Cisco SD-WAN FedRAMP Overview

Technical Marketing Engineers

What and Why SD-WAN FedRAMP?

Federal Risk and Authorization Management Program

- Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services
- Saves cost, time, and staff required to conduct redundant Agency security assessments
- Cloud based Controllers that are monitored and audited under federal guidelines (24/7)
- Centralized Secure Network Management Services to Manage DoDIN APL certified edge devices
- Provides complete management and visibility to federal agency network

Same car, same engine… just more secure!

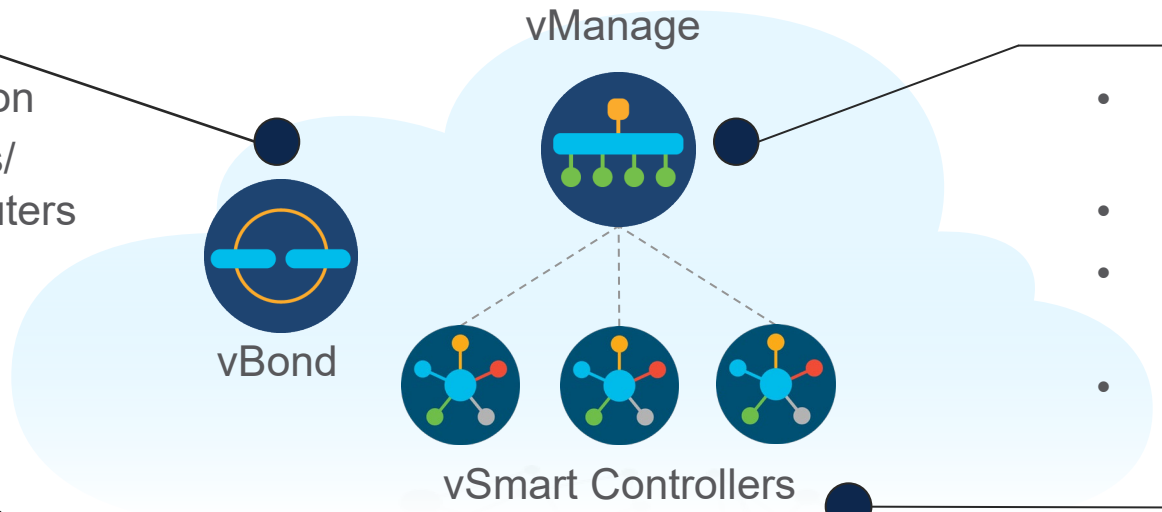
SD-WAN controllers are hosted securely on AWS GovCloud

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

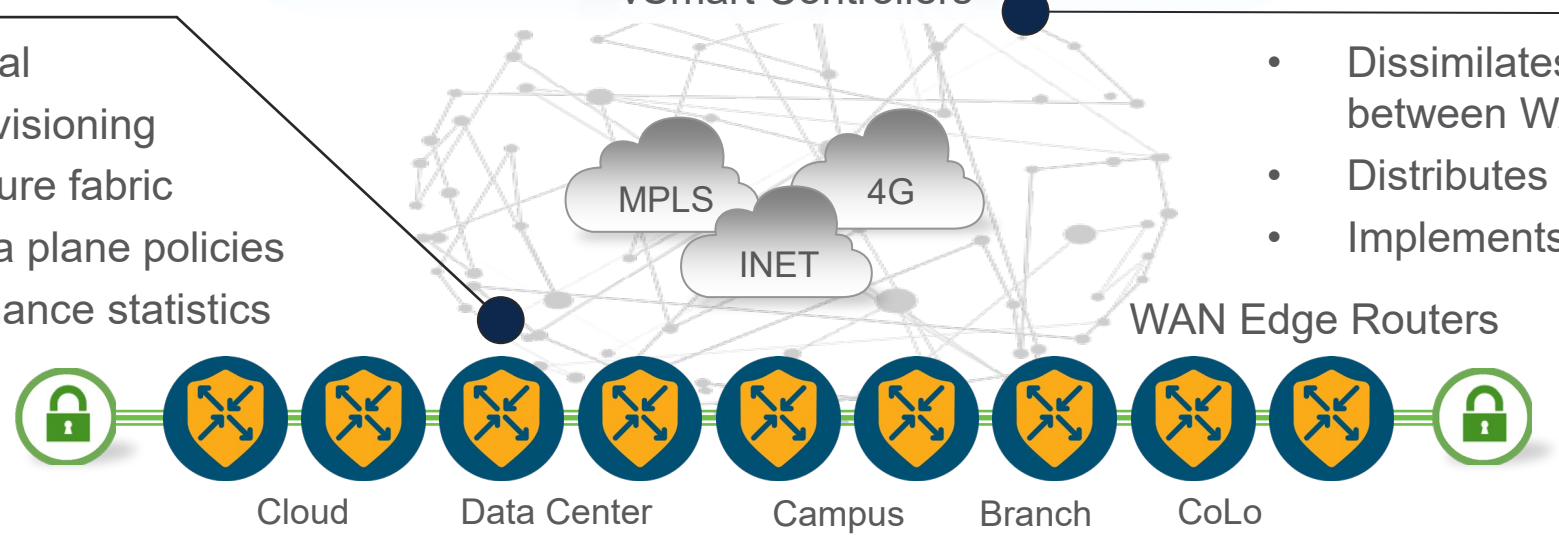


Data Plane

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

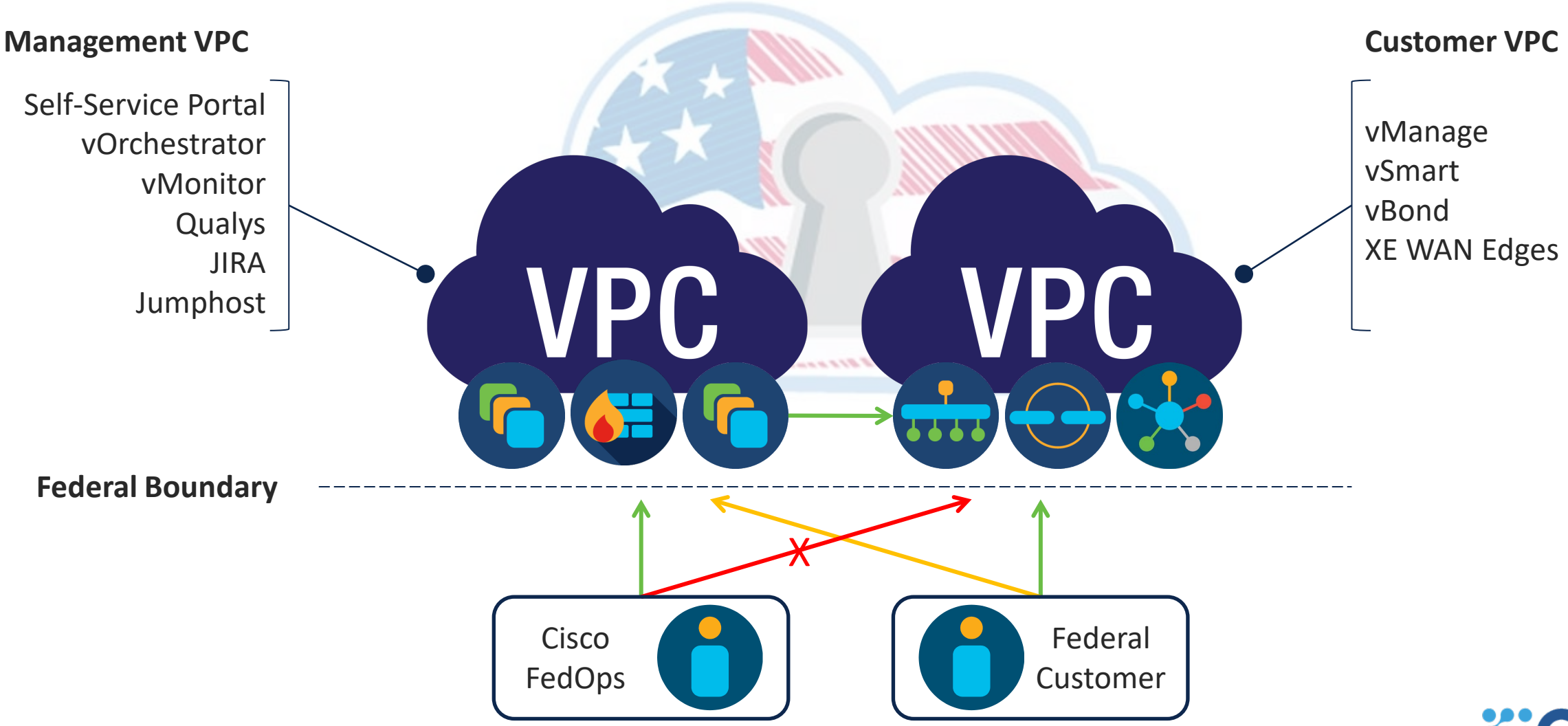
Control Plane

- Dissimilates control plane information between WAN Edges
- Distributes data plane policies
- Implements control plane policies



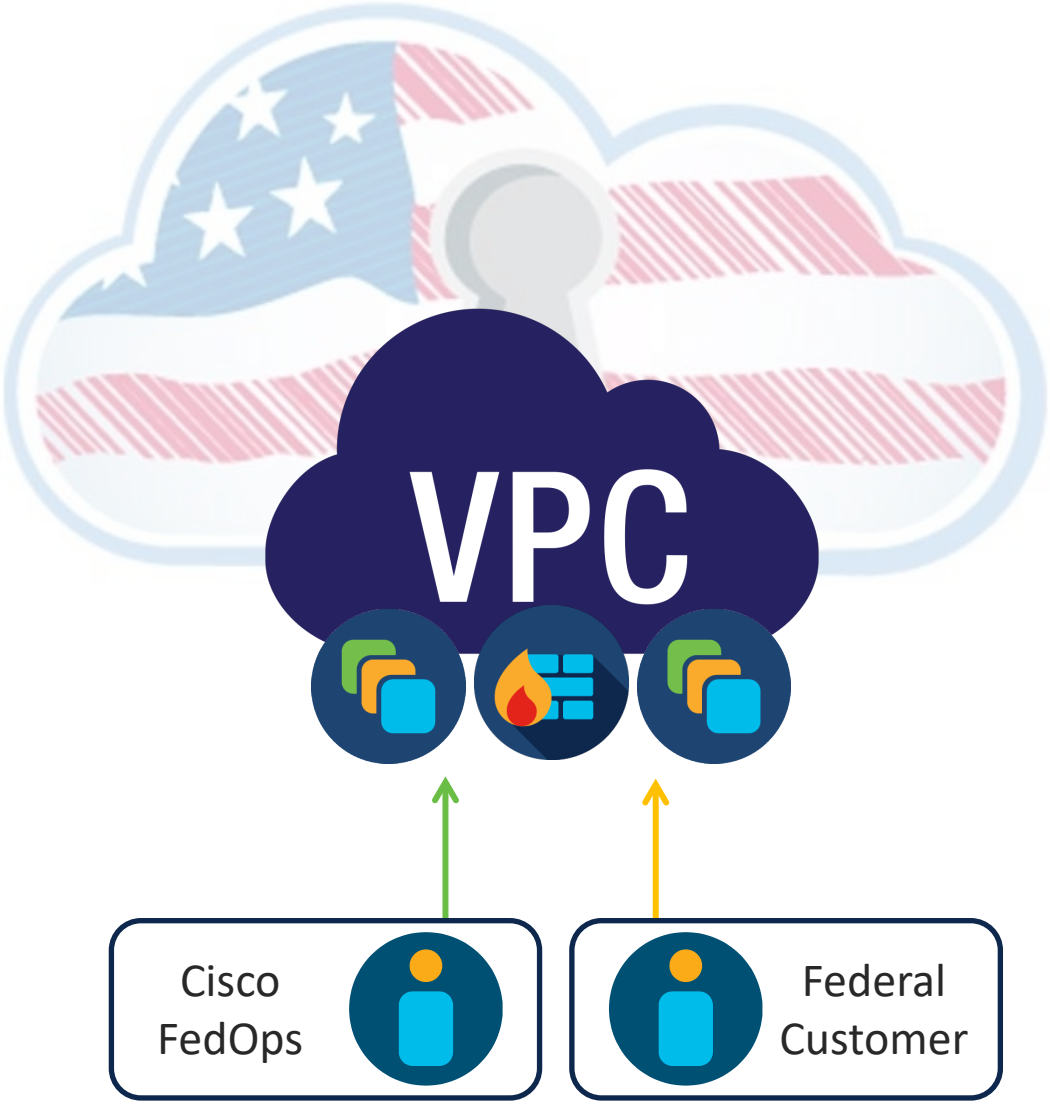
Technical Marketing Engineers

High Level Architecture



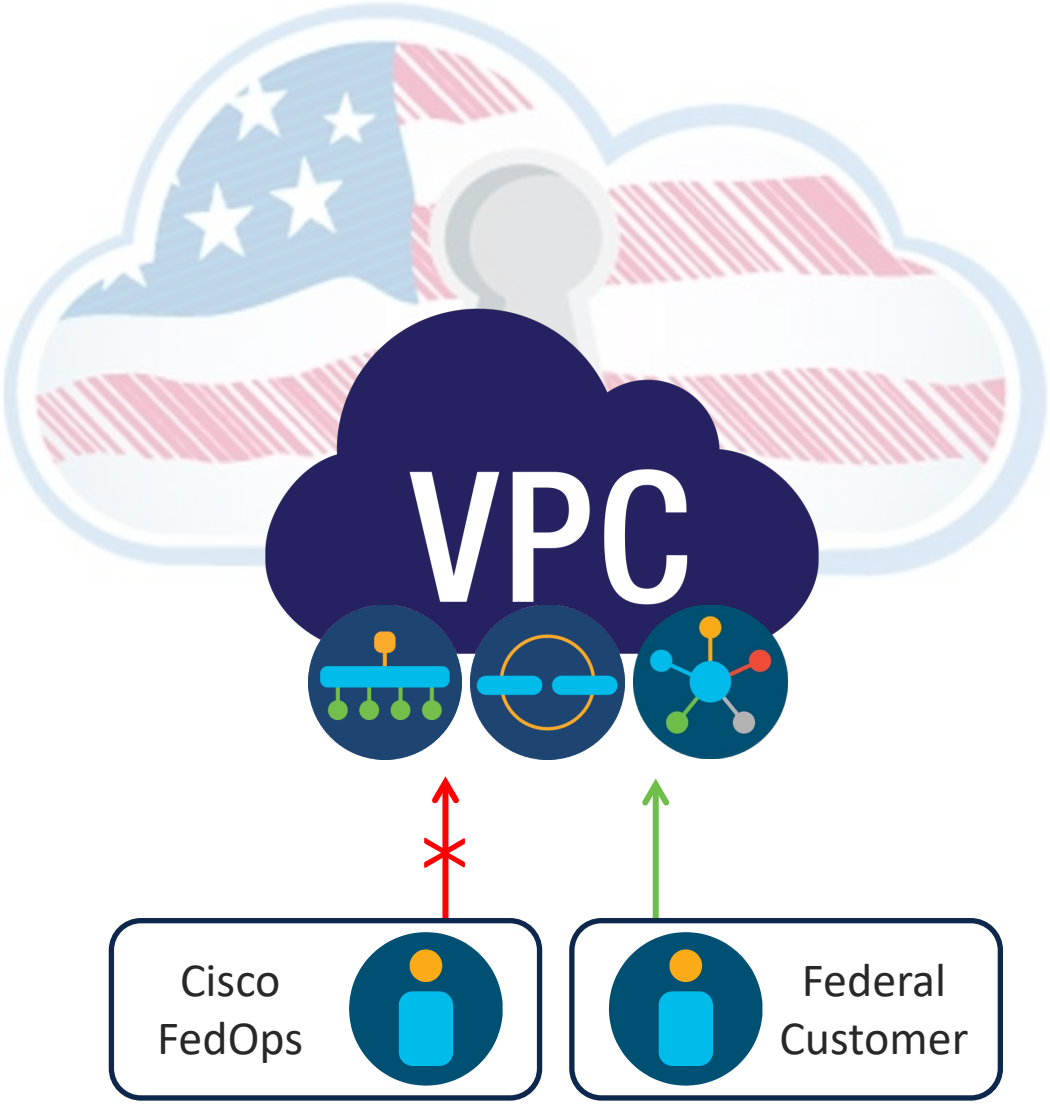
Management VPC

- Located in AWS GovCloud
- Provides secure end-to-end monitoring and auditing of customer VPC: *vMonitor, Qualys, Okta MFA, JIRA, Wazuh, vOrchestrator, AWS Bastion Host (Jumphost), Cisco DMS/DCA/DCS*
- Contains Self-Service Portal (only component customer can access)
- Cisco FedOps primarily accesses this VPC



Customer VPC

- Located in AWS GovCloud
- Hosts customer cloud controllers (vManage, vSmart and vBond)
- Hosts IOS-XE based WAN Edges
- FedOps cannot access this VPC
- Customers access SSP in Management VPC to open *trusted* access from their IP into Customer VPC
- All access into Customer VPC and cloud controllers uses external MFA configured in Management VPC SSP (no local vManage users)

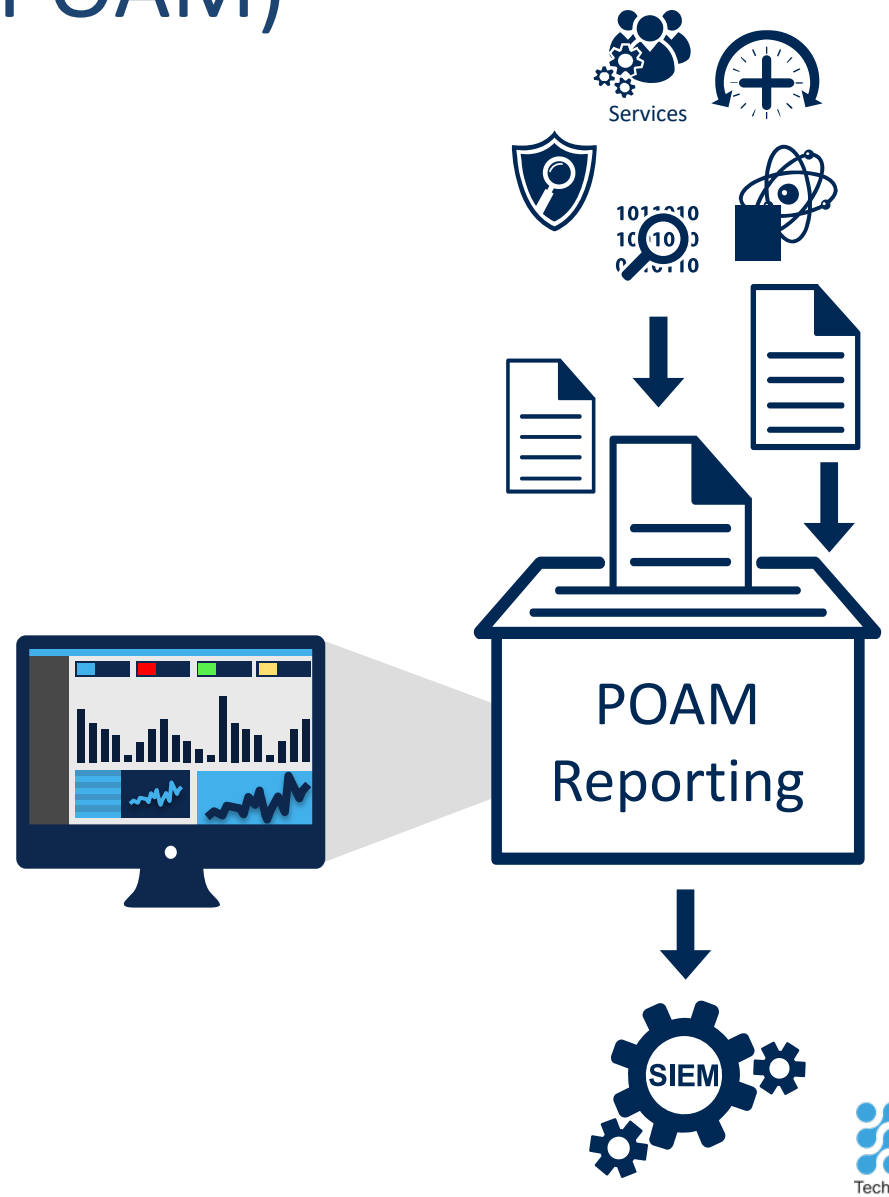


FedRAMP Self-Service Portal

- First pane-of-glass customer will interact with
- Initial login guides customer through Overlay Creation, Whitelisting and external Identity Provider (IdP) integration
- Allows customer to customize overlay (cloud-hosted / on-prem, production / lab, controller DNS hostnames, and snapshot settings
- Offers single UI for external monitoring of overlays and *Plan of Action and Milestones* (POAM)

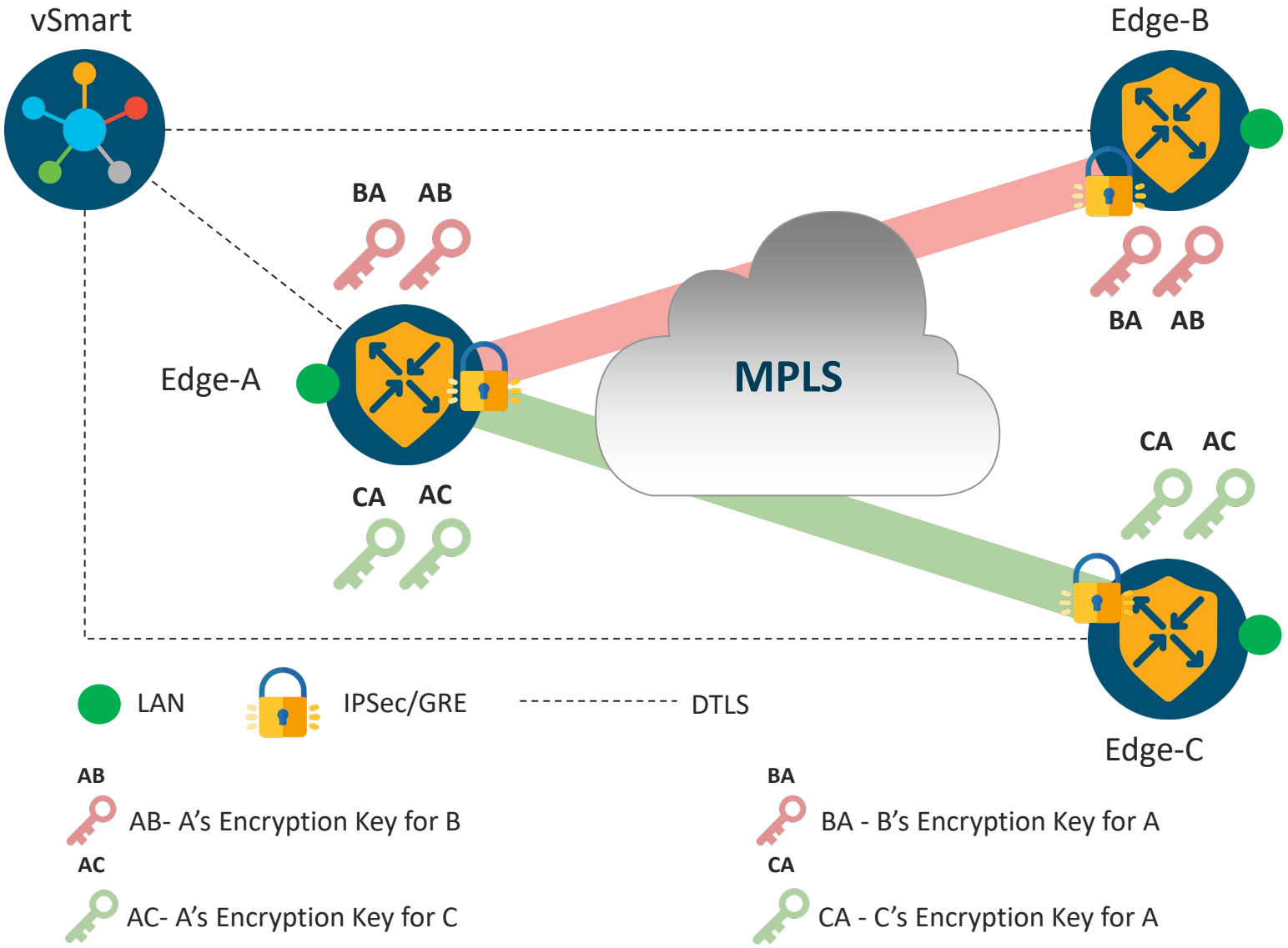
Plan of Action and Milestones (POAM)

- Accessed via SSP
- Provides a vulnerability feed of overlays (Qualys scans, IdP logins, etc.)
- Individual incidents can be reviewed via SSP
- Vulnerability report can be downloaded, or exported to 3rd party SIEM
- Can be used to automate remedial efforts (ticket generation, etc.)



Technical Marketing Engineers

IPsec Pairwise Key Management

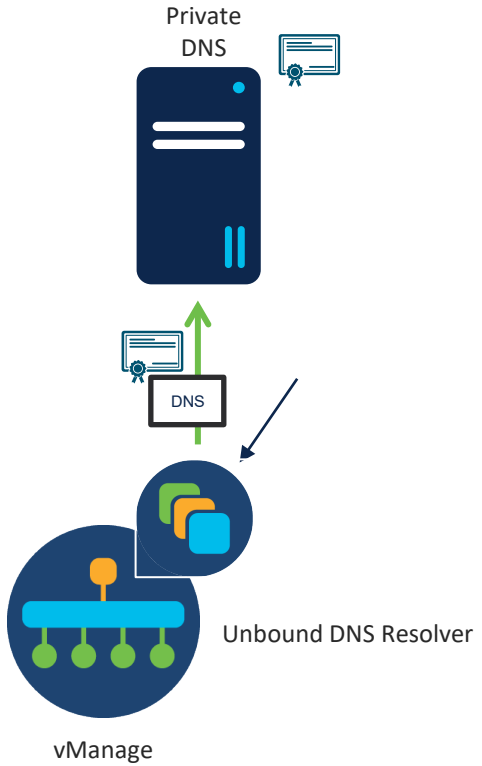


- Each WAN edge will create separate session key for each transport and for each peer
- Session keys will be advertised through vSmart using OMP
- When Edge-A needs to send traffic to Edge-B, it will use session key "AB" (B will use key "BA")
- Backward compatible with non PWK devices
- PWK should be enabled

Technical Marketing Engineers

DNSSec

- ✓ DNSSec provides DNS security by offering validation of DNS responses
- ✓ vManage runs *Unbound* daemon, which is an open source DNS resolver
- ✓ Local applications will query private DNS servers via Unbound
- ✓ Unbound will validate DNS responses



Technical Marketing Engineers

Data in Transit
Data at Rest

- US Federal Government requires data to be encrypted, regardless of its disposition
- Data in Transit is DTLS encrypted (i.e. control plane traffic to/from FedRAMP enabled cloud controllers
- Data at Rest is subject to CiscoSSL (a Cisco-enhanced version of OpenSSL)
- FIPS 140-2 is enabled by default on all SD-WAN cloud-based devices (controllers and Edges)

Deep Dive

vManage Password Policy

Problem

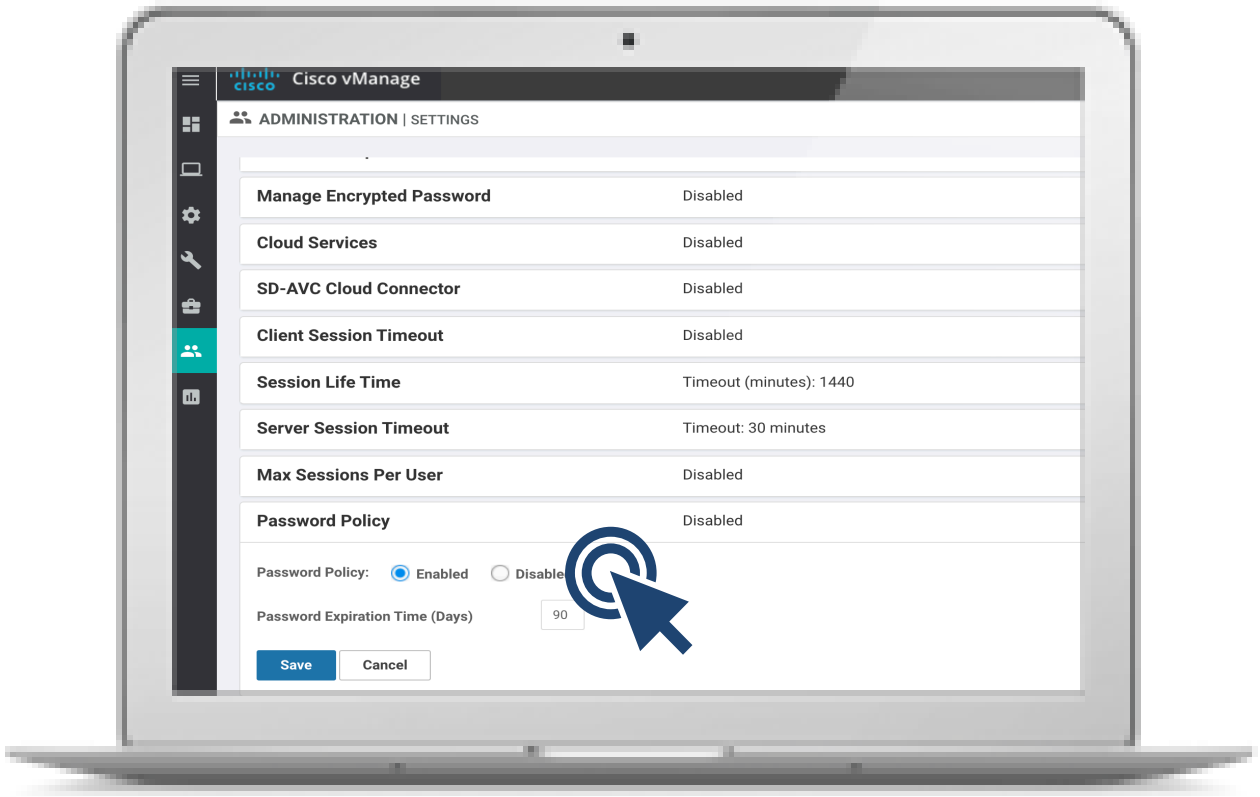
In compliance (CSDL) evaluation and various customers' SDWAN evaluation efforts, it has been found that password complexity for vManage local users does not meet well-established guidelines. Users can use any random string as a password and there are no rules imposed to ensure that it is strong and safe. vManage should enforce password storage, reset, complexity and lifetime policies.

Solution

In SD-WAN v20.3, vManage now supports complex passwords, lifetime policies and reuse (storage) policies – enabled at the system level in both single and multi-tenant organizations.

Caveats / Prerequisites

None



Technical Marketing Engineers

Deep Dive

vManage Audit Log Export

Problem

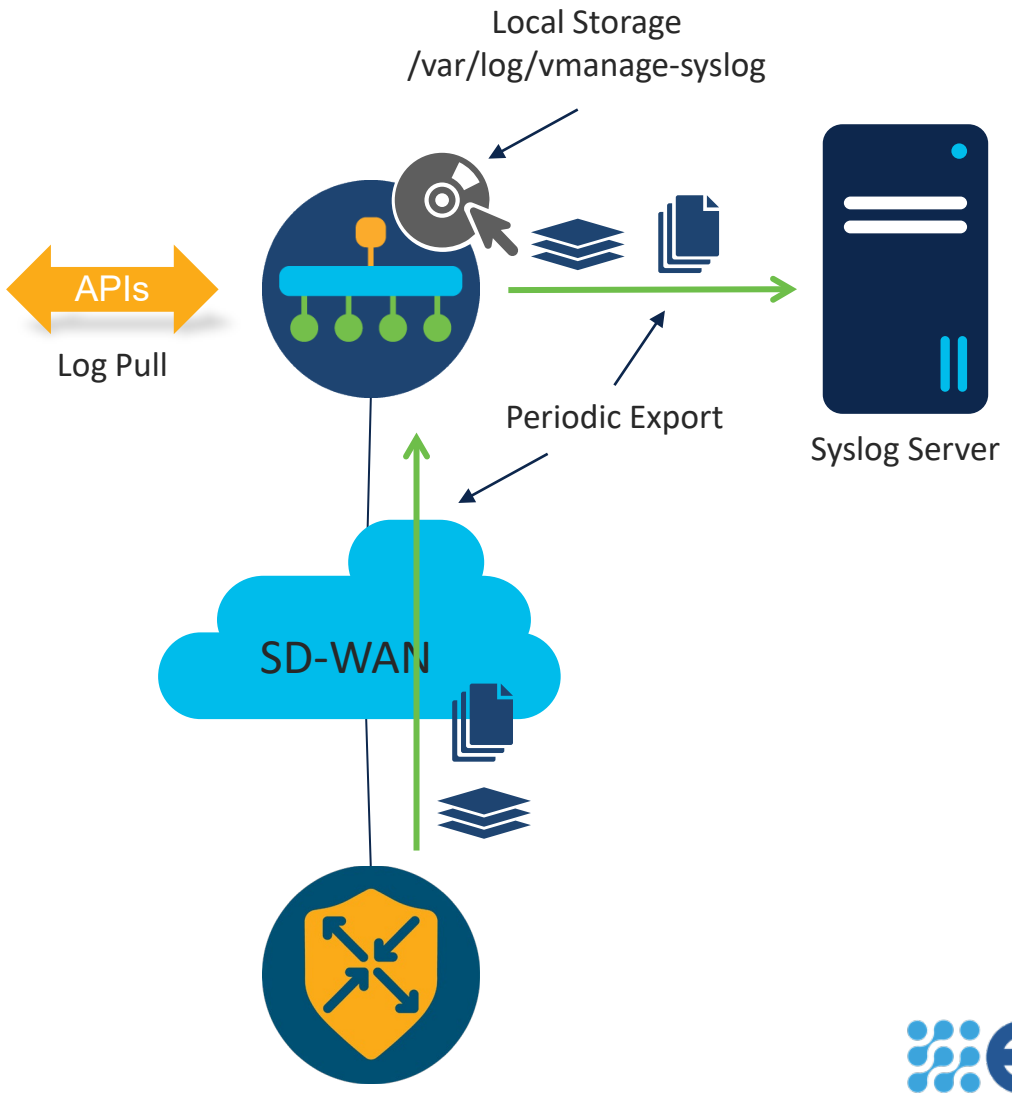
vManage collects Syslogs and Audit Logs. Both of these files can be acquired via REST API (Pull model). Periodically, vManage will also export Syslogs (Push model). However, vManage currently does not export Audit Logs (Push).

Solution

In SD-WAN v20.3, vManage will now convert Audit Logs into Syslog format and export to an external collector.

Caveats / Prerequisites

None



Technical Marketing Engineers

Federal Edge Products

	Access	Aggregation	Cloud
SD-WAN + Services (IOS XE)	 ISR 1000 • Integrated wired and wireless access, WWAN modules • VDSL2, ADSL2/2+	 ISR 4000 • WAN and voice module flexibility, Compute with UCS-E • Slot Modularity, Redundant PSU	 ASR 1000 • Hardware and software redundancy • High-performance service with hardware assist	 CSR 1000v • Extend enterprise routing, security & management to cloud

Google Cloud

Azure

aws

Features

- DoDIN-APL certified
- IPS/IDS built-in
- Unified image for migration
- Simplified onboarding
- FIPS 140-2 certified
- Common Criteria Certified
- TAA Compliant

Technical Marketing Engineers

Software PID for FedRAMP (TBD)

Cisco DNA FedRAMP Software PID Features

Connectivity and Management

- Cloud or On-Prem Management
- Flexible Topology
  - Hub and Spoke
  - Full Mesh/Partial Mesh
- App and SLA based policy
- Dynamic Routing (BGP, OSPF)
- VNF Lifecycle Management

SD-WAN Services

- Basic Path optimization with FEC and Packet Duplication
- TCP Optimization
- Web Caching, DRE (including SSL proxy)
- Voice Module and SRST Integration
- Multicast

Cloud/Analytics

- Cloud onRamp for IaaS and SaaS
- Automated Service Stitching
- Encrypted Traffic Analytics

X-Domain Innovations

- Integrated Border for Campus (SD-Access)
- Integration with ACI for Application SLA

Cisco SD-WAN's Government Advantage

- FIPS 140-2 Compliance
- Encryption at rest and in transit
- Session Management
- Daily Pen Testing
- File Incident Management
- 3PAO Audit
- Security Assessment Report
- System Security Plan
- Realtime POA&M

Technical Marketing Engineers

Technical Marketing Engineers