CCNP Enterprise Certification

ENSDWI : 300-415

5.0

- 5.1 Configure and verify service insertion
- 5.2 Describe application-aware firewall
- 5.3 Configure and verify QoS treatment on WAN edge routers
- 5.3.a Scheduling
- 5.3.b Queuing
- 5.3.c Shaping
- 5.3.d Policing

Cisco SD-WAN Security

SD-WAN security

Agenda

- Ent Firewall App Aware
- Intrusion Prevention
- URL-Filtering
- DNS/web-layer Security
- Advanced Malware Protection + Threat Grid

SD-WAN security challenges

Threat

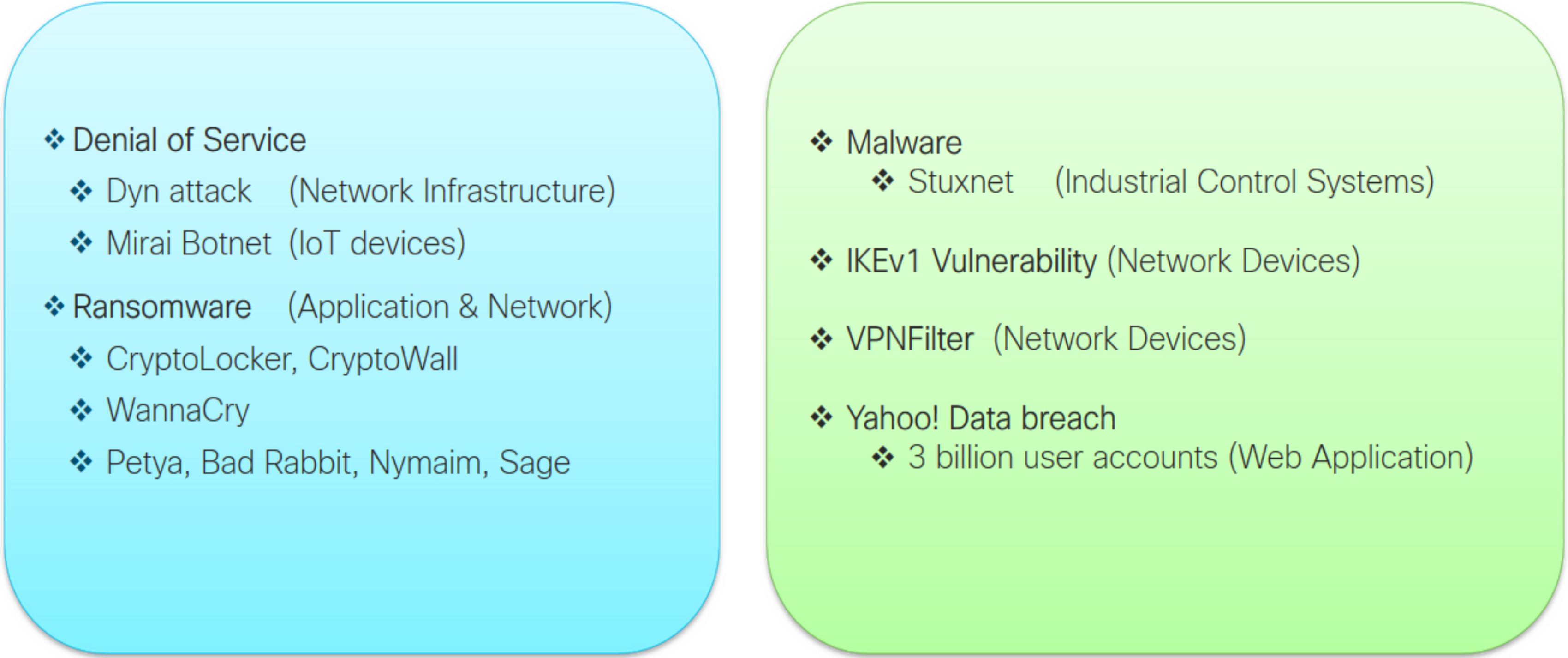
Threat Landscape

- ❖ Cyber Warfare
- ❖ Nation-State Sponsored
- ❖ Organized Crime / Targeted Attacks
- ❖ Ransomware
- ❖ Financially Motivated

Types of Threats

- ❖ Security bug / Vulnerability
  - ❖ e.g.: Heartbleed, SMBv1 vulnerability, IKEv1 vulnerability, SQL Injection, Buffer Overflow, Cross-site request forgery, Cross Site Scripting (XSS)
- ❖ Malware
  - ❖ Viruses, Worms, Trojans
  - ❖ Phishing, Adware, Spyware, Scareware
  - ❖ Keyloggers, Backdoors, Exploits, Rootkits
- ❖ Denial of Service
  - ❖ e.g.: Dyn Attack (Oct 2016)
- ❖ Botnets
  - ❖ e.g. : LinkedIn attack (Aug 2016), Deutsche Telekom (Nov 2016)

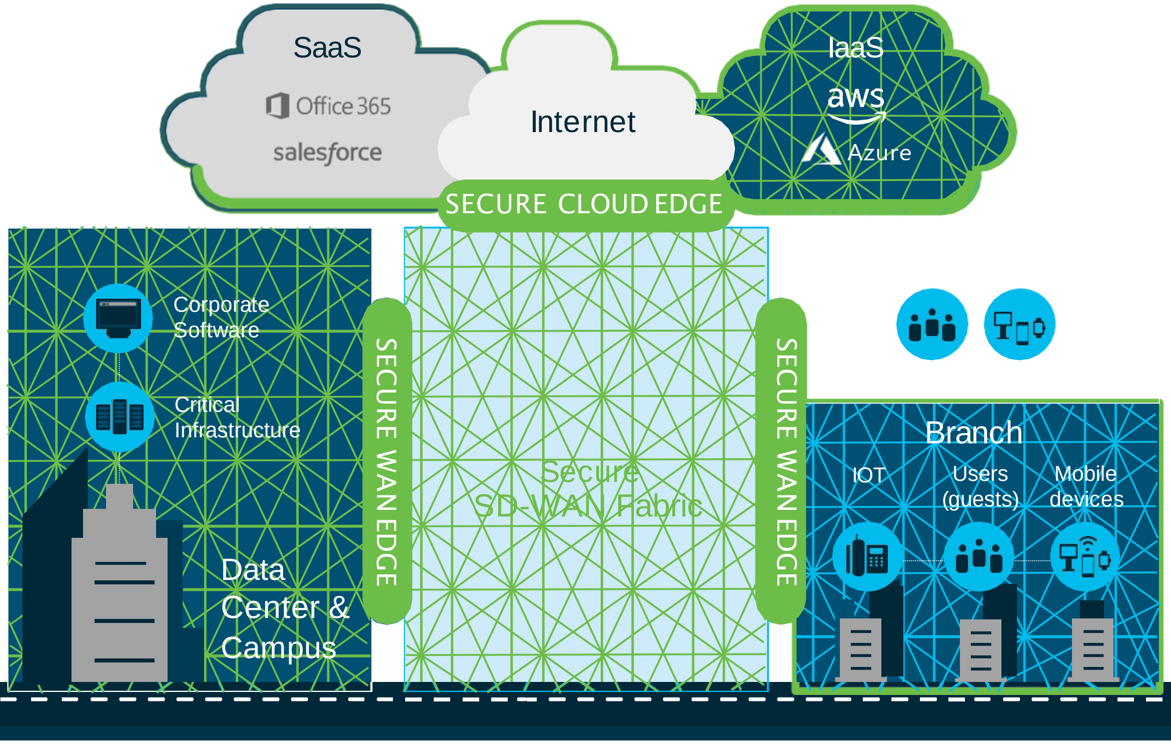
High Profile Incidents & their Targets



- Denial of Service
  - Dyn attack (Network Infrastructure)
  - Mirai Botnet (IoT devices)
- Ransomware (Application & Network)
  - CryptoLocker, CryptoWall
  - WannaCry
  - Petya, Bad Rabbit, Nymaim, Sage

- Malware
  - Stuxnet (Industrial Control Systems)
- IKEv1 Vulnerability (Network Devices)
- VPNFilter (Network Devices)
- Yahoo! Data breach
  - 3 billion user accounts (Web Application)

SD-WAN exposes new security challenges



Outside-in threats

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

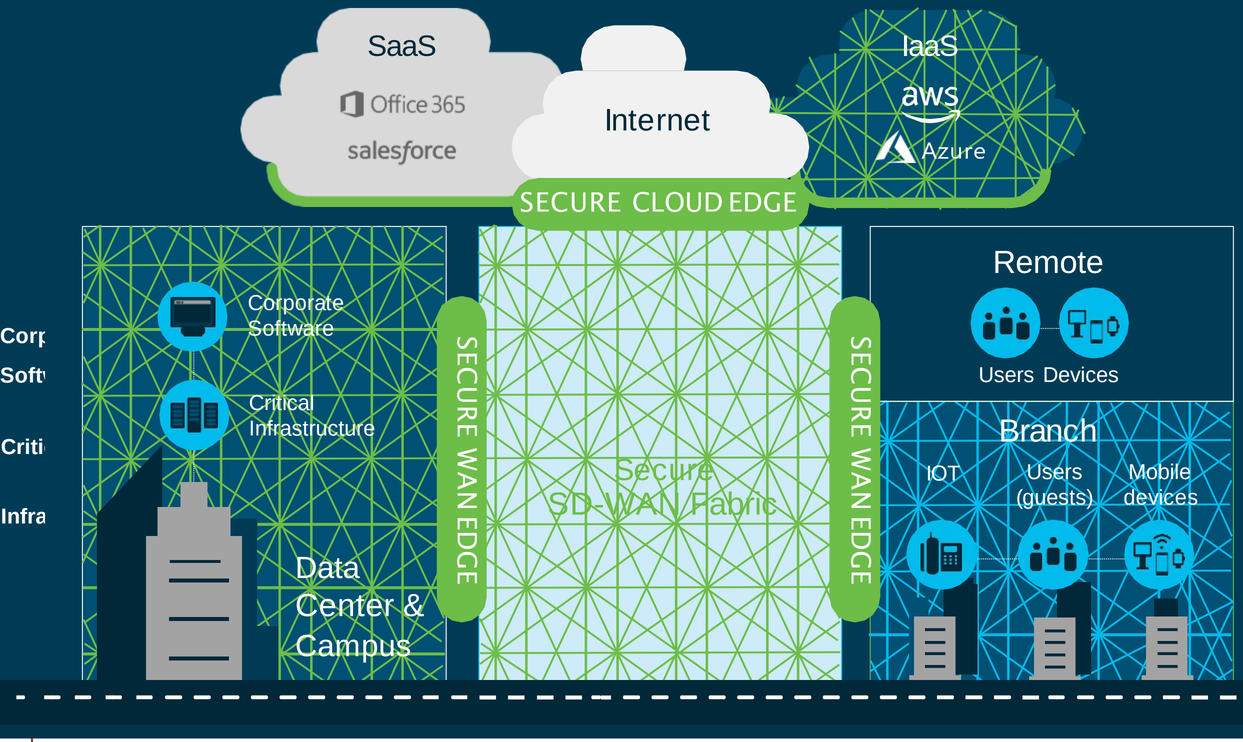
Inside-out threats

- 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

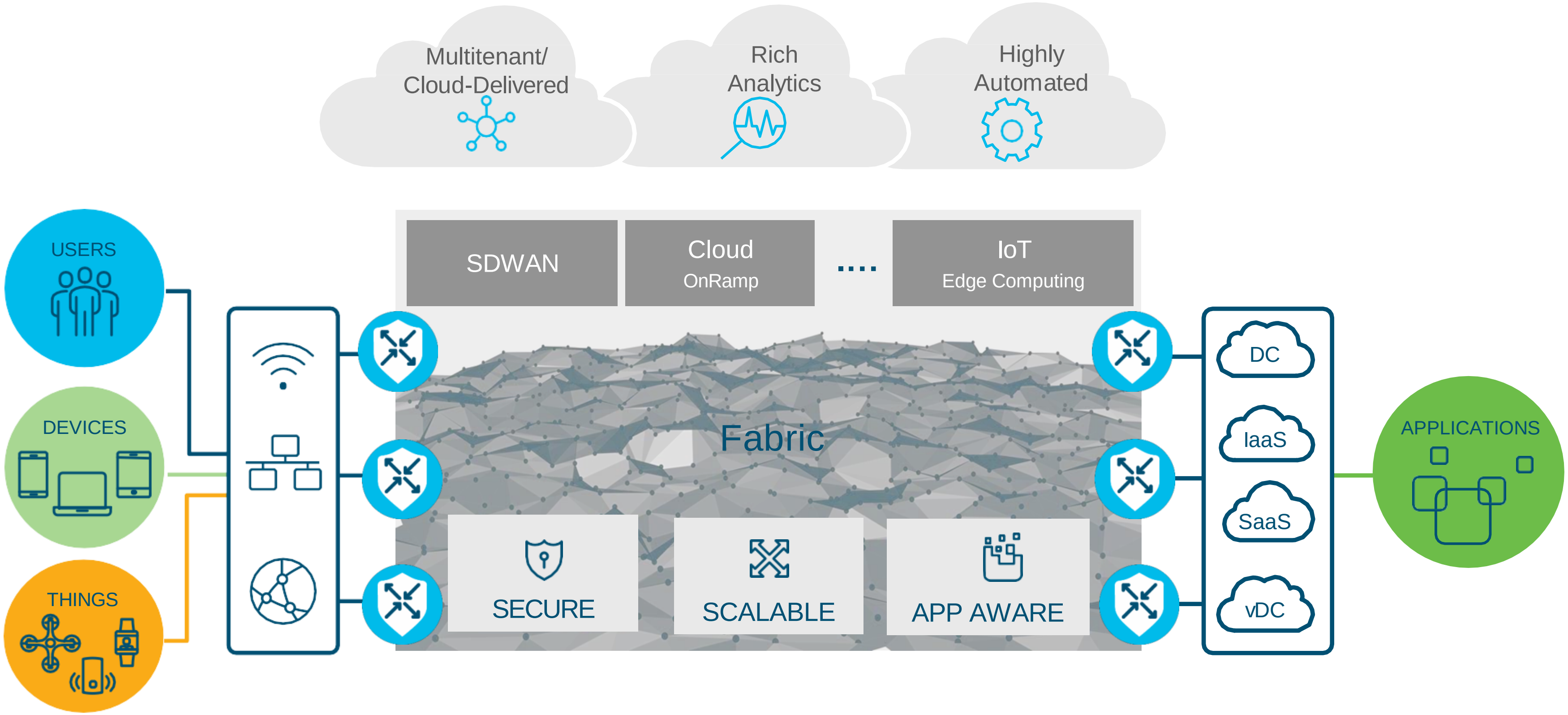
- Mitigate external security risks with integrated threat defense from the WAN to cloud edge

Thin, rich or full-stack router

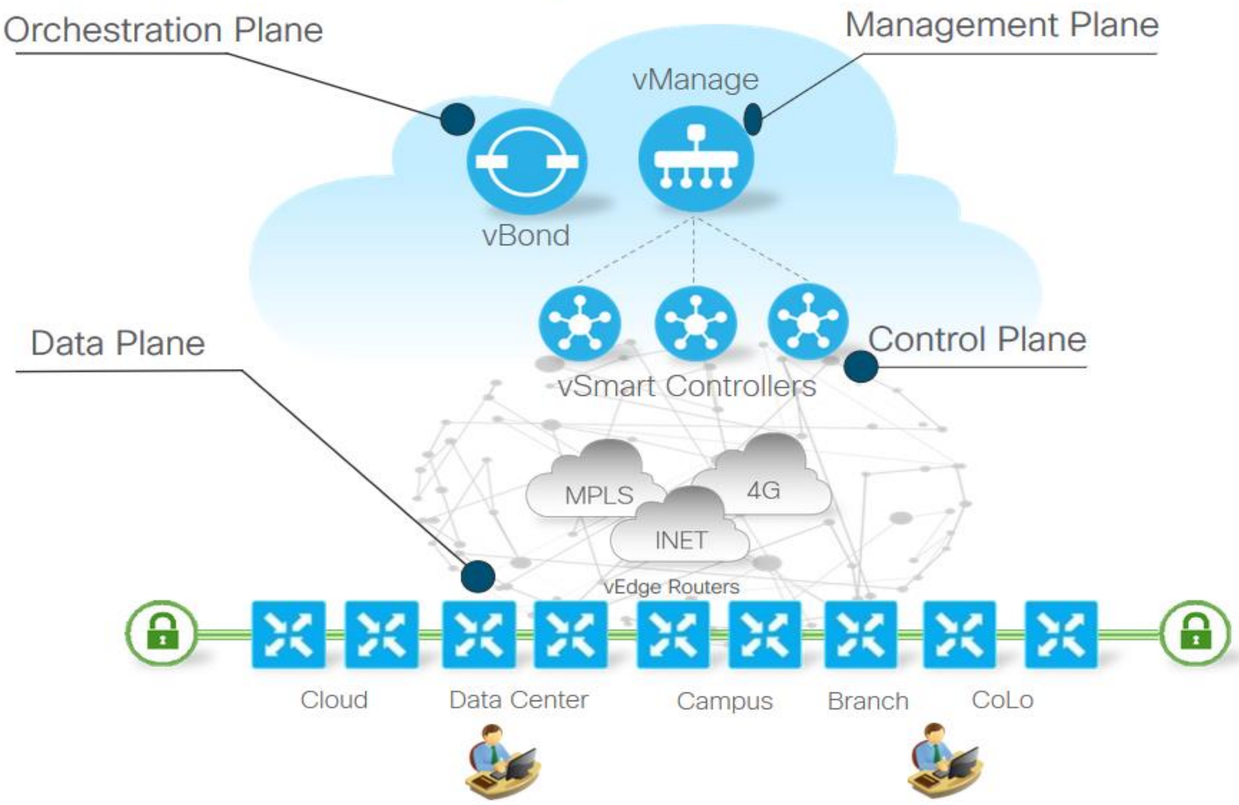
- Mitigate internal security risks with a secure SD-WAN fabric with simple or flexible routing configurations

SD-WAN Threat Defense Delivered

Cisco SD-WAN Approach



SD-WAN Security Overview



➢ Transport Security

- Control Plane Security

Traffic between WAN Edges & Controllers

- Data Plane Security

Traffic between WAN Edges

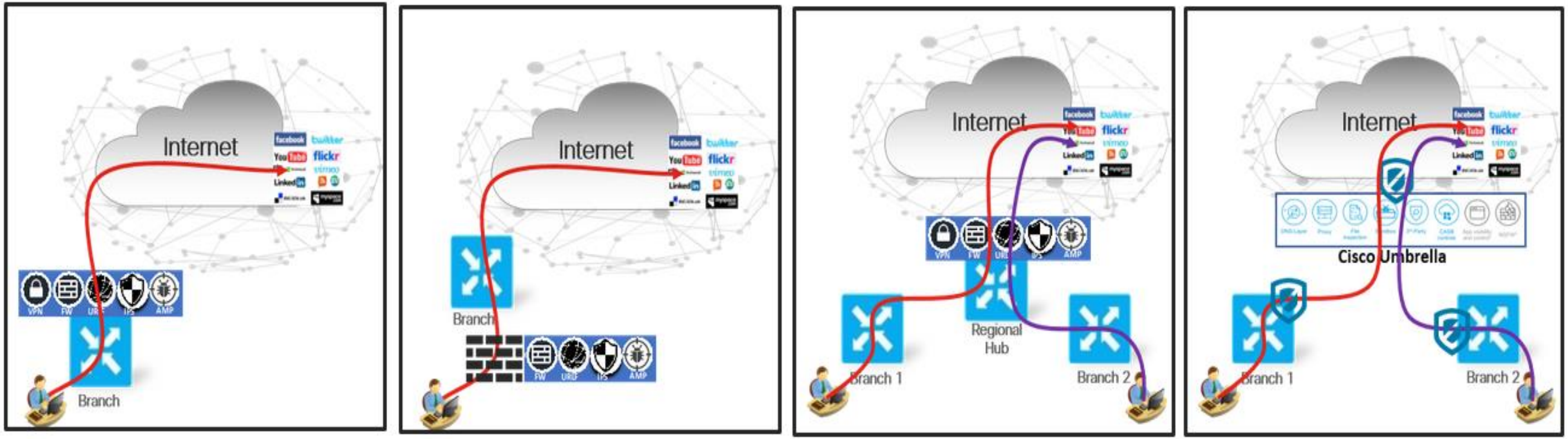
➢ Infrastructure Security

- WAN Edges
- Controllers

➢ Threat Defense

- WAN Edges to Internet

How is SD-WAN Threat Defense Delivered



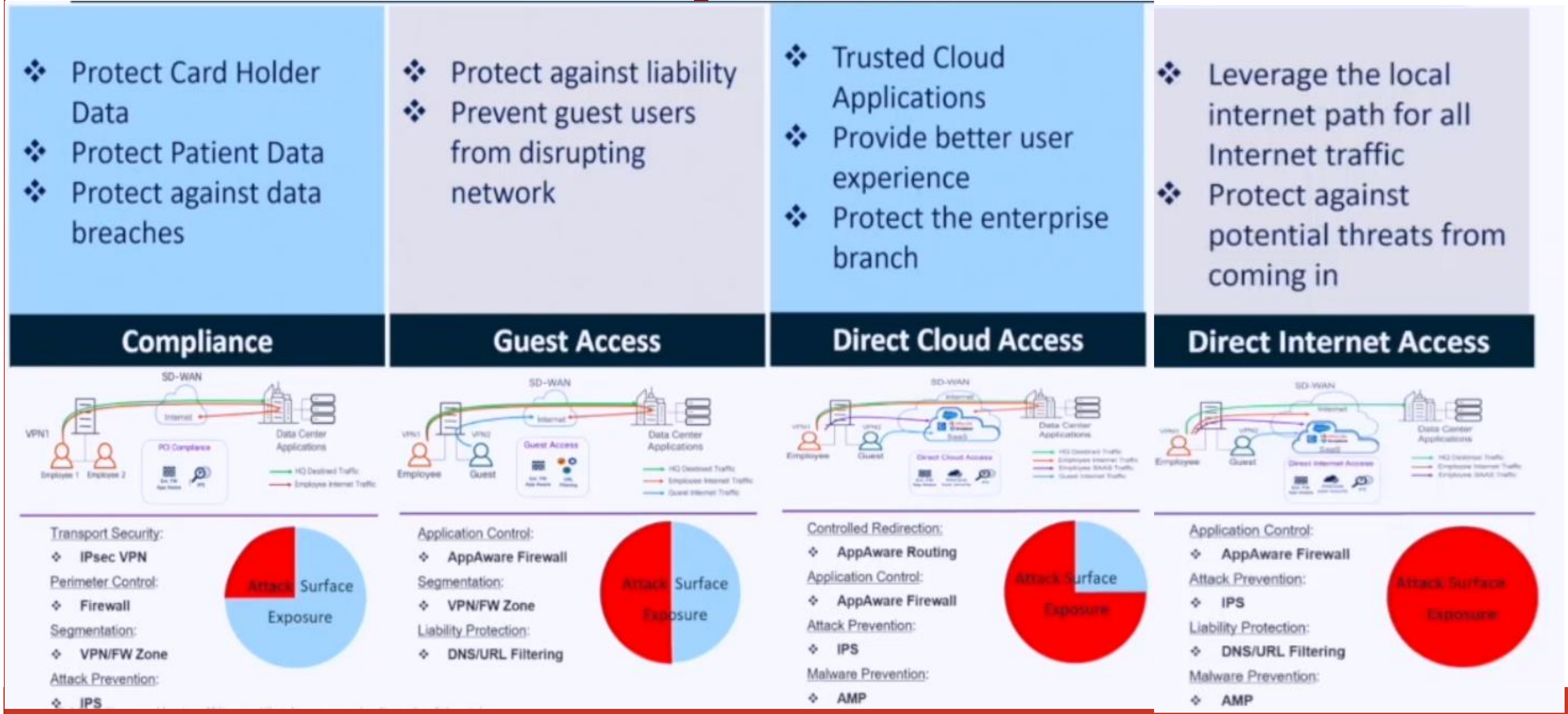
Integrated

Dedicated

Service Chained

Cloud Delivered

Intent Driven Security Use cases



Compliance

- ❖ Protect Card Holder Data
- ❖ Protect Patient Data
- ❖ Protect against data breaches

Transport Security:

- ❖ IPsec VPN

Perimeter Control:

- ❖ Firewall

Segmentation:

- ❖ VPN/FW Zone

Attack Prevention:

- ❖ IPS

Guest Access

- ❖ Protect against liability
- ❖ Prevent guest users from disrupting network

Application Control:

- ❖ AppAware Firewall

Segmentation:

- ❖ VPN/FW Zone

Liability Protection:

- ❖ DNS/URL Filtering

Direct Cloud Access

- ❖ Trusted Cloud Applications
- ❖ Provide better user experience
- ❖ Protect the enterprise branch

Controlled Redirection:

- ❖ AppAware Routing

Application Control:

- ❖ AppAware Firewall

Attack Prevention:

- ❖ IPS

Malware Prevention:

- ❖ AMP

Direct Internet Access

- ❖ Leverage the local internet path for all Internet traffic
- ❖ Protect against potential threats from coming in

Application Control:

- ❖ AppAware Firewall

Attack Prevention:

- ❖ IPS

Liability Protection:

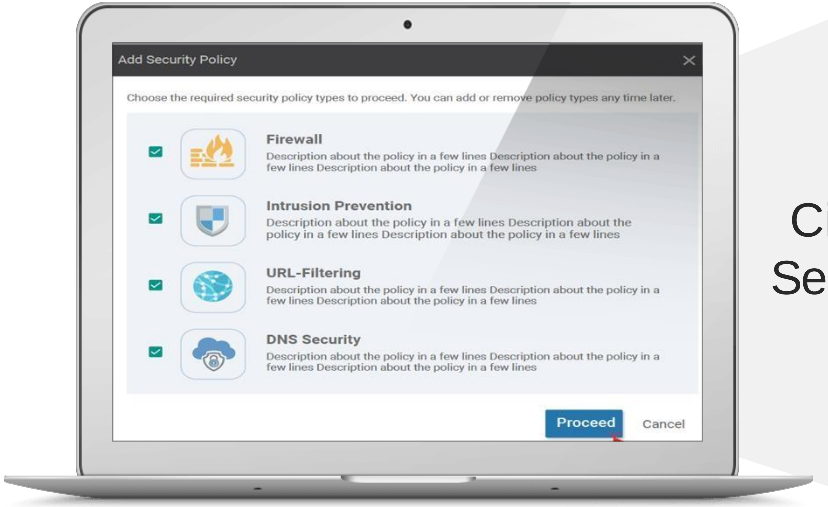
- ❖ DNS/URL Filtering

Malware Prevention:

- ❖ AMP

Combining Best of Breed in Security and SD-WAN

What is Cisco SD-WAN 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

Cisco 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

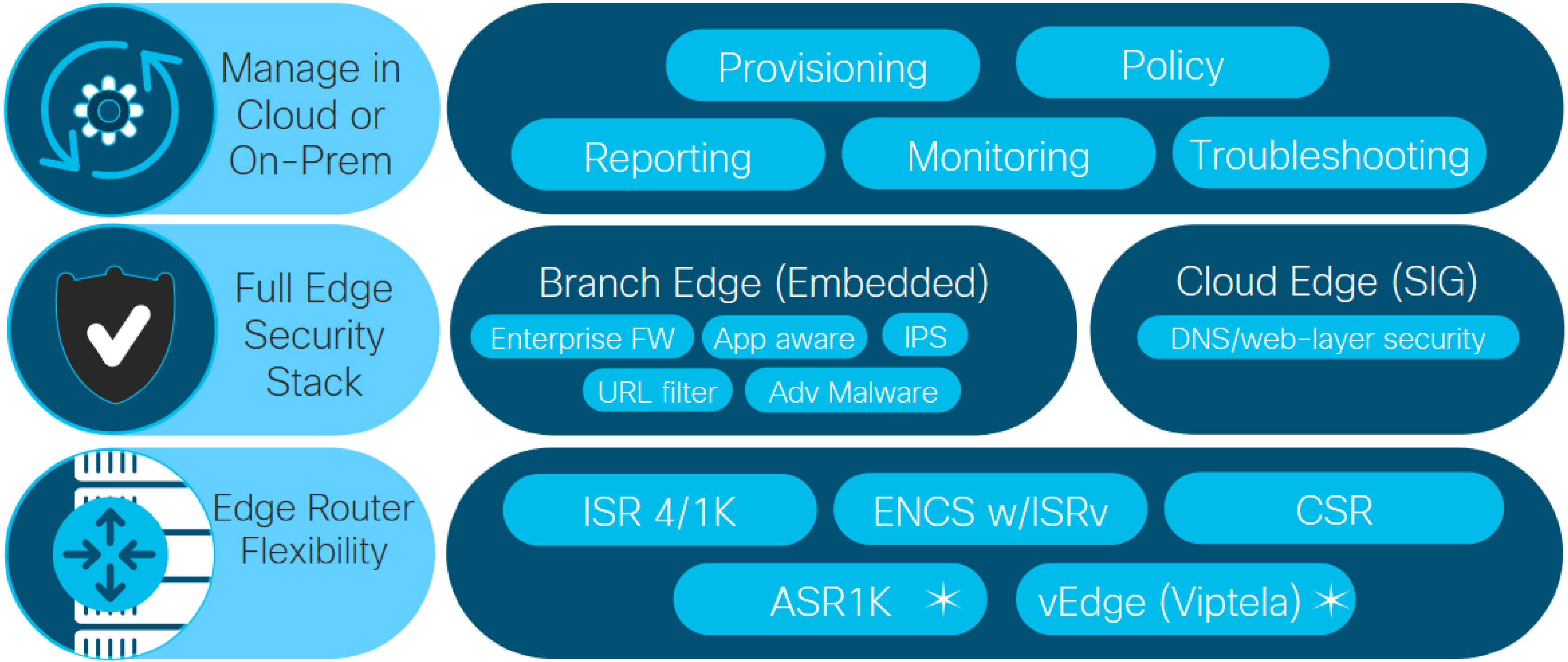
Adv. Malware Protection
With File Reputation and Sandboxing

Simplified Cloud Security
Easy Deployment for Cisco Umbrella

Hours instead of weeks and months

Combining Best of Breed in Security and SDWAN

What is Cisco SD-WAN Security?



Manage in Cloud or On-Prem

Provisioning

Policy

Reporting

Monitoring

Troubleshooting

Full Edge Security Stack

Branch Edge (Embedded)

Enterprise FW

App aware

IPS

URL filter

Adv Malware

Cloud Edge (SIG)

DNS/web-layer security

Edge Router Flexibility

ISR 4/1K

ENCS w/ISRv

CSR

ASR1K ✶

vEdge (Viptela) ✶

✶ Only FW and DNS/web-layer security

Secure Infrastructure

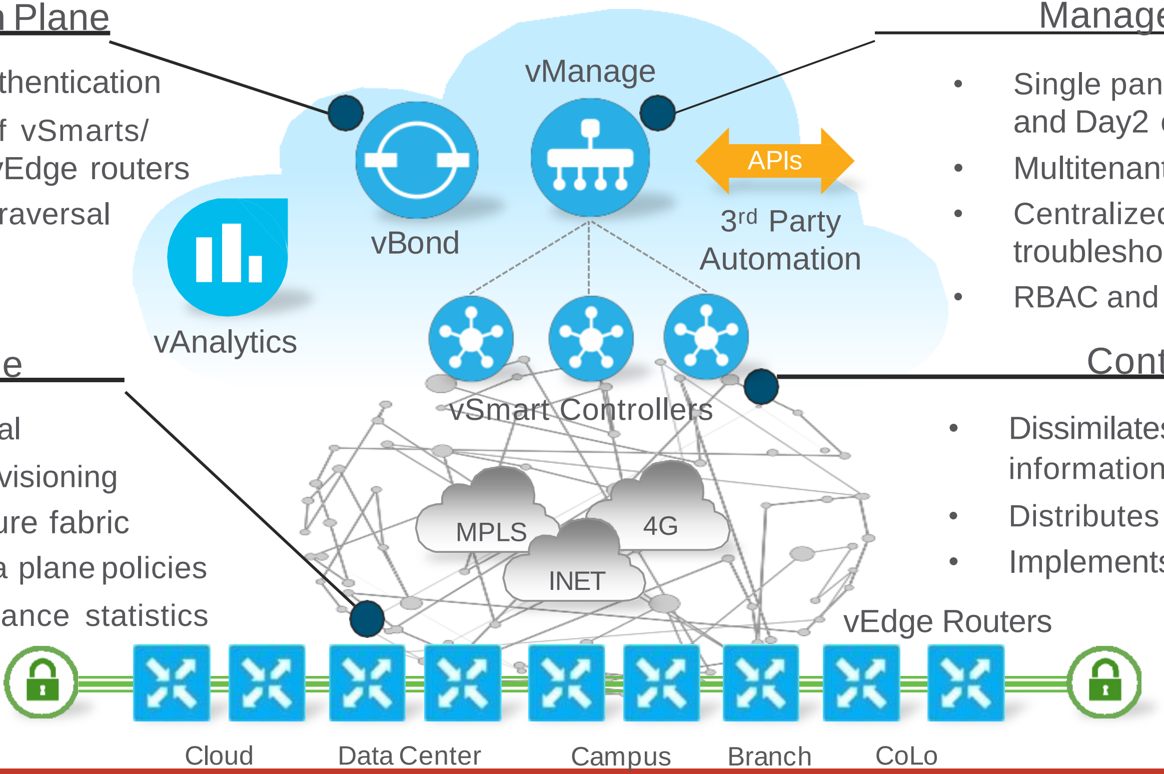
Cisco SD-WAN Architecture

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



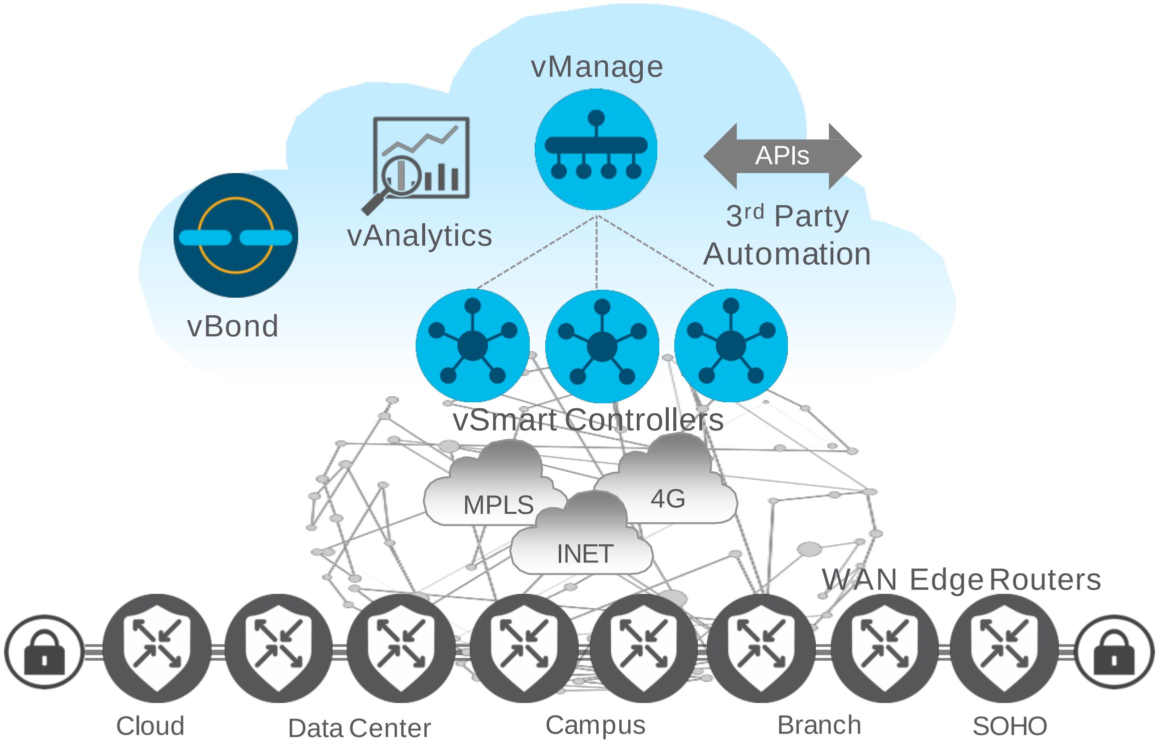
Data Plane

- 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

Orchestration Plane

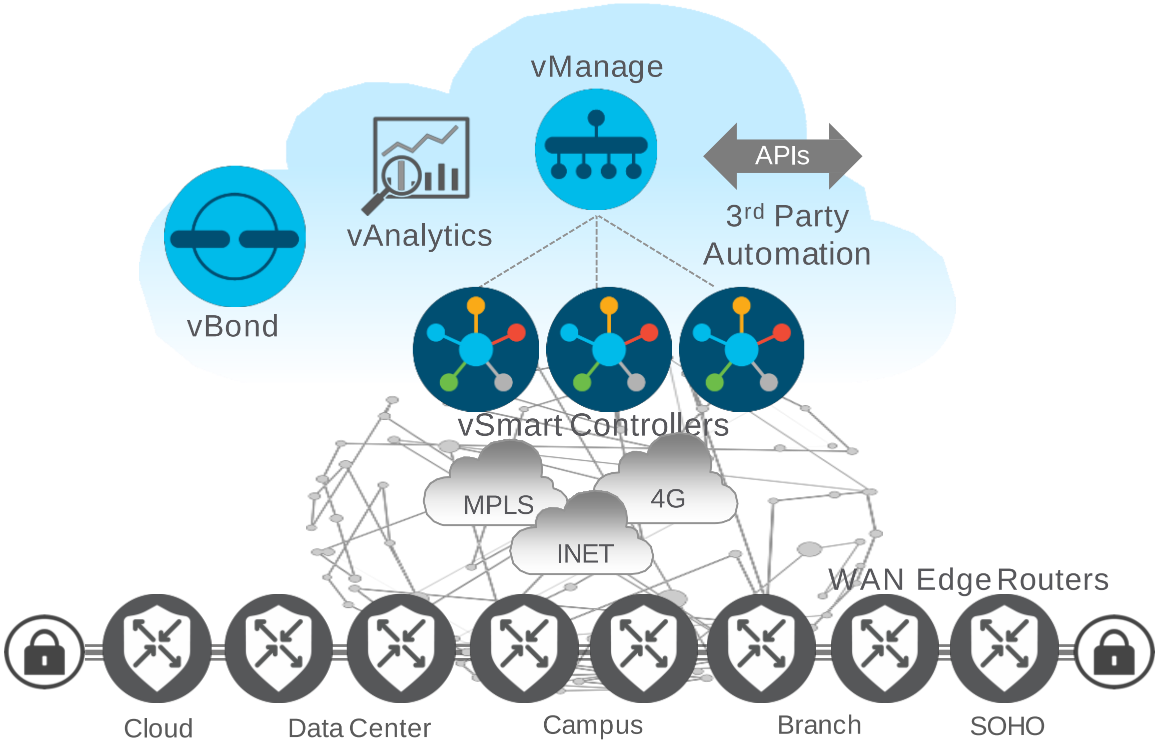


Orchestration Plane

Cisco vBond

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

Control Plane

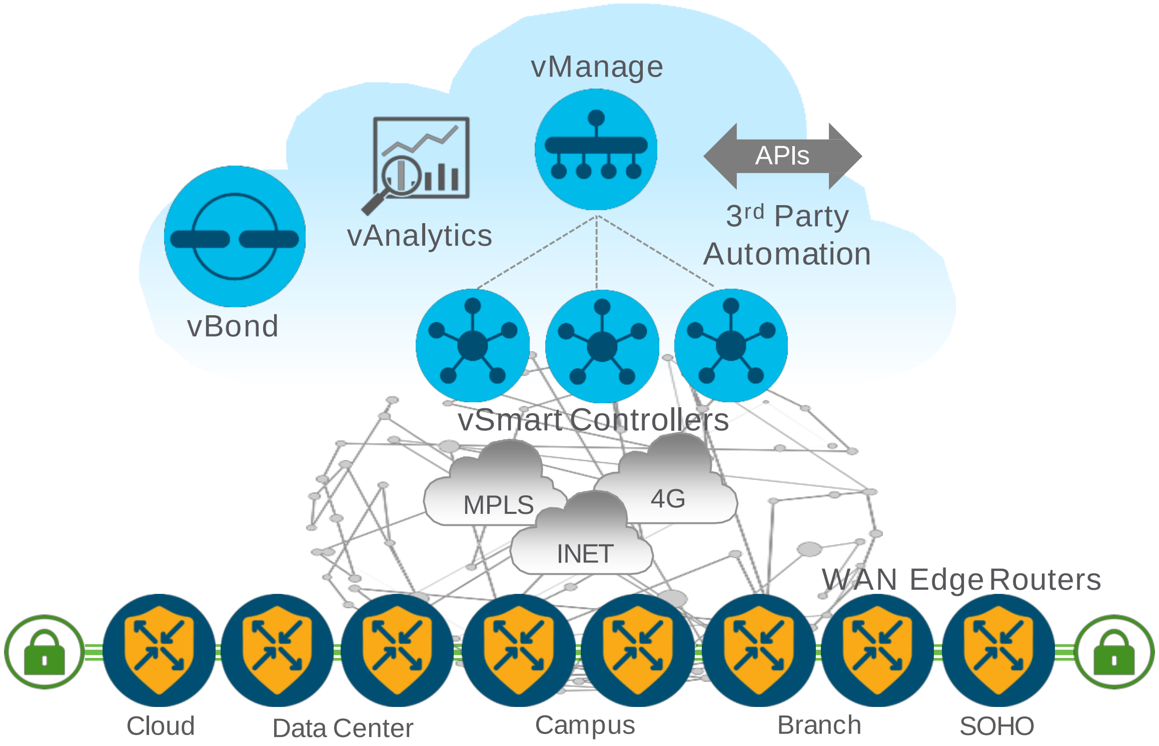


Control Plane

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, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

Data Plane

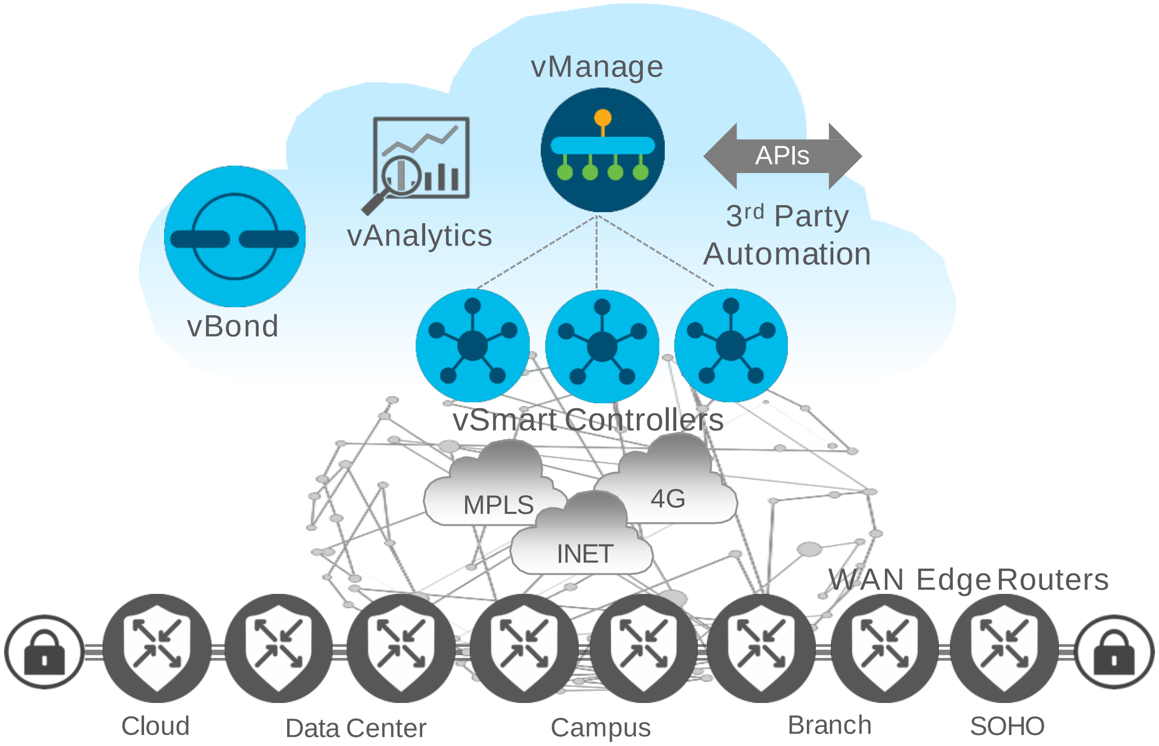


Data Plane
Physical/Virtual

WAN Edge

- WAN edge router
- Provides secure data plane with remote WAN Edge 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, EIGRP and VRRP
- Support Zero Touch Deployment
- Physical or Virtual form factor

Management Plane



Management Plane

Cisco vManage

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- GUI with RBAC and per VPN visibility
- Programmatic interfaces (REST, NETCONF)
- Highly resilient

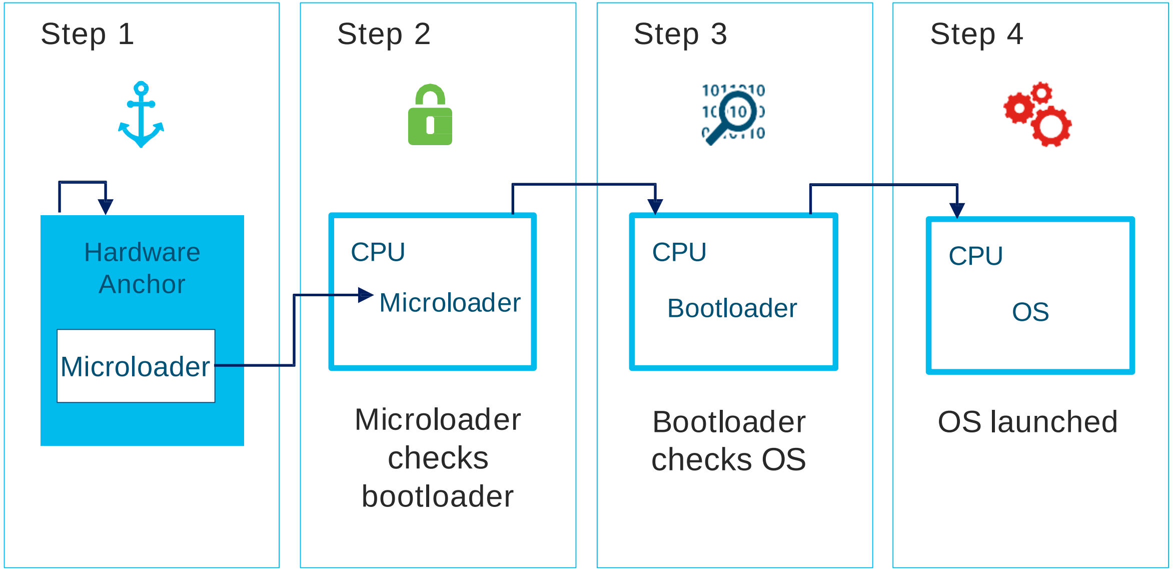
Device Identity & Security

Cisco Secure Boot

Anchors Secure Boot in Hardware to Create a Chain of Trust

Cisco Secure Boot

Boot Code Integrity Anchored in Hardware



Step 1

Hardware Anchor

Microloader

Step 2

CPU

Microloader

Microloader checks bootloader

Step 3

CPU

Bootloader

Bootloader checks OS

Step 4

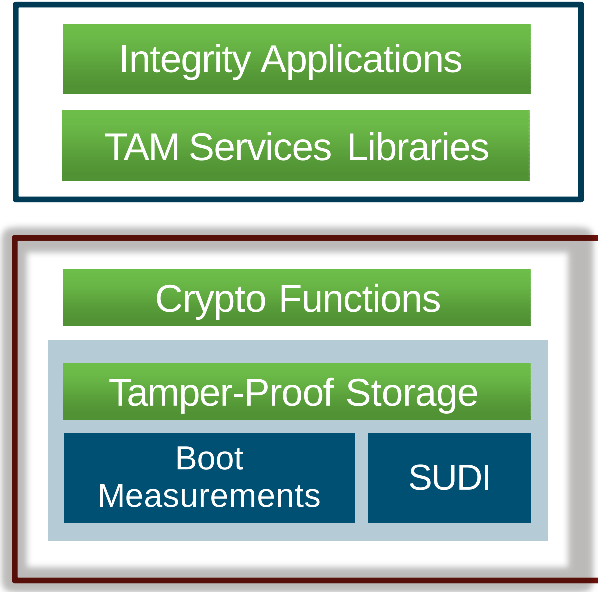
CPU

OS

OS launched

- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate

Cisco Trust Anchor Module (TAm)



Integrity Applications

TAM Services Libraries

Crypto Functions

Tamper-Proof Storage

Boot Measurements

SUDI

- HW Authenticity Check
- Secure PnP
- Integrity Verification

- Anti-Tamper Chip Design
- Built-In Crypto Functions
- Secure Storage

Platform Integrity: TPM and TAm Compared

TPM & TAm Capabilities

Anti-tamper	Non-volatile secure storage	Crypto engine
Key storage	Random number generation	Policy & Configuration

Cisco Trust Anchor Module

- Provides end-user and supply chain protections
- For specialized network devices

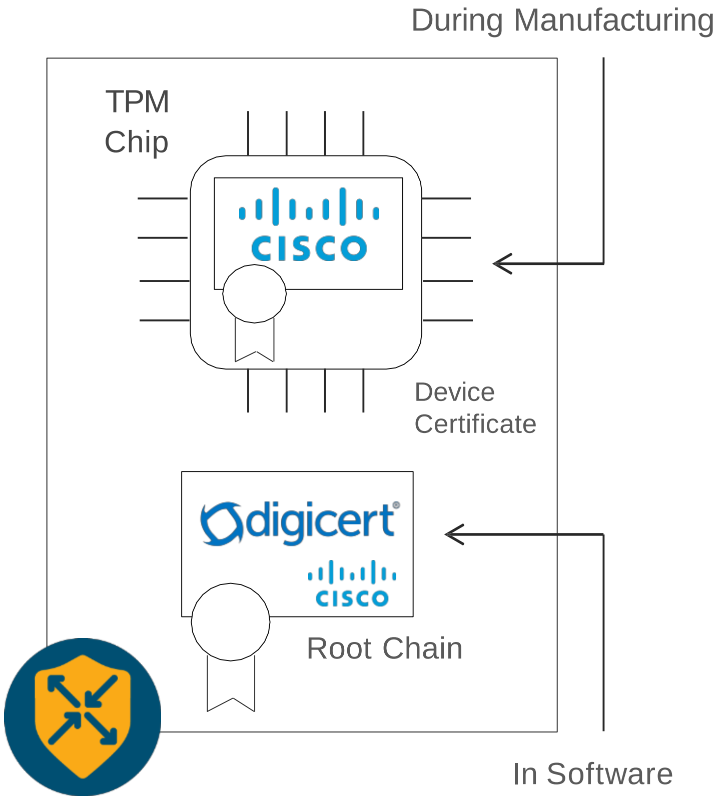
Trusted Platform Module (TPM)

- Focused on providing end-user capabilities
- For general purpose computing

Secure Unique Device Identification (Secure – UDI)

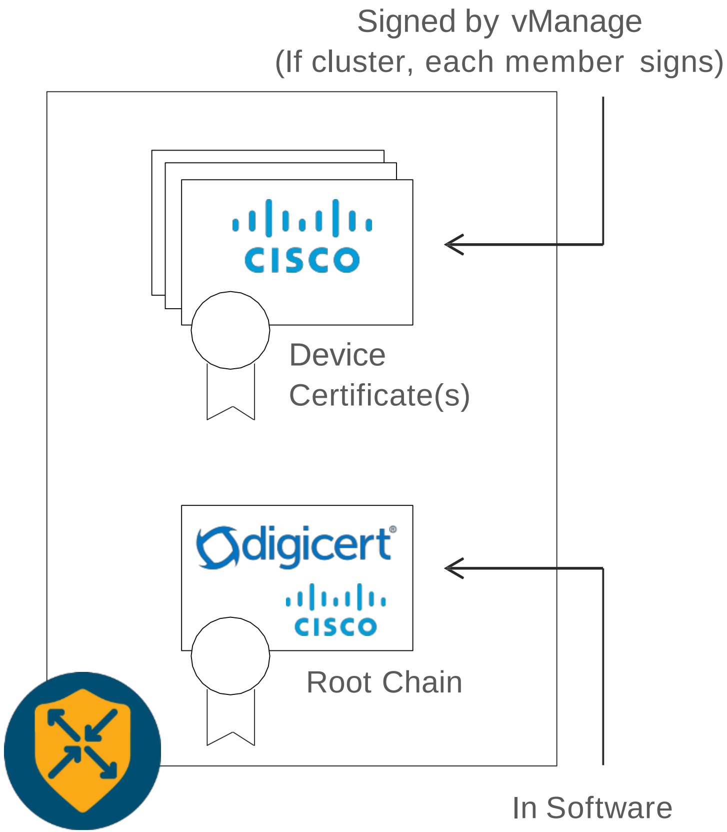
- Tamperproof ID for the device
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate PID during manufacturing
- Connections with the device can be authenticated by the SUDI credential
- IEEE 802.1AR Compliant

Router Identity



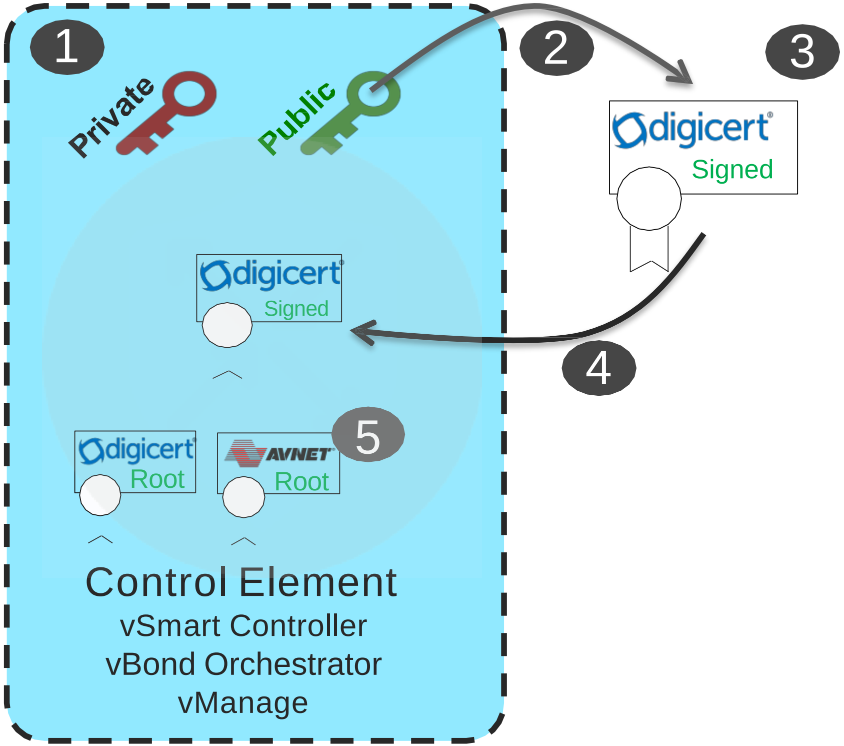
- Each physical router is uniquely identified by the chassis ID and certificate serial number
- Certificate is stored in on-board Temper Proof Module (TPM)
  - Installed during manufacturing process
- Certificate is signed by Avnet root CA or Cisco root CA
  - Trusted by Control Plane elements
- DigiCert 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 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.

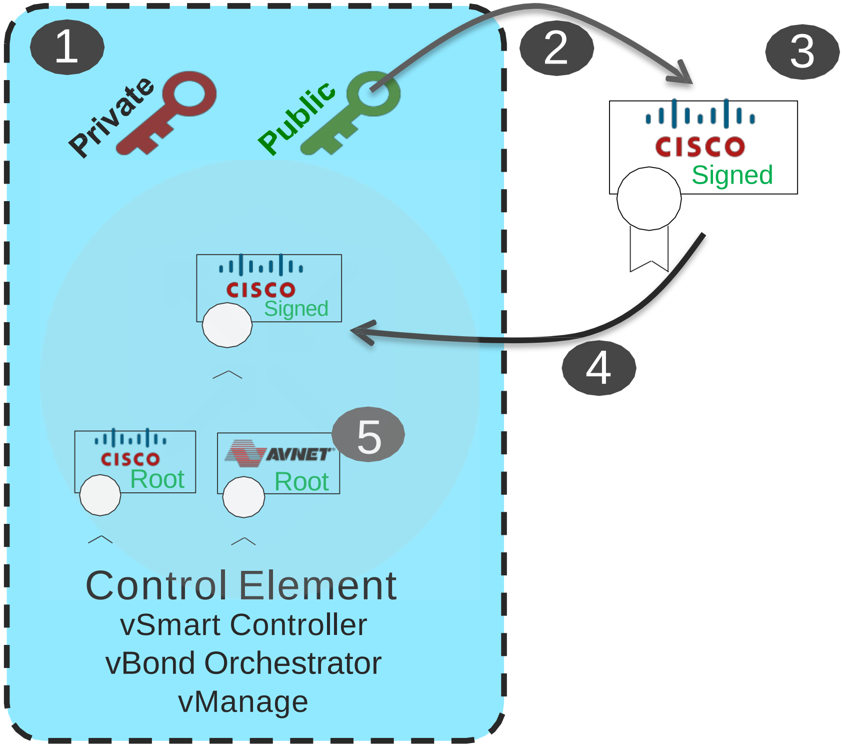
This process is fully automated within vManage.

?

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

Establishing Control Elements Identity – Cisco PKI

19.1



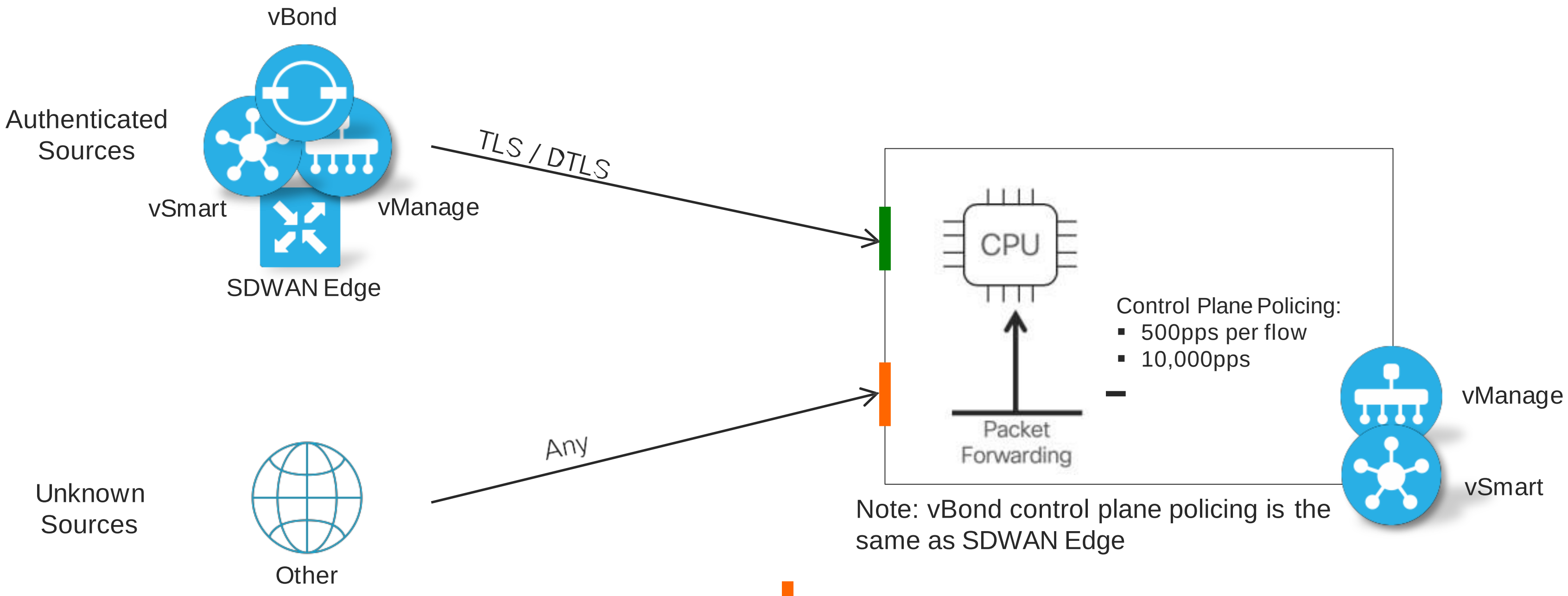
1. Private and public keys are generated on the control element
2. Certificate Signing Request is generated
3. Certificate automatically signed by Cisco PnP linked to your Smart Account (when Cisco signing is selected in vManage)
4. Certificate is installed into the control element
5. Control element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

This process is fully automated within vManage.

?

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

DDoS Protection for Controllers



Control Plane Policing:

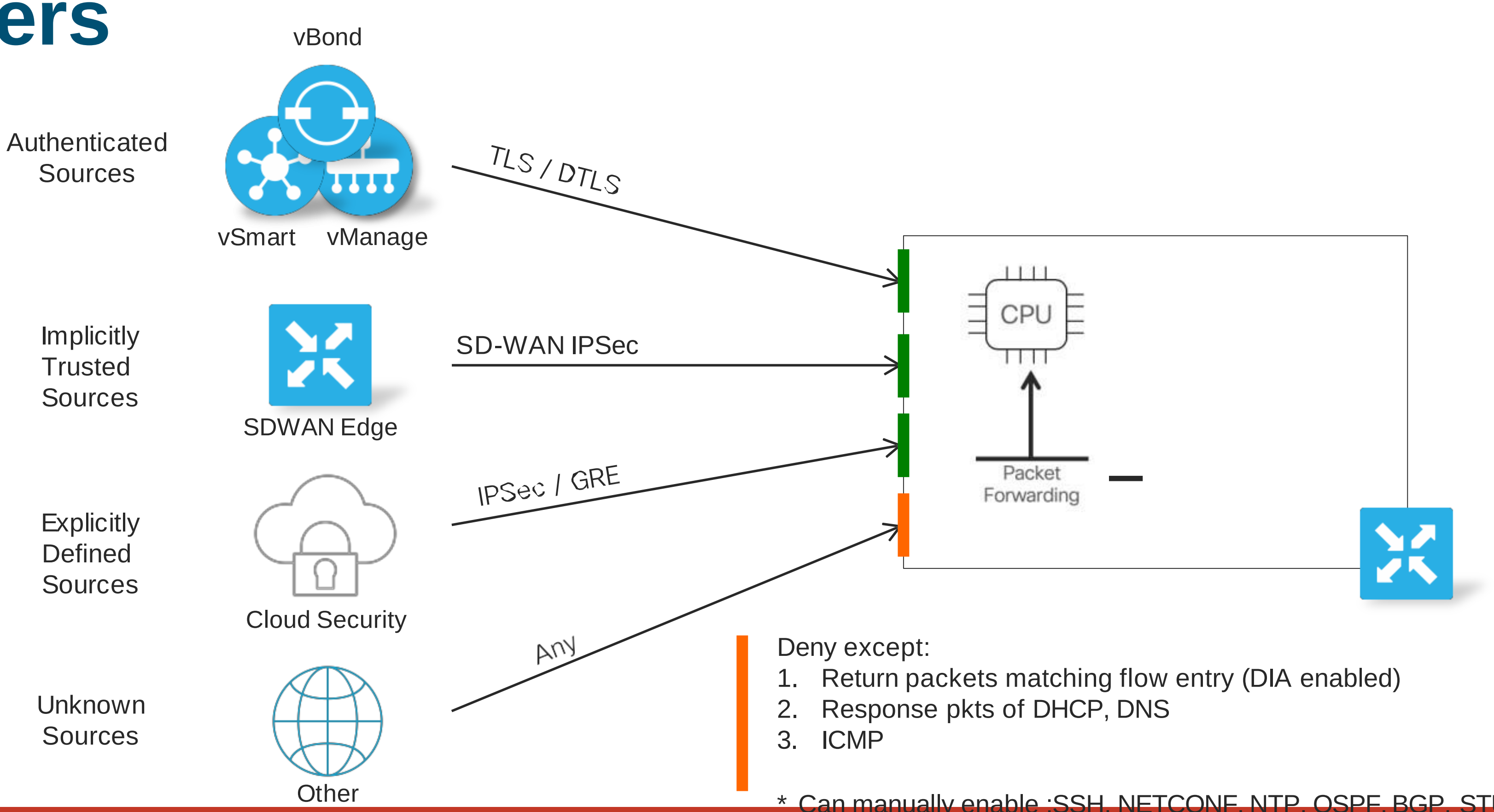
- 500pps per flow
- 10,000pps

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

Deny except:
DHCP, DNS, ICMP, NETCONF

* Can manually enable :SSH, NTP, STUN, HTTPS (vManage)

DDoS Protection for SDWAN Edge Routers

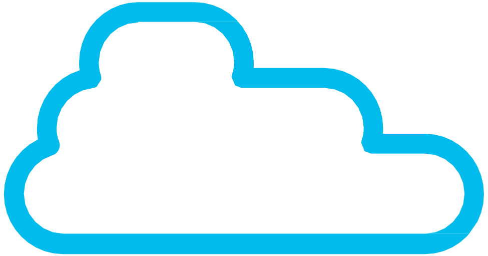


Deny except:

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

* Can manually enable :SSH, NETCONF, NTP, OSPF, BGP, STUN

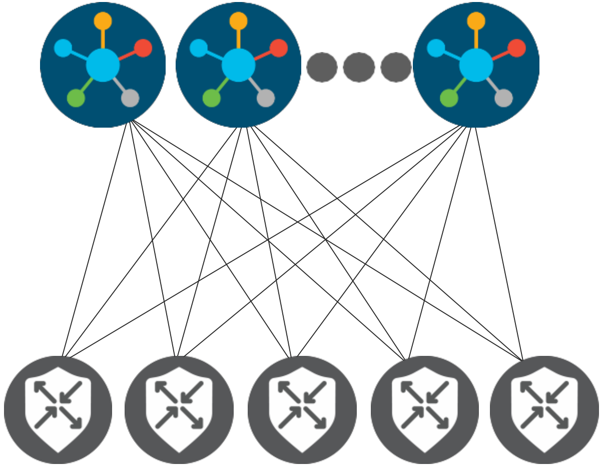
Secure Control Plane
&
Data Plane



Network-wide Control Plane

Cisco SD-WAN

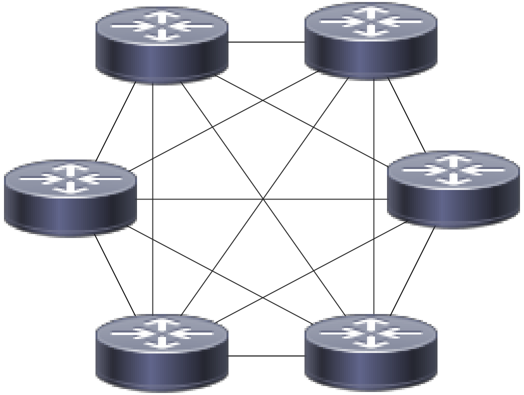
Network Control Plane



Data Plane + Local Control Plane

O(n) Control Complexity
High Scale

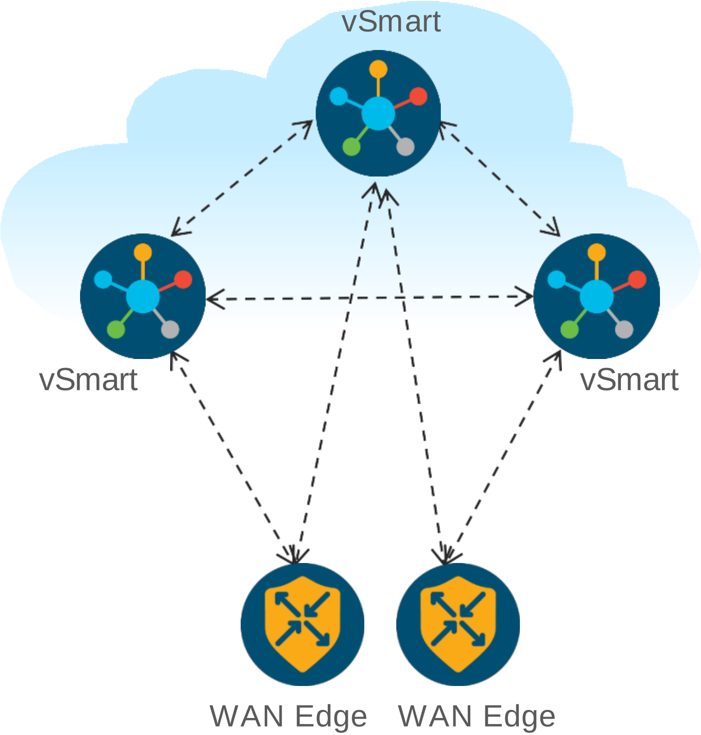
Traditional



Integrated Control and Data Plane

O(n^2) Control Complexity
Limited Scale

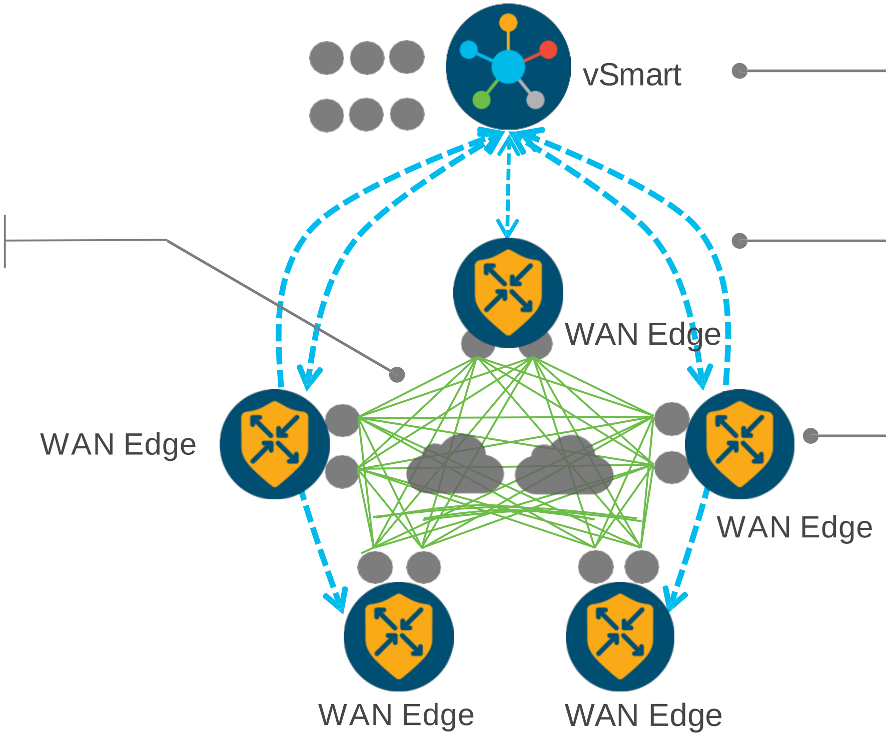
Overlay Management Protocol (OMP)



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

- TCP based extensible control plane protocol
- Runs between WAN Edge routers and vSmart controllers and between the vSmart controllers
    - Inside TLS/DTLS connections
- Leverages address families to advertise reachability for TLOCs, unicast/multicast destinations, service routes, BFD up/down stats and Cloud onRamp for SaaS probe stats
- Distributes IPSec encryption keys, and data and app-aware policies

Transport Locators (TLOCs)



Full Mesh
SD-WAN Fabric
(Default)

vSmarts advertise TLOCs to
all WAN Edges*
(Default)

TLOCs advertised to vSmarts

Local TLOCs
(System IP, Color, Encap)

● Transport Locator (TLOC) — OMP — IPSec Tunnel

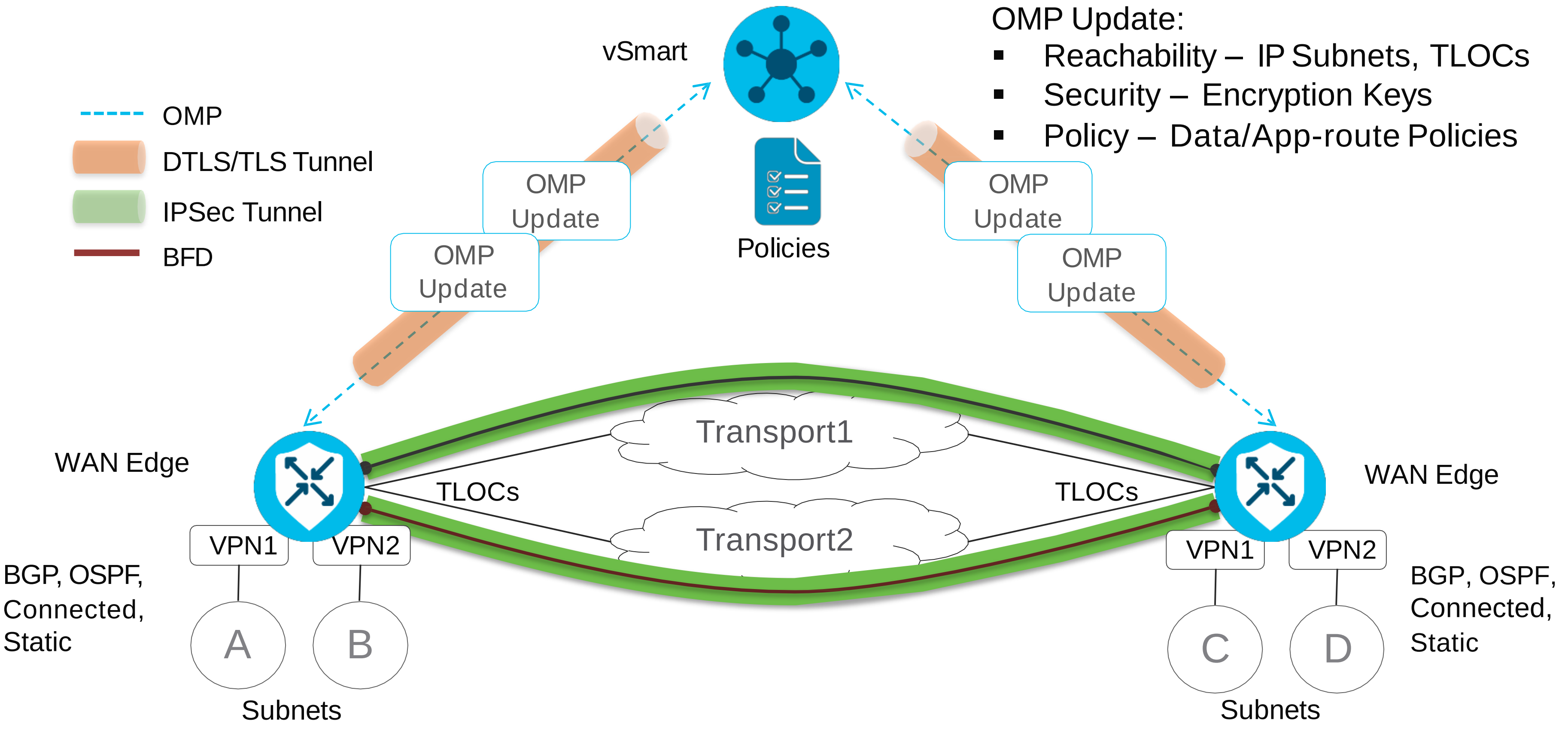
* Can be influenced by the control policies

Secure Data Plane

SD-WAN Fabric Operation Walk-Through

OMP Update:

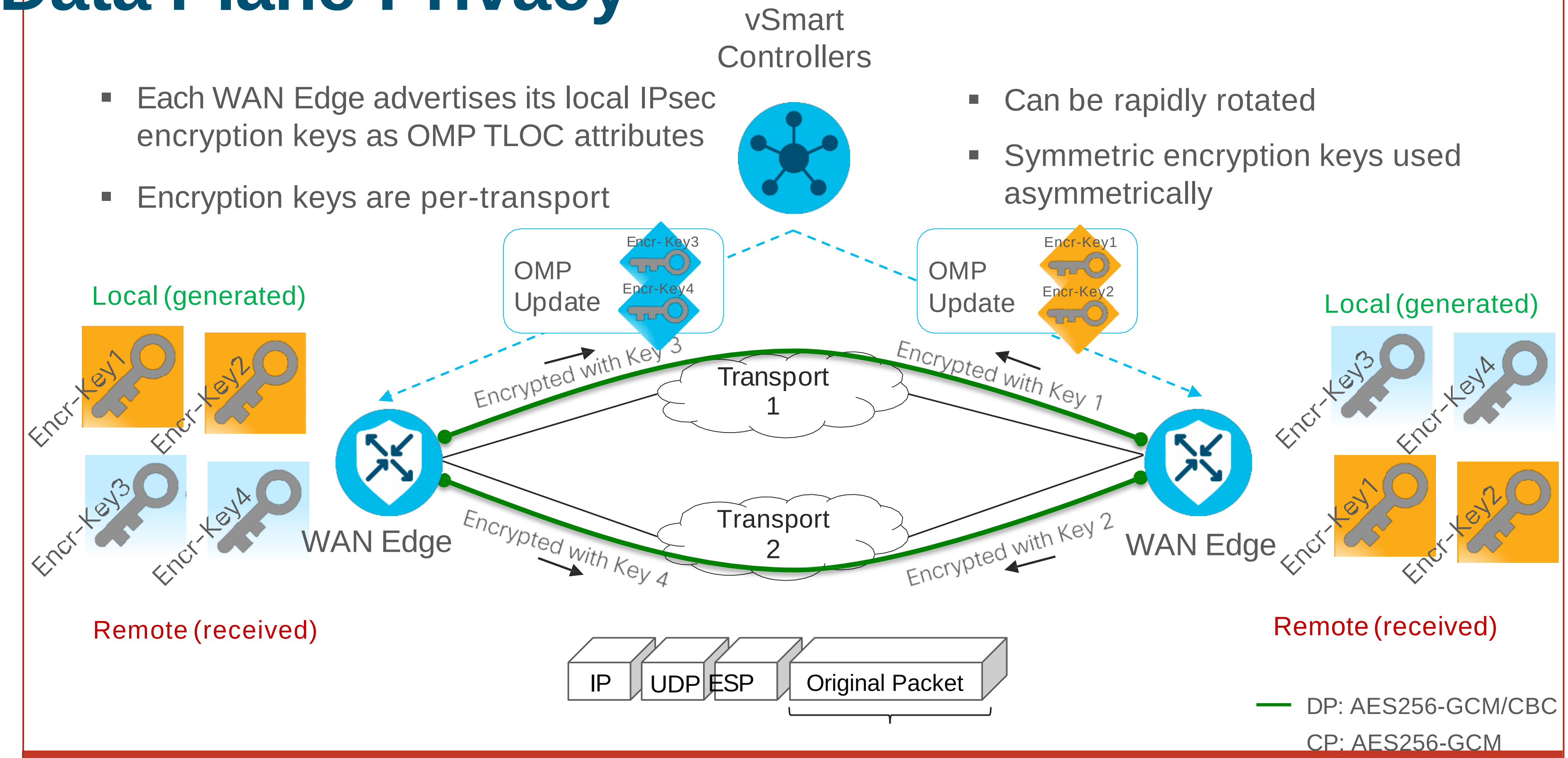
- Reachability – IP Subnets, TLOCs
- Security – Encryption Keys
- Policy – Data/App-route Policies



Data Plane Privacy

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

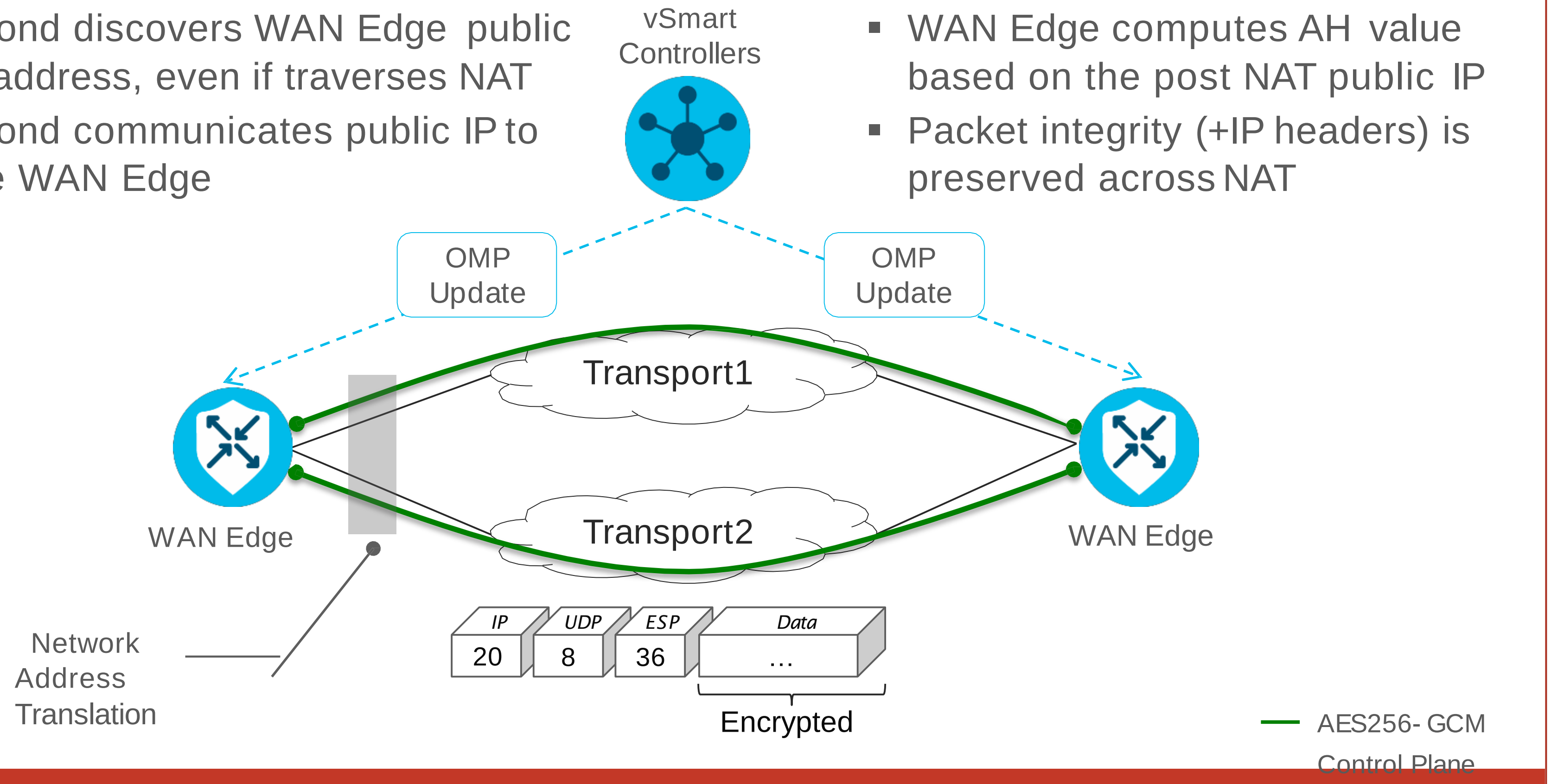
- Can be rapidly rotated
- Symmetric encryption keys used asymmetrically



Data Plane Integrity

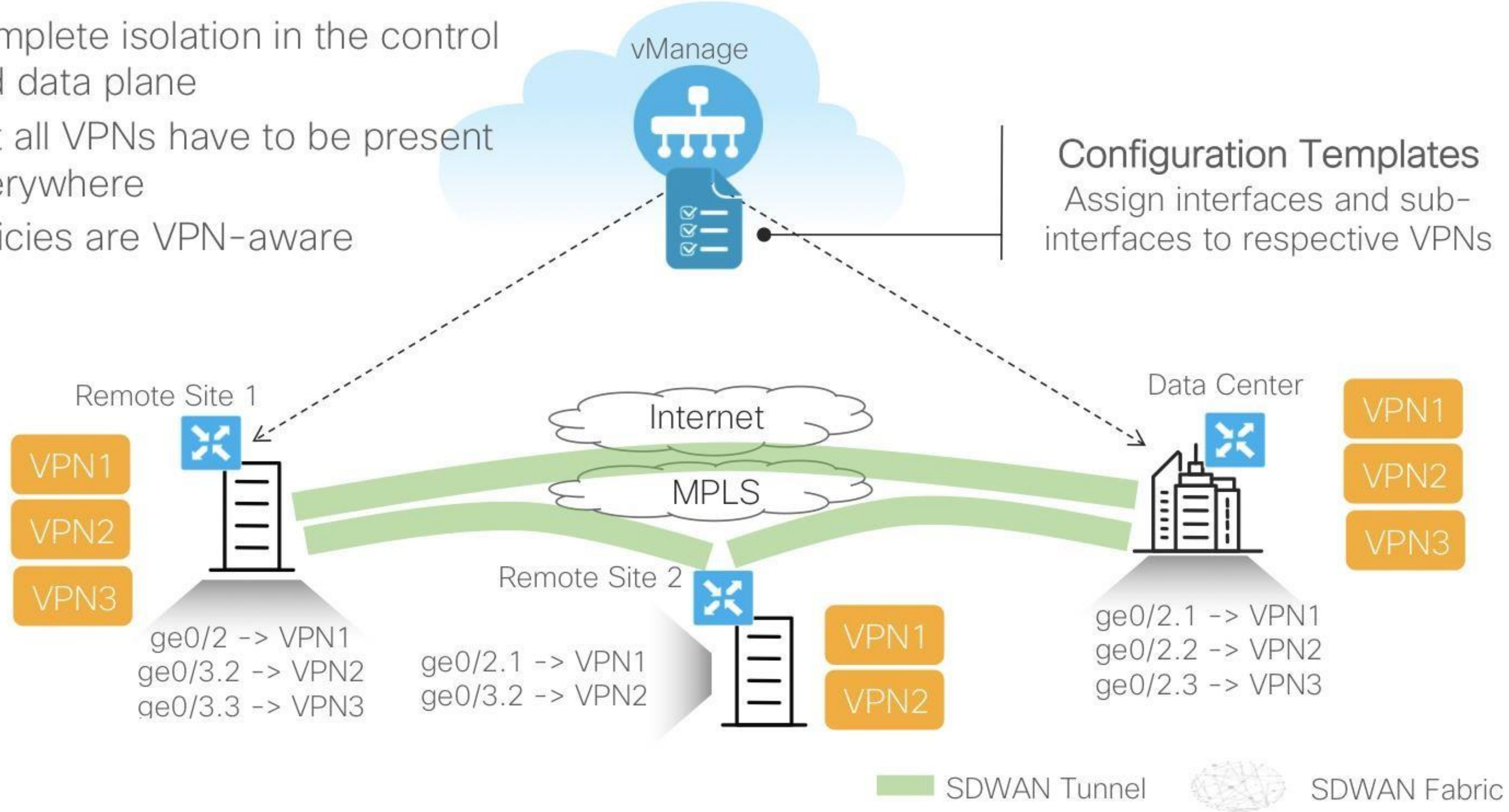
- vBond discovers WAN Edge public IP address, even if traverses NAT
- vBond communicates public IP to the WAN Edge

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



Secure Segmentation

- Complete isolation in the control and data plane
- Not all VPNs have to be present everywhere
- Policies are VPN-aware



Configuration Templates

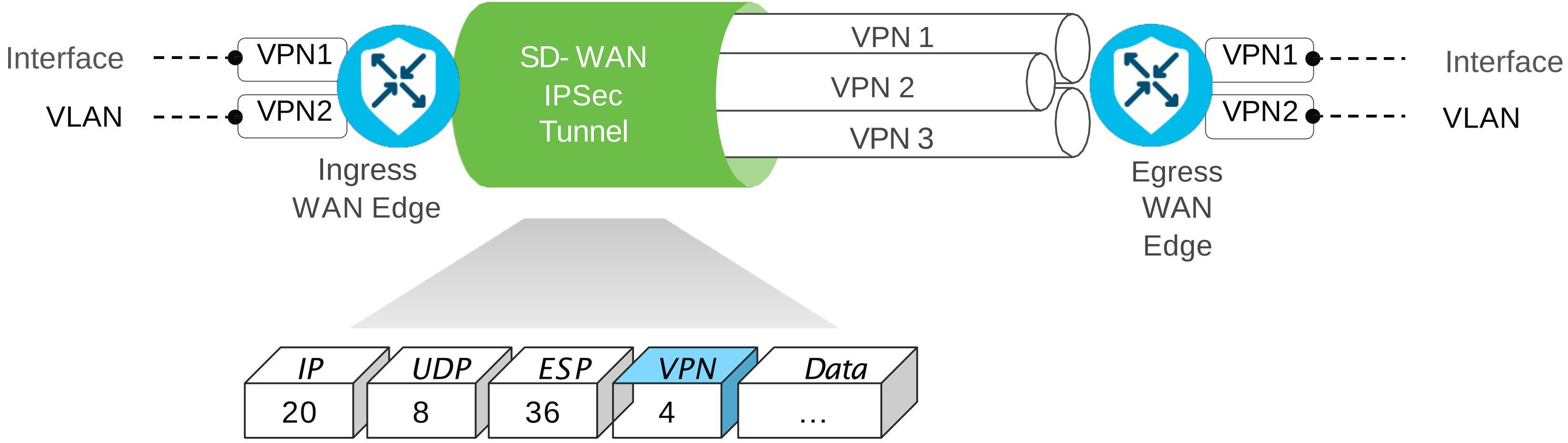
Assign interfaces and sub-interfaces to respective VPNs

Remote Site 1:
ge0/2 -> VPN1
ge0/3.2 -> VPN2
ge0/3.3 -> VPN3

Remote Site 2:
ge0/2.1 -> VPN1
ge0/3.2 -> VPN2

Data Center:
ge0/2.1 -> VPN1
ge0/2.2 -> VPN2
ge0/2.3 -> VPN3

End-to-End Segmentation

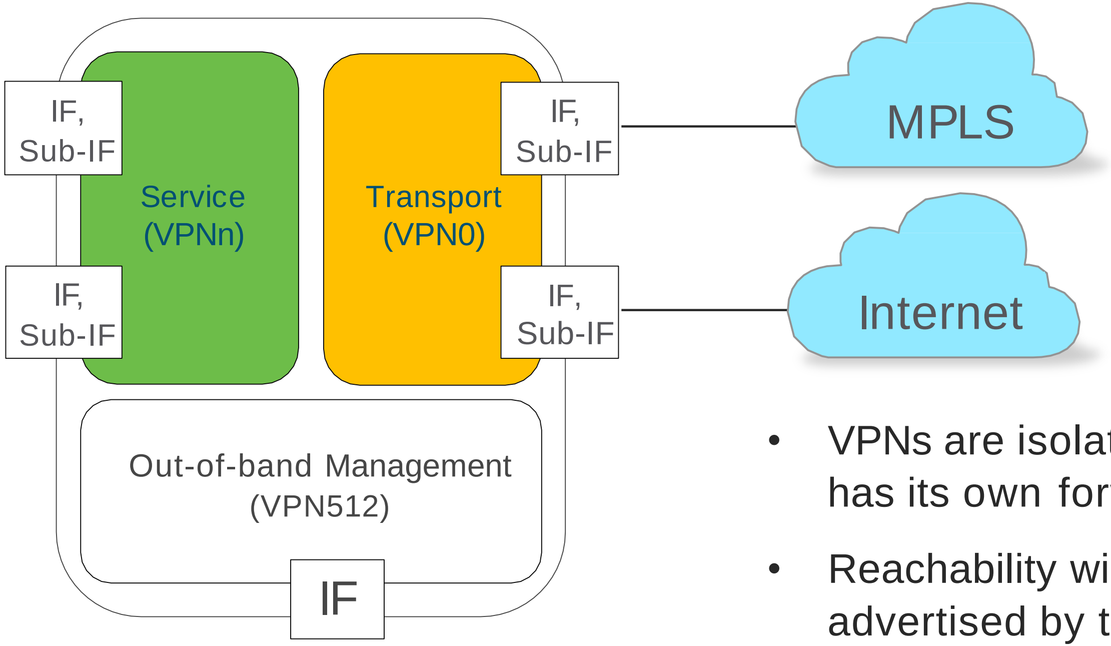


- Segment connectivity across fabric w/o reliance on underlay transport
- WAN Edge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup (rfc 4023)
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs

SDWAN VPNs and Security Zoning

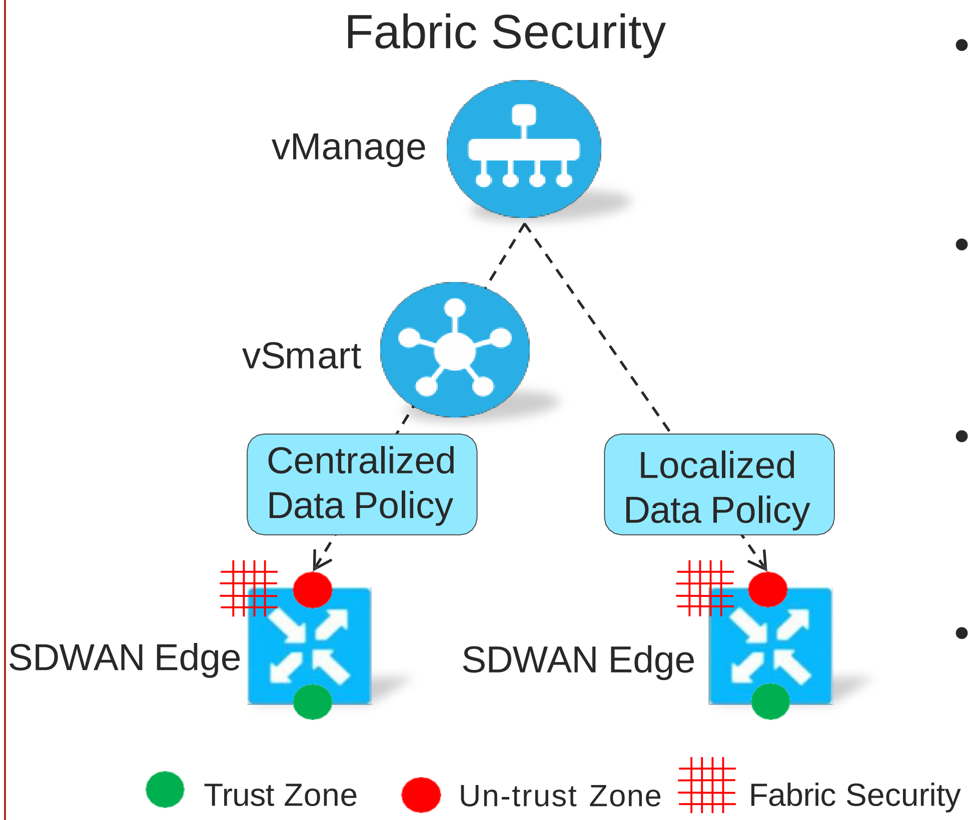
🟩 Trust Zone

🟨 Untrust Zone



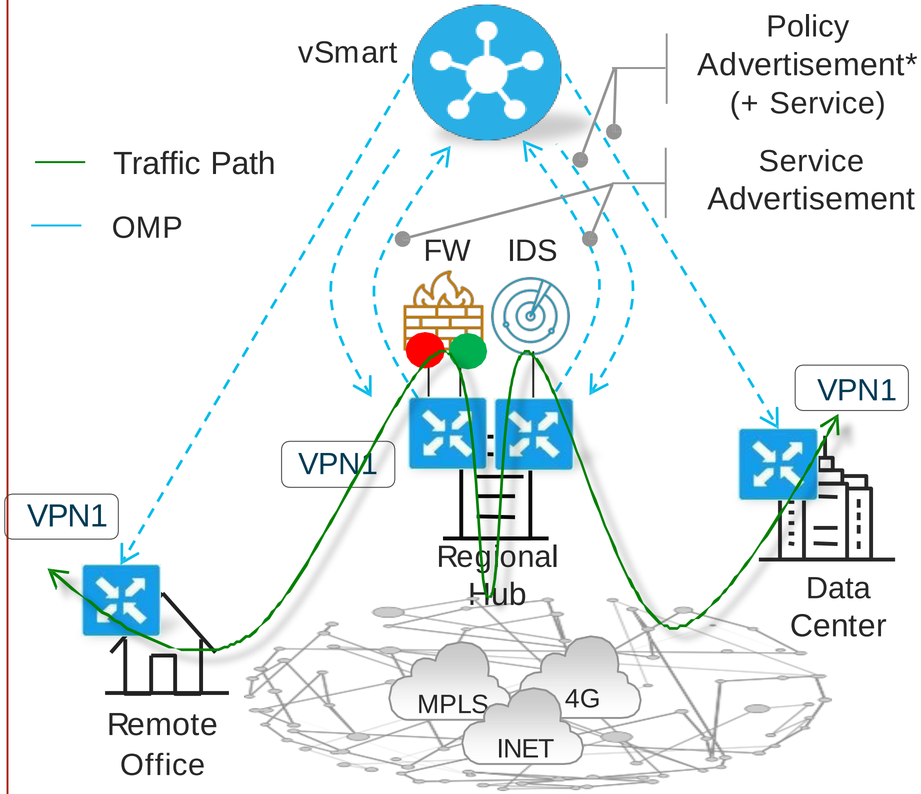
- VPNs are isolated from each other, each VPN has its own forwarding table
- Reachability within VPN is automatically advertised by the OMP

Local SD-WAN Fabric Secure Perimeter



- Centralized data policy is defined on vManage and distributed by vSmart controllers
- Centralized data policy match on application traffic of interest
  - DPI or 6 tuple matching
- Centralized data policy takes drop action to block unwanted traffic
  - Can log
- Localized data policy works similarly to centralized data policy, but it is distributed directly from vManage

Regional Secure Perimeter – Multiple Services



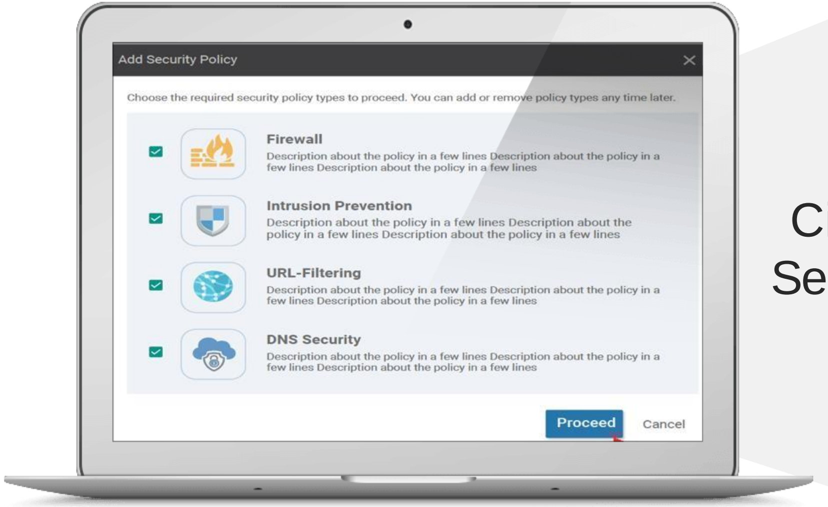
* For data policy only. Control policy enforced on vSmart.

- **Service nodes are connected to SDWAN Edge**
  - Directly or IPSec IKE v1/v2
  - Routed or bridged
- **Service nodes can be connected to different**

  SDWAN Edge routers
  - Can be in different sites
- **SDWAN Edge routers advertise service**
  - **Service route + Service label**
  - **Specific VPN**
- **Observe Firewall trust and untrust zones**
- **Control or data policies are used to insert the service nodes**

Combining Best of Breed in Security and SD-WAN

What is Cisco SD-WAN 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

Proceed Cancel

Cisco SD-WAN

Cisco Security

Enterprise Firewall
+1400 layer 7 apps classified

Intrusion Prevention System
Most widely deployed IPS engine in the world

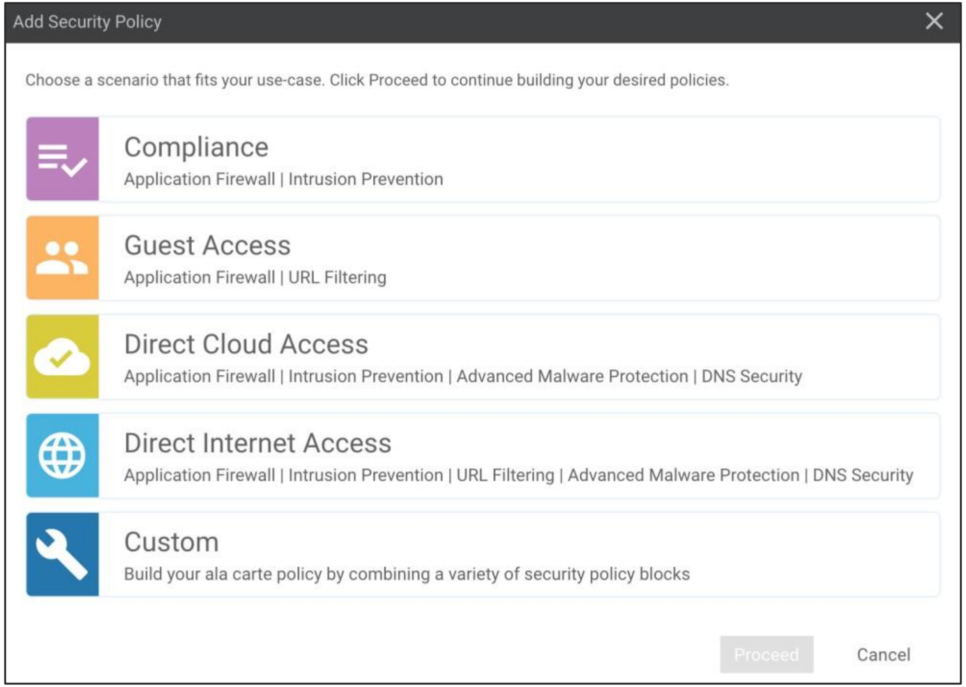
URL–Filtering
Web reputation score using 82+ web categories

Adv. Malware Protection
With File Reputation and Sandboxing

Simplified Cloud Security
Easy Deployment for Cisco Umbrella

Hours instead of weeks and months

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

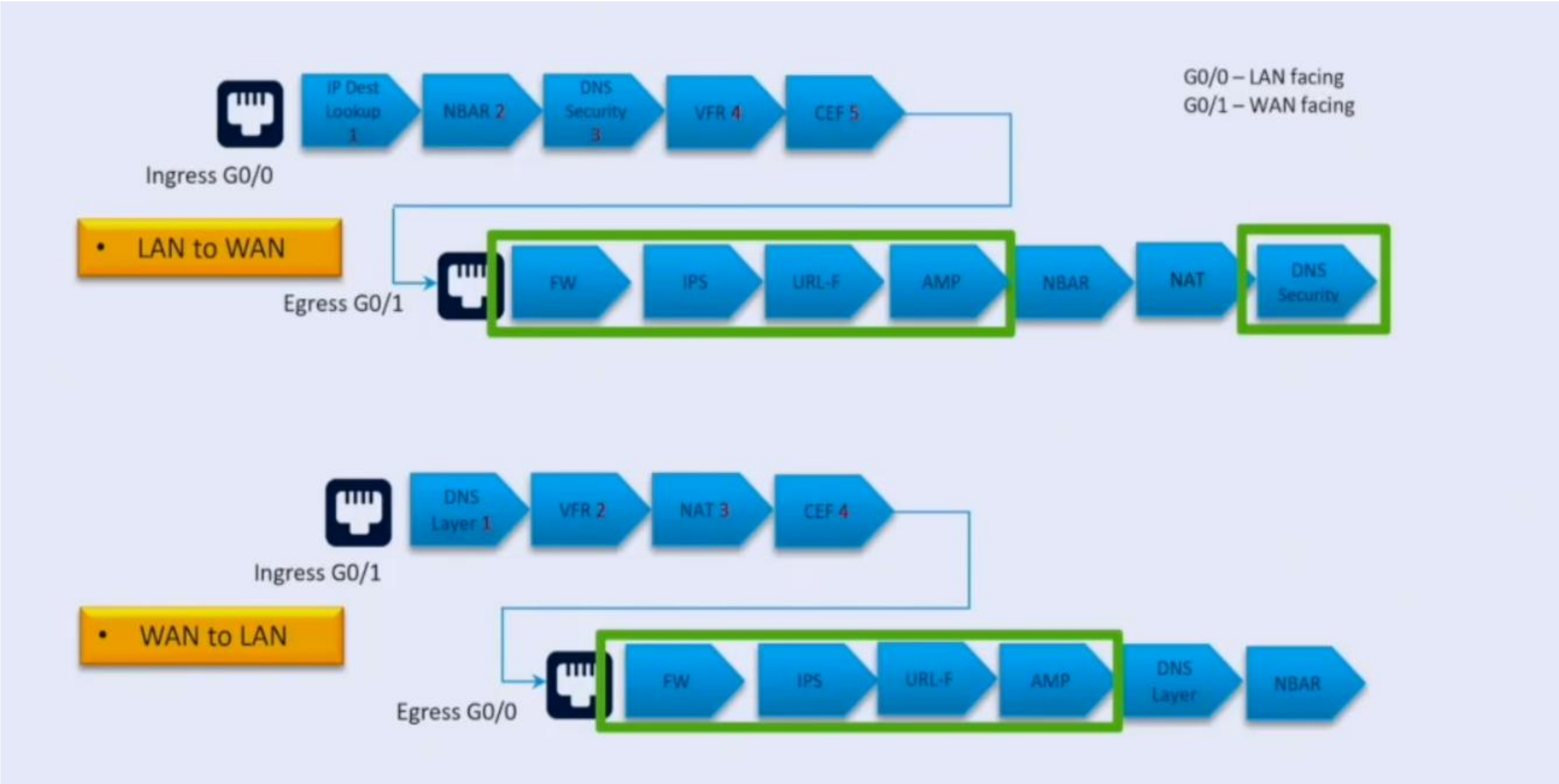
Direct Cloud Access
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security

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

Configuration > Security

Firewall DNS & IPS



G0/0 – LAN facing
G0/1 – WAN facing

- LAN to WAN

Ingress G0/0

IP Dest Lookup 1 → NBAR 2 → DNS Security 3 → VFR 4 → CEF 5

Egress G0/1

FW → IPS → URL-F → AMP → NBAR → NAT → DNS Security

- WAN to LAN

Ingress G0/1

DNS Layer 1 → VFR 2 → NAT 3 → CEF 4

Egress G0/0

FW → IPS → URL-F → AMP → DNS Layer → NBAR

SD-WAN Security Features

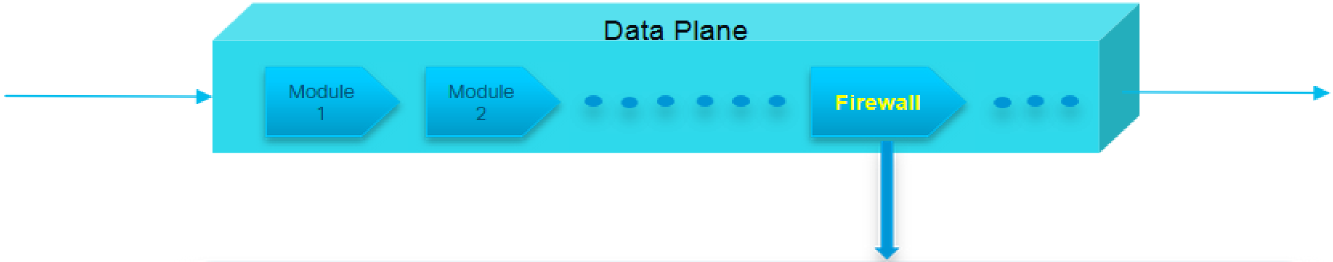
- App firewall – Implemented using Network Based Application Recognition (NBAR) engine.

- DNS Security – DNS requests (DNS-crypt) send to cloud where URL based filtering can be done.

- App Firewall and DNS Security modules are implemented in IOS data plane.

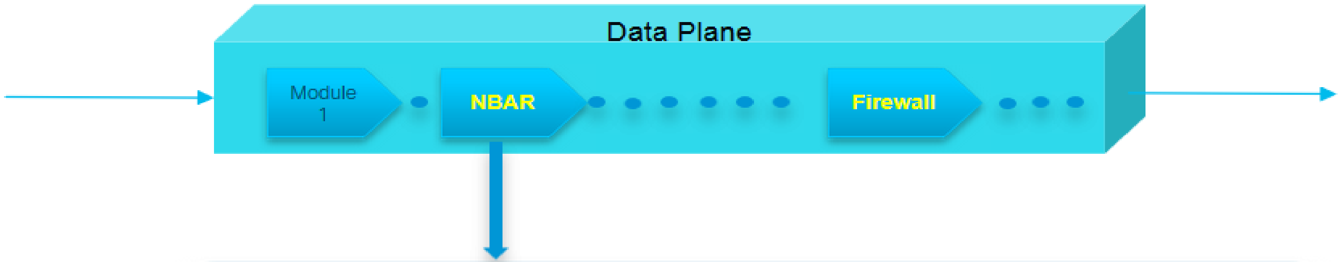
- IPS/IDS, Web-Filtering and AMP modules are implemented in LXC (Linux containers).

Stateful Firewall



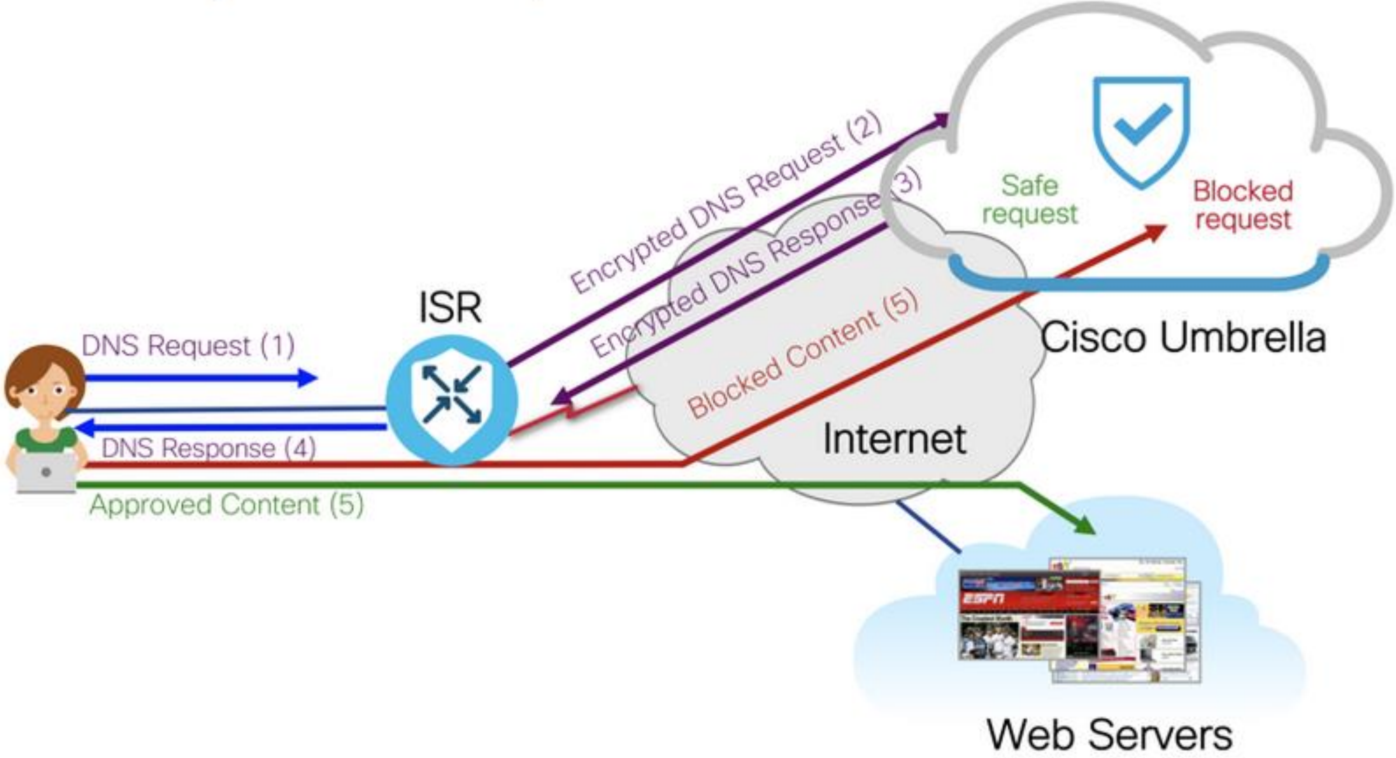
- Builds sessions to allow return traffic
  - TCP Enforcement
    - First packet must be a SYN
    - 3-way handshake must be completed before data is transferred
    - All subsequent traffic must fall within TCP window
- Stateful checking of traffic
  - Examines Layer 4 header, Verifies TCP Sequence and Acknowledgement numbers, Verifies TCP flags

Application Firewall

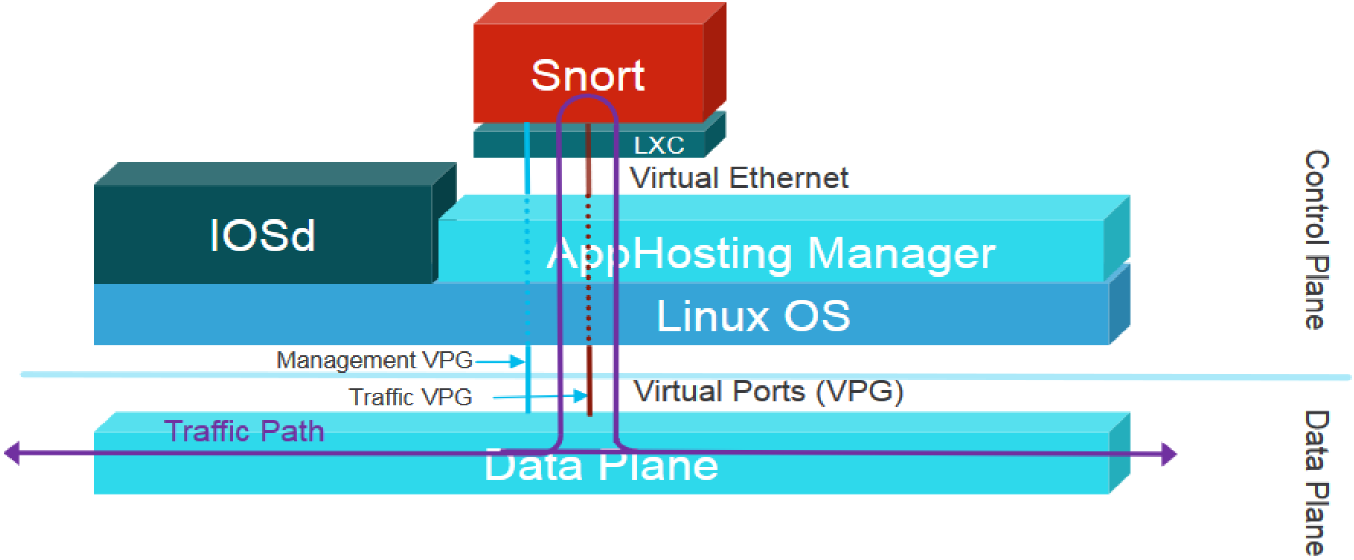


- ➢ NBAR engine will be added to data path once Application Visibility control (AVC) class map is configured.
- ➢ NBAR inspects L7 traffic and verifies packet conforms to application specification.
- ➢ NBAR attaches AppID in the packets meta data and firewall module does action based on the AppId.

DNS/web-layer Security - Solution Overview



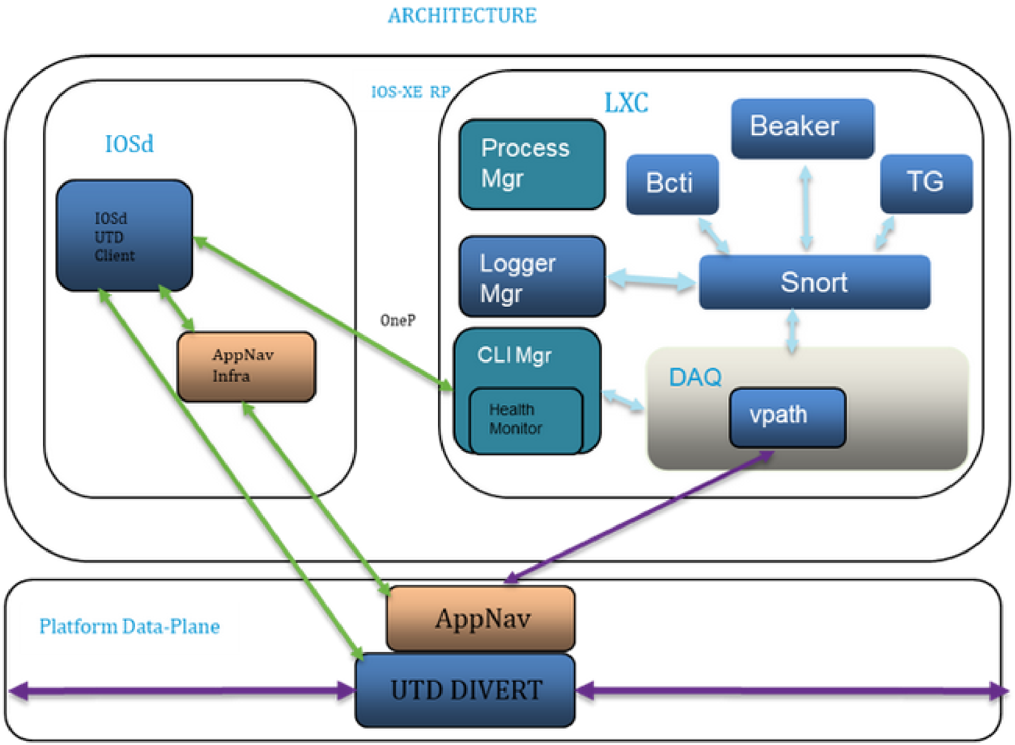
Snort IPS/IDS, URL Filtering & AMP Architecture



- IPS 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

Container Architecture & installation

Container Architecture



Control Plane:

IOSd takes care of app hosting installation, configuration and provisioning of feature to both service plane and data plane.

Data Plane:

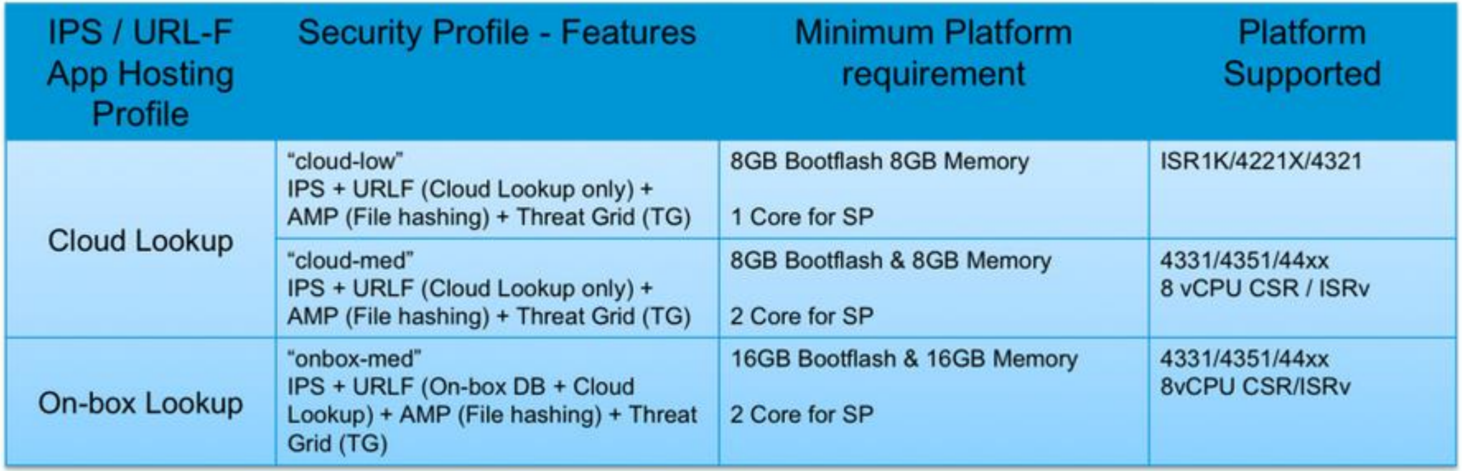
UTD divert feature in the Data Plane will divert the packets from the Data Plane to the Snort Container via AppNav GRE tunnel.

Snort injects the packets back into Data Plane which are handled by the UTD feature in the Data plane

Service Plane:

This houses open source snort engine, AppNAV health reporting agent, DAQ for processing packet data and Event/Log manager that is responsible for sending alerts to IOSd syslog or external server.

Security App Hosting Profile & Resources



IPS / URL-F App Hosting Profile	Security Profile - Features	Minimum Platform requirement	Platform Supported
Cloud Lookup	"cloud-low" IPS + URLF (Cloud Lookup only) + AMP (File hashing) + Threat Grid (TG)	8GB Bootflash 8GB Memory 1 Core for SP	ISR1K/4221X/4321
	"cloud-med" IPS + URLF (Cloud Lookup only) + AMP (File hashing) + Threat Grid (TG)	8GB Bootflash & 8GB Memory 2 Core for SP	4331/4351/44xx 8 vCPU CSR / ISRv
On-box Lookup	"onbox-med" IPS + URLF (On-box DB + Cloud Lookup) + AMP (File hashing) + Threat Grid (TG)	16GB Bootflash & 16GB Memory 2 Core for SP	4331/4351/44xx 8vCPU CSR/ISRv

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

Container Installation

Install application

- vManage installs LXC container on Edges as part of template push if the security policy template is attached to device template.
- Requires a UTD TAR file in Virtual Images Software Repository with a compatible app version
- UTD TAR file downloaded from CCO store

•N.B: Each router image version (16.10, 16.11, 16,12 etc.) has its own range of supported app versions for container application

TAR file name	Applicable platform
secapp-*.x86_64.tar	x86_64 - ISR-42xx ISR-43xx ISR-44xx CSR
secapp-*.aarch64_be.tar	ARM-based - C1111X-8P..

ABC of Cisco SDWAN Viptela Qos

Forwarding and QoS Overview

- Forwarding is the transmitting of data packets from one vEdge router to another. Once the control plane connections of the Viptela overlay network are up and running, data traffic flows automatically over the IPsec connections between vEdge routers.

- Using forwarding, there are ways you can affect the flow of data traffic. Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote vEdge router.

- To modify the default data packet forwarding flow, you create and apply centralized data policy or localized data policy. With centralized data policy, you can manage the paths along which traffic is routed through the network, and you can permit or block traffic based on the address, port, and DSCP fields in the packet's IP header. With localized data policy, you can control the flow of data traffic into and out of a vEdge router's interfaces, enabling features such as quality of service (QoS) and mirroring. Note that QoS is synonymous with class of service (CoS).

Default Behavior without Data Policy

When no centralized data policy is configured on the vSmart controller, all data traffic is transmitted from the local service-side network to the local vEdge router, and then to the remote vEdge router and the remote service-side network, with no alterations in its path. When no access lists are configured on the local vEdge router to implement QoS or mirroring, the data traffic is transmitted to its destination with no alterations to its flow properties.

Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured

- A data packet arriving from the local service-side network and destined for the remote service-side network comes to the vEdge-1 router. The packet has a source IP address and a destination IP address.
- The vEdge router looks up the outbound SA in its VPN route table, and the packet is encrypted with SA and gets the local TLOC. (The vEdge router previously received its SA from the vSmart controller. There is one SA per TLOC. More specifically, each TLOC has two SAs, an outbound SA for encryption and an inbound SA for decryption.)

- ESP adds an IPsec tunnel header to the packet.
- An outer header is added to the packet. At this point, the packet header has these contents: TLOC source address, TLOC destination address, ESP header, destination IP address, and source IP address.

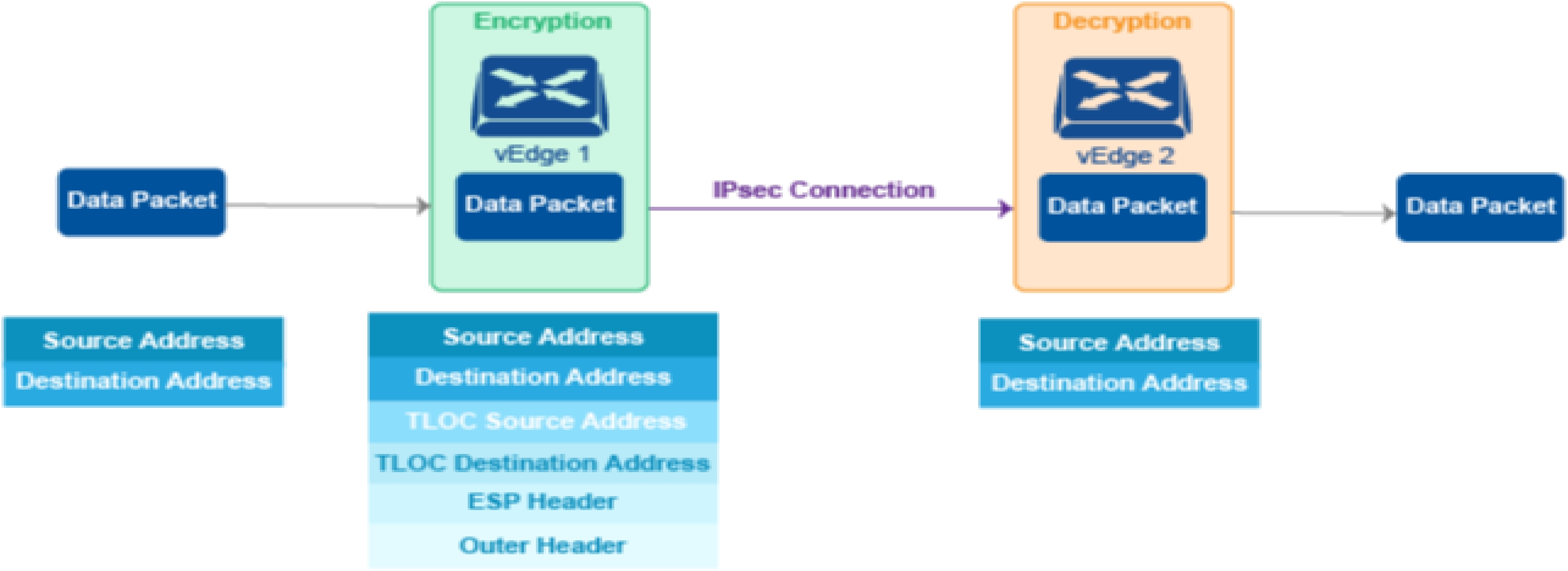
- The vEdge router checks the local route table to determine which interface the packet should use to reach its destination.

- The data packet is sent out on the specified interface, onto the network, to its destination. At this point, the packet is being transported within an IPsec connection.

- When the packet is received by the vEdge router on the remote service-side network, the TLOC source address and TLOC destination address header fields are removed, and the inbound SA is used to decrypt the packet.

- The remote vEdge router looks up the destination IP address in its route table to determine the interface to use to reach to the service-side destination.

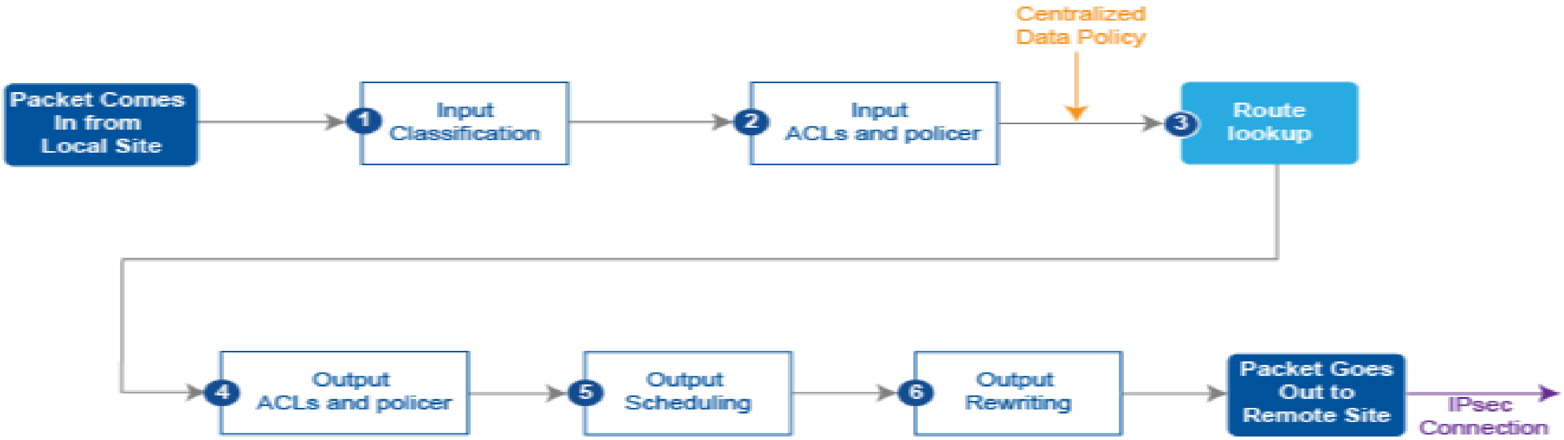
The figure below details this process



Behavior Changes with QoS Data Policy

When you want to modify the default packet forwarding flow, you design and provision QoS policy. To activate the policy, you apply it to specific interfaces in the overlay network in either the inbound or the outbound direction. The direction is with respect to the vEdge routers in the network.

You can have policies for packets coming in on an interface or for packets going out of an interface. The figure below illustrates the QoS policies that you can apply to a data packet as it is transmitted from one branch to another. The policies marked Input are applied on the inbound interface to the vEdge router, and the policies marked Output are applied on the outbound interface to the vEdge router, before the packets are transmitted out the IPSec tunnel.



The table below describes each of the above steps

Steps	Description	Comments
1	Define class map to classify packets, by importance, into appropriate forwarding classes. Reference the class map in an access list.	Class-map
2	Define policer to specify the rate at which traffic is sent on the interface. Reference the policer in an access list. Apply the access list on an inbound interface.	Policer
3	vEdge router checks the local route table to determine which interface the packet should use to reach its destination.	N/A
4	Define policer and reference the policer in an access list. Apply the access list on an outbound interface.	Policer
5	Define QoS map to define the priority of data packets. Apply the QoS map on the outbound interface.	Qos-map
6	Define rewrite-rule to overwrite the DSCP field of the outer IP header. Apply the rewrite-rule on the outbound interface.	Rewrite-rule

Understanding How QoS Works

The QoS feature on the vEdge routers works by examining packets entering at the edge of the network. With localized data policy, also called access lists, you can provision QoS to classify incoming data packets into multiple forwarding classes based on importance, spread the classes across different interface queues, and schedule the transmission rate level for each queue. Access lists can be applied either in the outbound direction on the interface (as the data packet travels from the local service-side network into the IPsec tunnel toward the remote service-side network) or in the inbound direction (as data packets are exiting from the IPsec tunnel and being received by the local vEdge router.

To provision QoS, you must configure each vEdge router in the network. Generally, each router on the local serviceside network examines the QoS settings of the packets that enter it, determines which packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

Classify Data Packets

- You can classify incoming traffic by associating each packet with a forwarding class. Forwarding classes group data packets for transmission to their destination. Based on the forwarding class, you assign packets to output queues. The vEdge routers service the output queues according to the associated forwarding, scheduling, and rewriting policies you configure.

Schedule Data Packets

You can configure a QoS map for each output queue to specify the bandwidth, delay buffer size, and packet loss priority (PLP) of output queues. This enables you to determine how to prioritize data packets for transmission to the destination. Depending on the priority of the traffic, you can assign packets higher or lower bandwidth, buffer levels, and drop profiles. Based on the conditions defined in the QoS map, packets are forwarded to the next hop. On hardware vEdge routers, each interface haseight queues, which are numbered 0 to 7.

Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ. All control traffic is transmitted. Queues 1 to 7 are available for data traffic, and the default scheduling for these seven queues is weighted round-robin (WRR). For these queues, you can define the weighting according to the needs of your network. On Cloud vEdge virtualized routers, each interface has four queues, numbered from 0 through 3. Queue 0 is reserved for control traffic, and queues 1, 2, and 3 are available for data traffic. The scheduling method for all four queues is WRR. LLQ is not supported

Rewrite Data Packets

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network. Rewrite rules allow you to map traffic to code points when the traffic exits the system.

Rewrite rules use the forwarding class information and packet loss priority (PLP) used internally by the vEdge routers to establish the DSCP value on outbound packets. You can then configure algorithms such as RED/ WRED to set the probability that packets will be dropped based on their DSCP value.

Police Data Packets

You can configure policers to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels. Traffic that conforms to the policer rate is transmitted, and traffic that exceeds the policer rate is sent with a decreased priority or is dropped.

You can apply a policer to inbound or outbound interface traffic. Policers applied to inbound interface traffic allow you to conserve resources by dropping traffic that does not need to be routed through the network. Policers applied to outbound interface traffic control the amount of bandwidth used.

Forwarding and QoS Configuration Examples

- This section shows examples of how you can use access lists to configure quality of service (QoS), classifying data packets and prioritizing the transmission properties for different classes. Note that QoS is synonymous with class of service (CoS).

Forwarding and QoS Example

This example shows how to configure class of service (CoS) to classify data packets and control how traffic flows out of and in to the interfaces on a vEdge router and on the interface queues.

To configure a QoS policy:

1. Map each forwarding class to an output queue.
2. Configure the QoS scheduler for each forwarding class.
3. Group the QoS schedulers into a QoS map.
4. Define an access list to specify match conditions for packet transmission.
5. Apply the access list to a specific interface.
6. Apply the queue map and the rewrite rule to the egress interface.

The sections below show examples of each of these steps

Map Forwarding Class to Output Queue

This example shows a data policy that classifies incoming traffic by mapping each forwarding class to an output queue. Here, traffic classified as "be" (Best Effort) is mapped to queue 2, traffic classified as "af1" (Assured Forwarding) is mapped to queue 3, and so on.

```
policy
class-map
class be queue 2
class af1 queue 3
class af2 queue 4
class af3 queue 5
!
 !
```

Configure QoS Scheduler for Each Forwarding Class

This example illustrates how to configure the QoS scheduler for each queue to define the importance of data packets. Depending on the priority of the traffic, you assign the bandwidth, buffer level, and random early detection (RED) drop profile associated with the queue.

Here, "af3" traffic has higher priority over other traffic classes and so is configured to have 40% bandwidth and 40% buffer. Traffic in class "af2" has 30% bandwidth and 30% buffer; traffic in class "af1" class has 20% bandwidth and 20% buffer and traffic in class "be" has 10% bandwidth and 10% buffer size reflecting the respective priority of the traffic on the network.

All traffic classes are configured with a drop profile of RED, meaning that instead of waiting for the queue to be full, packets are dropped randomly based on the thresholds defined.

```
qos-scheduler af1
class           af1
bandwidth-percent 20
buffer-percent   20
drops           red-drop
!
qos-scheduler af2
class           af2
bandwidth-percent 30
buffer-percent   30
drops           red-drop
 !
qos-scheduler af3
class           af3
bandwidth-percent 40
buffer-percent   40
drops           red-drop
!
qos-scheduler be
class           be
bandwidth-percent 10
buffer-percent   10
drops          red-drop
 !
```

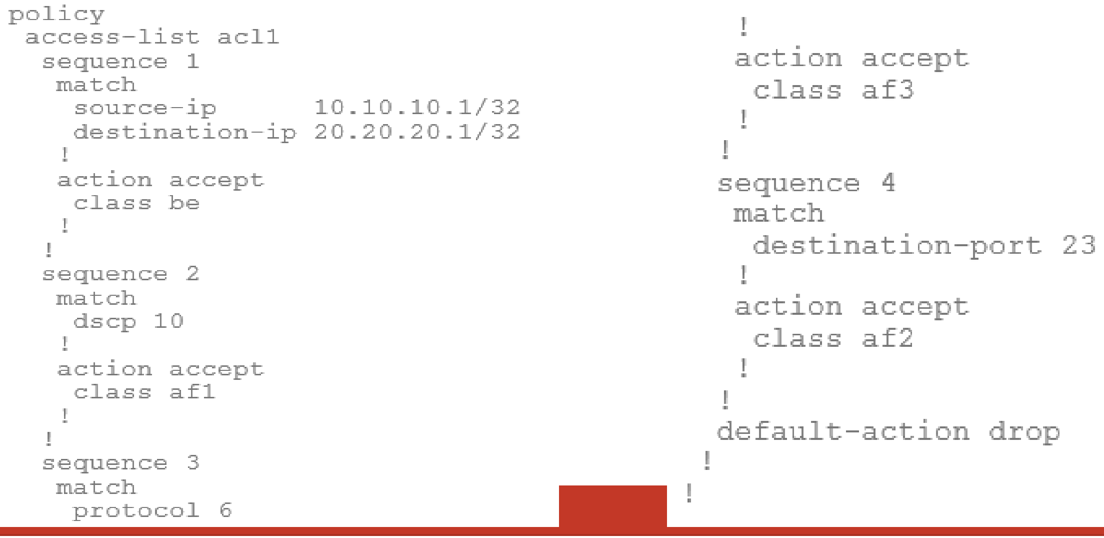
Group QoS Schedulers into a QoS Map

This example illustrates the grouping of "qos scheduler af1," "qos scheduler af2," and "qos scheduler be" into a single QoS map called "test."

```
qos-map test
    qos-scheduler af1
    qos-scheduler af2
    qos-scheduler be
!
!
```

Classify Data Packets into Appropriate Class

This example shows how to classify data packets into appropriate forwarding classes based on match conditions. Here "access-list acl1" classifies data packets originating from the host at source address 10.10.10.1 and going to the destination host at 20.20.20.1 into the "be" class. Data packets with a DSCP value of 10 in the IP header field are classified in the "af1" class, TCP packets are classified in the "af3" class, and packets going to destination port 23, which carries Telnet mail traffic, are classified in the "af2" class. All other traffic is dropped.



```
policy
 access-list acl1
  sequence 1
   match
    source-ip      10.10.10.1/32
    destination-ip 20.20.20.1/32
   !
   action accept
    class be
   !
  !
  sequence 2
   match
    dscp 10
   !
   action accept
    class af1
   !
  !
  sequence 3
   match
    protocol 6
   !
   action accept
    class af3
   !
  !
  sequence 4
   match
    destination-port 23
   !
   action accept
    class af2
   !
  !
  default-action drop
 !
!
```

Apply Access List to Specific Interface

This example illustrates how to apply the access list defined above on the input of a service interface. Here "access-list acl1" is applied on the input of interface ge0/4 in VPN 1.

```
vpn 1
interface ge0/4
 ip address 10.20.24.15/24
no shutdown
access-list acl1 in
 !
!
```

Configure Rewrite Rule

This example shows how to configure the rewrite rule to overwrite the DSCP field of the outer IP header. Here the rewrite rule "transport" overwrites the DSCP value for forwarding classes based on the drop profile. Since all classes are configured with RED drop, they can have one of two profiles: high drop or low drop.

The rewrite rule is applied only on the egress interface, so on the way out, packets classified as "af1" and a Packet Loss Priority (PLP) level of low are marked with a DSCP value of 3 in the IP header field, while "af1" packets with a PLP level of high are marked with 4. Similarly, "af2" packets with a PLP level of low are marked with a DSCP value of 5, while "af2" packets with a PLP level of high are marked with 6, and so on.

```
Policy
 rewrite-rule transport
class af1 low dscp 3
class af1 high dscp 4
class af2 low dscp 5
class af2 high dscp 6
class af3 low dscp 7
class af3 high dscp 8
class be low dscp 1
class be high dscp 2
 !
```

Apply the Queue Map and Rewrite Rule on an Interface

This example applies the queue map "test" and the rewrite rule "transport" to the egress interface ge0/0 in VPN 0. Queue maps and rewrite rules are applied only on outgoing traffic.

```
vpn 0
interface ge0/0
 ip address 10.1.15.15/24
tunnel-interface
preference 10
weight     10
color      lte
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service ntp
no allow-service stun
!
no shutdown
 qos-map  test
 rewrite-rule transport
!
```

Police Data Packets

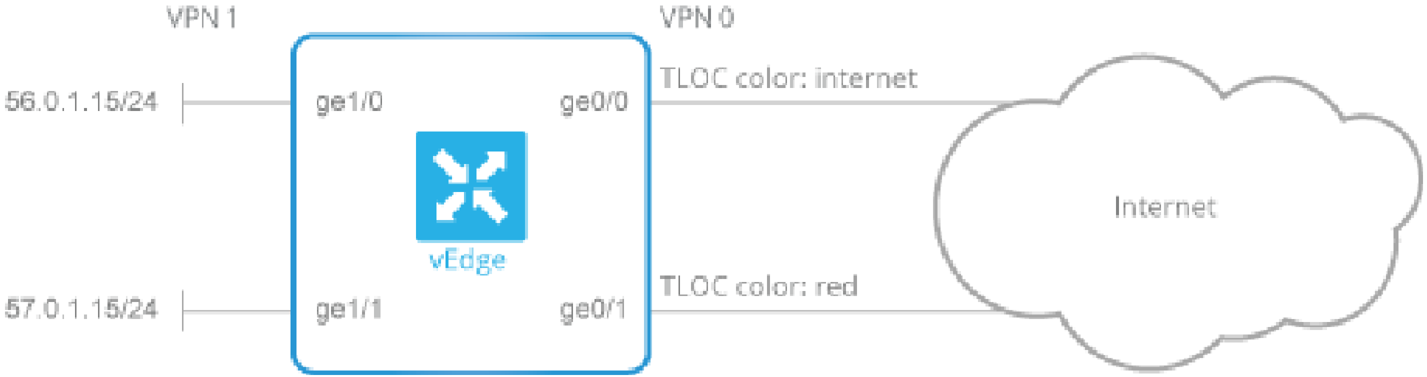
- This section shows two examples of policing data packets. The first example illustrates how to configure a policer to rate limit traffic received on an interface. After you configure the policer, include it in an access list. Here "policer p1" is configured to have a maximum traffic rate of 1,000,000 bits per second and a maximum burst-size limit of 15000 bytes.

- Traffic exceeding these rate limits is dropped. The policer is then included in the access list "acl1," which is configured to accept all TCP or UDP traffic originating from the host at source 2.2.0.0 and going to the destination host at 10.1.1.0 on port 20 or 100.1.1.0 on port 30. You can use "access-list acl1" on the input or output of the interface to do flow-based policing.

You can also apply a policer directly on an inbound or an outbound interface when you want to police all traffic ingressing or egressing this interface:

```
policy
policer p1
rate   1000000
burst  15000
exceed drop
!
 vpn 1
interface ge0/4
 ip address 10.20.24.15/24
no shutdown
policer p1 in
!
 vpn 2
interface ge0/0
 ip address 10.1.15.15/24
no shutdown
policer p1 out
!
```

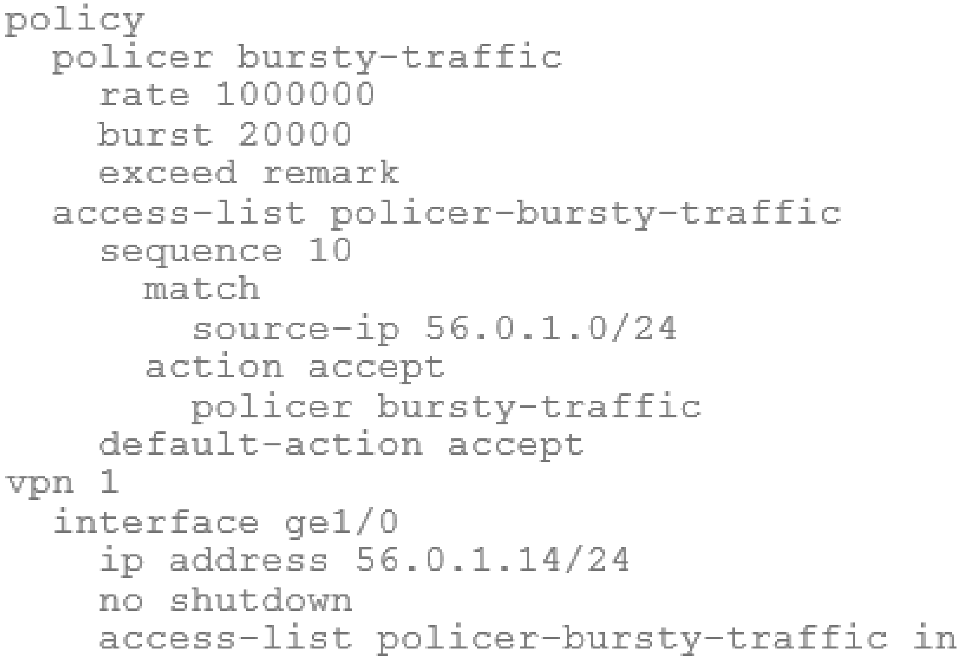
In the second example, we have a vEdge router with two WAN interfaces in VPN 0. The ge0/0 interface connects to a 30-MB link, and we want to always have 10 MB available for very high priority traffic.
When lower-priority traffic bursts exceed 20 MB, we want to redirect that traffic to the second WAN interface, ge0/1.



Implementing this traffic redirection requires two policies:

- You apply an access list to the service-side interface that polices the incoming data traffic.
- You apply a data policy to the ge0/0 WAN interface that directs bursty traffic to the second WAN interface, ge0/1.

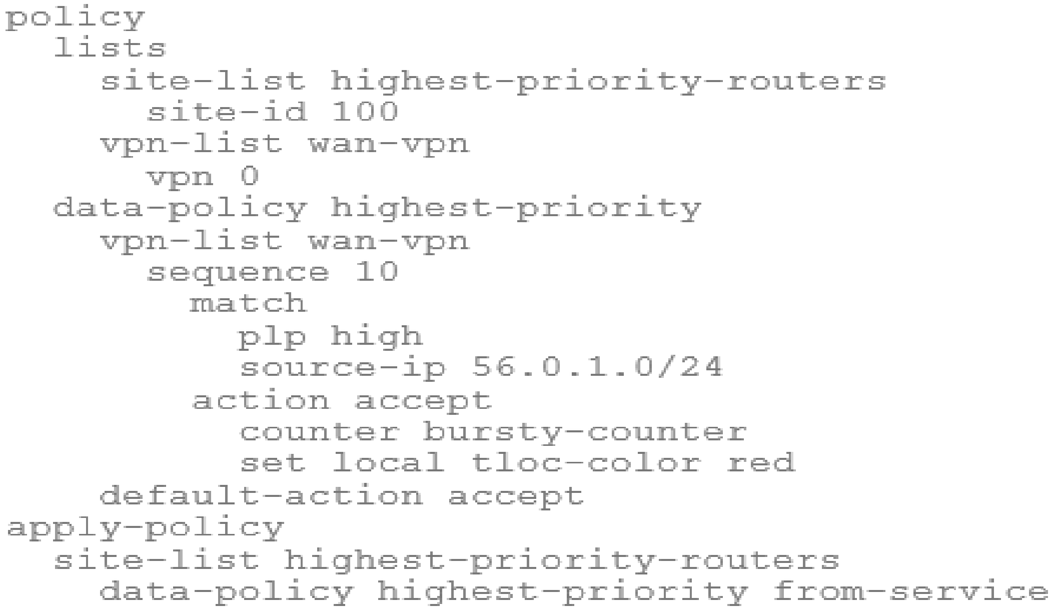
For the access list, the configuration snippet belows if for interface ge1/0, in VPN 1. The policer monitors incoming traffic on the interface. When traffic exceeds 20 MB (configured in the policer burst command), we change the PLP from low to high (configured by the policer exceed remark command). You configure the following on the vEdge router:



```
policy
  policer bursty-traffic
    rate 1000000
    burst 20000
    exceed remark
  access-list policer-bursty-traffic
    sequence 10
      match
        source-ip 56.0.1.0/24
      action accept
        policer bursty-traffic
    default-action accept
vpn 1
  interface ge1/0
    ip address 56.0.1.14/24
    no shutdown
    access-list policer-bursty-traffic in
```

To display a count of the packets that have been remarked, issue the show interface detail or the show system statistics command on the vEdge router. The count is reported in the rx-policer-remark field. The centralized data policy directs bursty traffic away from the ge0/0 interface (color: internet) to interface ge0/1 (color: red).

You apply this data policy to all the routers at a particular site, specifying the direction from-service so that the policy is applied only to traffic originating from the service side of the router. You configure the following on the vSmart controller:



```
policy
  lists
    site-list highest-priority-routers
      site-id 100
    vpn-list wan-vpn
      vpn 0
  data-policy highest-priority
    vpn-list wan-vpn
      sequence 10
        match
          plp high
          source-ip 56.0.1.0/24
        action accept
          counter bursty-counter
          set local tloc-color red
    default-action accept
apply-policy
  site-list highest-priority-routers
    data-policy highest-priority from-service
```

Thanks ☺