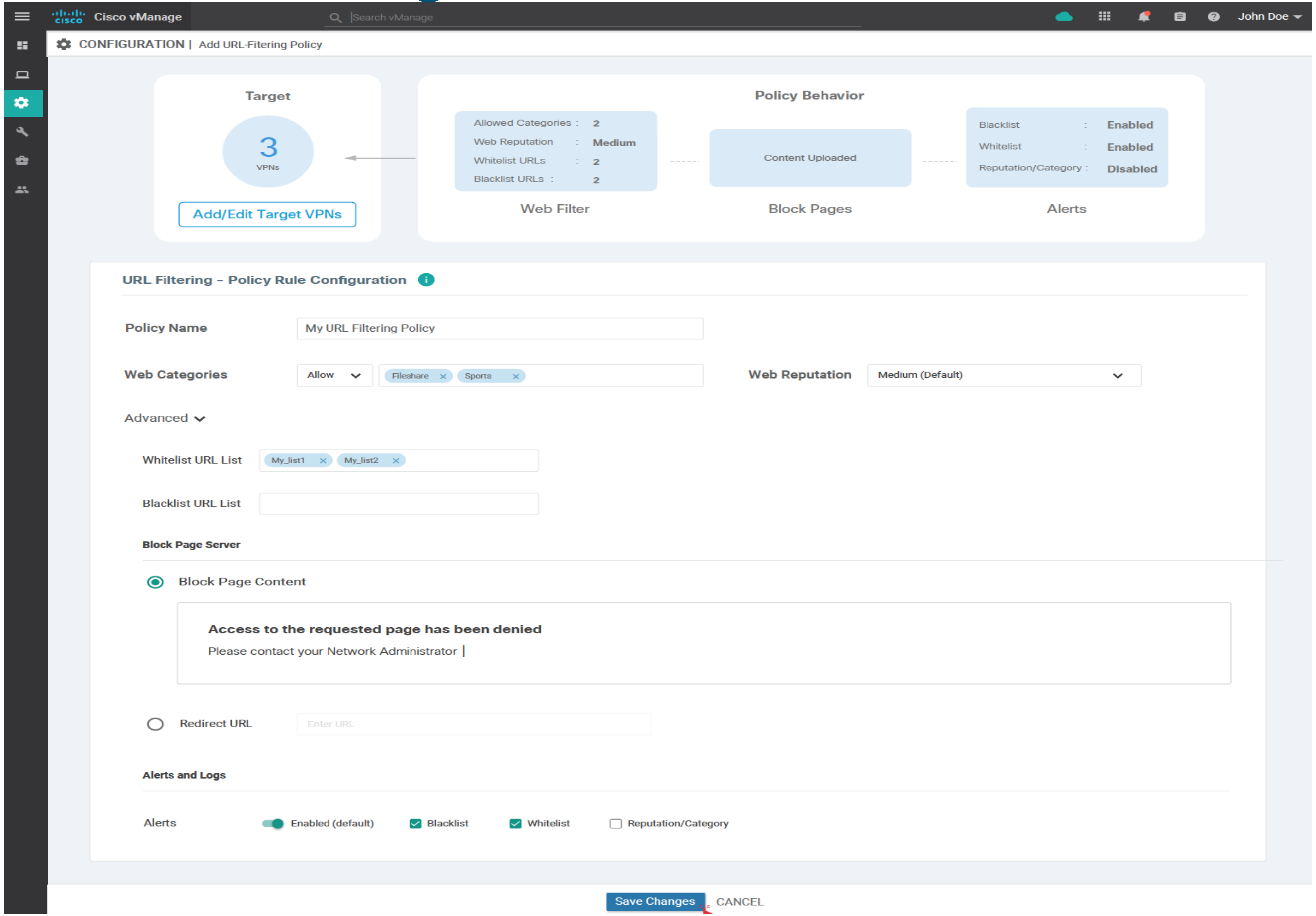
URL Filtering

- 82+ Web Categories with dynamic updates
- Block based on Web Reputation score
- Create custom Black and White Lists
- Customizable End-user notifications


Requests for “risky” domain requests
URL Filtering
White/Black lists of custom URLs
Block/Allow based on Categories, Reputation

vManage - URL Filtering

For Your Reference



CONFIGURATION | Add URL-Fitering Policy

Target

3 VPNs

Add/Edit Target VPNs

Policy Behavior

Web Filter

- Allowed Categories : 2
- Web Reputation : Medium
- Whitelist URLs : 2
- Blacklist URLs : 2

Block Pages

Content Uploaded

Alerts

- Blacklist : Enabled
- Whitelist : Enabled
- Reputation/Category : Disabled

URL Filtering - Policy Rule Configuration

Policy Name: My URL Filtering Policy

Web Categories: Allow — Fileshare ×, Sports ×

Web Reputation: Medium (Default)

Advanced

Whitelist URL List: My_list1 ×, My_list2 ×

Blacklist URL List:

Block Page Server

● Block Page Content

> **Access to the requested page has been denied**
> Please contact your Network Administrator |

○ Redirect URL — Enter URL

Alerts and Logs

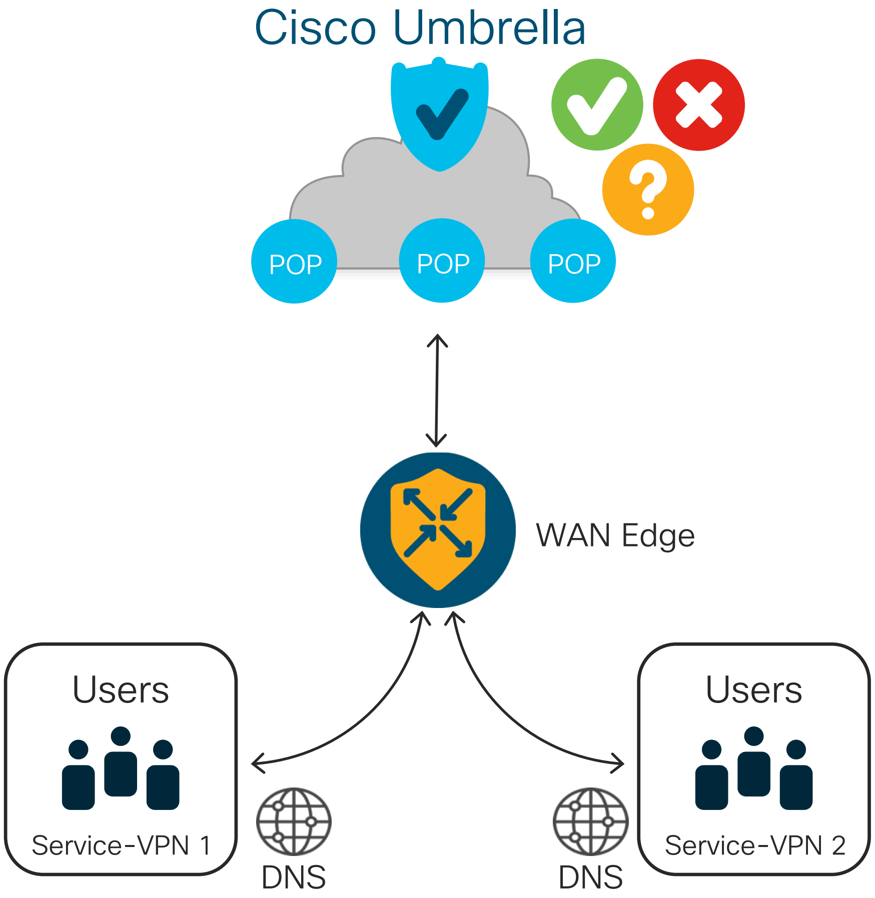
Alerts: Enabled (default) ☑ Blacklist ☑ Whitelist □ Reputation/Category

Save Changes CANCEL

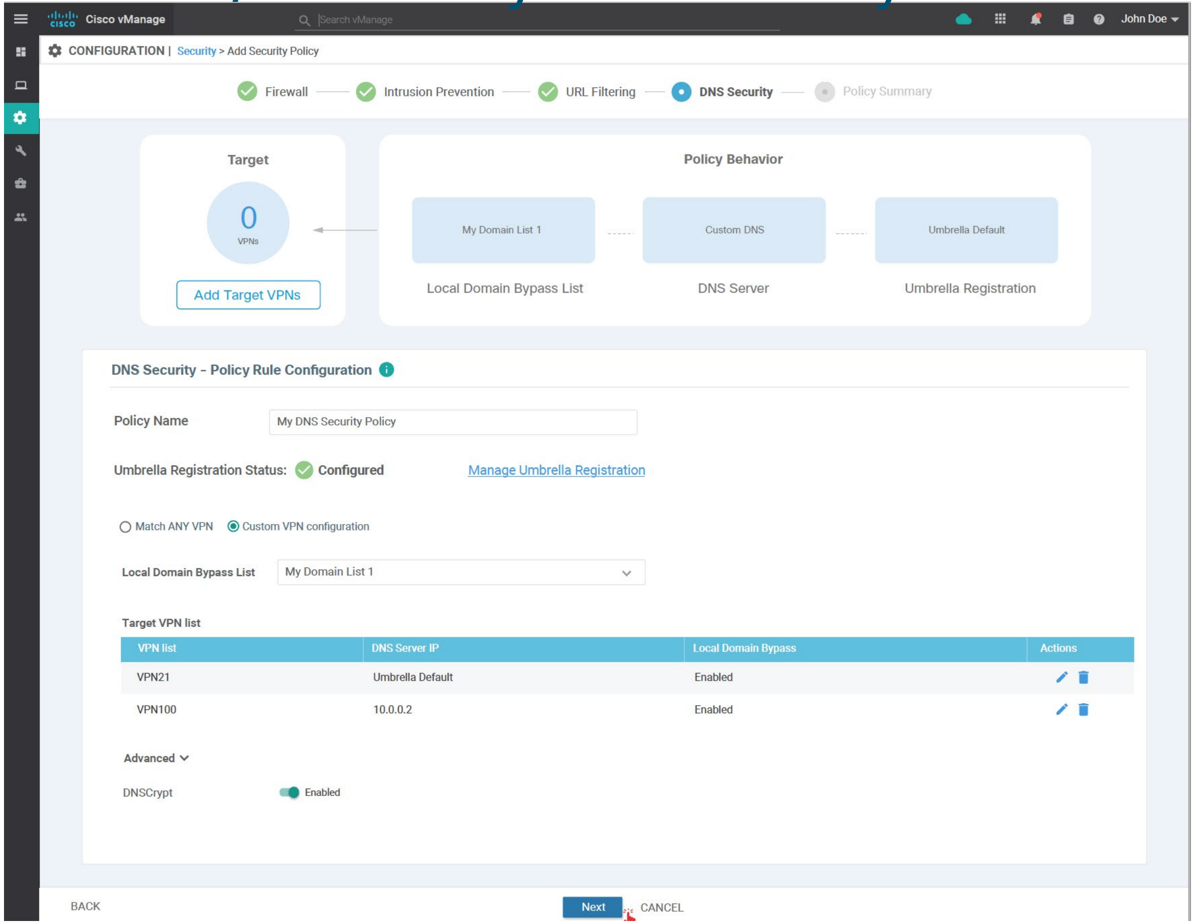
DNS/web-layer Security

DNS/web-layer security

- Block malware, phishing, and non-compliance domain requests
- Automatic API Key registration
- Supports DNScrypt
- VPN-aware policies
- Local Domain-bypass
- TLS decryption
- Intelligent Proxy



vManage – DNS/web-layer Security



DNS Security - Policy Rule Configuration

Policy Name: My DNS Security Policy

Umbrella Registration Status: ✓ Configured   Manage Umbrella Registration

○ Match ANY VPN ● Custom VPN configuration

Local Domain Bypass List: My Domain List 1

Target VPN list

VPN list	DNS Server IP	Local Domain Bypass	Actions
VPN21	Umbrella Default	Enabled	
VPN100	10.0.0.2	Enabled	

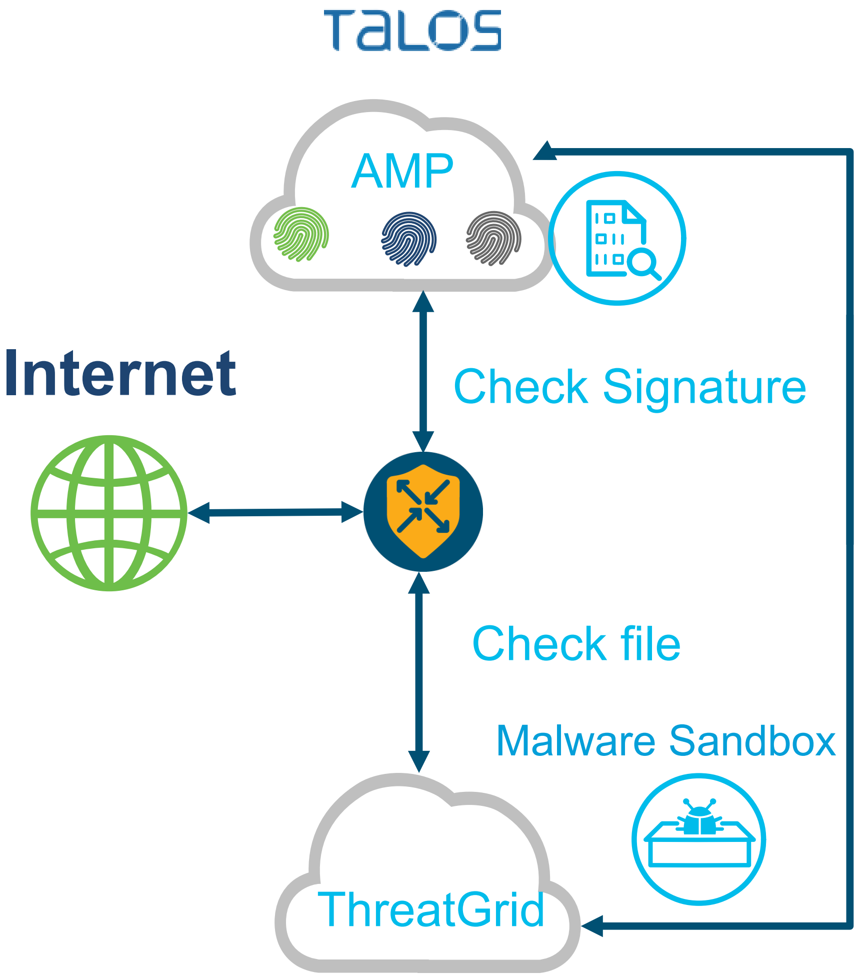
Advanced

DNSCrypt: Enabled

Advanced Malware Protection and Threat Grid

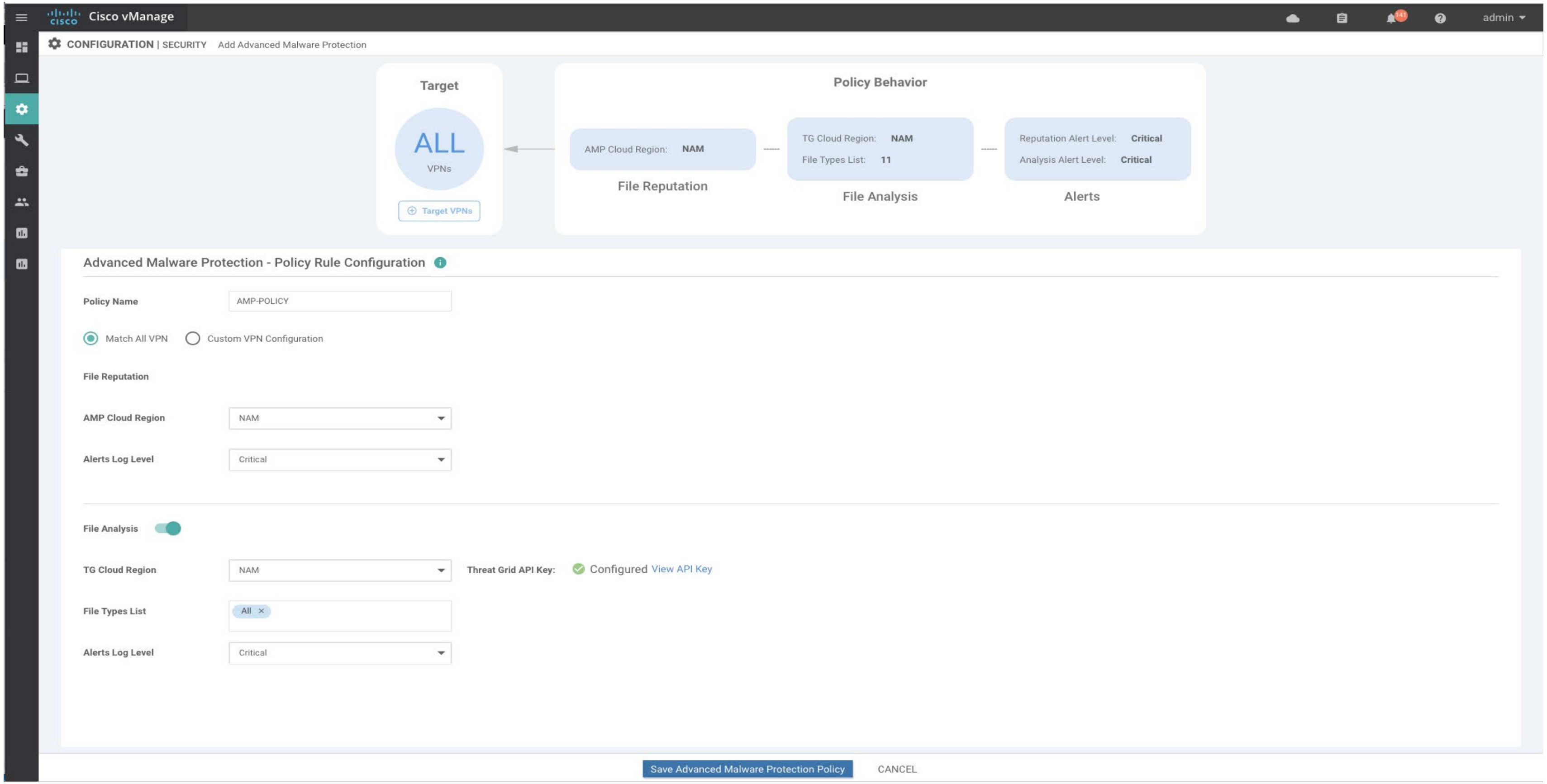
Advanced Malware Protection + Threat Grid

- Integration with AMP
  - File reputation
  - File retrospection
- Integration with ThreatGrid
  - File Analysis
- Inspects traffic in VPNs of interest
- Leverages Snort engine to identify file transfers



vManage – AMP + ThreatGrid

For Your Reference



Cisco vManage
admin
CONFIGURATION | SECURITY Add Advanced Malware Protection
Target
ALL
VPNs
Target VPNs
Policy Behavior
AMP Cloud Region: NAM
File Reputation
TG Cloud Region: NAM
File Types List: 11
File Analysis
Reputation Alert Level: Critical
Analysis Alert Level: Critical
Alerts

Advanced Malware Protection - Policy Rule Configuration

Policy Name: AMP-POLICY

● Match All VPN ○ Custom VPN Configuration

File Reputation

AMP Cloud Region: NAM

Alerts Log Level: Critical

File Analysis: On

TG Cloud Region: NAM

Threat Grid API Key: ✓ Configured View API Key

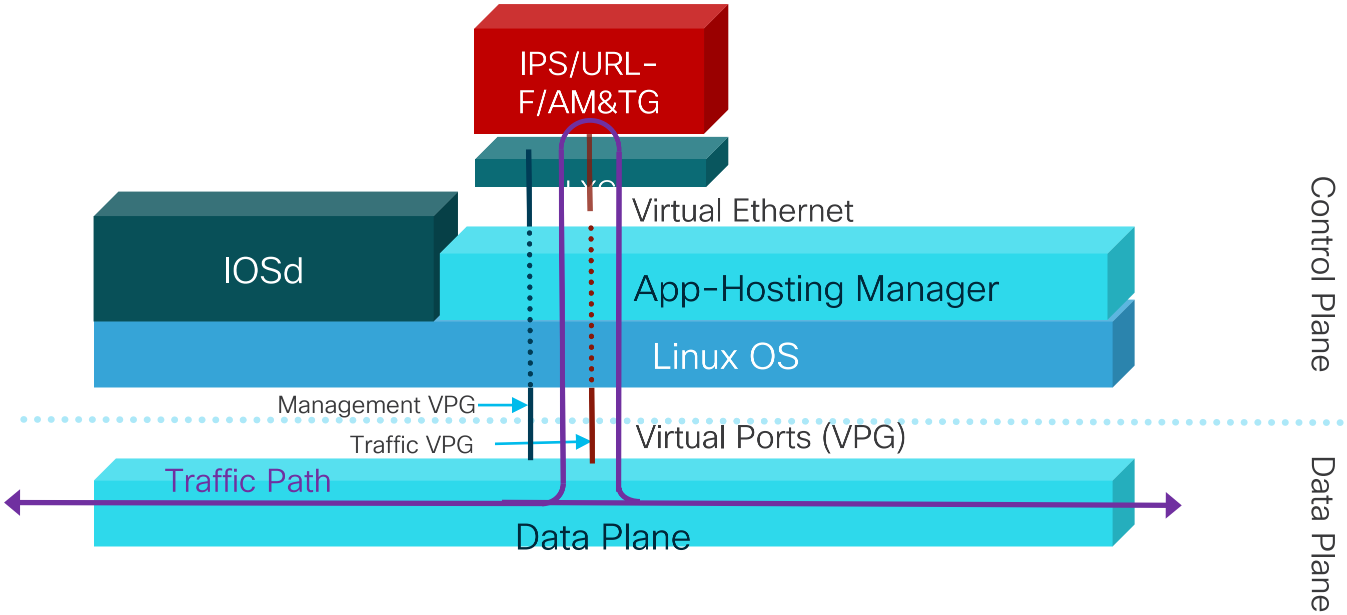
File Types List: All ×

Alerts Log Level: Critical

Save Advanced Malware Protection Policy
CANCEL

IPS, URL-F & AMP Architecture

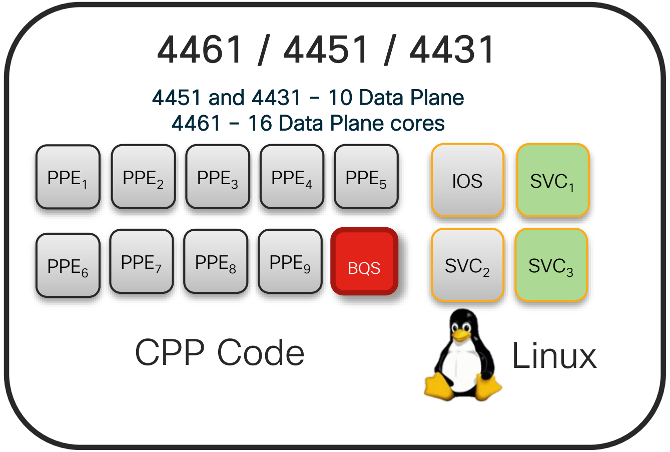
For Your Reference

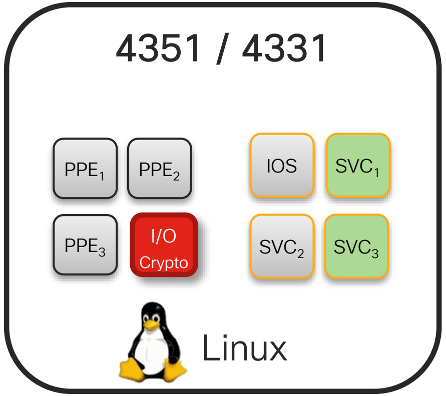


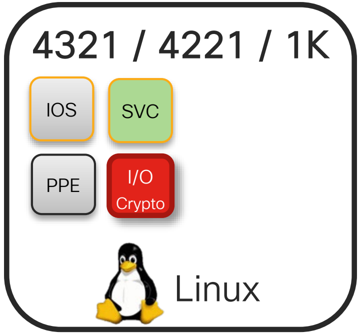
- IPS, AMP & URL Filtering services runs on a Linux Container (LXC), using control plane resources
- Traffic is punted to Container using Virtual Port Group (VPG) interface
- Reserved CPU and memory for Container process enables deterministic performance

Security App Hosting Profile & Resources

For Your Reference







Platforms	Total No of DP Cores	Total No of CP Cores	Total No of CP Cores for Security
4321/4221/1K	2	2	1
4331	4	4	2
4351	4	4	2
4431	6	4	2
4451	10	4	2
4461	16	4	2

DP = Data Plane
CP = Control Plane
SVC = Services

SD-WAN Security Support

For Your Reference

Platforms/Features	Ent FW	Ent FW App Awareness	IPS/IDS	URL Filtering	AMP/TG	DNS/web-layer security *
Viptela - (100, 1000, 2000, 5000 and 1100-4G/6G)	Y	N **	N/A	N/A	N/A	N
Cisco - CSR	Y	Y	Y	Y	Y	Y
Cisco – ENCS (ISRv)	Y	Y	Y	Y	Y	Y
Cisco – ISR4K (4461, 4451, 4431, 4351, 4331, 4321, 4221-X)	Y	Y	Y	Y	Y	Y
Cisco – ISR1K	Y	Y	Y	Y	Y	Y
Cisco - ASR1K 1001-HX, 1002-HX, 1001-X, 1002-X)***	Y	Y	N/A	N/A	NA	Y

* Umbrella Subscription required for enforcement

** Stateful Firewall and DPI using Qosmos are separate on the vEdges
Ent FW App Aware and DNS/web layer security is supported with default 4GB DRAM

Security App Hosting Profile & Resources

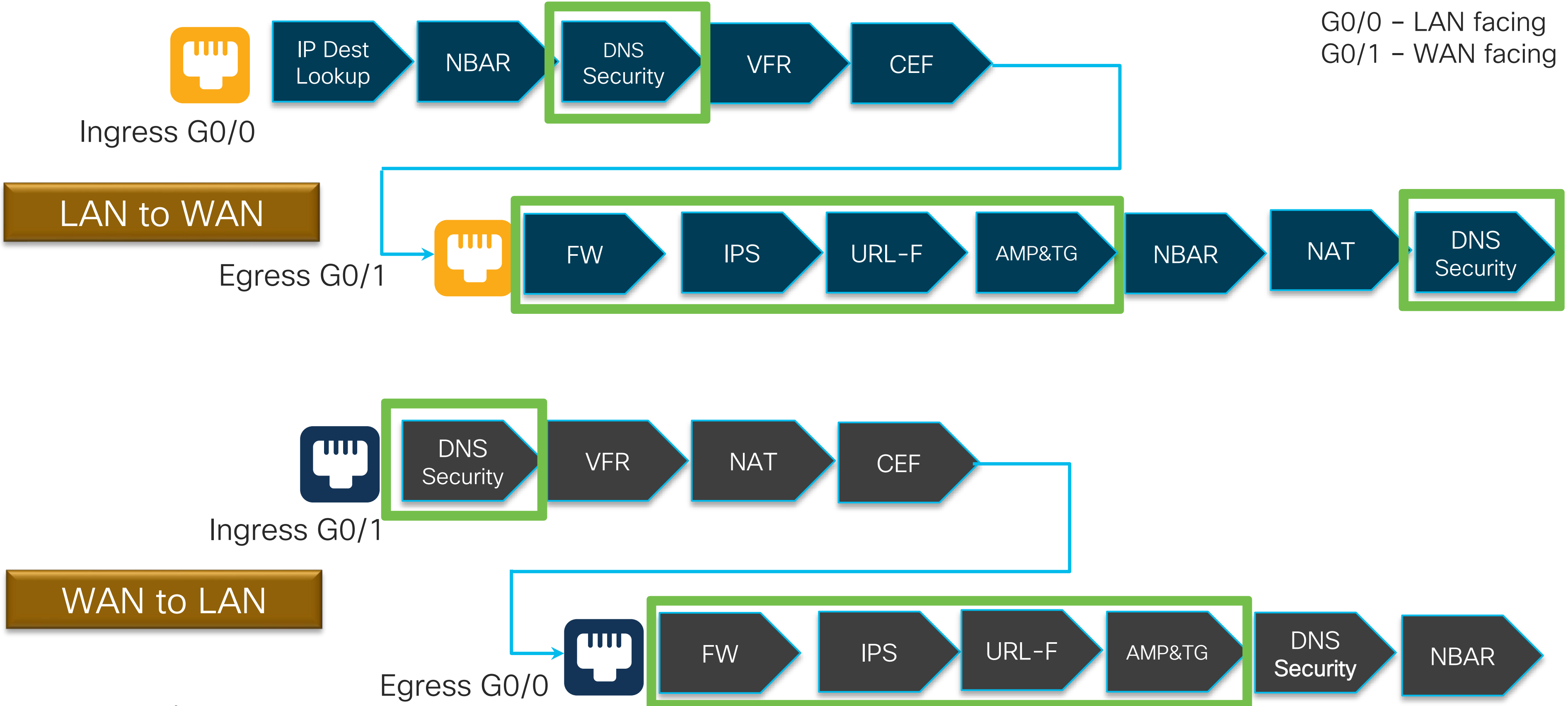
IPS / URL-F App Hosting Profile	Security Profile - Features	Minimum Platform requirement	Platform Supported
Default	IPS + URLF (Cloud Lookup only) + AMP (File hashing)	8GB Bootflash & 8GB Memory 1 / 2 service plane cores	ISR1K/4221X/4321 4331/4351/44xx 4/8vCPU CSR / ISRv
High	IPS + URLF (On-box DB + Cloud Lookup) + AMP (File hashing) + Threat Grid (TG)	16GB Bootflash & 16GB Memory 2 service plane cores	4331/4351/44xx 4/8vCPU CSR/ISRv

Enterprise FW and DNS/web-layer security will work with default 4 GB DRAM

SD-WAN Security Features – Order of Operation

For Your Reference

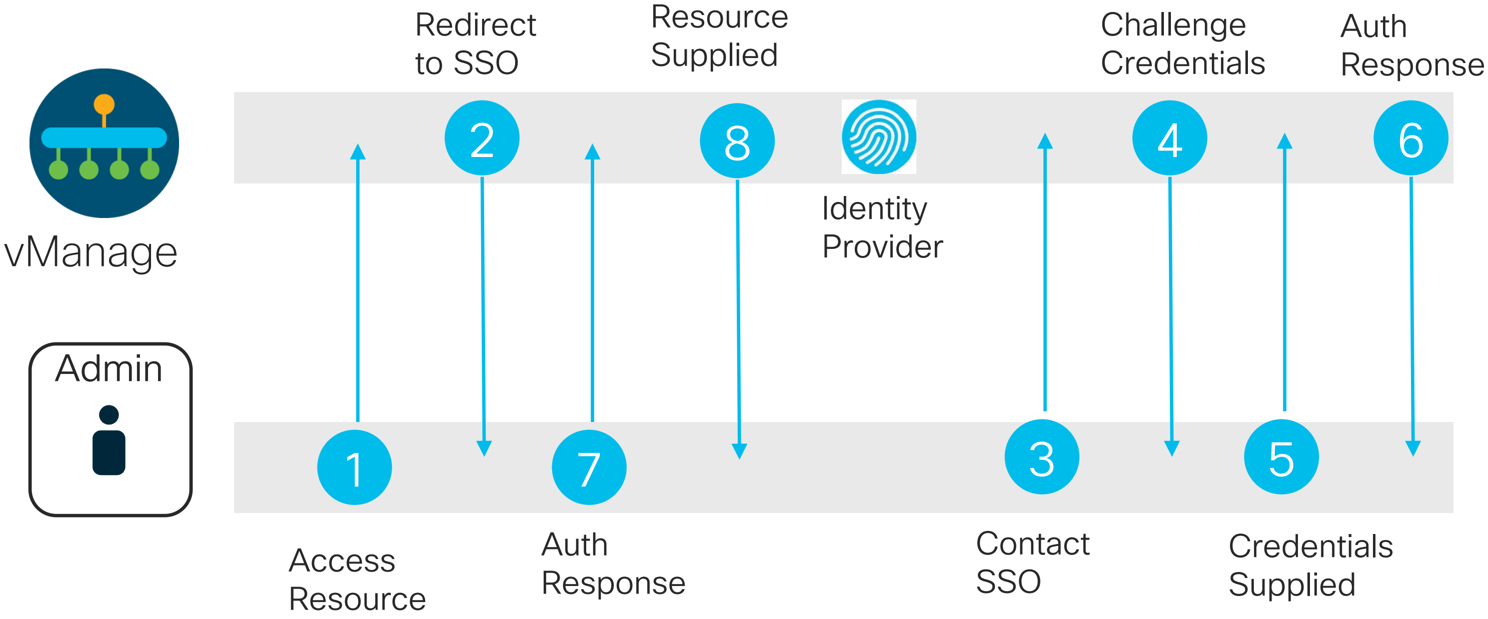
G0/0 – LAN facing
G0/1 – WAN facing



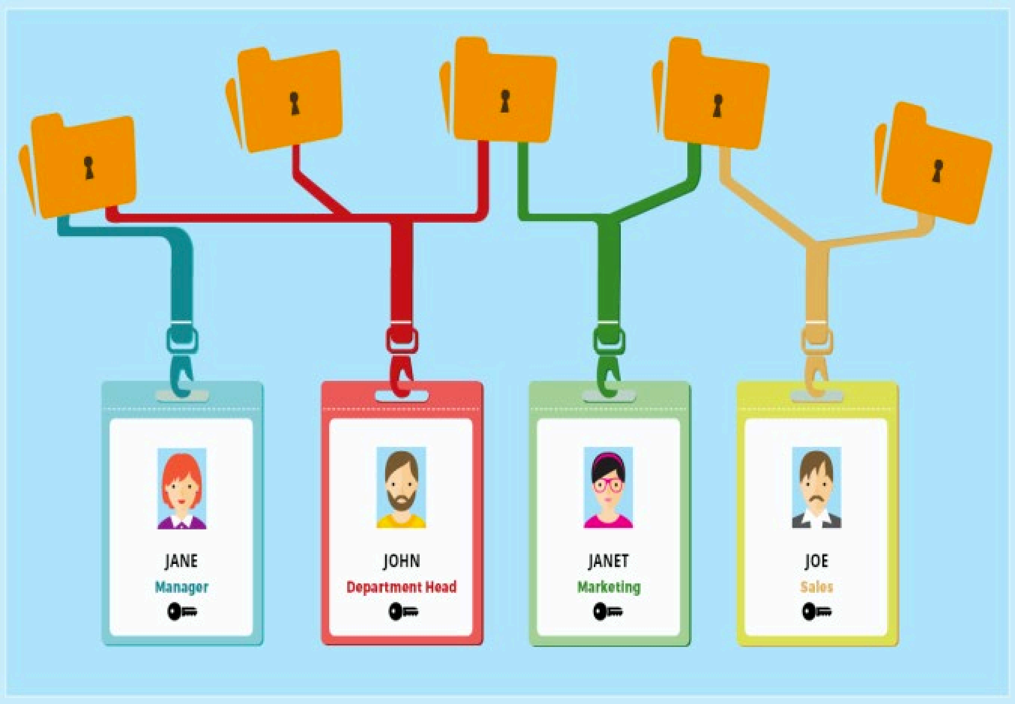
Secure Management

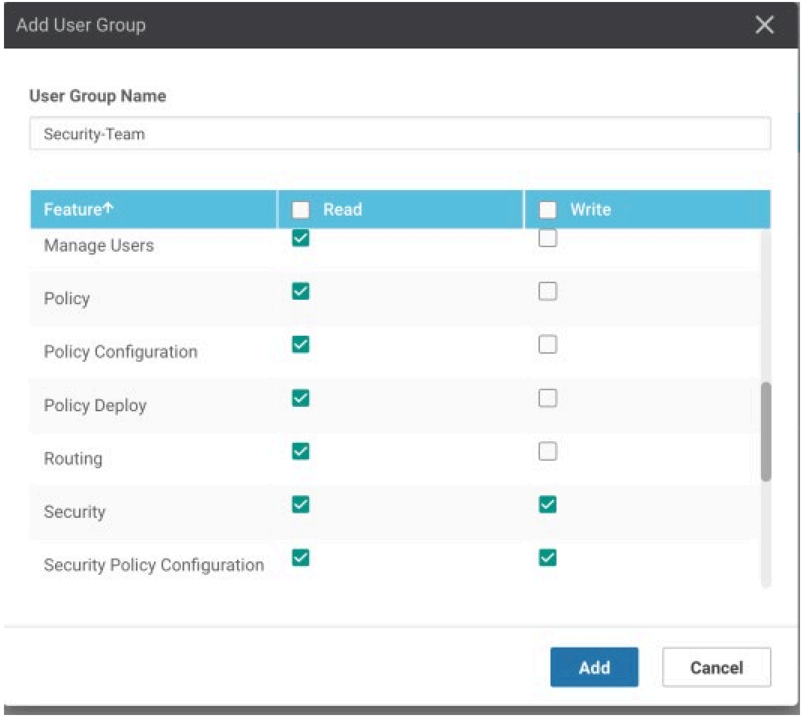
vManage Authentication methods

- Local Database / RADIUS / TACACS
- Single-Sign ON



RBAC





Add User Group ✕

User Group Name

Security-Team

Feature↑	□ Read	□ Write
Manage Users	☑	□
Policy	☑	□
Policy Configuration	☑	□
Policy Deploy	☑	□
Routing	☑	□
Security	☑	☑
Security Policy Configuration	☑	☑

RBAC by VPN Feature

For Your Reference

Admin user:

- Create VPN dashboards:
  - ✓ Create/discover VPN segments in a network
  - ✓ Create VPN groups
  - ✓ New VPN dashboard for each VPN group
- Create users with VPN group access:
  - ✓ Link user group to VPN group
  - ✓ Create users with access to VPN group

VPN group user:

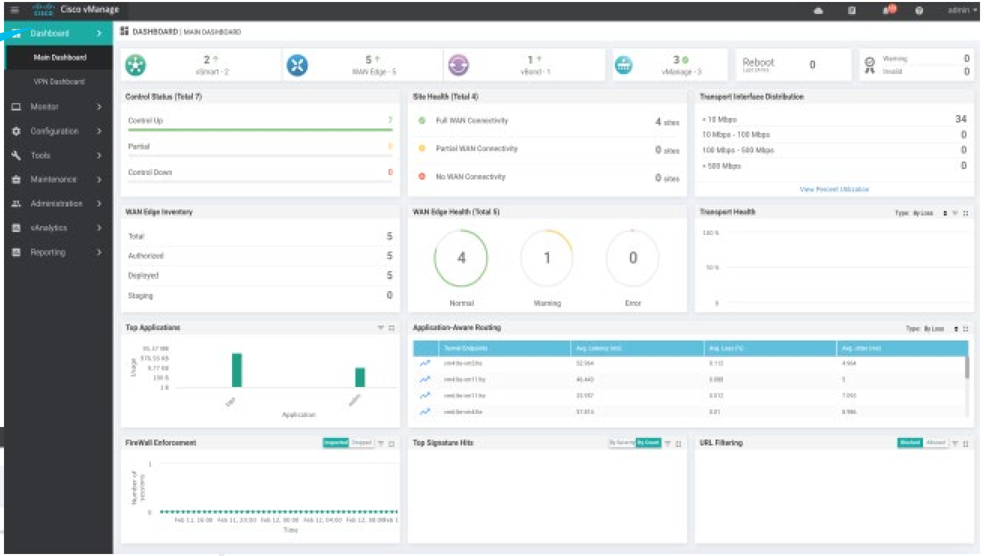
- Access to VPN Dashboard only
  - ✓ Monitor devices, network, and application status via VPN dashboard
  - ✓ VPN dashboard information restricted to devices with segments in VPN group
  - ✓ Monitor option restricted to devices with segments in VPN group
  - ✓ Interface monitoring on device restricted to interfaces of segments in the VPN group

vManage

Admin Dashboard (full access)

VPN Dashboard (Restricted access)

VPN Group: British Airways (VPN 1, 2)



Control Status (Total 7)

Control Up	7
Partial	0
Control Down	0

Site Health (Total 4)

Full WAN Connectivity	4 sites
Partial WAN Connectivity	0 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

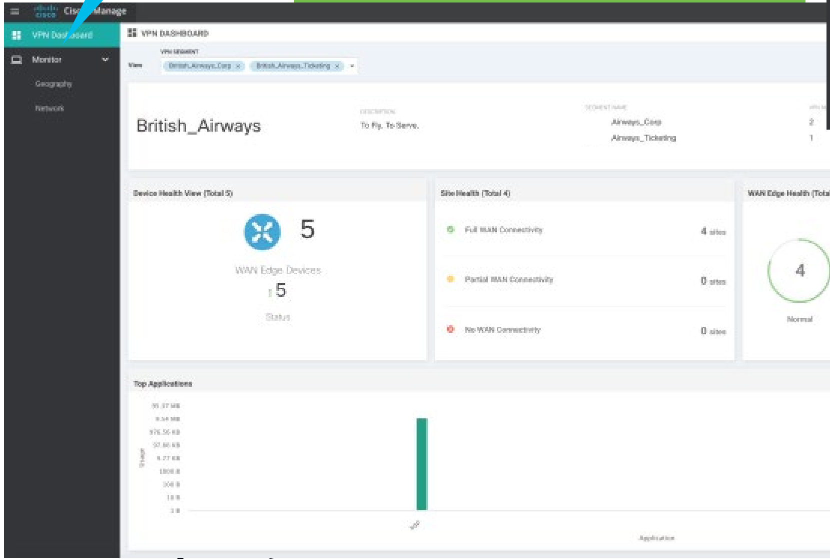
< 10 Mbps	34
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Inventory

Total	5
Authorized	5
Deployed	5
Staging	0

WAN Edge Health (Total 5)



British_Airways

DESCRIPTION	SEGMENT NAME	VPN ID
To Fly. To Serve.	Airways_Corp	2
	Airways_Ticketing	1

Device Health View (Total 5)

5 WAN Edge Devices

5 Status

Site Health (Total 4)

Full WAN Connectivity	4 sites
Partial WAN Connectivity	0 sites
No WAN Connectivity	0 sites

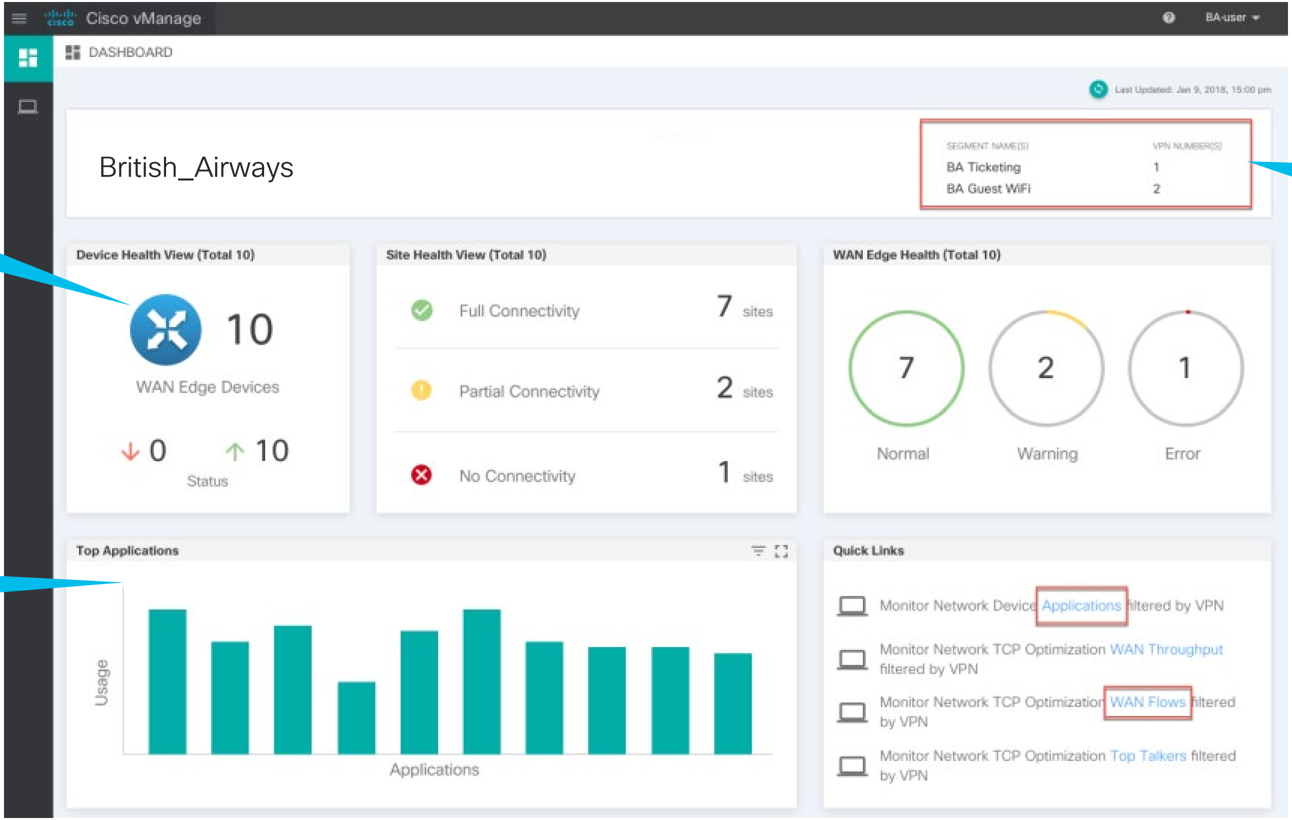
WAN Edge Health (Total 5)

VPN Dashboard View

Device health status

Application status

VPN details



Last Updated: Jan 9, 2018, 15:00 pm

British_Airways

SEGMENT NAME(S)	VPN NUMBER(S)
BA Ticketing	1
BA Guest WiFi	2

Device Health View (Total 10)

10 WAN Edge Devices

↓ 0 ↑ 10

Status

Site Health View (Total 10)

Full Connectivity	7	sites
Partial Connectivity	2	sites
No Connectivity	1	sites

WAN Edge Health (Total 10)

Normal	Warning	Error
7	2	1

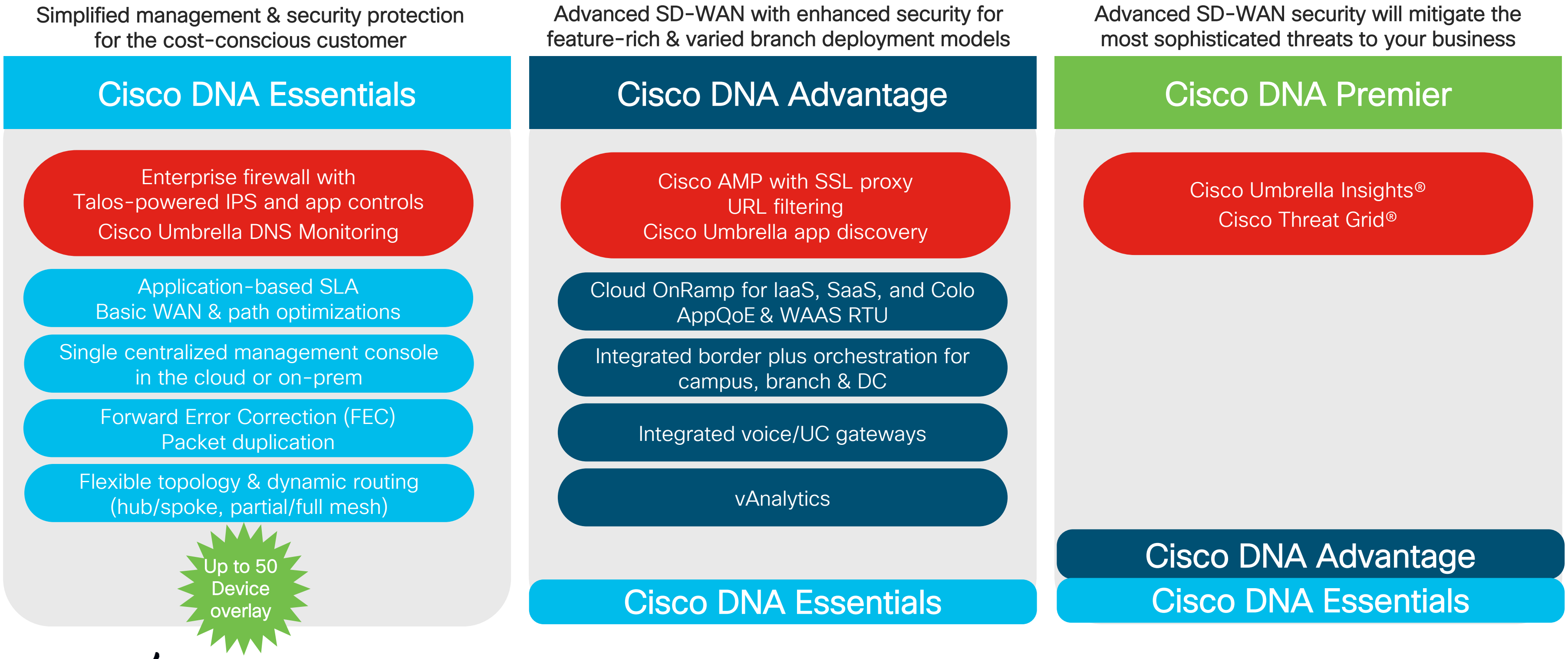
Top Applications

Quick Links

- Monitor Network Device Applications filtered by VPN
- Monitor Network TCP Optimization WAN Throughput filtered by VPN
- Monitor Network TCP Optimization WAN Flows filtered by VPN
- Monitor Network TCP Optimization Top Talkers filtered by VPN

Cisco DNA SD-WAN Licensing

Capability Based Packaging



Simplified management & security protection for the cost-conscious customer

Cisco DNA Essentials

- Enterprise firewall with Talos-powered IPS and app controls
  Cisco Umbrella DNS Monitoring
- Application-based SLA
  Basic WAN & path optimizations
- Single centralized management console in the cloud or on-prem
- Forward Error Correction (FEC)
  Packet duplication
- Flexible topology & dynamic routing (hub/spoke, partial/full mesh)

Up to 50 Device overlay

Advanced SD-WAN with enhanced security for feature-rich & varied branch deployment models

Cisco DNA Advantage

- Cisco AMP with SSL proxy
  URL filtering
  Cisco Umbrella app discovery
- Cloud OnRamp for IaaS, SaaS, and Colo
  AppQoE & WAAS RTU
- Integrated border plus orchestration for campus, branch & DC
- Integrated voice/UC gateways
- vAnalytics

Cisco DNA Essentials

Advanced SD-WAN security will mitigate the most sophisticated threats to your business

Cisco DNA Premier

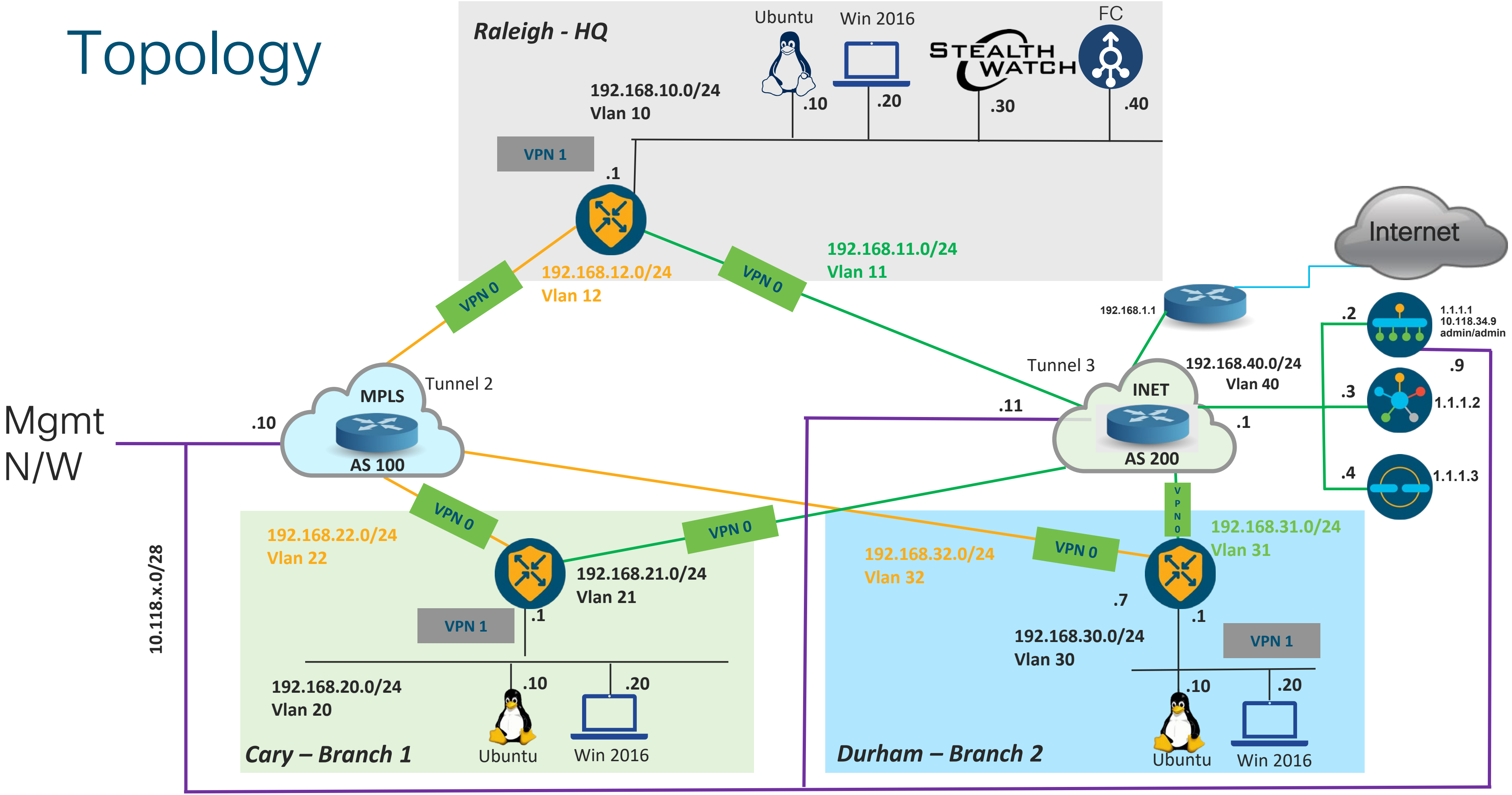
- Cisco Umbrella Insights®
  Cisco Threat Grid®

Cisco DNA Advantage

Cisco DNA Essentials

Demo

Topology


Raleigh - HQ
Ubuntu
Win 2016
STEALTHWATCH
FC
192.168.10.0/24
Vlan 10
.10
.20
.30
.40
VPN 1
.1
192.168.12.0/24
Vlan 12
VPN 0
VPN 0
192.168.11.0/24
Vlan 11
Internet
192.168.1.1
.2
1.1.1.1
10.118.34.9
admin/admin
.9
.3
1.1.1.2
.4
1.1.1.3
Tunnel 3
192.168.40.0/24
Vlan 40
INET
.11
.1
AS 200
Tunnel 2
MPLS
AS 100
Mgmt
N/W
.10
10.118.x.0/28
VPN 0
VPN 0
192.168.22.0/24
Vlan 22
192.168.21.0/24
Vlan 21
VPN 1
.1
192.168.20.0/24
Vlan 20
.10
.20
Ubuntu
Win 2016
Cary – Branch 1
VPN 0
192.168.31.0/24
Vlan 31
192.168.32.0/24
Vlan 32
VPN 0
.7
.1
192.168.30.0/24
Vlan 30
VPN 1
.10
.20
Ubuntu
Win 2016
Durham – Branch 2

Recap - Cisco SD-WAN Controllers

Orchestration Plane Cisco vBond

- Orchestrates control and management plane
- First point of authentication
- Distributes list of vSmarts/ vManage to all WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address [or 1:1 NAT]
- Highly resilient

Control Plane Cisco vSmart

- Facilitates fabric discovery
- Disseminates control plane information between WAN Edges
- Distributes data plane and app-aware routing policies to the WAN Edge routers
- Implements control plane policies
- Reduces control plane complexity
- Highly resilient

Management Plane Cisco vManage

- Single pane of glass
- Multitenant with scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC and per VPN visibility
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

Data Plane Physical/Virtual WAN Edge

- Provides secure data plane
- Establishes secure control plane with vSmart controllers
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages protocols OSPF, BGP, EIGRP and VRRP
- Zero Touch Provisioning

Recap - SD-WAN Security Capabilities

Requires 4 GB of additional DRAM = 8 GB Platform

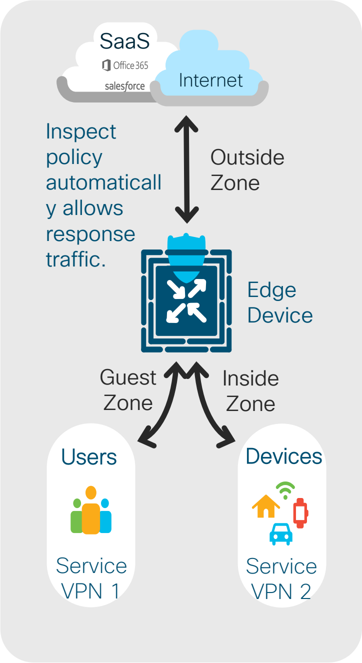
Ent. Firewall App Aware

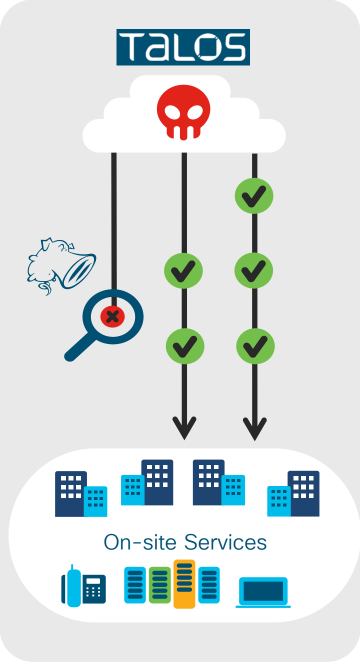
Intrusion Prevention

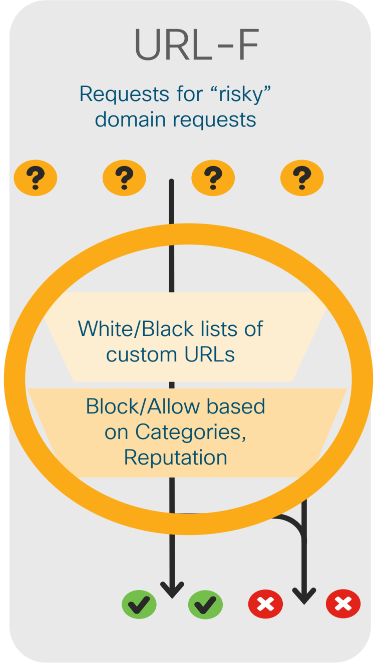
URL Filtering

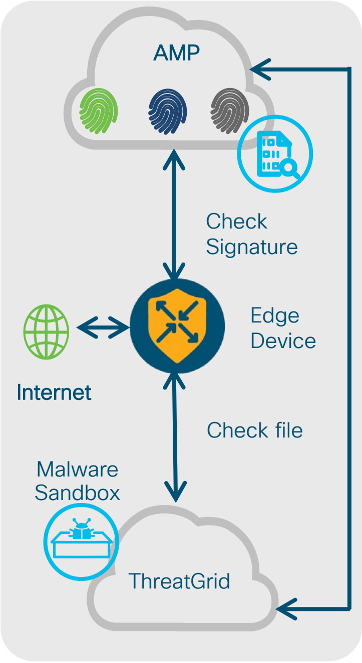
Advance Malware Protection and TG

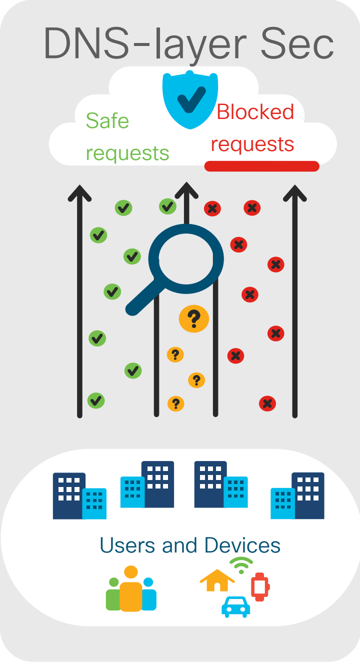
DNS/web-layer security






URL-F
Requests for “risky” domain requests
?
?
?
?
White/Black lists of custom URLs
Block/Allow based on Categories, Reputation





Release Notes and Image Download Links

For Your Reference

Release Notes for both 19.2.x
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/19-2/sd-wan-rel-notes-19-2.html#id_102854

16.12.2r Software Download Link for ISR 1K/4K and ASR:
ISR 1K: https://software.cisco.com/download/home/286321996/type/286321980/release/16.12.2r
ISR 4K: https://software.cisco.com/download/home/286321991/type/286321980/release/16.12.2r
ASR1K: https://software.cisco.com/download/home/286321999/type/286321980/release/16.12.2r

19.2.1 vManage New Deployment Download Link: https://software.cisco.com/download/home/286320995/type/286321039/release/19.2.1

18.4 vManage upgrade image download Link: https://software.cisco.com/download/home/286320995/type/286321394/release/19.2.1

SD-WAN Security – External Resources

For Your Reference

Cisco SD-WAN - http://www.cisco.com/go/sdwan

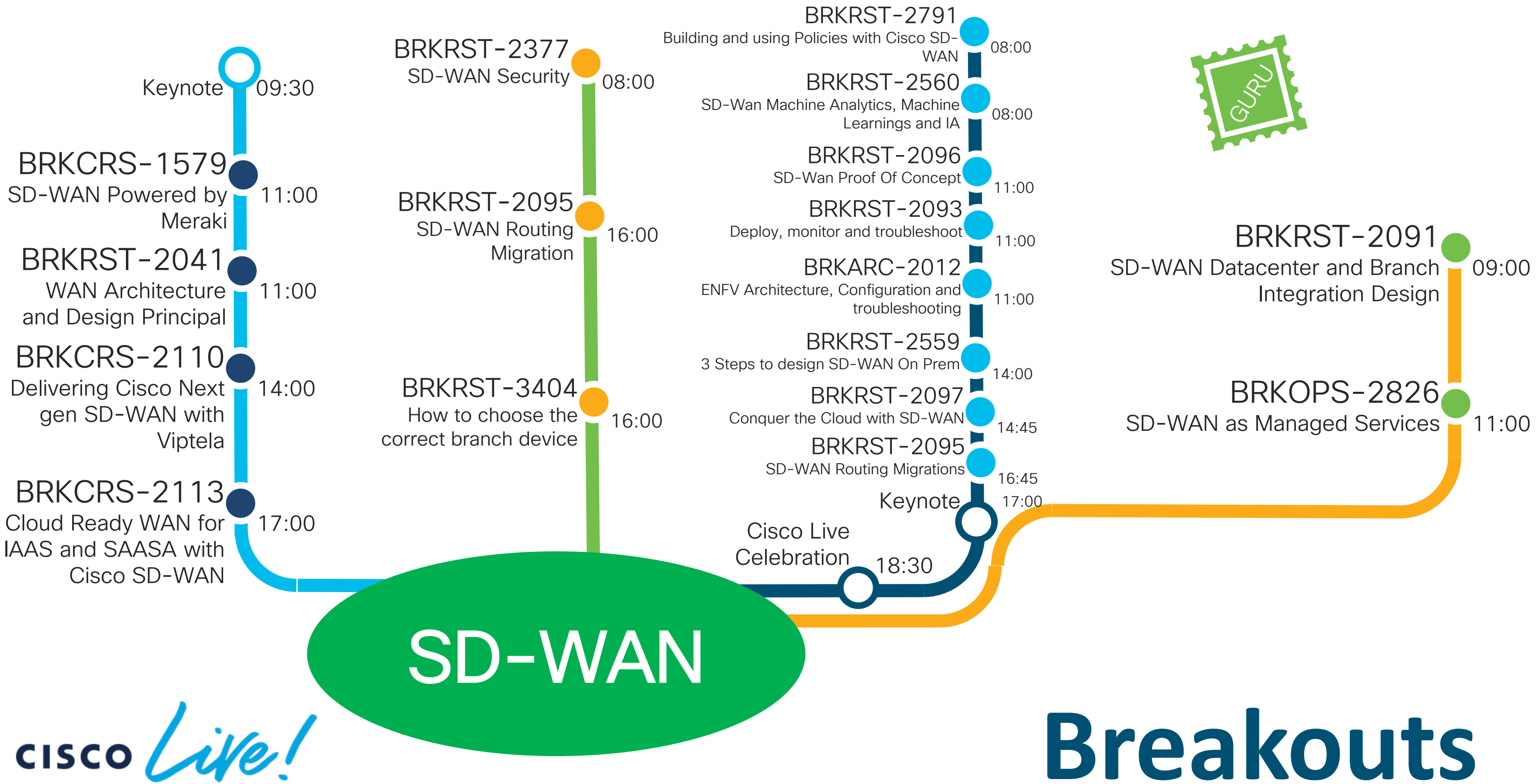
Network World - https://tinyurl.com/yabey6f2

WSJ - https://tinyurl.com/yb75loxn

Lightreading - https://tinyurl.com/yba9zb4s

FB: https://tinyurl.com/y9u375hk

YouTube Network Field Day (demo): https://tinyurl.com/y955ufde



Keynote 09:30

BRKCRS-1579 SD-WAN Powered by Meraki 11:00

BRKRST-2041 WAN Architecture and Design Principal 11:00

BRKCRS-2110 Delivering Cisco Next gen SD-WAN with Viptela 14:00

BRKCRS-2113 Cloud Ready WAN for IAAS and SAASA with Cisco SD-WAN 17:00

BRKRST-2377 SD-WAN Security 08:00

BRKRST-2095 SD-WAN Routing Migration 16:00

BRKRST-3404 How to choose the correct branch device 16:00

BRKRST-2791 Building and using Policies with Cisco SD-WAN 08:00

BRKRST-2560 SD-Wan Machine Analytics, Machine Learnings and IA 08:00

BRKRST-2096 SD-Wan Proof Of Concept 11:00

BRKRST-2093 Deploy, monitor and troubleshoot 11:00

BRKARC-2012 ENFV Architecture, Configuration and troubleshooting 11:00

BRKRST-2559 3 Steps to design SD-WAN On Prem 14:00

BRKRST-2097 Conquer the Cloud with SD-WAN 14:45

BRKRST-2095 SD-WAN Routing Migrations 16:45

Keynote 17:00

Cisco Live Celebration 18:30

BRKRST-2091 SD-WAN Datacenter and Branch Integration Design 09:00

BRKOPS-2826 SD-WAN as Managed Services 11:00

Breakouts

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco campus
- Walk-in labs
- Meet the engineer 1:1 meetings
- Related sessions

cisco Live!

Thank you

You make **possible**