Cisco TechTalks

Cisco SD WAN

Новая программно-управляемая архитектура филиальной сети

Вебинар #9

Andrew Ovrashko
System Engineer

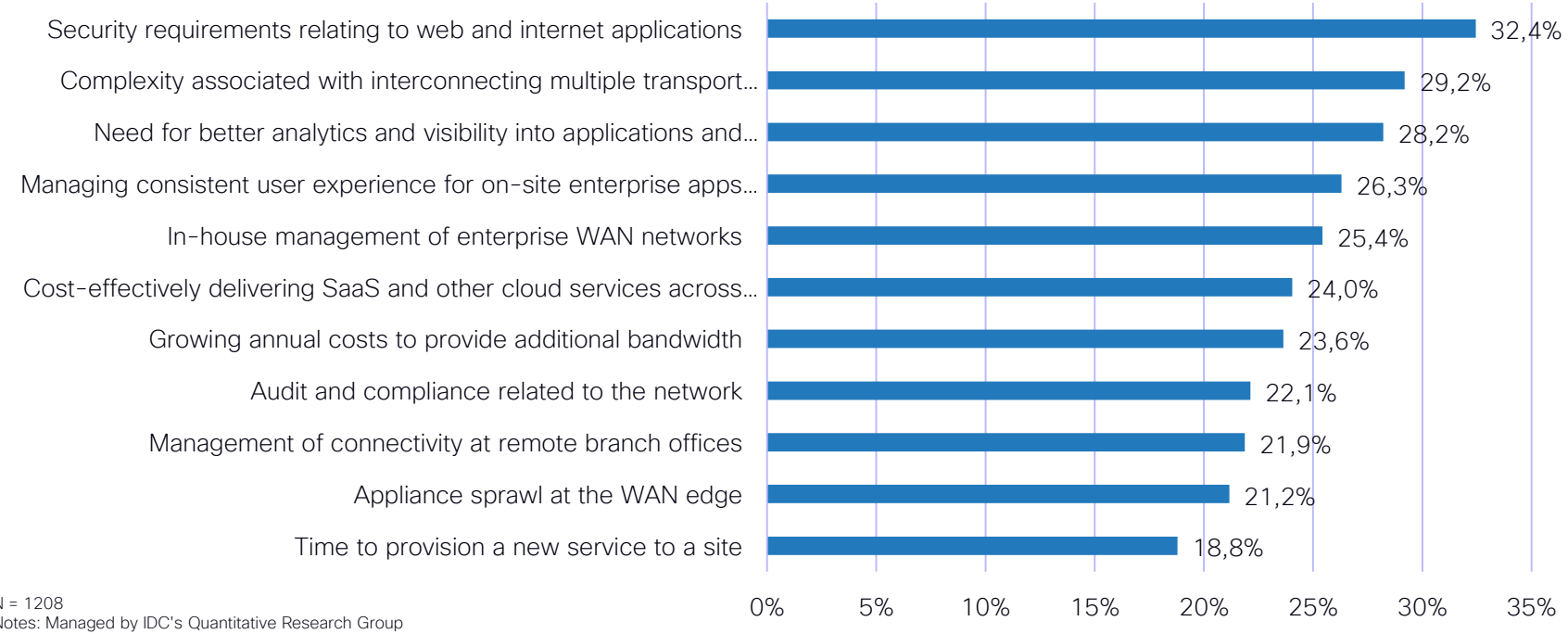
22th June 2018

Зачем нужна новая архитектура для WAN?

Addressing WAN Challenges

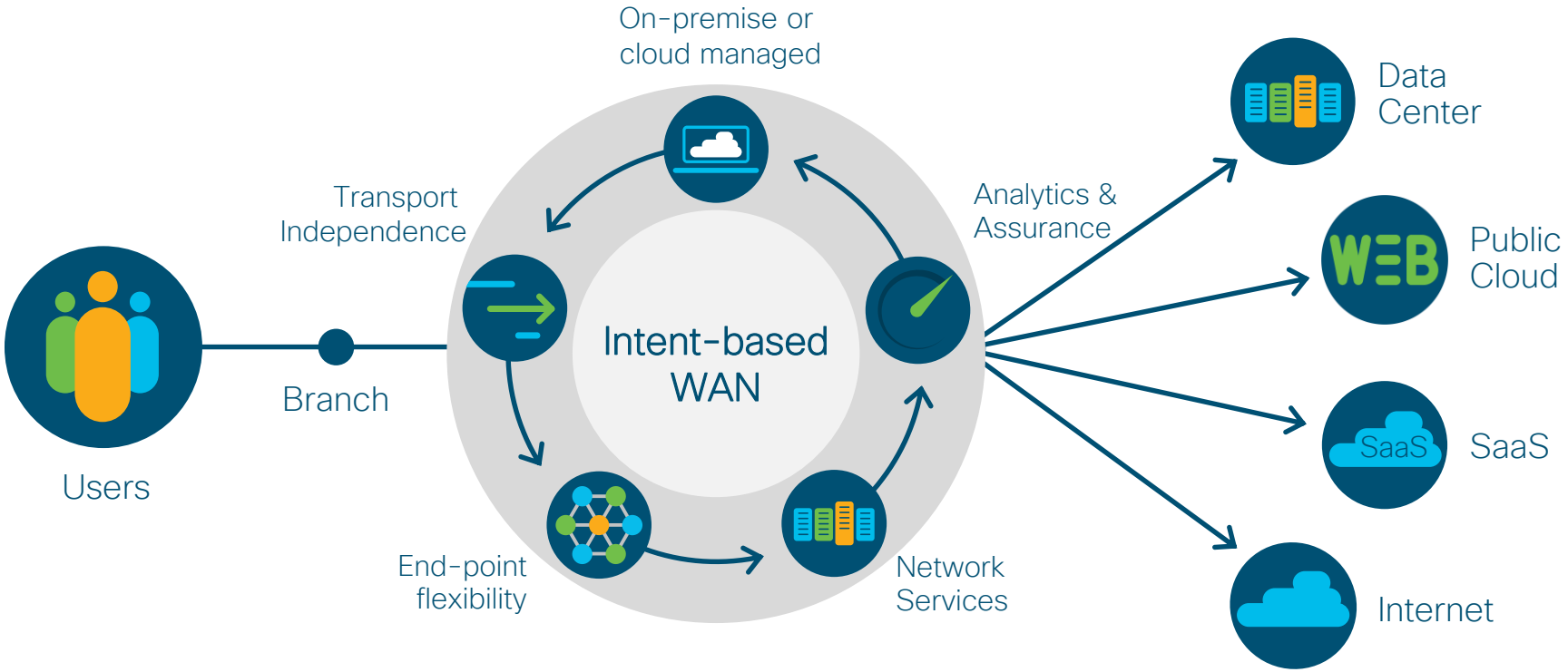
Security Requirements and Complexity Headline WAN Challenges

Q. Select the three most important WAN challenges (from the following) that best relate to your company?



N = 1208
Notes: Managed by IDC's Quantitative Research Group
Source: Software-Defined WAN (SD-WAN) Survey, IDC, August, 2017

Intent-based networking for the WAN



Securely connect any user to any application with the best experience

Journey to Intent-based WAN

Centralized Management

Simplify the WAN for operational savings, better visibility and faster deployments.

Secure Connectivity

Lower WAN costs using hybrid or SD-WAN with integrated security and intelligent path control.

Policy-based Automation

Optimize user experience and cloud access with direct internet access and application aware polices.

Analytics and Assurance

Reduce operational costs and optimize application performance with predictive and self-healing capabilities

Intent-based WAN

Securely connect any user, device or thing to any application, with the best user experience.

Constantly learning, adapting and protecting.

Software subscription is the foundation

Тренды ведущие к модернизации WAN

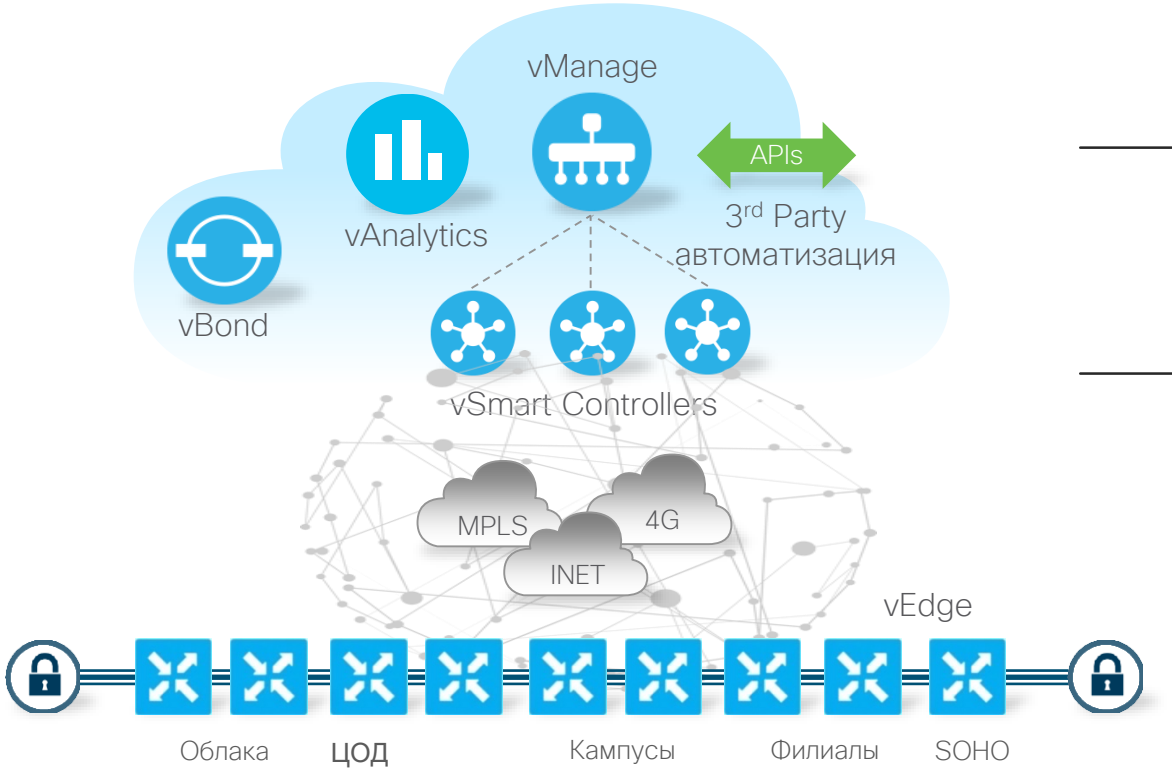
Цифровая трансформация требует трансформации сети

Акцент на оборудование	Программно-определяемая
Вручную	Автоматизация
Закрытая	Программируемая
Реактивная	Предсказывающая
Сетевые намерения	Намерения бизнеса

Четыре основных принципа Cisco SD-WAN

Обзор решения Cisco SD-WAN

Применение SDN принципов к распределенным сетям

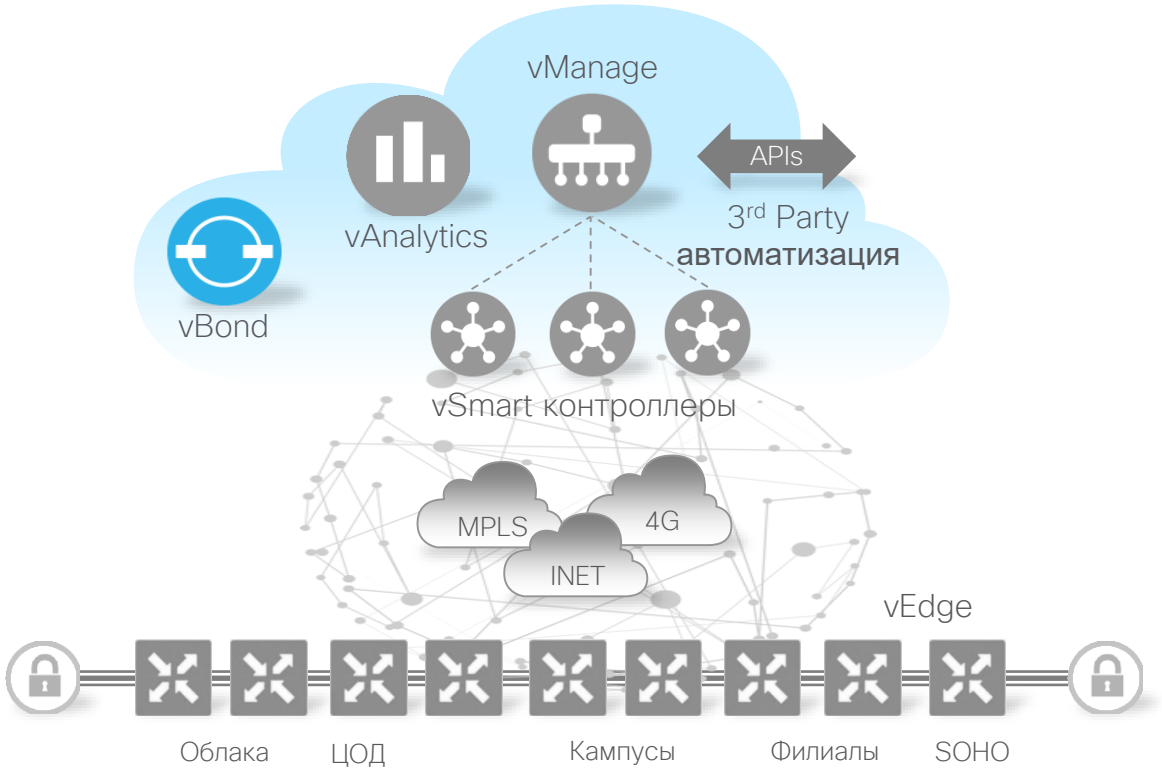


Администрирование/
Оркестрация

Плоскость управления
(Control Plane)

Плоскость
передачи данных
(Data Plane)

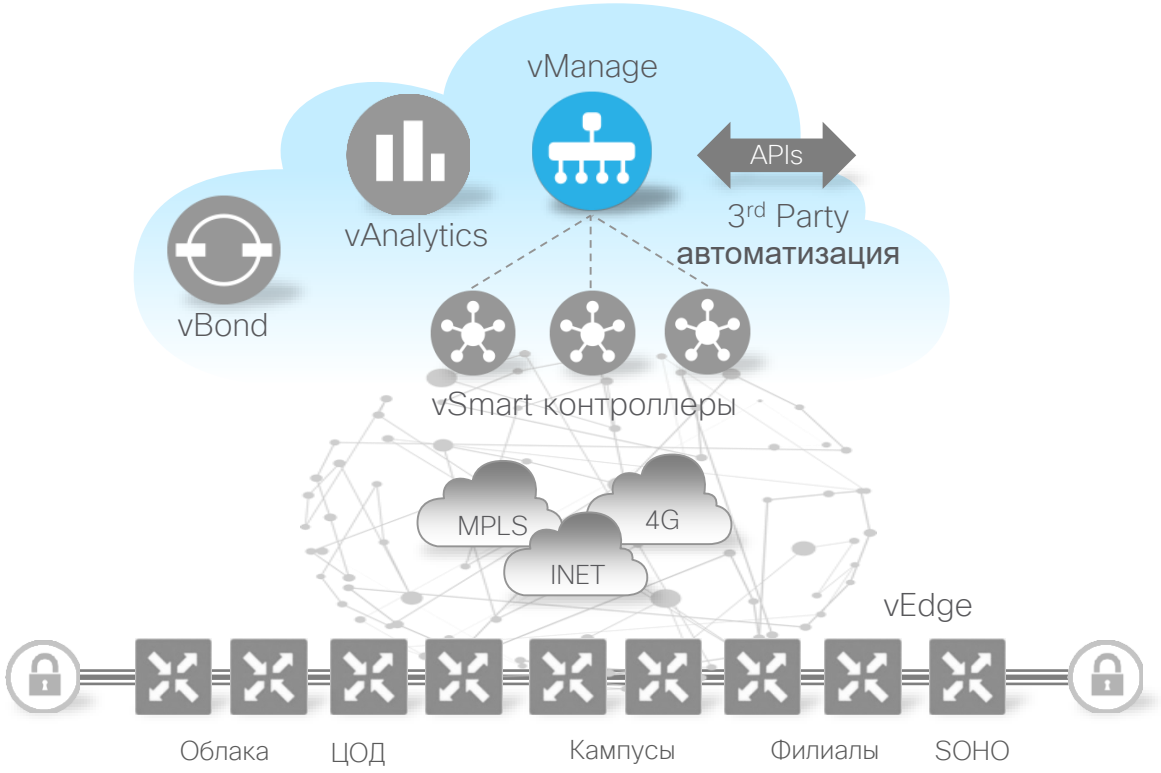
Оркестрация фабрики (vBond)



Основные характеристики

- Обеспечивает связность между плоскостями администрирования, управления и передачи данных
- Начальная точка аутентификации
- Распространяет список vSmart/vManage на все vEdge устройства
- Помогает с обходом NAT
- Требует публичного IP адреса (может находиться за 1:1 NAT)
- Высокая отказоустойчивость
- Multitenant или выделенный
- Все компоненты Cisco SD-WAN должны знать IP адрес или доменное имя vBond
- Авторизует все управляющие соединения (модель «белых списков»)

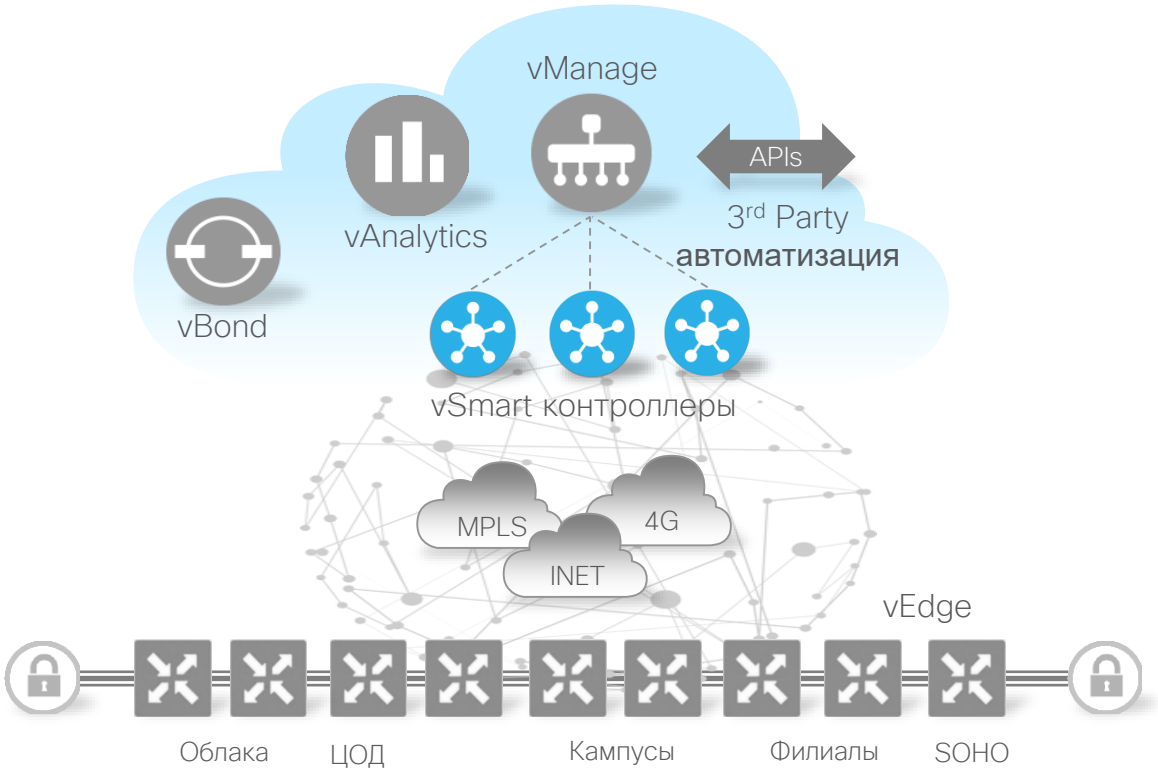
Плоскость администрирования (vManage)



Основные характеристики

- Единая консоль управления для операций Day0, Day1 и Day2 (развертывание, настройка, эксплуатация)
- Централизованный провиженининг
- Multitenant или выделенный
- Формирование политик и шаблонов
- Мониторинг и поиск и устранение неисправностей
- Обновление ПО
- Программный интерфейс (REST, NETCONF)
- Высокая отказоустойчивость
- Графический интерфейс с RBAC

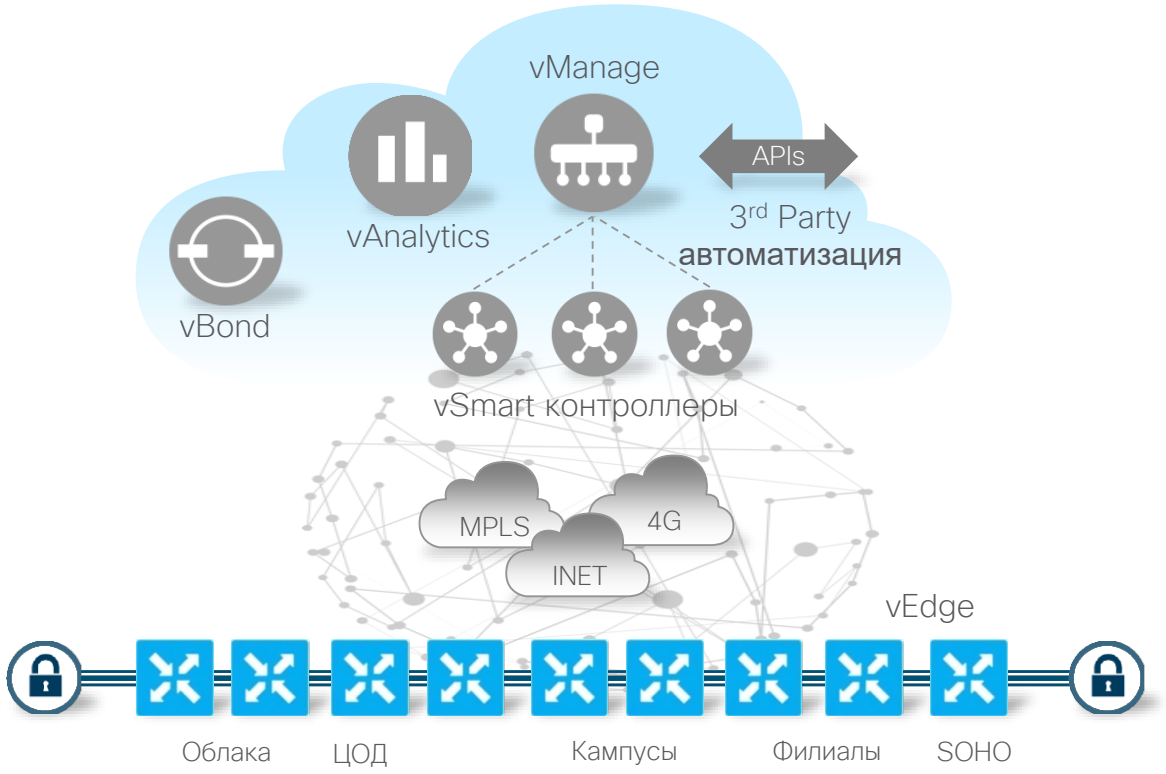
Плоскость управления (vSmart)



Основные характеристики

- Обеспечивает обнаружение устройств в фабрике
- Распространяет информацию плоскости управления на vEdge устройства
- Распространяет политики плоскости передачи данных и политики маршрутизации по приложениям на vEdge устройства
- Применяет политики плоскости управления
- Существенно снижает сложность плоскости управления
- Высокая отказоустойчивость

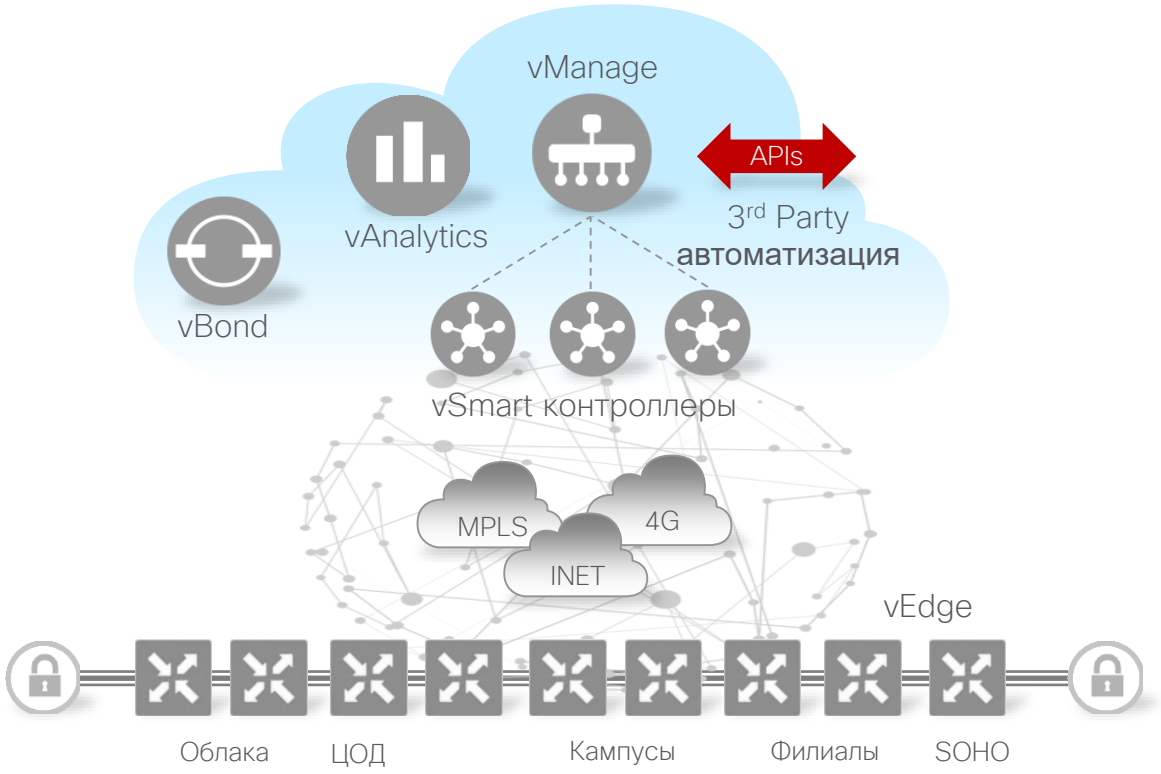
Плоскость передачи данных (vEdge)



Основные характеристики

- Граничные маршрутизаторы WAN
- Обеспечивают безопасную передачу данных с удаленными vEdge маршрутизаторами
- Устанавливают безопасные управляющие соединения с vSmart контроллерами (OMP)
- Осуществляют передачу данных и маршрутизацию трафика на основе политик по приложениям
- Используют стандартные протоколы маршрутизации, такие как BGP, OSPF и VRRP
- Поддержка ZTP (Zero Touch Provisioning)
- Экспортирует статистику о производительности и качестве обслуживания
- Может быть физическим (100Мбит/с – 20+Гбит/с) или виртуальным

Программируемый API (REST)



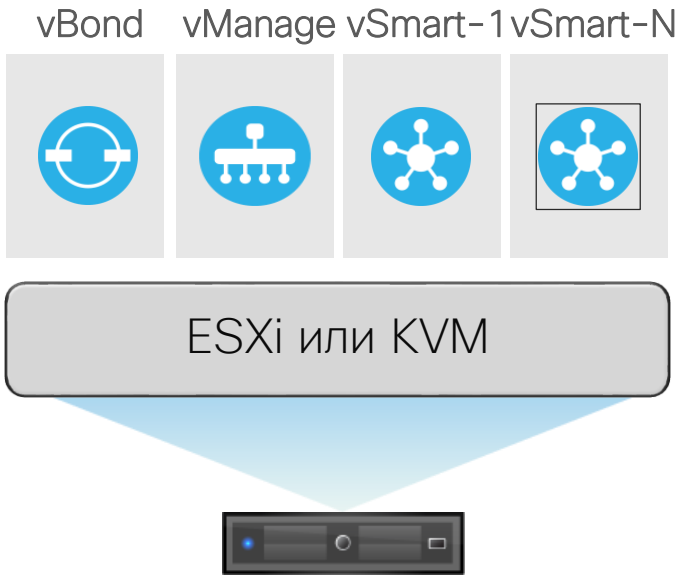
Основные характеристики

- Программный контроль над всеми аспектами администрирования через vManage
- Безопасный HTTPS интерфейс
- GET, PUT, POST, DELETE методы
- Аутентификация и авторизация
- Bulk API вызовы
- Скрипты на Python

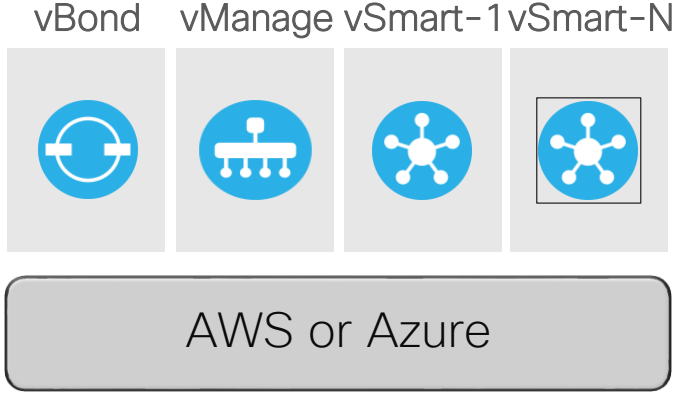
vBond, vSmart, vManage

Контроллеры могут быть развернуты как в корпоративной сети, так и в публичной облачной среде

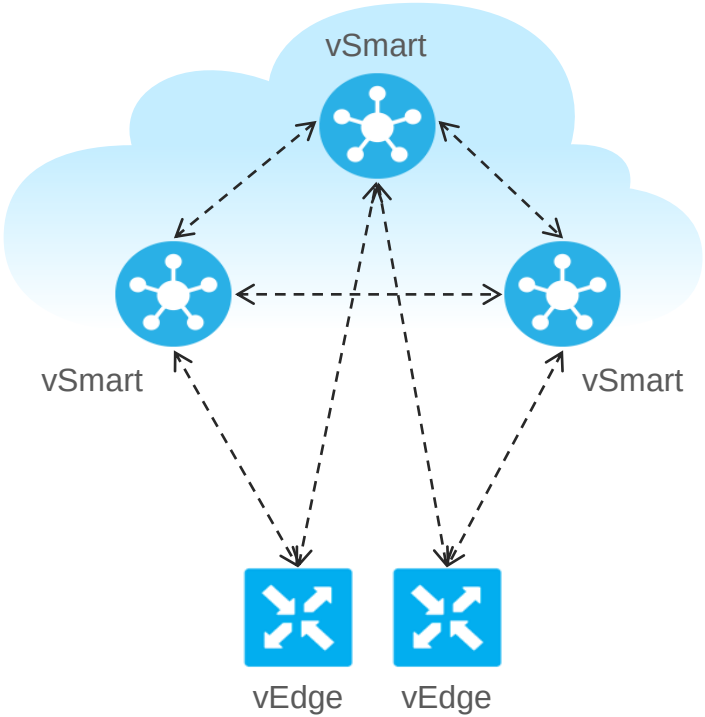
В корпоративной сети



В публичном облаке



Плоскость управления (Control plane)

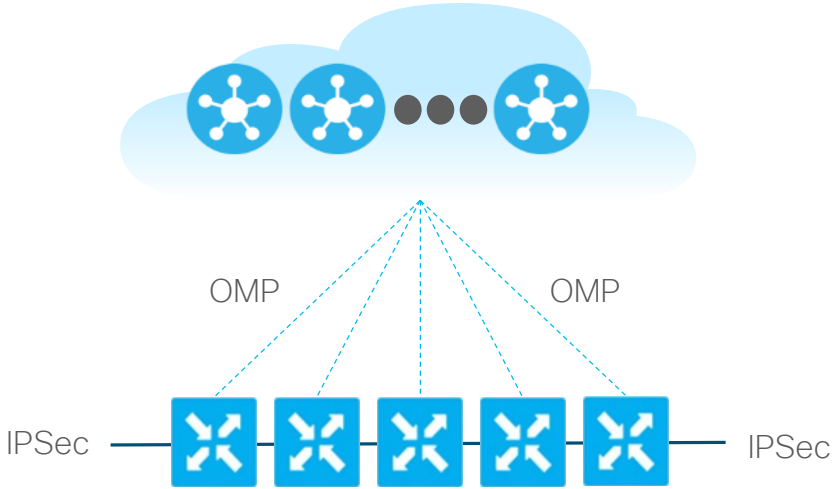


ВАЖНО: Нет необходимости в соединении vEdge маршрутизаторов со всеми vSmart контроллерами

- Протокол управления наложенной сетью OMP (Overlay Management Protocol)
- Улучшенный протокол плоскости управления на базе TCP
- Функционирует между vEdge и vSmart контроллерами и между всеми vSmart контроллерами
- Передается внутри TLS/DTLS соединений
- Распространяет контекст плоскости управления и политики
- Значительно снижает сложность управления и существенно увеличивает возможности масштабирования решения

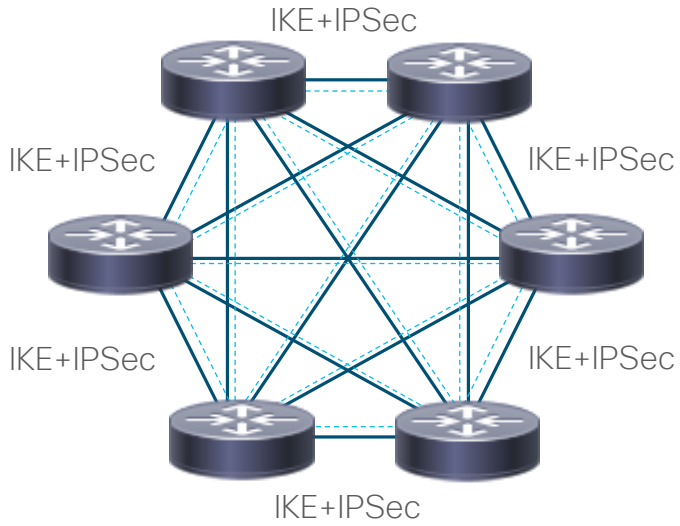
Сложность плоскости управления

SD-WAN



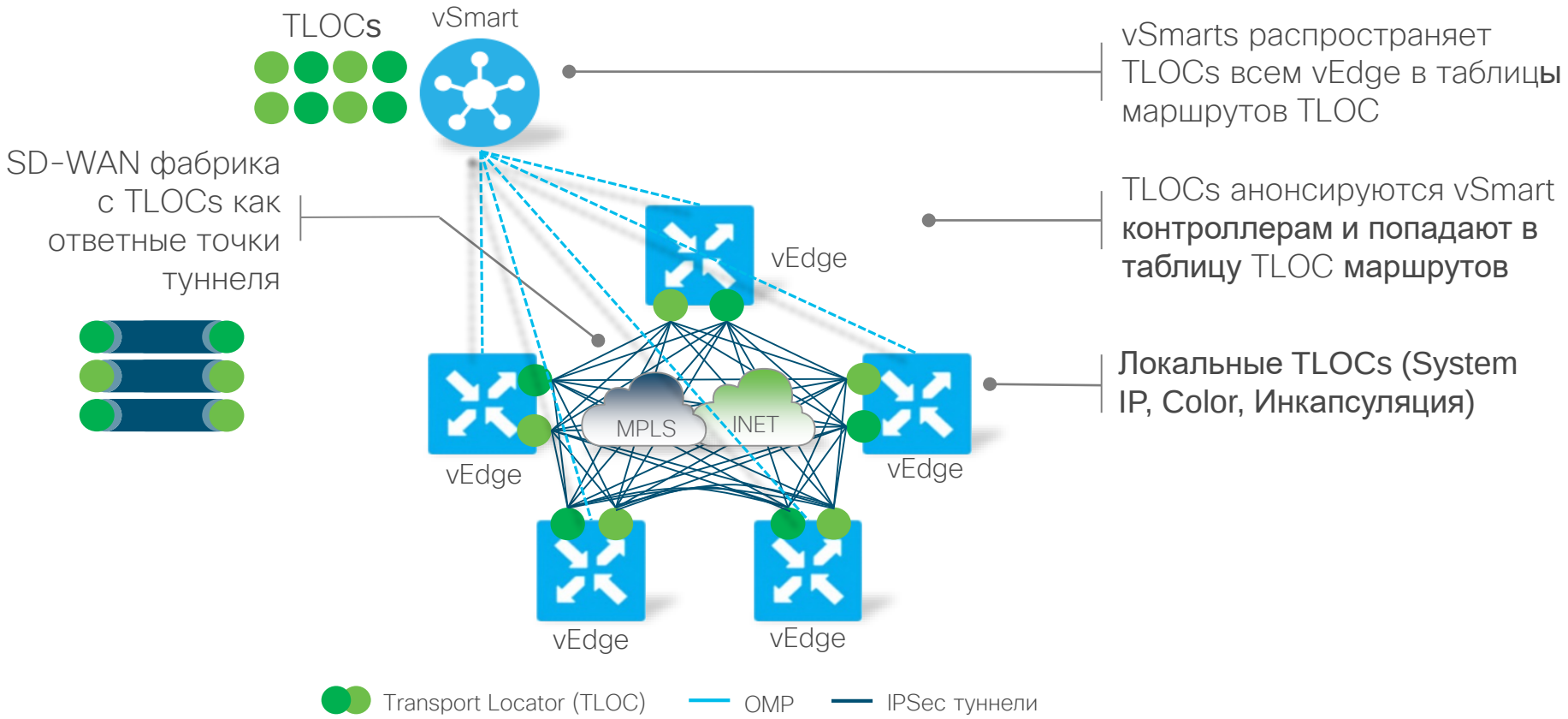
Линейная сложность Control Plane
O(n)

Традиционные IPSec сети



Квадратичная сложность Control Plane
O(n^2)

Развертывание плоскости передачи данных

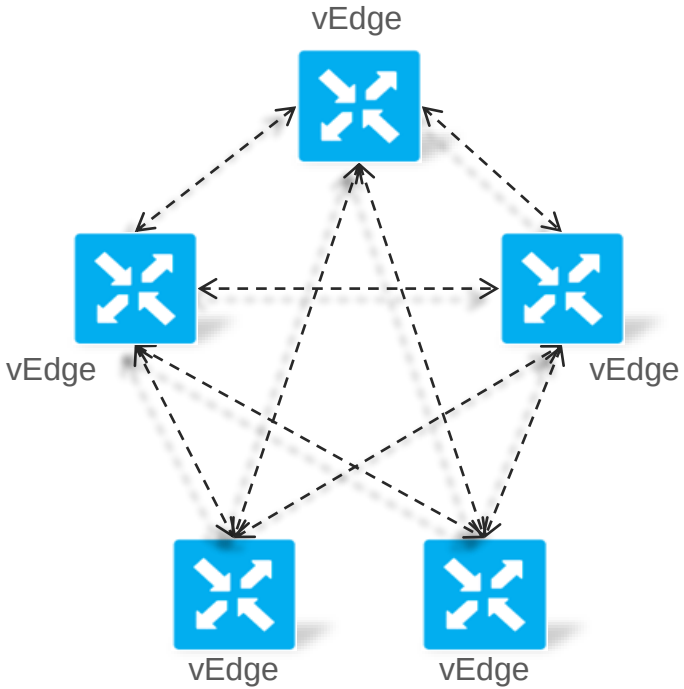


vSmarts распространяет TLOCs всем vEdge в таблицы маршрутов TLOC

TLOCs анонсируются vSmart **контроллерам и попадают в таблицу** TLOC **маршрутов**

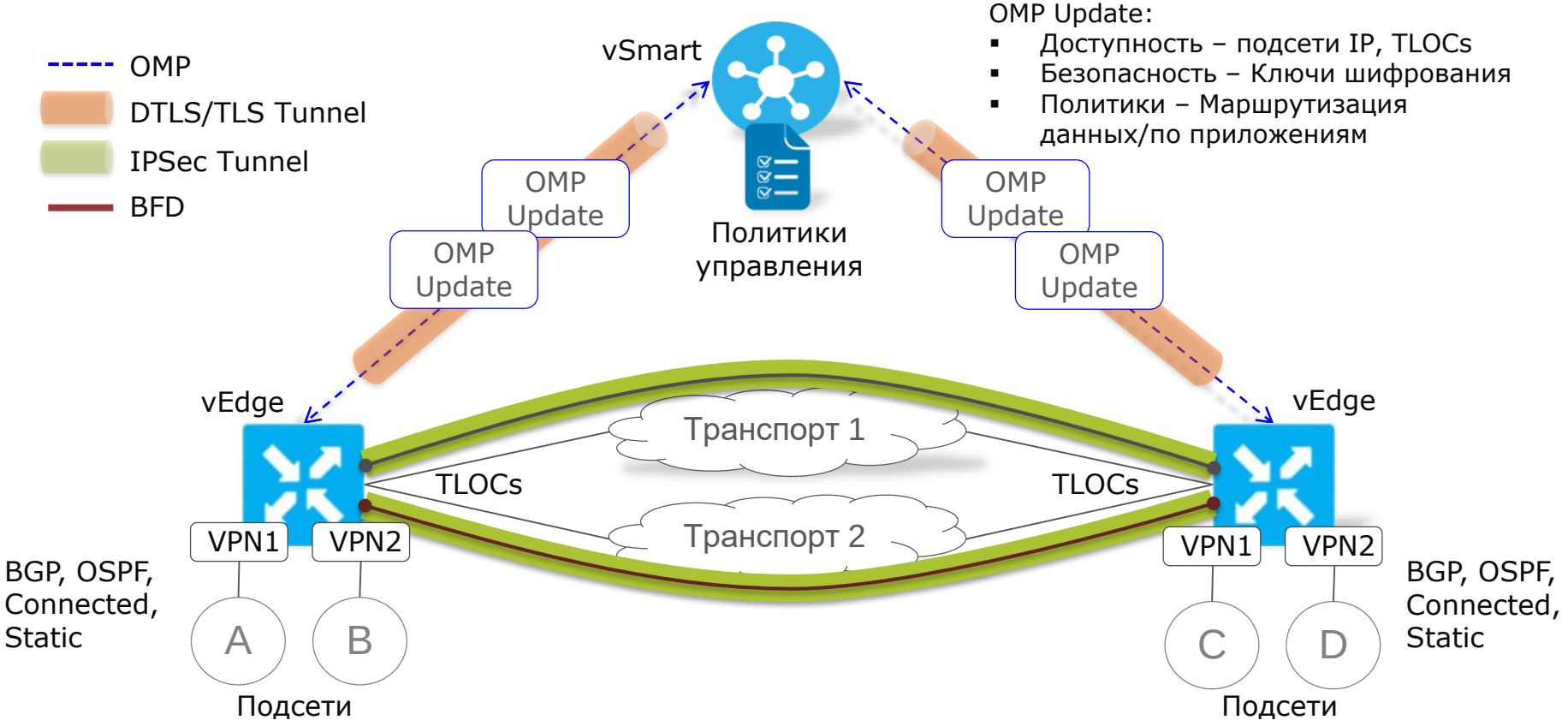
Локальные TLOCs (System IP, Color, Инкапсуляция)

Плоскость передачи данных (Data Plane)



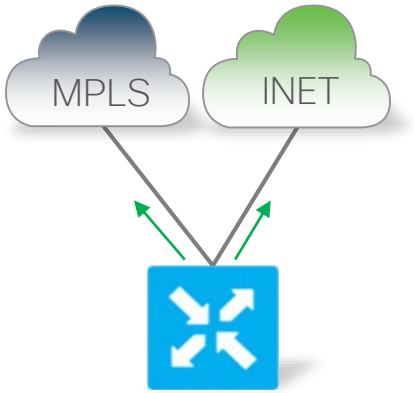
- Bidirectional Forwarding Detection (BFD)
- Мониторинг состояния каналов и качества прохождения трафика
  - Up/Down, потери/задержки/вариации задержек (jitter), MTU через IPsec туннель
- Работает между всеми vEdge маршрутизаторами в топологии
  - Внутри IPsec туннелей
  - Функционирует в Echo режиме
  - Автоматически запускается при установлении IPsec туннеля
  - Не может быть отключен
- Использует hello интервал (для Up/Down), poll интервал (для маршрутизации по приложениям) и multiplier для для обнаружения ухудшений
  - Полностью перенастраиваемый (pre-vEdge, perColor)

Как работает SD-WAN фабрика



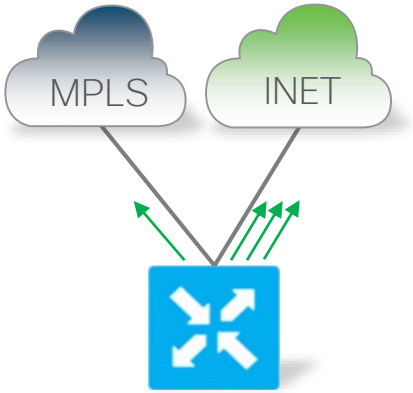
Распространенные типы взаимодействия через плоскость передачи данных (Data Plane)

Per-Session распределение Active/Active



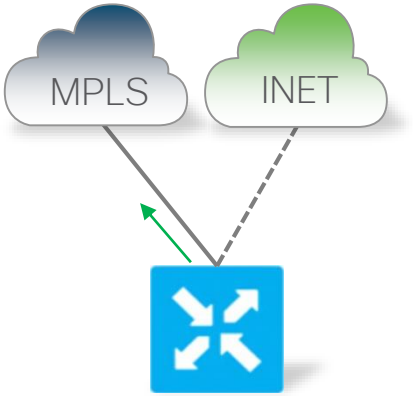
По умолчанию

Per-Session взвешенное Active/Active



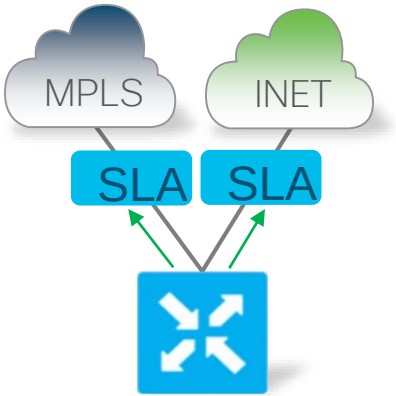
Настраиваемо на устройстве

Привязка приложений Active/Standby



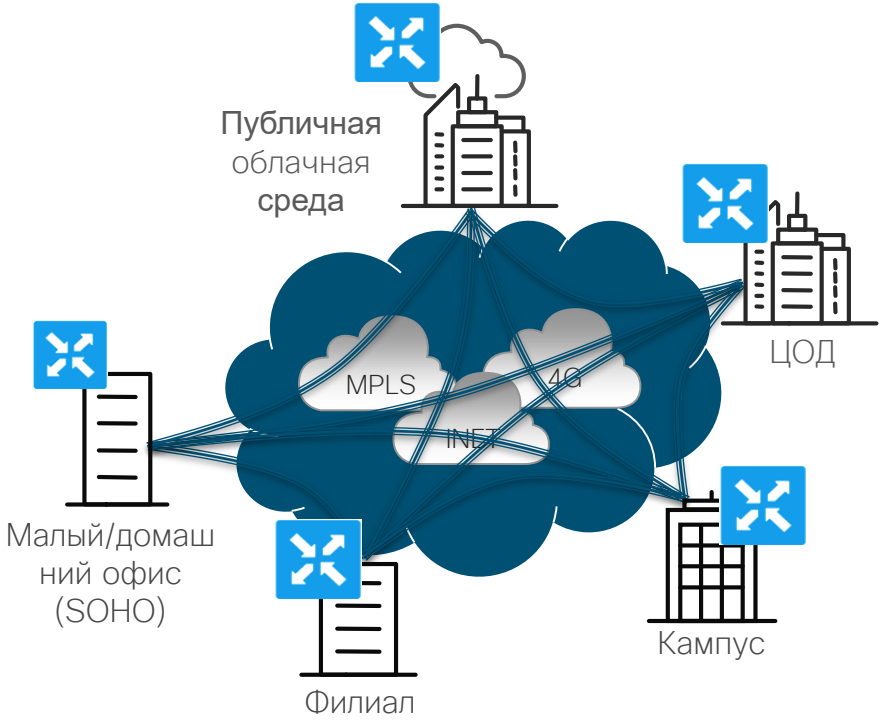
Принудительная политика

Маршрутизация по приложениям с учетом SLA

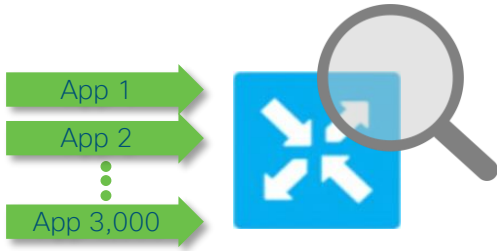


Принудительная политика

Определение приложений



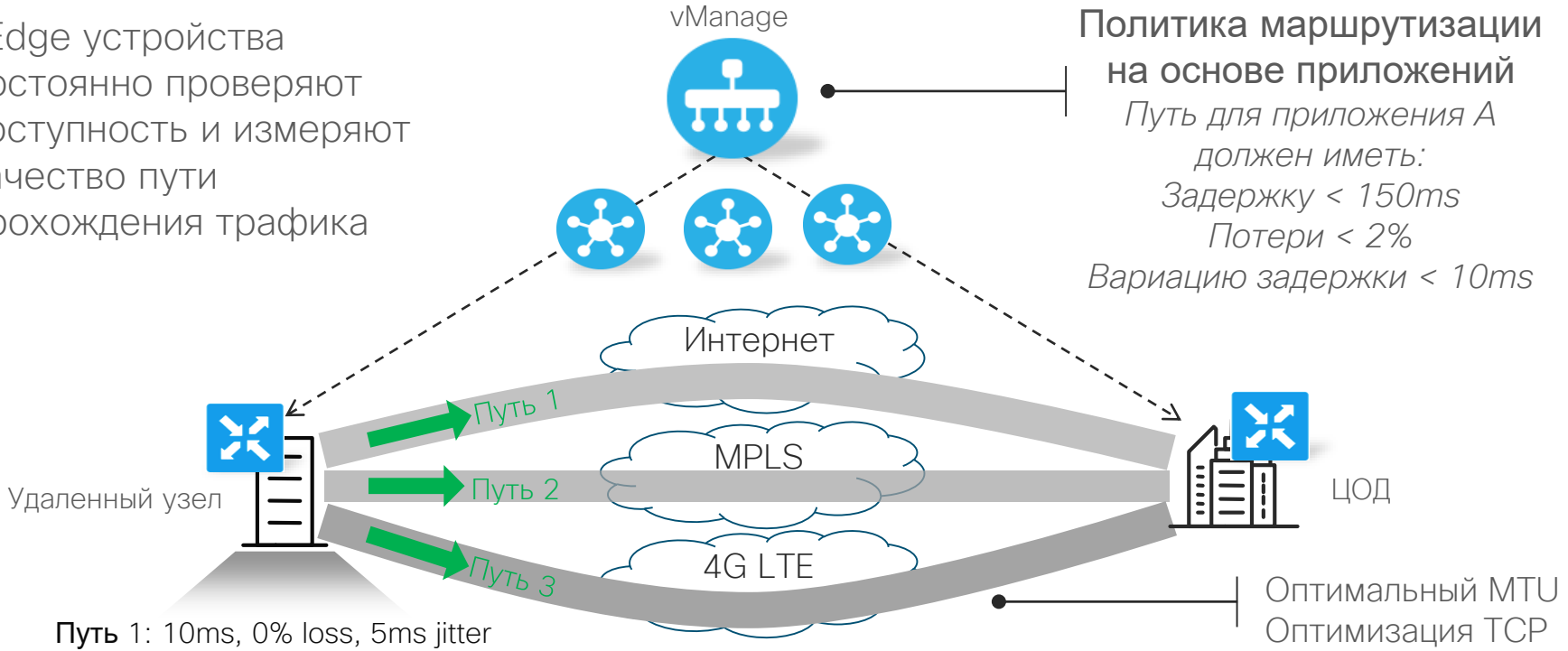
Deep Packet Inspection (DPI)



- ✓ Межсетевое экранирование
- ✓ Приоритезация трафика
- ✓ Выбор трафика

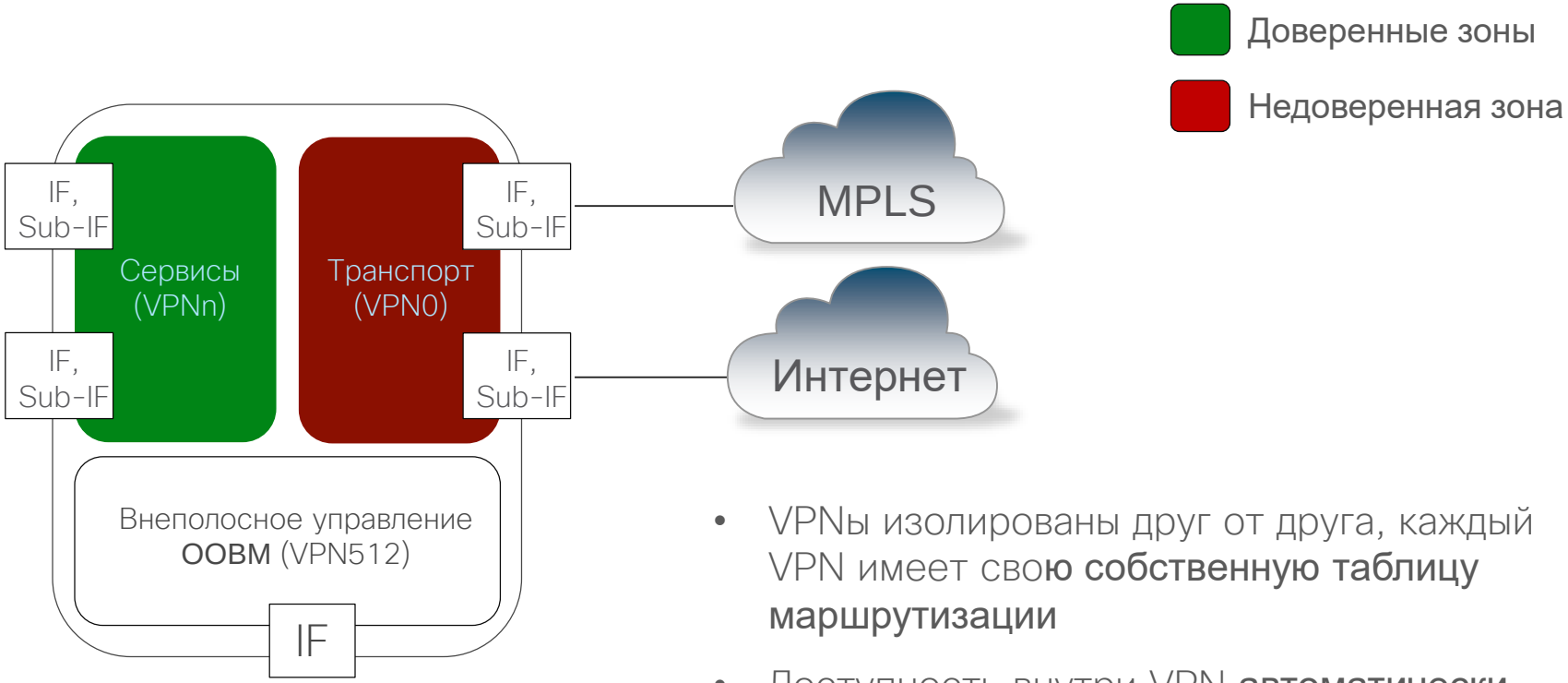
Обеспечение SLA для критичных приложений

- vEdge устройства постоянно проверяют доступность и измеряют качество пути прохождения трафика



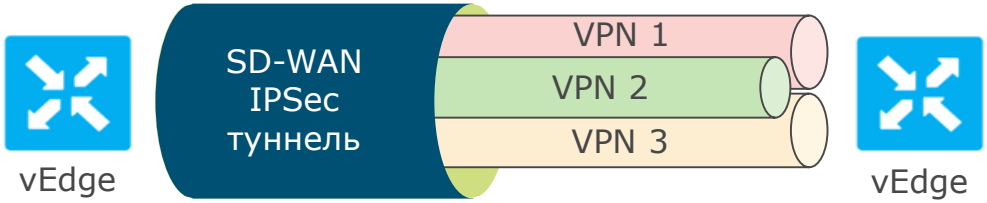
Путь 1: 10ms, 0% loss, 5ms jitter
Путь 2: 200ms, 3% loss, 10ms jitter
Путь 3: 140ms, 1% loss, 10ms jitter

Понятие VPN и зон безопасности в vEdge



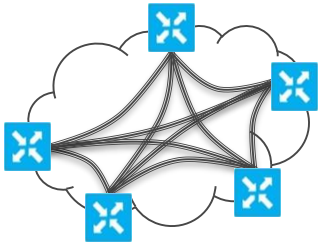
- VPNы изолированы друг от друга, каждый VPN имеет свою **собственную таблицу маршрутизации**
- Доступность внутри VPN **автоматически анонсируется через** OMP

Безопасная сегментация

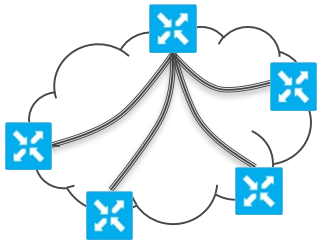


- Безопасное зонирование
- Соответствие политикам безопасности
- Гостевой Wi-Fi
- Multi-Tenancy
- Внешние сети (Extranet)

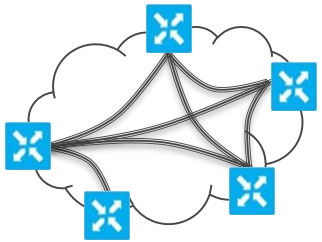
Уникальная топология для каждого VPN



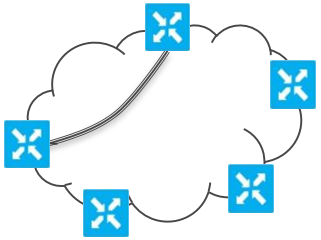
Полносвязная
Full-Mesh



Централизованная
Hub-and-Spoke



Частично связанная
Partial Mesh

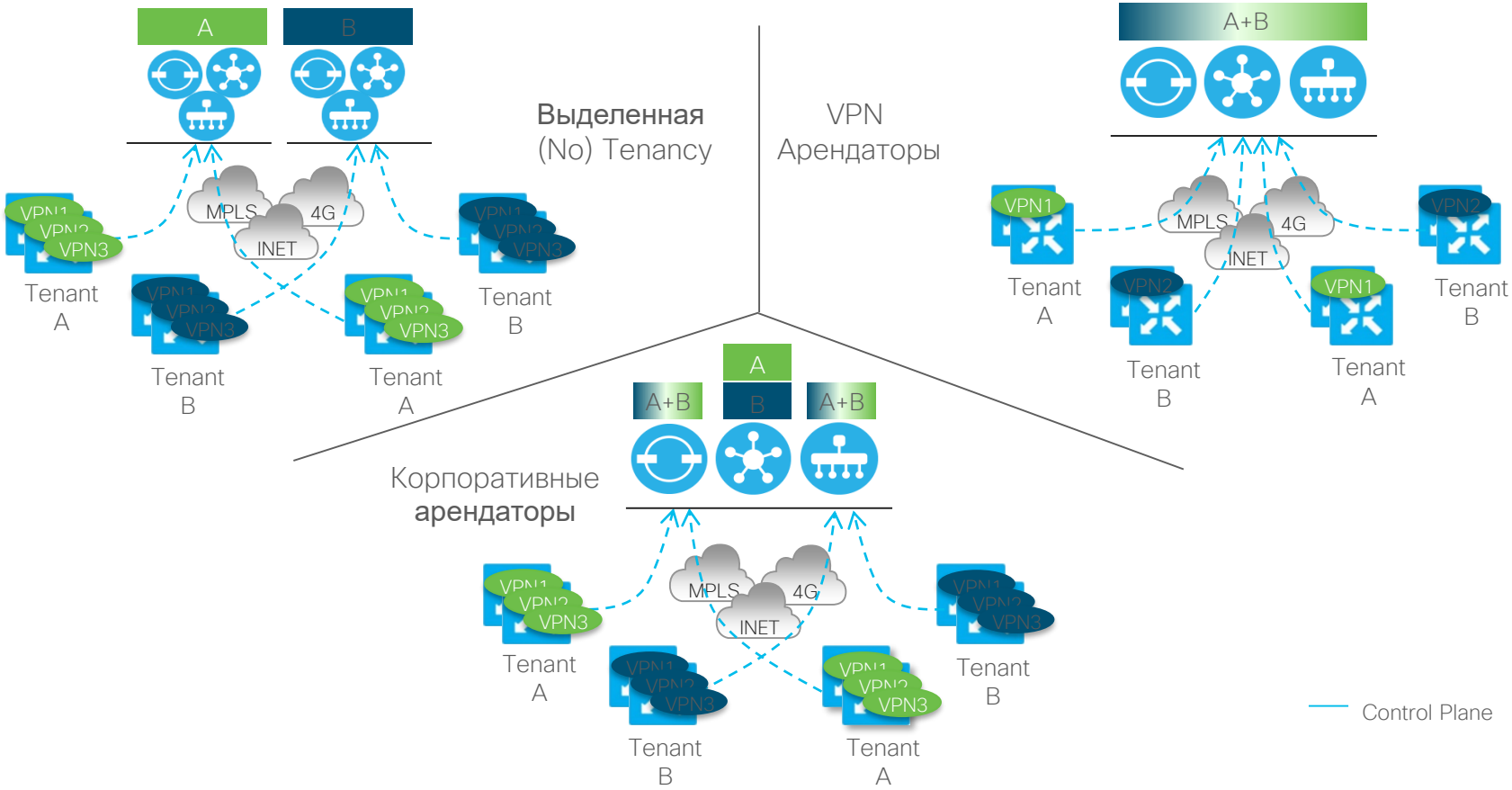


Точка-точка
Point-to-Point

Оптимизация TCP

- Высокая задержка и/или **потери в канале** между пользователями и приложениями, т.е. гео-**распределенные подключения**
- vEdge терминирует TCP сессию и делает **локальные** acknowledgements
  - Хост не должен ждать TCP ACK от ответной стороны и приостанавливать TCP передачу
- Оптимизированные TCP соединения используют механизмы выборочных acknowledgements с целью предотвращения ненужных пересылок уже принятых сегментов
- Хосты, использующие устаревший стек TCP/IP увидят максимальную выгоду

Multitenancy



Масштабирование решения по горизонтали

Оркестрация
(vBond)

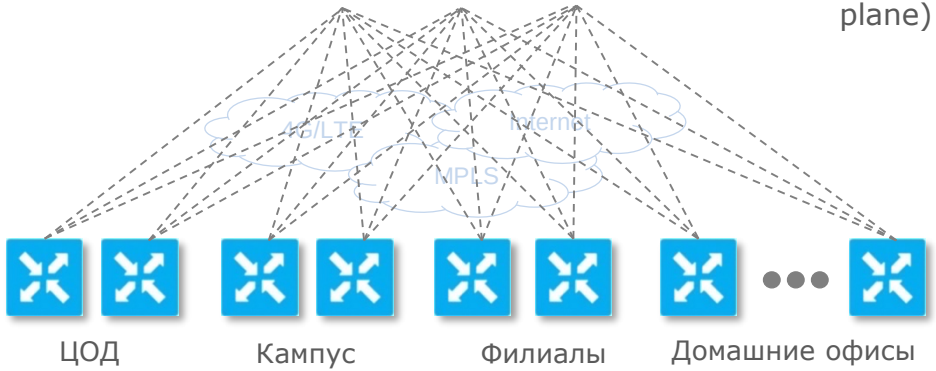
Администрирование
(Multi-tenant или выделенное)
(vManage)

Управление
(Контейнеры или ВМ)
(vSmart)

Модель масштабирования по горизонтали

Добавить оркестратор vBond для увеличения числа подключаемых vEdge

Создать vManage кластер чтобы вместить больше vEdge устройств

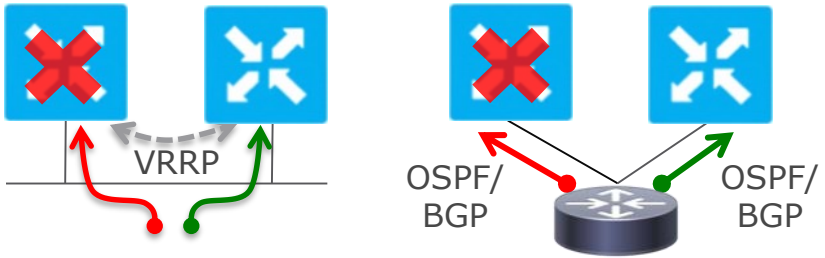


Добавить vSmart контроллеры для большей вместимости плоскости управления (control plane)

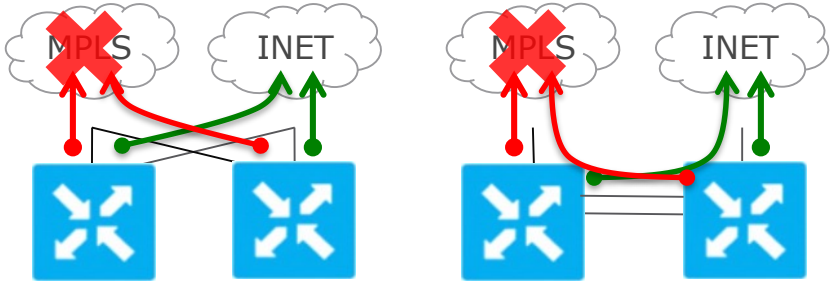
- Необходимо выбирать vEdge платформы с подходящей масштабируемостью по IPSec туннелям
- Необходимо использовать политики управления для определения VPN топологий

Высокая доступность и отказоустойчивость

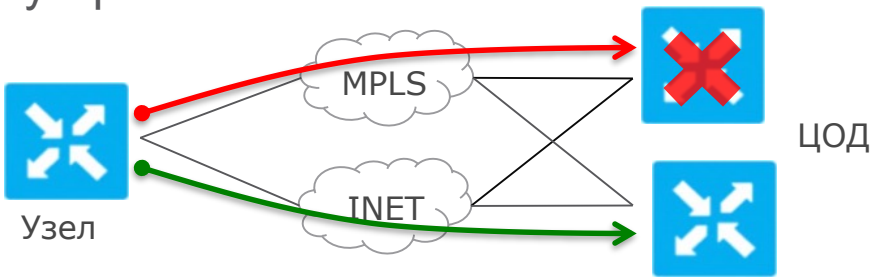
Отказоустойчивость узла



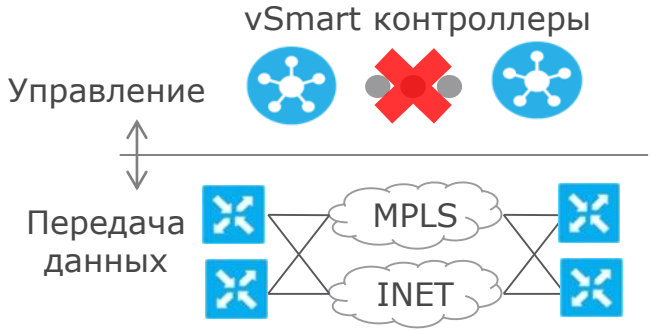
Отказоустойчивость транспорта



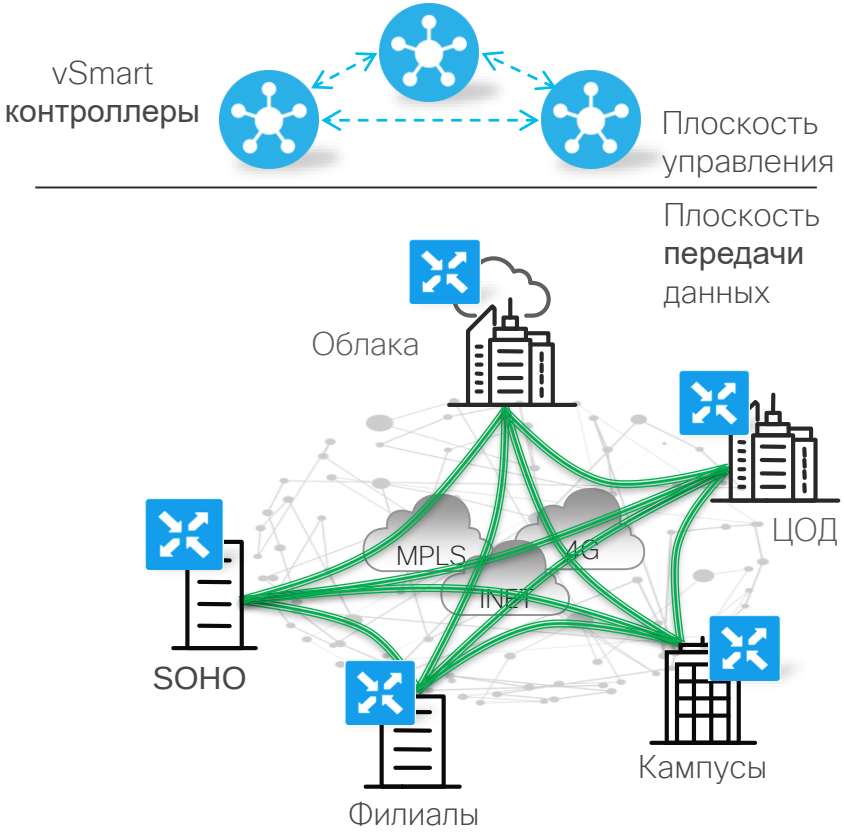
Отказоустойчивость сети/головного устройства



Отказоустойчивость управления

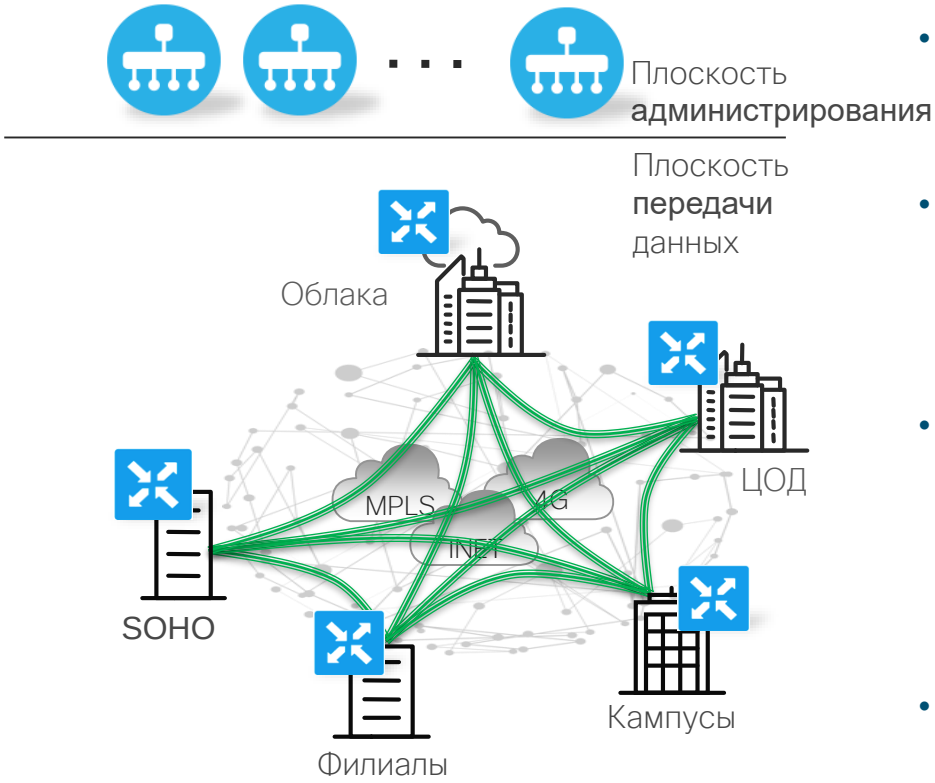


Отказоустойчивость – плоскость управления (vSmart)



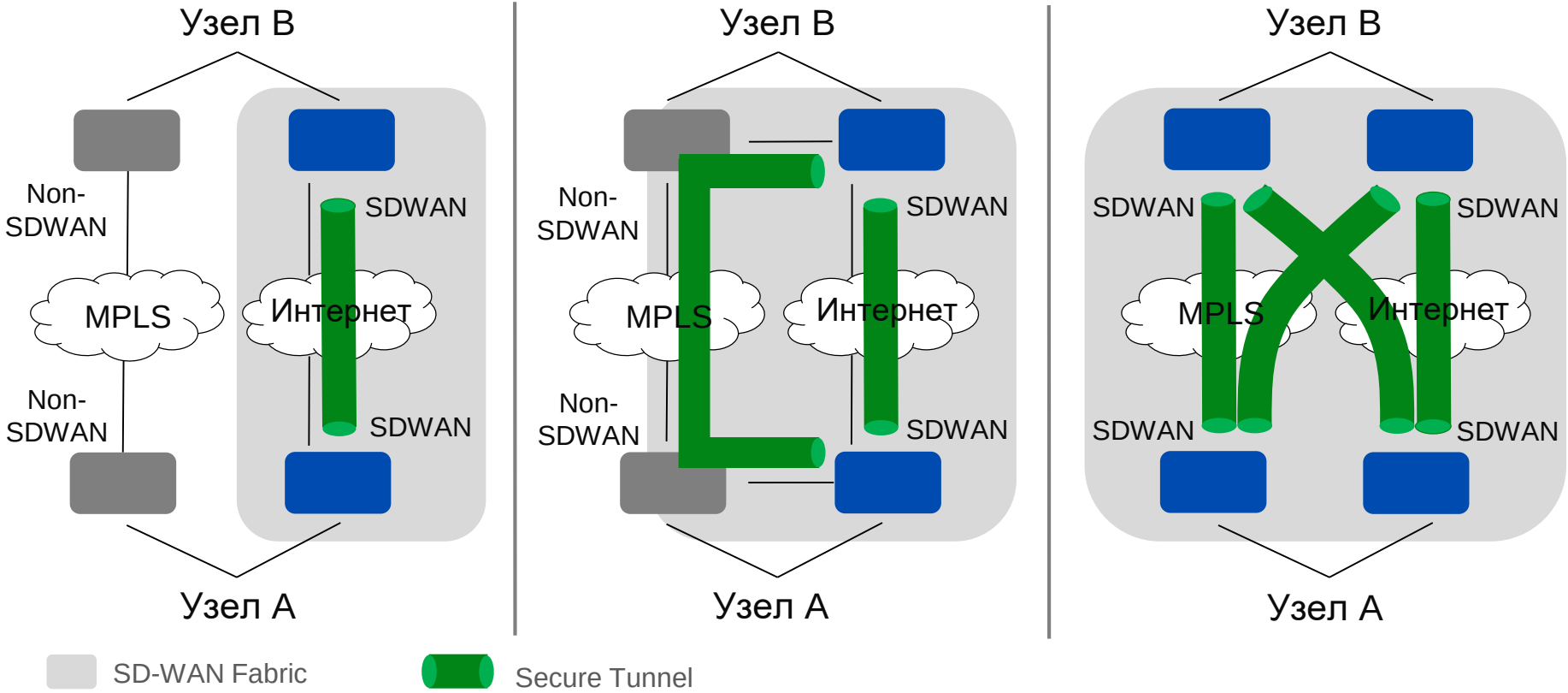
- vSmart контроллеры обмениваются OMP сообщениями и имеют идентичный вид всей SD-WAN фабрики
- Каждый маршрутизатор vEdge подключается к трем контроллерам vSmart для отказоустойчивости
- Отсутствует какое либо воздействие на фабрику пока vEdge подключен хотя бы к одному vSmart контроллеру
- Если все контроллеры стали недоступны ввиду аварии, vEdge маршрутизатор продолжает функционировать в крайнем известном хорошем состоянии в течение настраиваемого промежутка времени
  - Изменения невозможны

Отказоустойчивость – Администрирование (vManage)



- vManage серверы формируют кластер для отказоустойчивости и высокой доступности
- Все серверы в кластере работают в режиме Active/Active
  - Все члены кластера должны быть в одном ЦОД или merto area
- Для гео-резервирования vManage работают в режиме Active/Standby
  - Не кластеризуются
  - Используется репликация данных между площадками
- Потеря всех vManage серверов не накладывает ограничений на работу SD-WAN фабрки, невозможно только
  - Вносить административные изменения

Варианты перехода на SD-WAN



Доступные аппаратные платформы от Viptela

Routing Offer Details

Cisco ONE Advantage
DNA Essentials
DNA Advantage

Centralized Management

- On-prem or cloud managed
- Zero touch deployment
- Branch virtualization with Cisco VNF orchestration
- Day 0 and Day 2 provisioning
- Lifecycle management

Secure Connectivity

- Unlimited segmentation

- SD-WAN and advanced WAN topologies
- Limited segmentation
- Cloud connectivity

- All types of connectivity
- Secure VPN overlay
- Basic L3-L4 firewall, IPS
- Basic application visibility

Policy Based Automation

- Advanced network and application visibility
- WAN Optimization

- Application aware policies using path control, bandwidth optimization
- Contextual insights with assurance
- Encrypted traffic analytics

Analytics and Assurance

- Network optimization analytics
- Application trending and forecasting

Network Essentials & Advantage (IP Base + Sec)*

*Network Essentials and Network Advantage are perpetual and not required for vEdge or ENCS

Capabilities for Cloud Managed through vManage

DNA Essentials

3,5 Year Terms

Connectivity
VPN Overlay, Topology: Hub-n-spoke,
NAT, Split tunnel,
2 VPNs: 1 transport, 1 service side
VPN with L2 or L3

Security
Encryption: AES-256,
Policy support: Local ACL only, Data policy

Application Experience
QoS (classification, policing, remarking, scheduling), App-aware routing (5 tuple only), DPI for visibility, App visibility (name, throughput)

Management
Viptela vManage platform, Zero Touch Provisioning, Day 0 , day 1, day N Changes

DNA Advantage (Include DNA Essentials)

3,5 Year Terms

Connectivity
Service-side routing, Mesh topology, Multicast
VPNs: 5 (1 transport, 4 service side)

Security
Control policy
Advanced policies: Service chaining, extranet

Application Experience:
DPI for app-aware routing and policies
SaaS on-ramp (was CloudExpress)
TCP Optimization

Management & Orchestration
End to end SD-WAN policy orchestration, network and application trouble shooting

C1 Advantage (Include DNA Essentials & DNA Advantage)

3,5 Year Terms

Connectivity: VPNs: Up to system scale

Advanced Application Experience
WAN Full stack WAAS

Analytics:
VAnalytics platform

Platforms Supported Now: vedge
Platforms Support Post July: ISR, ASR, ENCS

Capabilities for On-Prem Managed through DNA Center

DNA Essentials

3,5 Year Terms

Router Deployment
Day 0 and Day 2 Changes

Branch Virtualization
NFV provisioning on ENCS and UCS-E
Cisco VNF orchestration only(ISRv, vEdge, vASA and vWAAS**)

Application Visibility :name, throughput

Assurance: Router Monitoring (Basic)
VNF monitoring (ISRv, vWAAS**), ENFV (ENCS, UCSE), Dashboards (Overall Health, Network Health, Client Health), topology, pre- canned Reports, custom Thresholds

Automation: Inventory, Discovery, Topology, Software Image Management, Site Management, Network Settings, Credential Update, Integrity Verification, Template Programmer, Canned Reports, PnP Application

DNA Advantage (Include DNA Essentials)

3,5 Year Terms

IWAN
IWAN Application

Branch Virtualization
3rd party VNF orchestration, Backup / Snapshot / restore*, Stateful High Availability*, Clustering*

Assurance: Router 360 ,ENFV 360*, Router underlay insights, ENFV Insights*, 360 pages, Health score, Time Travel, Targeted Insights, Neighbor topology, Path trace, KPIs, Baselining, Trends, custom reports (application experience, SDA, Wifi KPIs etc.)

Automation: Application Policy, SWIM (Patching), SD Bonjour, ETA*, Reporting (Tableau)

C1 Advantage (Include DNA Essentials & DNA Advantage)

3,5 Year Terms

Advance application experience
AppNav, WAN Full stack WAAS (managed by WCM- WAAS Central Manager)

Branch Virtualization
Storage Virtualization*

Network Essentials

Perpetual

Essential Routing Capabilities
BGP, OSPF, EIGRP, IGMP, IGRP, ISIS, LACP, RIP

Router Management
EEM, TACACS+, NETCONF, AAA, DNS, DHCP, DPI Visibility (Full FNF), IPSLA, Basic Qos (classification, Policing, Remarking, scheduling), NAT

VPNs: GETVPN, FlexVPN, GRE, DMVPN (Hub Spoke)

Security: IKE, IPSEC, PKI, MacSec
Zone Based Firewall, encryption algorithms (AES,DES,3DES, SHA,MD5), IPS(community signature), ALG, SSLVPN, Trustsec SXP

Network Advantage

Perpetual

Routing Capabilities:
Multicast, MPLS

App based policy:
PFR, PBR, App Aware Qos Policy, TCP optimization, App performance troubleshooting (co-related insights)

Segmentation:
Trustsec (SGT, SGACL), SDA Border, SDA Ctrl plane, VRF Segmentation

VPNs: DMVPN- full Mesh topology support, LISP

* Roadmap
** WaaS license part of C1 Advantage

Platforms: ISR, ASR, ENCS

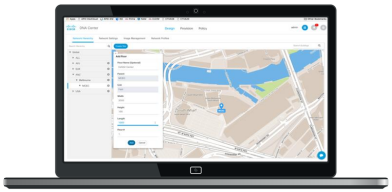
What can you use?

Today

Cloud Management
vManage

Platforms: **vEdge**

On-prem Management
DNA Center



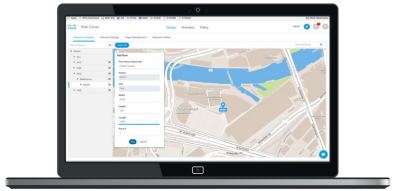
Platforms: **ISR, ASR, ENCS**

Post Integration (July 2018)

Cloud Management
vManage

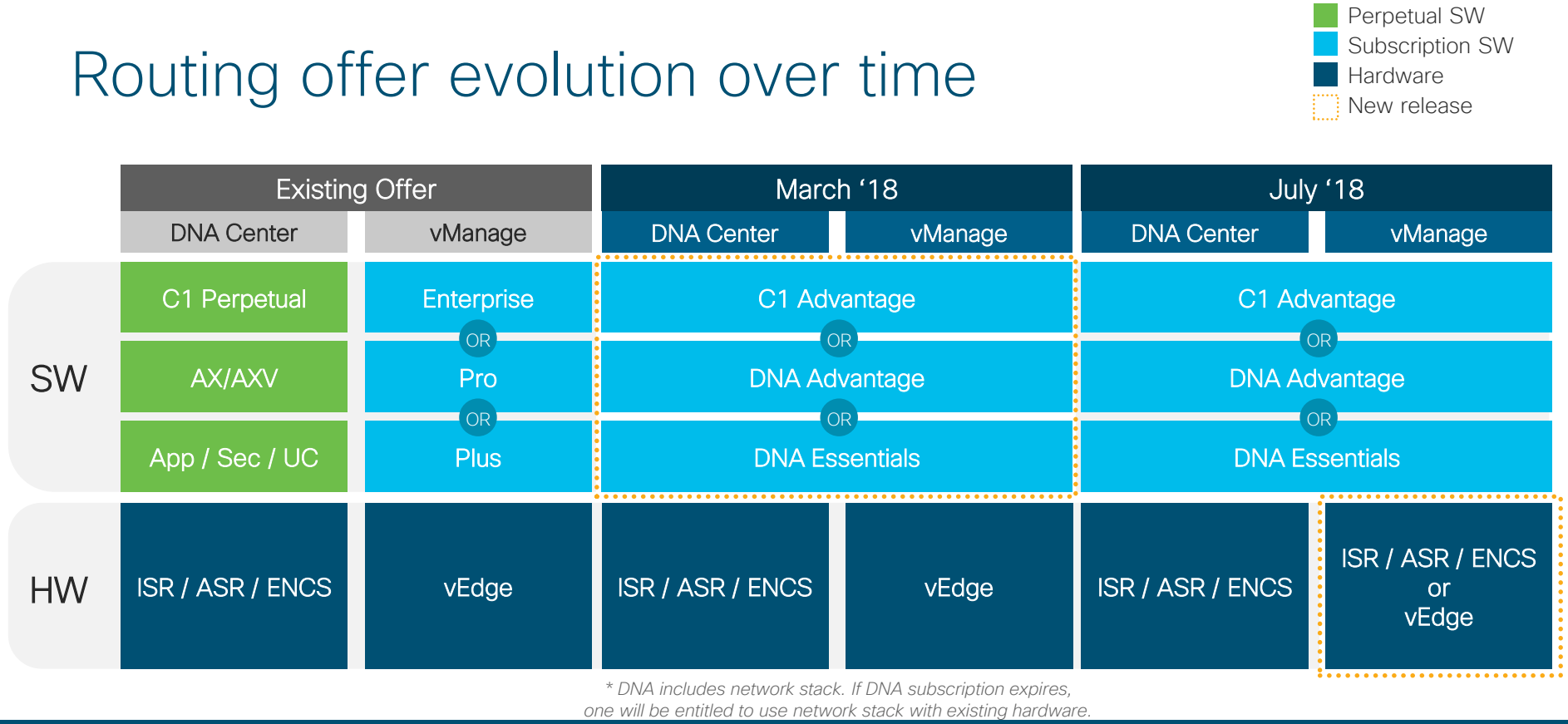
Any routing Platform:
ISR, ASR, ENCS, vEdge

On-prem Management
DNA Center



Platforms: **ISR, ASR, ENCS**

Routing offer evolution over time



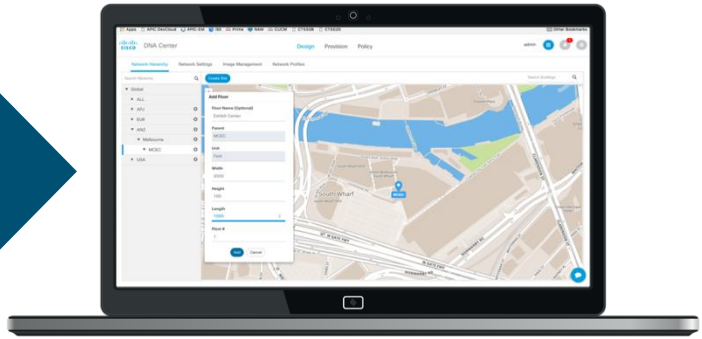
** DNA includes network stack. If DNA subscription expires, one will be entitled to use network stack with existing hardware.*

Key take-away

From March '18, DNA subscription offers for both DNA Center and vManage
From July '18, ISR 1000, ISR 4000, ASR 1000 and ENCS 5000 will be supported by vManage

vManage vs DNA Center

vManage merges with DNA Center in CY19



Cisco vManage

Cisco Routing customers who want Cloud management and SD-WAN and are on the journey to the Intent-based WAN

Cisco DNA Center

Cisco's on-prem management platform for customers who have Cisco Switching and Wireless

Lead with vManage for Intent–based WAN

Applicability Matrix

		10M	20M	50M	100M	500M	1G	2.5G	10G
Cisco 1100 Series ISRs	Cisco ONE Advantage	✓	✓	✓	✓				
	Advantage	✓	✓	✓	✓				
	Essentials	✓	✓	✓	✓				
Cisco 4221 ISR	Cisco ONE Advantage	✓	✓	✓					
	Advantage	✓	✓	✓					
	Essentials	✓	✓	✓					
Cisco 4331 ISR	Cisco ONE Advantage	✓	✓	✓	✓				
	Advantage	✓	✓	✓	✓				
	Essentials	✓	✓	✓	✓				
Cisco 4451 ISR	Cisco ONE Advantage				✓	✓	✓		
	Advantage				✓	✓	✓		
	Essentials				✓	✓	✓		
ENCS	Cisco ONE Advantage				✓	✓	✓		
	Advantage				✓	✓	✓		
	Essentials								
ASR 1001-X	Cisco ONE Advantage							✓	
	Advantage							✓	
	Essentials								
ASR 1002-X	Cisco ONE Advantage								✓
	Advantage								✓
	Essentials								
Cisco vEDGE 100 Series	Cisco ONE Advantage	✓	✓	✓	✓				
	Advantage	✓	✓	✓	✓				
	Essentials	✓	✓	✓	✓				
Cisco vEDGE 1000 Series	Cisco ONE Advantage	✓	✓	✓	✓	✓	✓		
	Advantage	✓	✓	✓	✓	✓	✓		
	Essentials	✓	✓	✓	✓	✓	✓		
Cisco vEDGE 2000 Series	Cisco ONE Advantage	✓	✓	✓	✓	✓	✓	✓	✓
	Advantage	✓	✓	✓	✓	✓	✓	✓	✓
	Essentials	✓	✓	✓	✓	✓	✓	✓	✓
Cisco vEDGE 5000 Series	Cisco ONE Advantage	✓	✓	✓	✓	✓	✓	✓	✓
	Advantage	✓	✓	✓	✓	✓	✓	✓	✓
	Essentials	✓	✓	✓	✓	✓	✓	✓	✓

New Easy to Order PID's

Lead with new PID'S for key product families

Easy attach of DNA offers

Better Pricing

Product Family*	NEW PIDs	Description
ISR 4000 Series	**ISR4331-DNA**	**Cisco ISR 4331 (3 GE, 2 NIM, 1 SM) with DNA Support**
ISR 4000 Series	ISR4451-DNA	Cisco ISR 4451 (4 GE, 3 NIM, 2 SM) with DNA Support
ISR 1000 Series	C1111-8P-DNA	ISR 1100 8 Ports Dual GE WAN with DNA Support
ISR 1000 Series	C1111-8PLTEEA-DNA	ISR 1100 8 Port Dual GE LTE EA with DNA Support
ISR 1000 Series	C1111-8PLTELA-DNA	ISR 1100 8 Port Dual GE LTE LA with DNA Support
ASR 1000 Series	ASR1001-X-DNA	Cisco ASR 1001-X Crypto,6GE, Dual-PS with DNA Support
ASR 1000 Series	ASR1002-HX-DNA	Cisco ASR 1002-HX, 4x10GE+4x1GE, Dual PS with DNA Support
VEDGE 100 Series	VEDGE-100B-AC-K9	vEdge-100 AC chassis with 5 Ethernet ports, rack mount kit and cables
VEDGE 100 Series	VEDGE-100M-AC-K9*	vEdge-100 AC chassis with single 4G/LTE SIM, integrated power supply, 5 Ethernet ports
VEDGE 100 Series	VEDGE-100WM-AC-K9*	vEdge-100 AC chassis with single 802.11 radio and single 4G/LTE SIM, integrated power supply, 5 Ethernet ports and cables
VEDGE 1000 Series	VEDGE-1000-AC-K9	vEdge-1000 AC base chassis with 8x1GE fixed ports, dual AC power adapters and cables
VEDGE 2000 Series	VEDGE-2000-AC-K9	vEdge-2000 AC base chassis with 4x1GE fixed ports and dual Pluggable Interface Module
VEDGE 5000 Series	VEDGE-5000-AC-K9	vEdge-5000 AC router base chassis with 4x10G, 8x1G copper, 8x1G fiber modular NIMS

To get DNA subscription for existing ISR/ ASR/ vEdge, use PID: **LIC-DNA-ADD**

Subscription for product families not shown here can be purchased as a-la-carte

Cisco SD-WAN Evolution – Looking Ahead

6-12 months

12-24 months

Leapfrog With E2E Arch

Enhance With Portfolio

Core SDWAN

SDWAN + SDA

Analytics EN wide

Multi-cloud connect

Voice, App acceleration

Platform diversity

Appliance security

ZBF, URL filtering, IPS/IDS

SAE

Security Integration

(Umbrella, CloudLock, ISE)

MSP NaaS

Application QOE

TestDrive

Quick Deploy

NaaS P2

Easy Troubleshooting & Ops

Analytics Visibility

One-click Cloud Networking

VDI Acceleration

Scale cloud-ops

Integration Roadmap

In Planning

Capabilities in "SD-WAN Integrated IOSXE"

SD-WAN Capabilities

SD WAN Features
- ✓ ZTP
- ✓ App Route Policy
- ✓ HQoS- Parent shaper with Child Policy
- ✓ Cloud Onramp –IAAS
- ✓ Segmentation
- ✓ NAT DIA
- ✓ BFD PMTU

Routing Protocols
- ✓ BGP, OSPF

Other Features
- ✓ VRRP
- ✓ DHCP server, DNS, RADIUS, Syslog, NTP

Monitoring & Troubleshooting
- ✓ System & Interface stats

SD WAN Feature
- ✓ All EFT features
- ✓ TLOC Extension

Monitoring & Troubleshooting
- ✓ vManage with DPI & Cflowd, Analytics

SD WAN Features
- Cloud Onramp-SAAS
- TCP Optimizations
- IPv6 support (Service & Transport)
- Service chaining
- Loopback interface

Services
- Multicast

IOS Capabilities

Capabilities
- ✓ NBAR2

Platform
- ✓ ISR 4331

New Interfaces
- ✓ Ethernet, 4G LTE, T1/E1

Capabilities
Security
- ✓ Umbrella (DNS redirect)
- ✓ Zone Based Firewall

Services
- ✓ NBAR2

Platforms
- ✓ ISR43xx, ISR4221, ASR1001-X, ASR1002-X, ASR 1001-HX, ASR 1002 –HX, ISRv (ENCS) 5412, C1111-8P LTEEA/LA, C1117-4PLTEEA/LA, C1111-8P

New Interfaces
- ✓ xDSL

Capabilities
- App QoE
- Security
  - Umbrella

Services
- AppNav Functionality
- UC –SRST, PSTN GW, SIP GW
- NBAR2-SD-AVC, Custom App

SDA segmentation use case Platforms:
- CSR, ENCS, ISR-4451, ISR-4431, ASR1006-X, ASR1009-X , 11xx

New Interfaces
- Port Channel


CISCO