



# Cisco Community Live event

Primeiros passos com Cisco SD-WAN (Viptela)

Guilherme Lyra

Solutions Architect – Enterprise Networking

12 de Novembro, 2020

# Novidades & Próximos eventos



# Ask Me Anything- DevNet Associate: Como posso ajudá-lo a se qualificar para a certificação?

Este evento ocorrerá do dia 30 de Novembro até 11 de Dezembro, 2020.



The banner features a dark blue background with a white and orange abstract shape. At the top left, it says 'Cisco Community | DevNet'. Below that is a circular profile picture of Jonas Fonseca. To the right of the profile picture, the dates '30 NOV - 11 DEC' and the name 'Jonas Fonseca' are listed, with 'Public Event' in smaller text below. A central image shows Jonas Fonseca pointing at a whiteboard in a meeting room. At the bottom left, there is a blue icon with a question mark and two people. At the bottom right, there is an orange button that says 'Ask a Question' with two white arrows pointing right. At the very bottom, a blue bar contains the text 'Ask Me Anything', 'General', and 'Cisco DevNet Associate: How can I help you qualify for the certification?'.

Cisco Community | DevNet

30 NOV - 11 DEC  
Jonas Fonseca  
*Public Event*

Ask a Question >>

**Ask Me Anything**  
General  
Cisco DevNet Associate: How can I help you qualify for the certification?

Prepare suas dúvidas para o evento Ask Me Anything- DevNet Associate: Como posso ajudá-lo a se qualificar para a certificação?

Link: <http://bit.ly/AMA-DevNet>

# Community Live Evento- Como NÃO implementar corretamente uma rede Wireless

Este evento ocorrerá na quinta-feira, 10 de Dezembro de 2020 às 11:00 am (Brasília) / 2:00 pm (Lisboa) / 3:00 pm (Luanda)



Community Live Evento

«Como **NÃO** implementar corretamente uma rede Wireless»

Apresentado por: Marco Bartulhe Question Manager: Ricardo Lacarra

Evento público

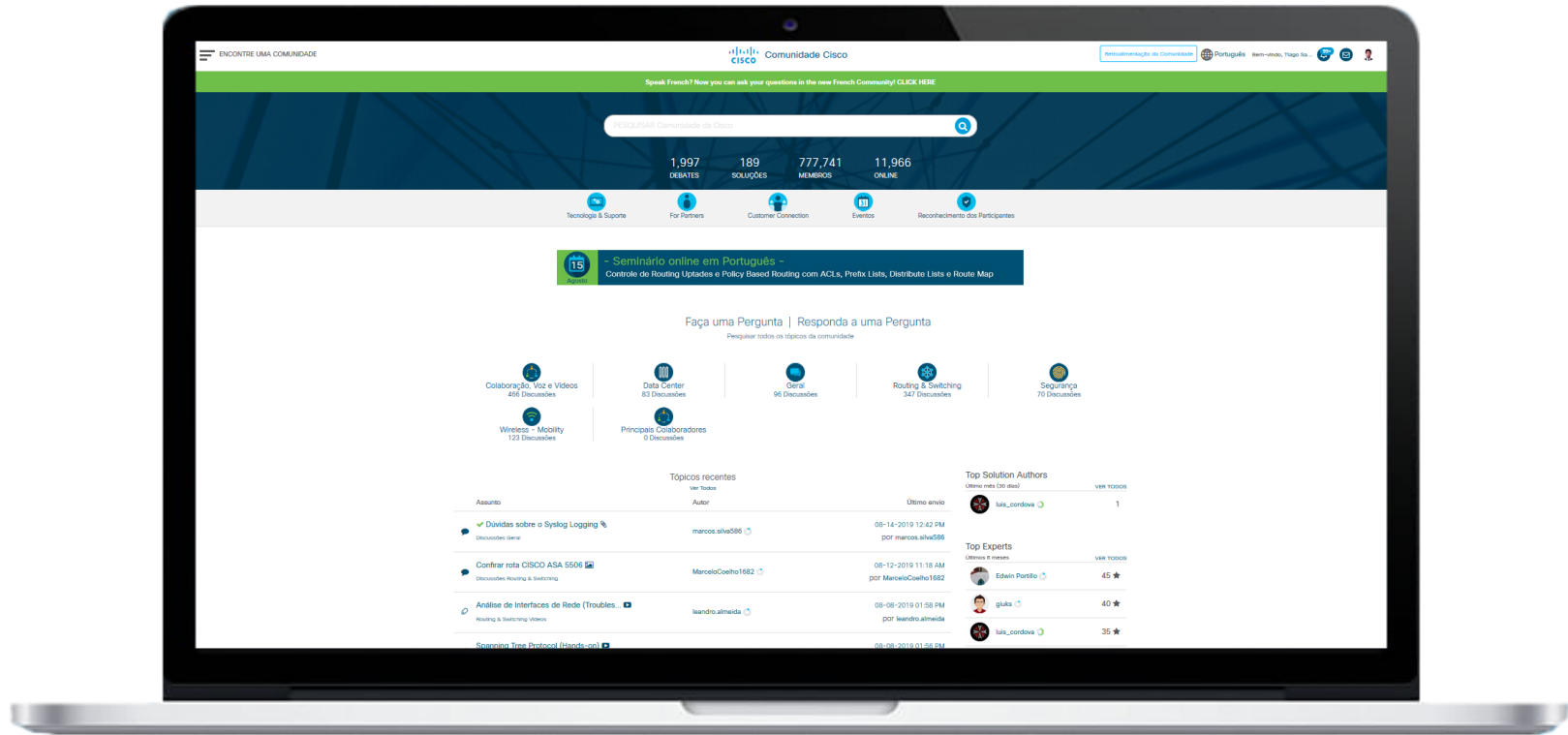
10 de Dezembro

Registre-se

Em parceria com:  Transforme sua empresa com tecnologia

Faça sua inscrição para o evento Community Live Evento- Como NÃO implementar corretamente uma rede Wireless

Link: <http://bit.ly/CLDez-wireless>



<http://community.cisco.com>

# Avalie os conteúdos publicados na Comunidade



Agradeça as pessoas que compartilham generosamente seus conhecimentos dentro da Comunidade dando um Kudo, ou seja, (clicando sobre a estrelinha).

Respostas

Blogs

Documentos

Eventos

Vídeos



Conheça o ranking dos membros com mais Kudos recebidos aqui:

<http://bit.ly/Cisco-Kudos>

# Mostre que a sua dúvida foi resolvida!

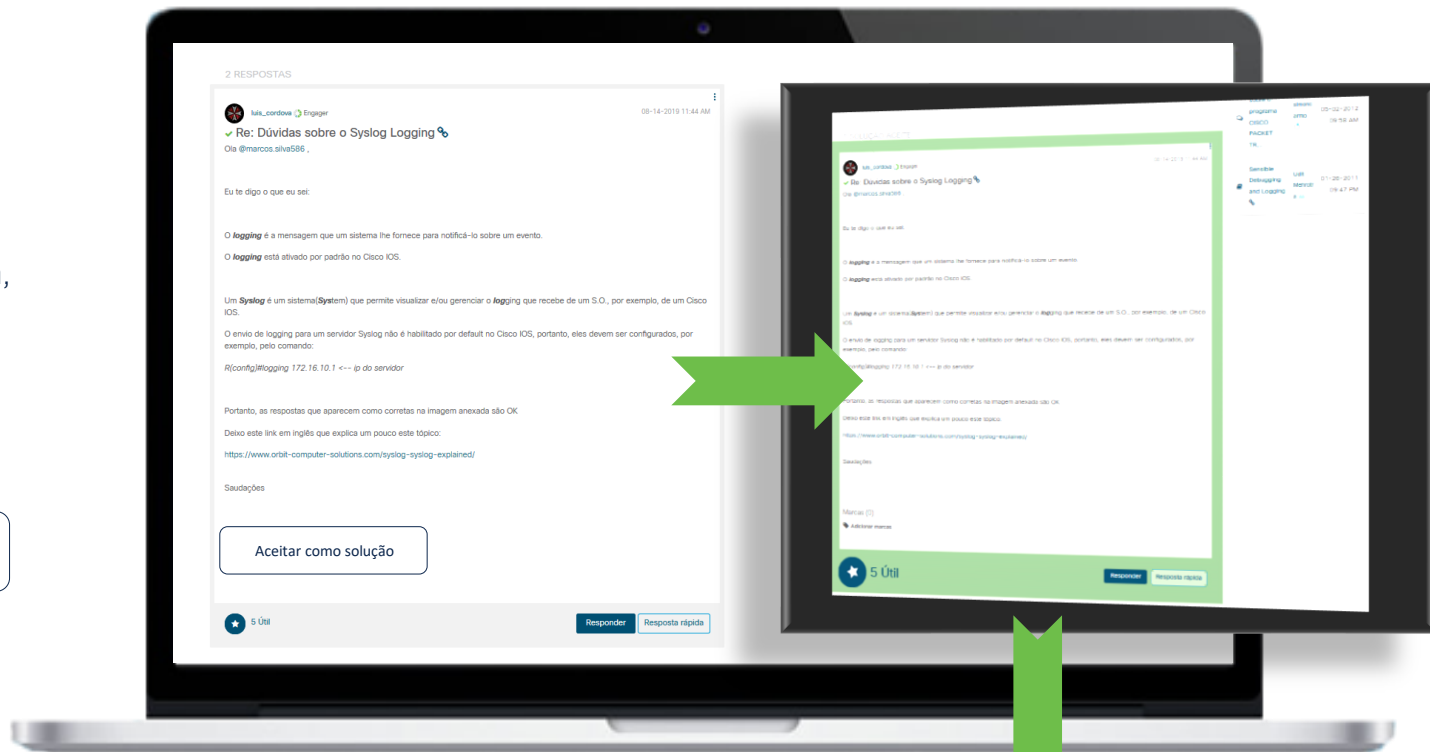
Embaixo de cada resposta se encontra o botão “Aceitar como solução”.

Se a resposta recebida resolve o seu problema, por favor faça como que todos saibam!

Simplesmente clique nesse botão:

Aceitar como solução

Aceitar como solução



Soluçionado!

# Especialista Convidado



**Guilherme Lyra**  
SOLUTIONS ARCHITECT



# Question Manager



**Lucas Borges**  
NETWORK ENGINEER

Obrigado por  
estar com a gente  
hoje!



<https://bit.ly/cl-Nov12slides>

# Publique as suas perguntas desde agora!

Use o painel de:  
Perguntas & Respostas (Q&A) para  
enviá-las.

Essas serão respondidas ao vivo  
no final da apresentação pelo  
especialista convidado.





# Primeiros passos com Cisco SD-WAN (Viptela)

Guilherme Lyra

Solutions Architect – Enterprise Networking

12 de Novembro, 2020

# Agenda

- Conceitos de Redes Definidas por Software
- Arquitetura da solução Cisco SD-WAN
- Como o Cisco SD-WAN pode ajudar sua empresa
- Demonstração

# Polling Question 1

Você já teve contato com alguma solução SD-WAN? Se sim, de qual fabricante?

- a) Cisco.
- b) VMware.
- c) Silver Peak.
- d) Fortinet.
- e) Outros.
- f) Ainda não tive contato.

# Redes Definidas por Software (SDN)

# Redes Definidas por Software (SDN)

## Conceitos básicos

- Desagregação do Plano de Controle e do Plano de Dados.
- Plano de Controle: atua como o cérebro da rede, tomando todas as decisões.
- Plano de Dados: se dedica ao encaminhamento do tráfego, seguindo as políticas recebidas do Plano de Controle.



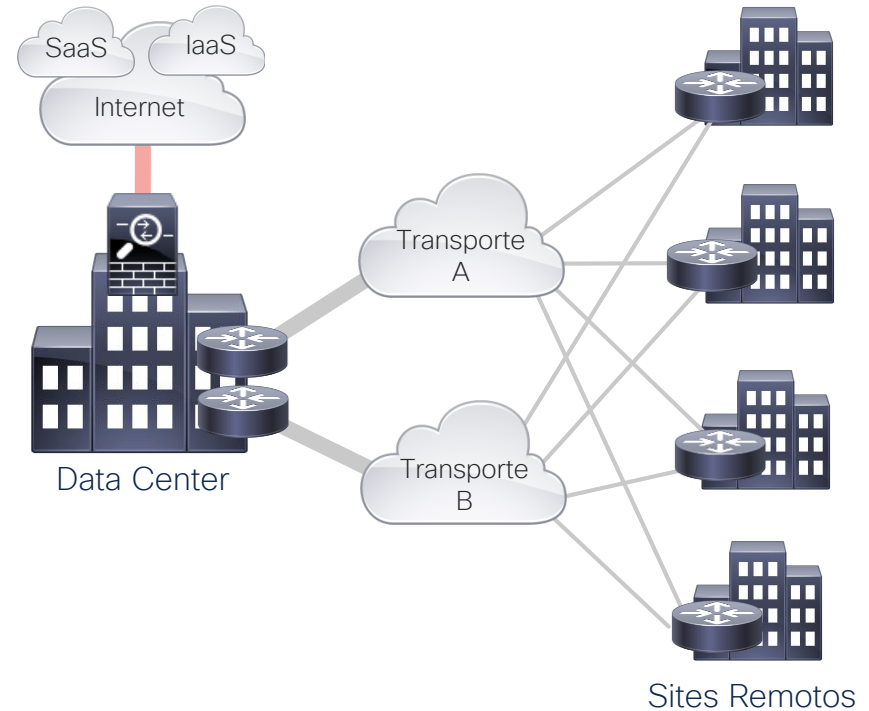
# Redes Definidas por Software (SDN)

## Conceitos básicos

- Gerenciamento, automação e monitoramento do ambiente são centralizados em um elemento dedicado.
- Abstração da infraestrutura físicas, permitindo a formação de topologias arbitrárias (conceito de Overlay).

# Limitações da rede WAN tradicional

- Alto custo com links de transporte.
- Operação é complexa e cara.
- Má experiência para o usuário final.
- Ambientes Multi-cloud são o “novo normal”.



Cisco SD-WAN

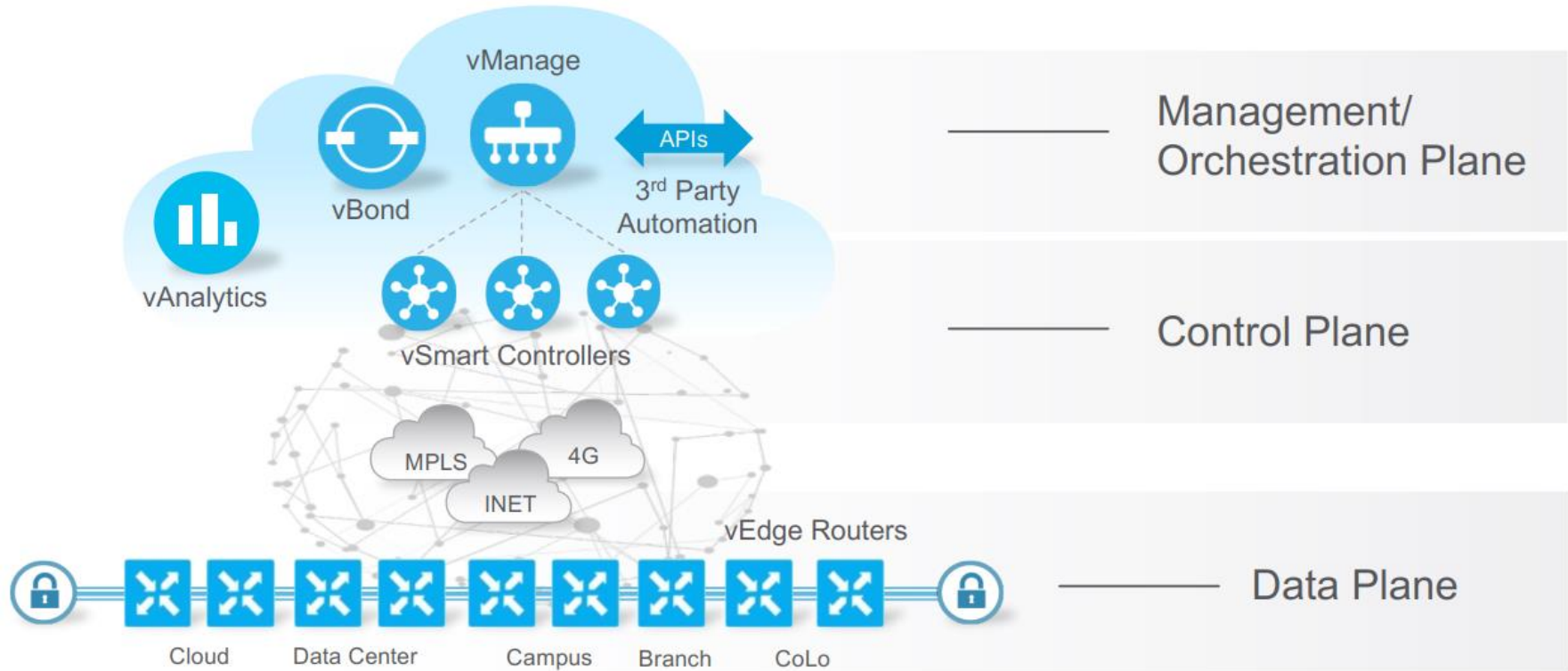


Control Plane

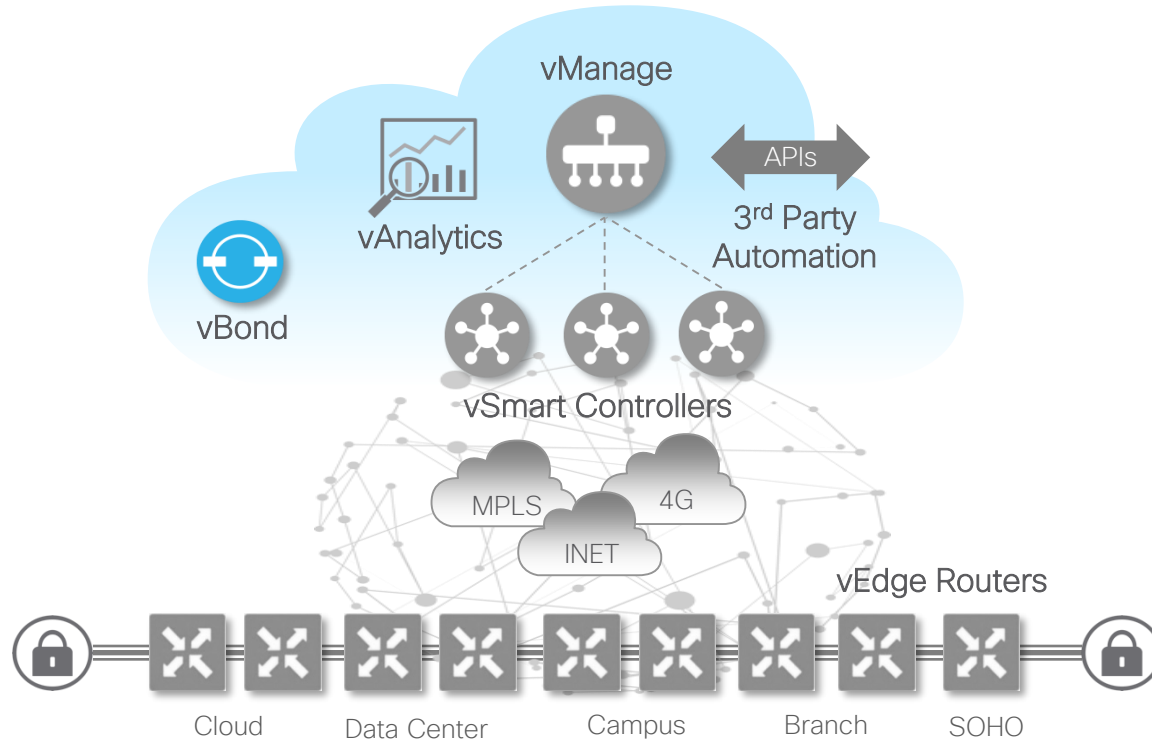
Data Plane I/O Modules

Switch Fabric

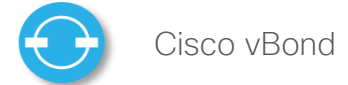
# Componentes da solução Cisco SD-WAN



# Plano de Orquestração

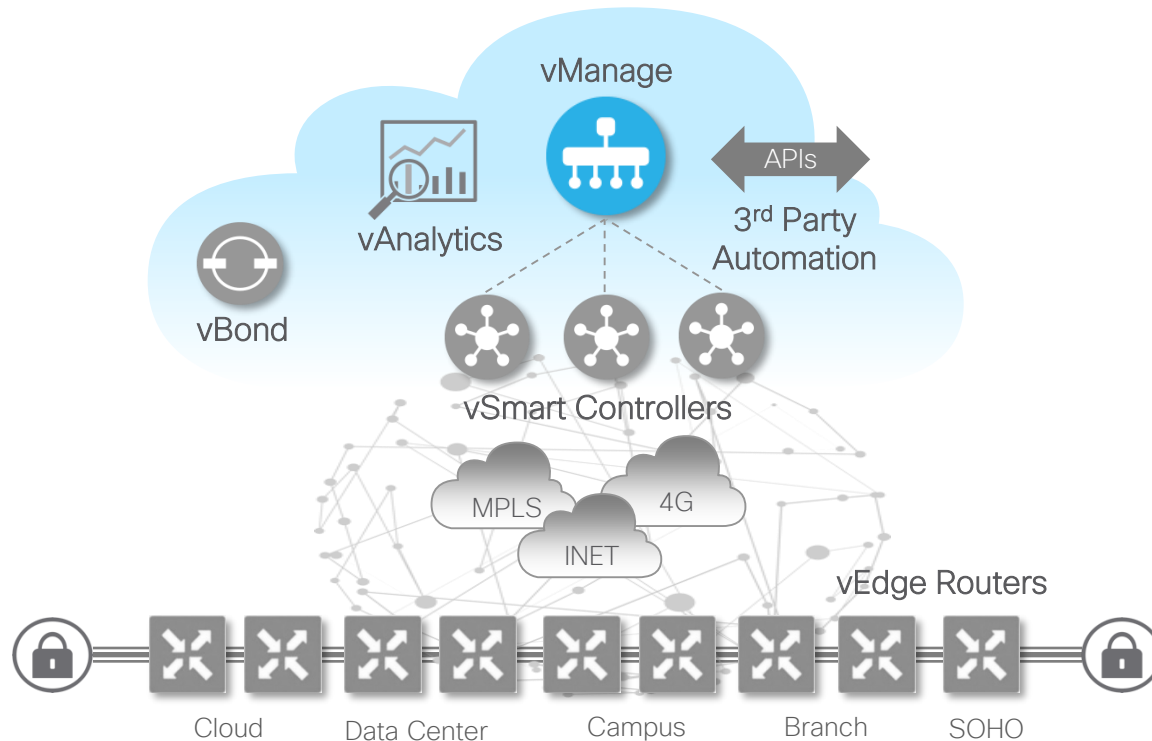


## Orchestration Plane



- Orchestrates control and management plane
- First point of authentication (white-list model)
- Distributes list of vSmarts/ vManage to all vEdge routers
- Facilitates NAT traversal

# Plano de Gerência



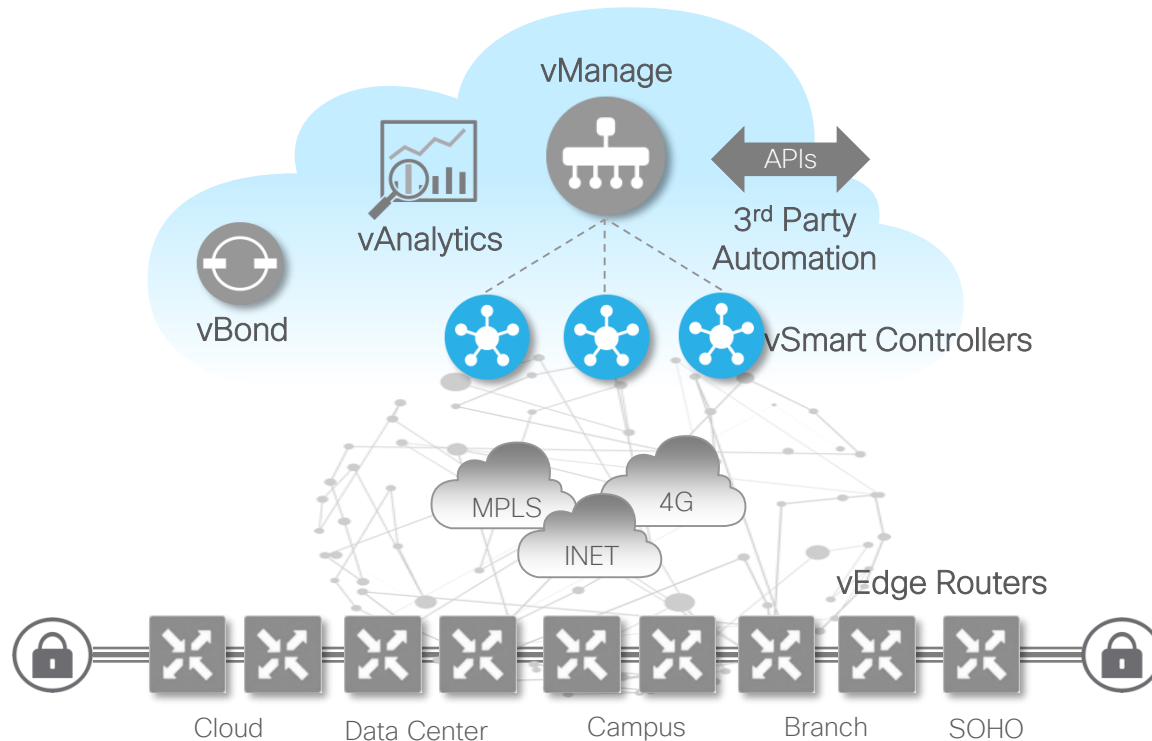
## Management Plane



Cisco vManage

- Single pane of glass
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades
- Programmatic interfaces (REST, NETCONF)

# Plano de Controle



## Control Plane

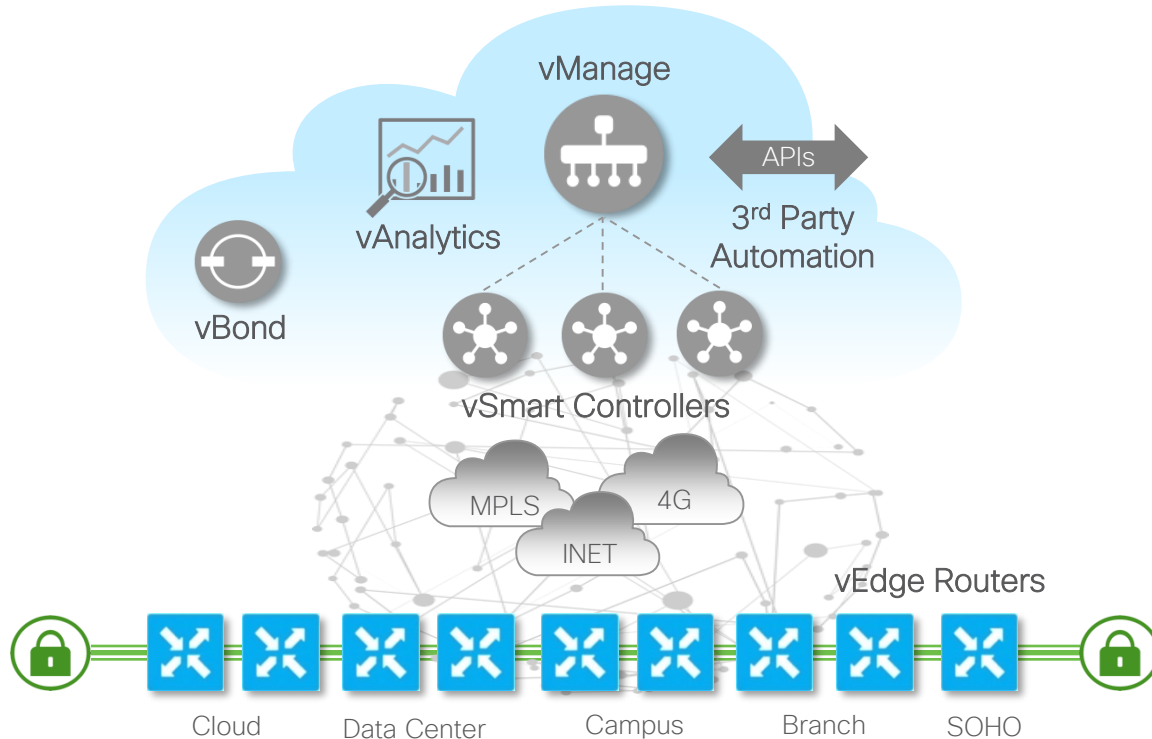


Cisco vSmart

- Facilitates fabric discovery
- Dissimilates Control Plane information between vEdges
- Distributes Data plane and App-aware Routing policies to the vEdge routers
- Implements Control plane policies
- Dramatically reduces control plane complexity



# Plano de Dados



## Data Plane Physical/Virtual

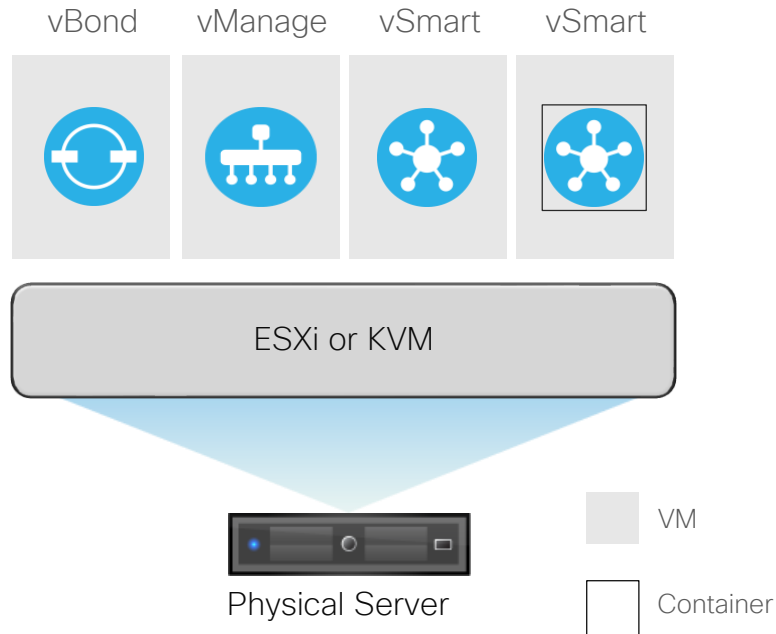


Cisco vEdge or cEdge

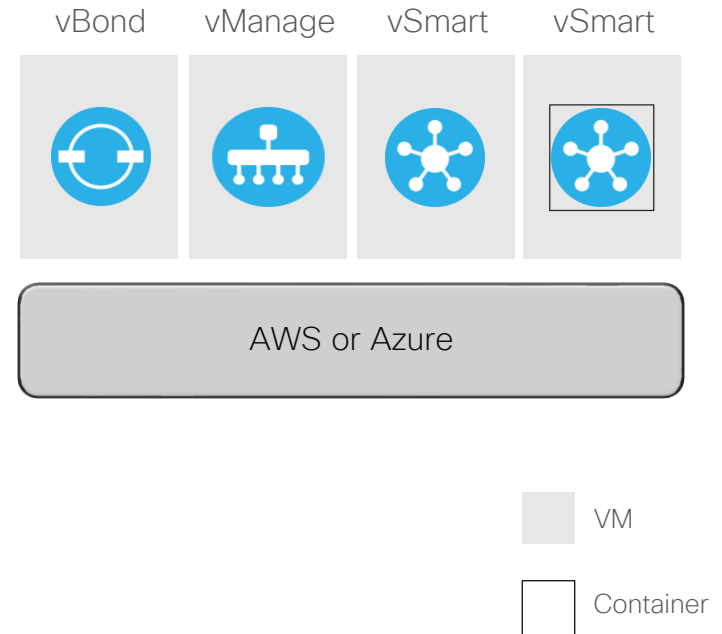
- WAN Edge router
- Provides secure data plane with remote vEdge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements Data plane and App-aware Routing policies
- Leverages traditional routing protocols like OSPF, BGP and VRRP

# Métodos de implantação dos controladores

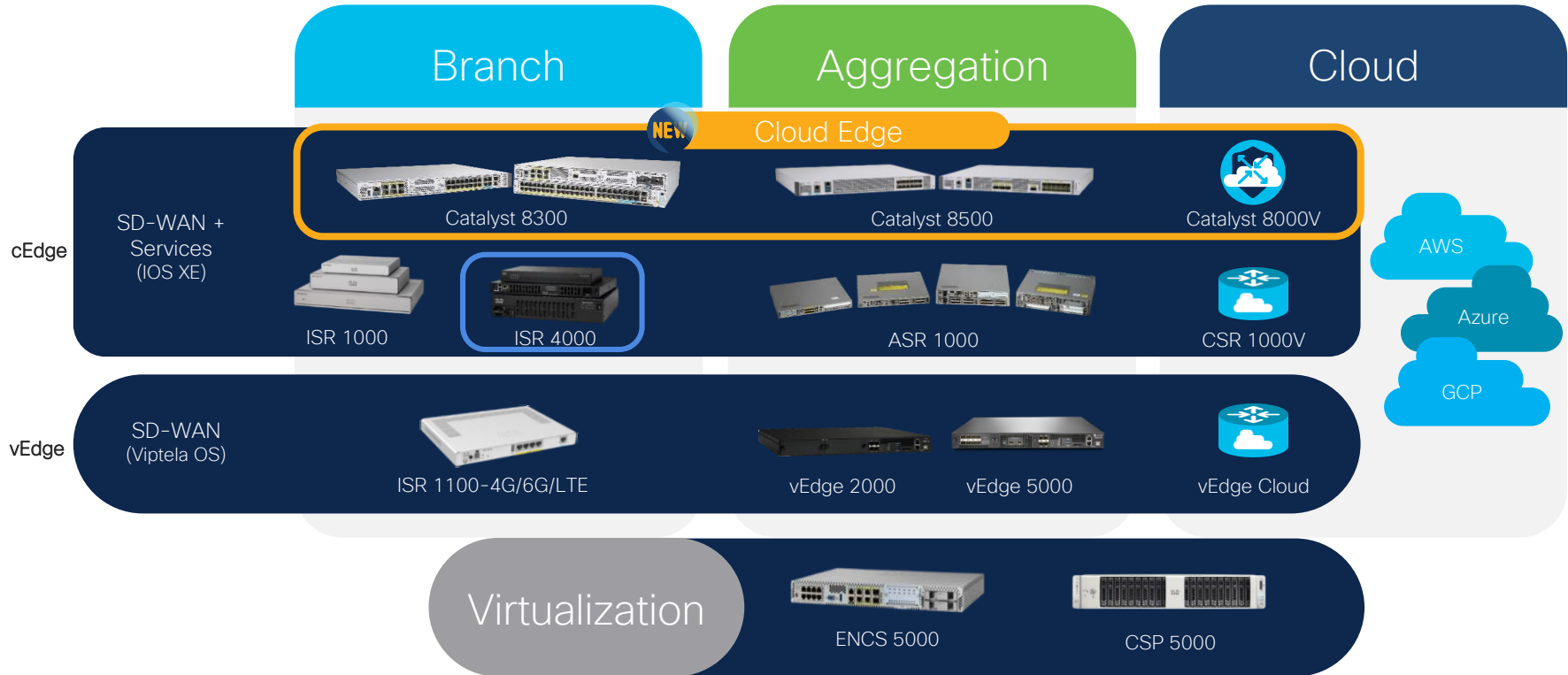
## On-Premise



## Hosted



# Plataformas suportadas



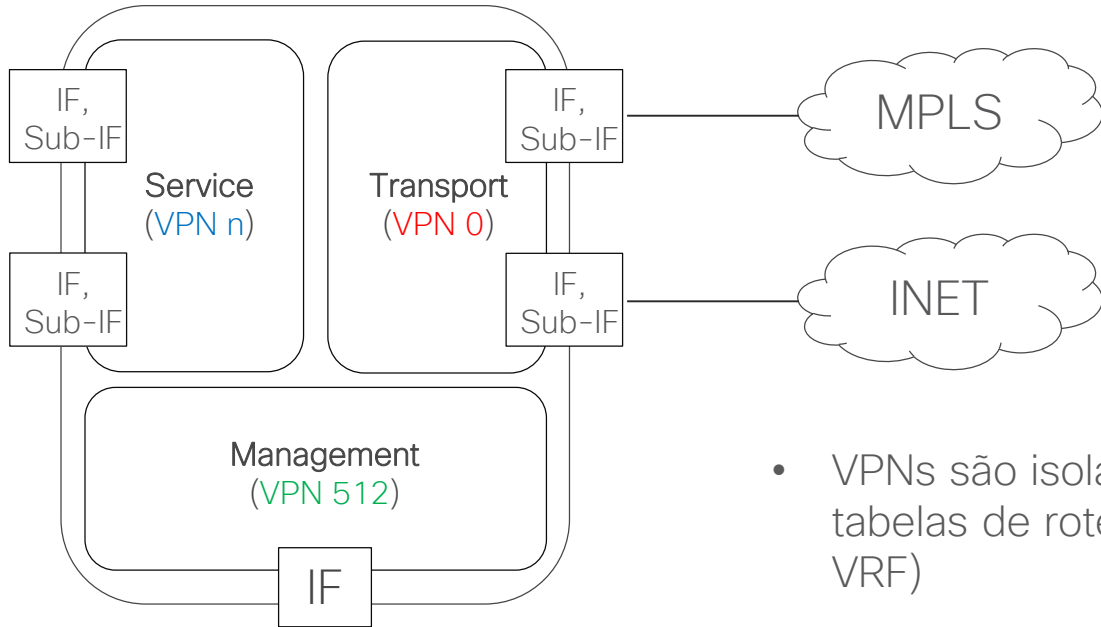
## Polling Question 2

Por qual motivo a desagregação do Control Plane e Data Plane é importante para as redes do futuro?

- a) Manter o ambiente seguro contra ameaças.
- b) Permitir o acesso à Internet e Cloud.
- c) Escalabilidade.
- d) Centralizar o gerenciamento.

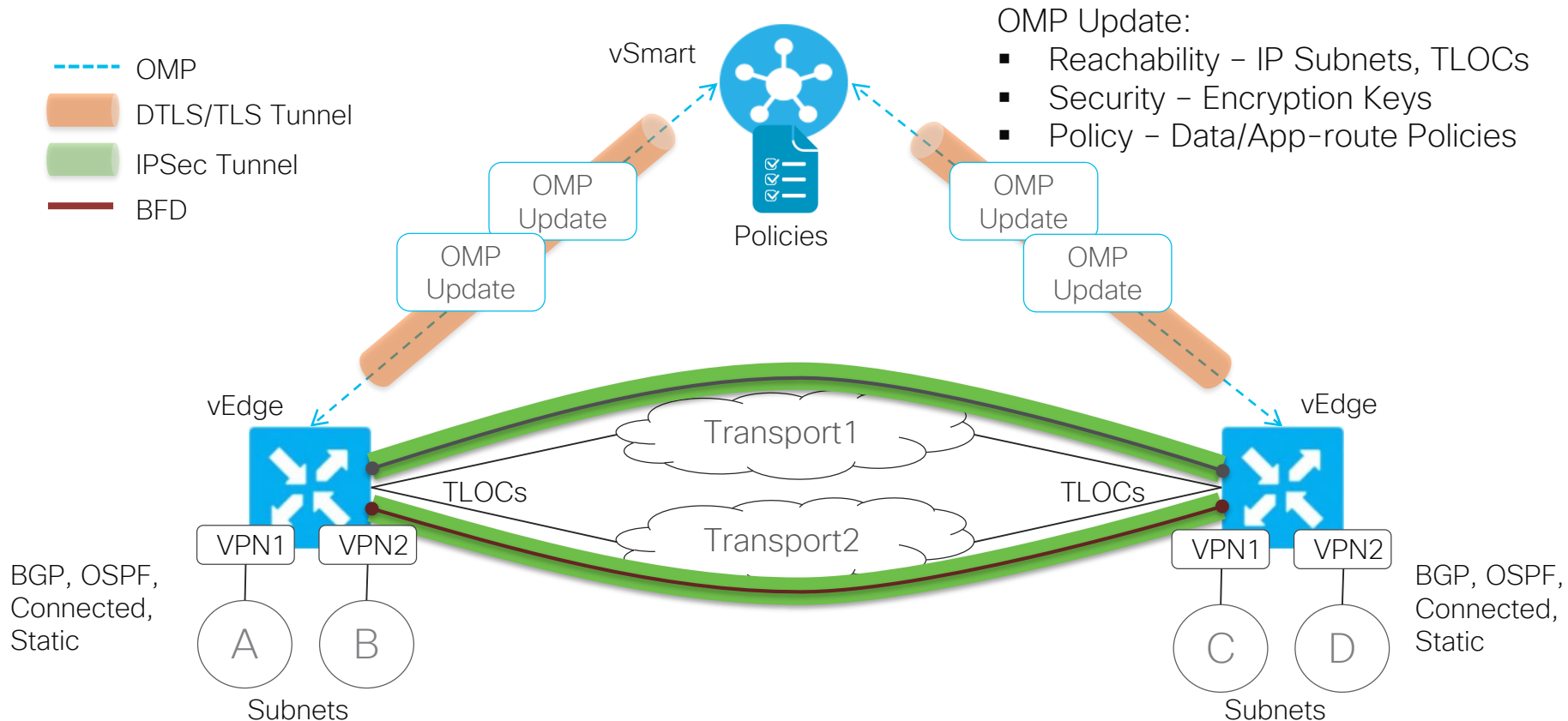
# Plano de Controle e Plano de Dados

# Cisco SD-WAN VPNs

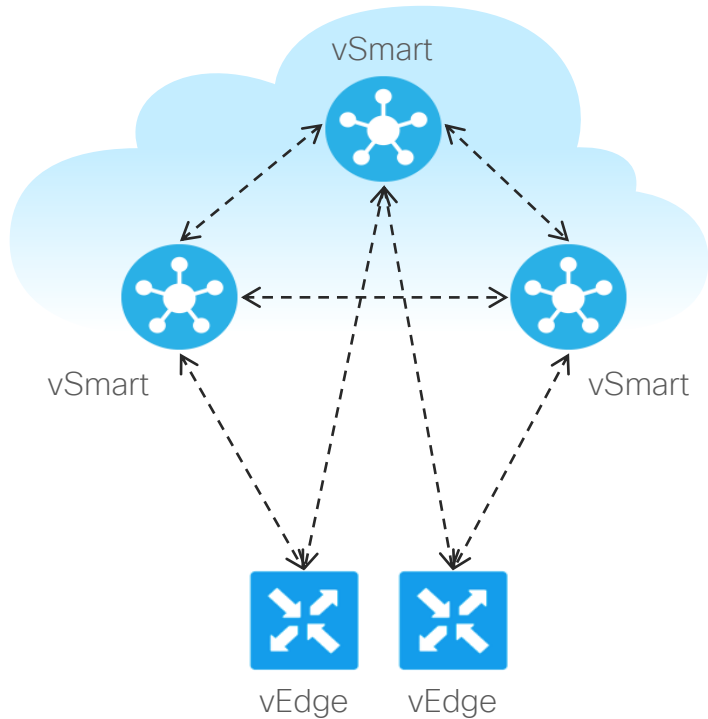


- VPNs são isoladas umas das outras, através de tabelas de roteamento distintas (conceito de VRF)
- Acessibilidade é anunciada via OMP

# Passo-a-passo de operação



# Overlay Management Protocol (OMP)

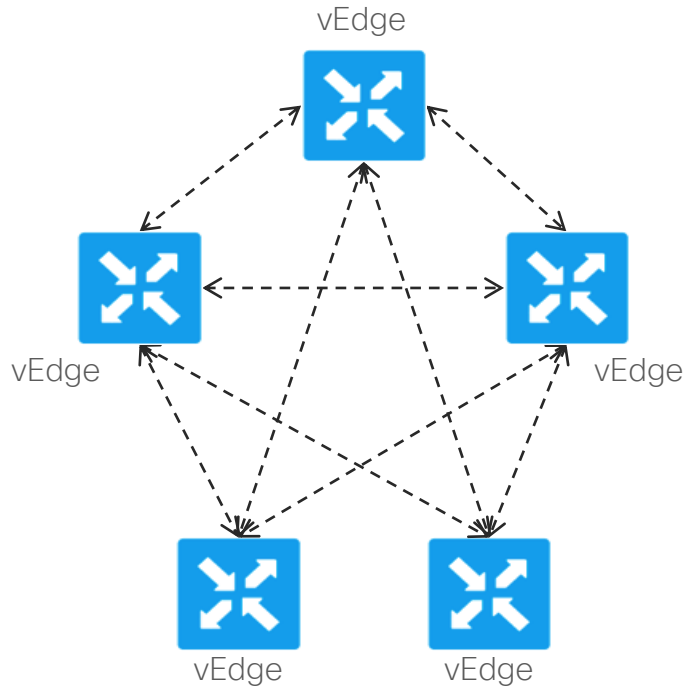


Note: vEdge routers need not connect to all vSmart Controllers

- TCP based extensible control plane protocol
- Runs between vEdge routers and vSmart controllers and between the vSmart controllers
  - Inside TLS/DTLS connections
- Leverages address families to advertise reachability for TLOCs, unicast/multicast destinations (statically/dynamically learnt service side routes), service routes (L4-L7), BFD stats (TE and H-SDWAN) and Cloud onRamp for SaaS probe stats (gateway)
  - Uses attributes
- Distributes IPsec encryption keys, and data and app-aware policies (embedded NETCONF)

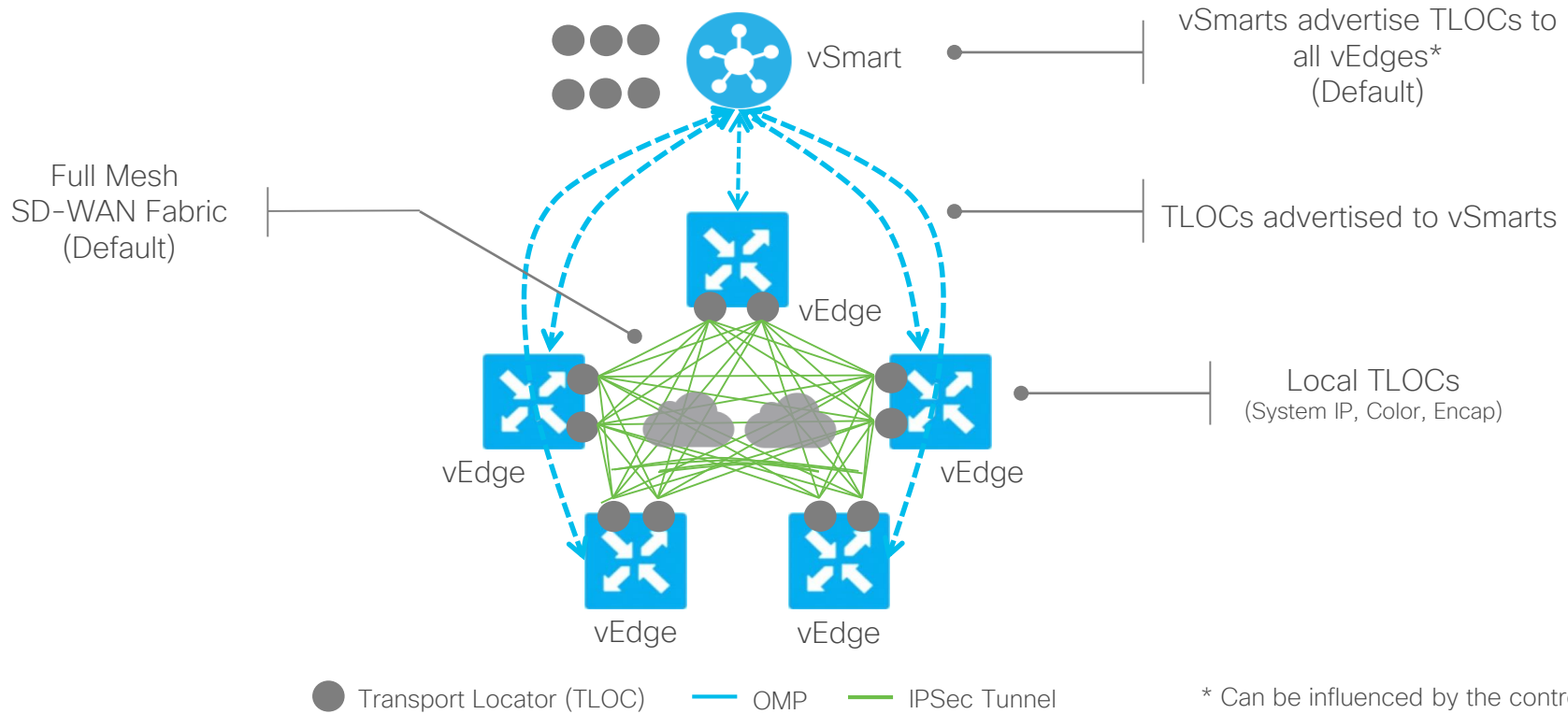


# Bidirectional Forwarding Detection (BFD)

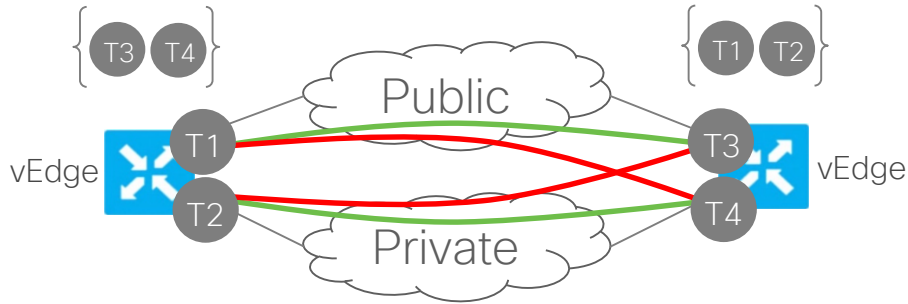


- Path liveliness and quality measurement detection protocol
  - Up/Down, loss/latency/jitter, IPSec tunnel MTU
- Runs between all vEdge and vEdge Cloud routers in the topology
  - Inside IPSec tunnels
  - Operates in echo mode
  - Automatically invoked at IPSec tunnel establishment
  - Cannot be disabled
- Uses hello (up/down) interval, poll (app-aware) interval and multiplier for detection
  - Fully customizable per-vEdge, per-color

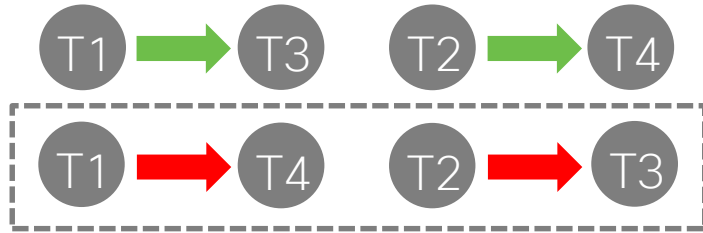
# Transport Locators (TLOCs)




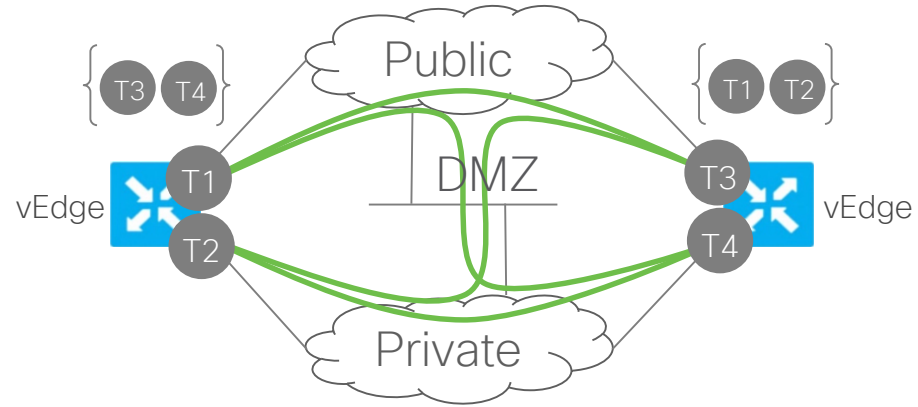
# Transport Colors



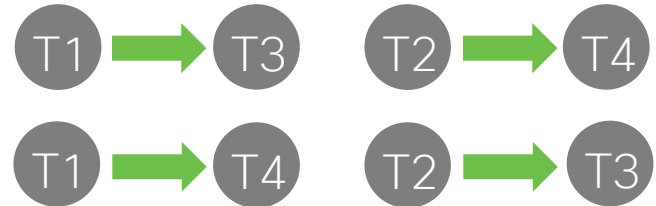
T1, T3 - Public Color    T2, T4 - Private Color



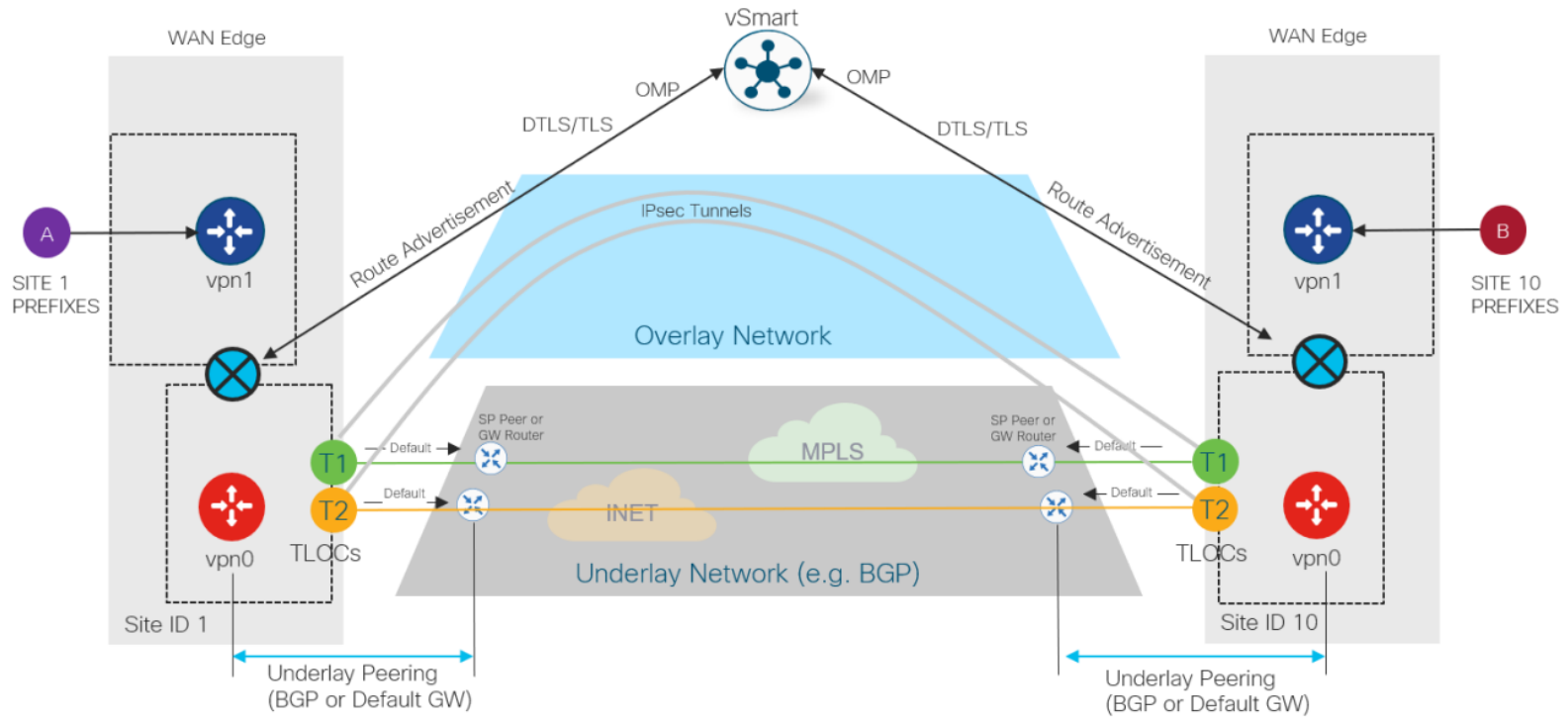
 Color restrict will prevent attempt to establish IPsec tunnel to TLOCs with different color



T1, T3 - Public Color    T2, T4 - Private Color

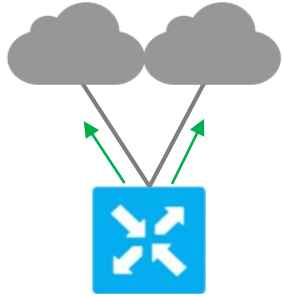


# Underlay vs. Overlay

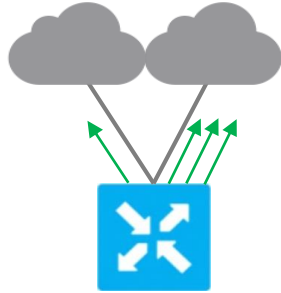


# Fabric Communication

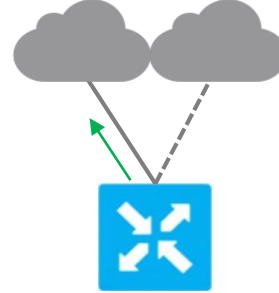
Per-Session Loadsharing  
Active/Active



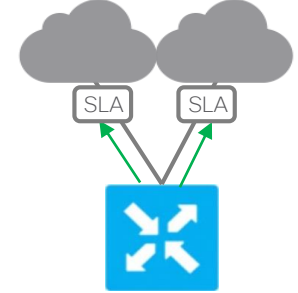
Per-Session Weighted  
Active/Active



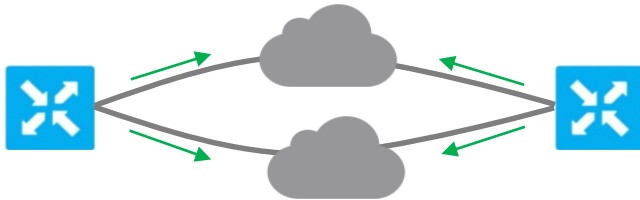
Application Pinning  
Active/Standby



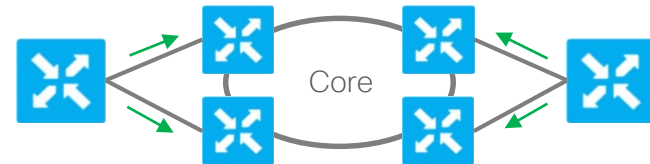
Application Aware Routing  
SLA Compliant



Single-hop Fabric

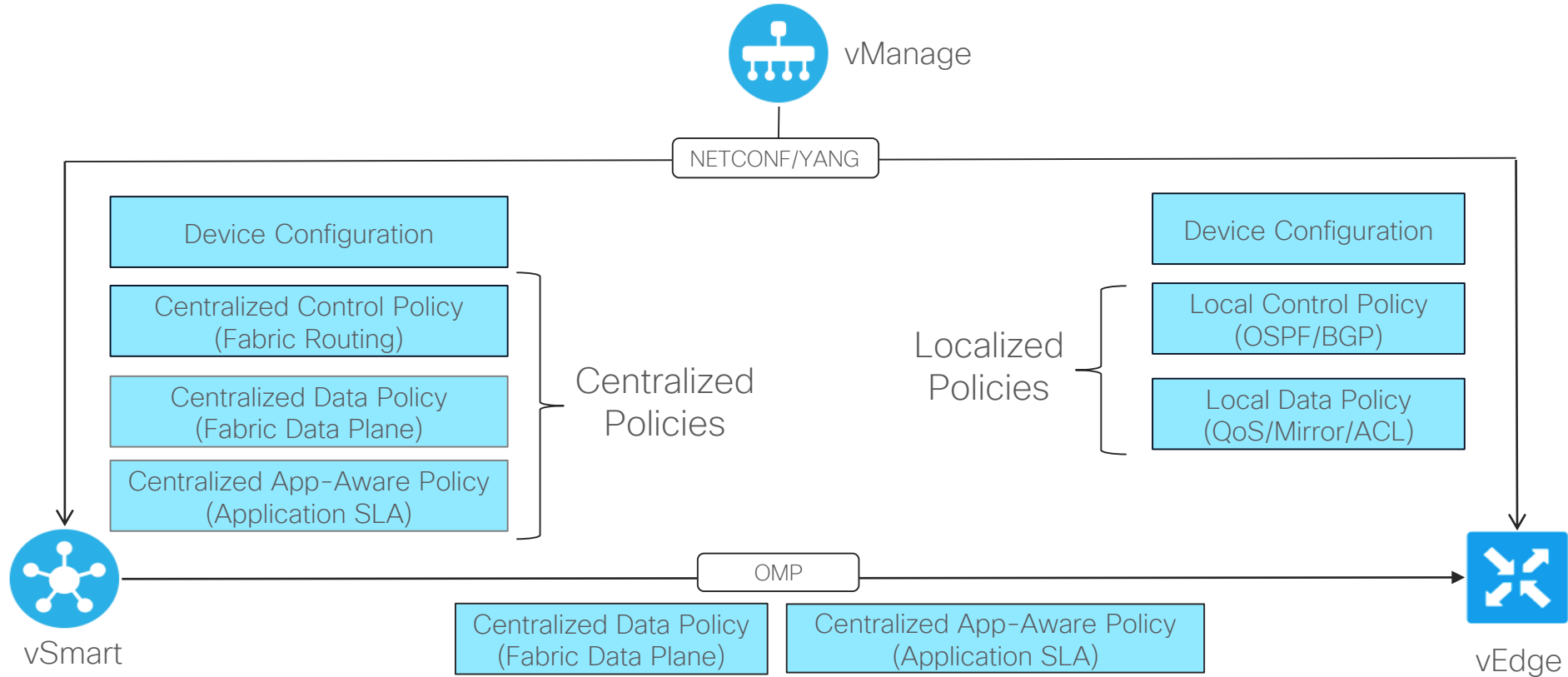


Hierarchical Multi-hop Fabric



Políticas, Templates e ZTP

# Framework de Políticas



# Configuração centralizada com o uso de Templates

Basic Information    Transport & Management VPN    Service VPN

**Basic Information**

System \*    vEdge-System

Logging    Factory\_Default\_Logging\_Template

AAA \*    vEdge-AAA

OMP \*    Factory\_Default\_vEdge\_OMP\_Template

- Centralized Feature Templates
- Enforces configuration compliance
- Self-recover on misconfiguration

IPv6 Configuration     Dynamic     Static

IPv6 address

Global

Device Specific

Default

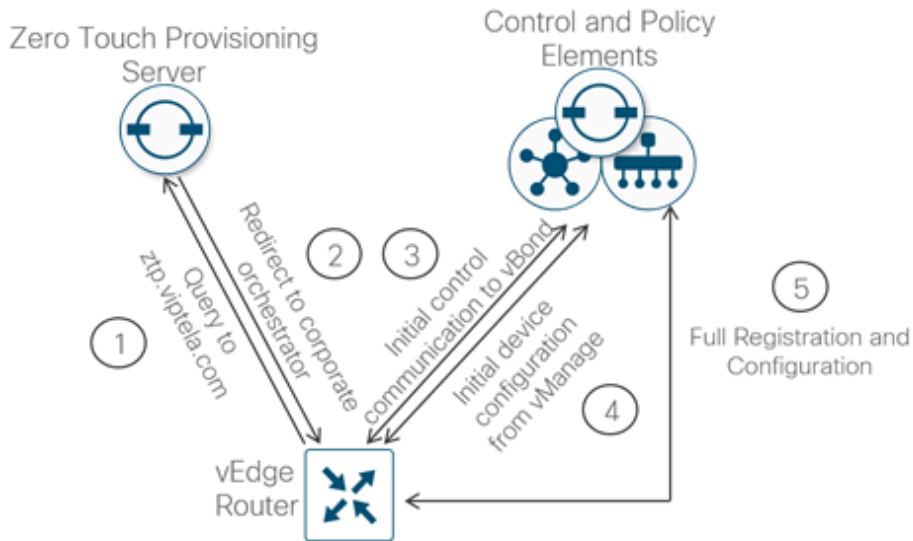
- Feature Configuration with Variables

Status	Chassis Number	System IP	Hostname	Latitude	Longitude	System IP	Site ID	Bandwidth Upstream
✓	4de0b85f-a2ae-42ec-8b45-3808285cd008	1.1.1.4	RemoteSite	37.33	-121.88	1.1.1.4	104	100
✓	5f05358a-bef7-4e15-9ade-8ffd8f27ec93	1.1.1.6	AWS	45.52	-122.67	1.1.1.6	106	100
✓	9391da23-f0d1-4259-88d9-e10ae714708c	1.1.1.5	DataCenter	40.71	-74.0	1.1.1.5	105	250



# Provisionamento automatizado

## Zero Touch Provisioning (vEdge)

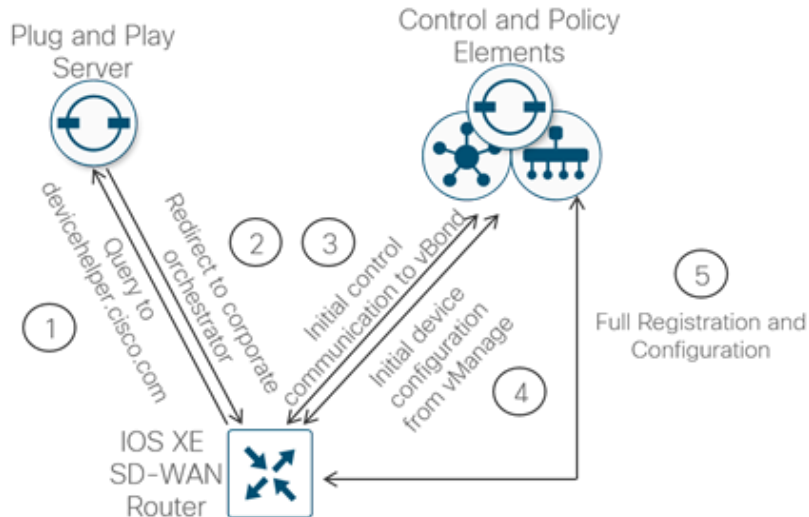


### Assumption:

- DHCP on Transport Side (WAN)
- DNS to resolve ztp.viptela.com\*

\* Factory default config

## Plug and Play (cEdge / IOS XE)



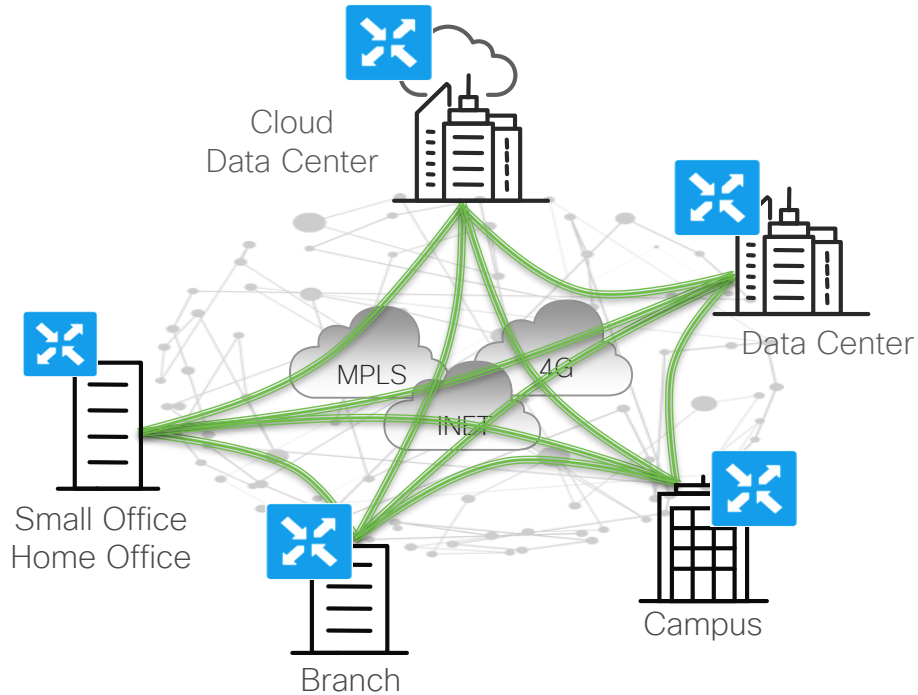
### Assumption:

- DHCP on Transport Side (WAN)
- DNS to resolve devicehelper.cisco.com\*

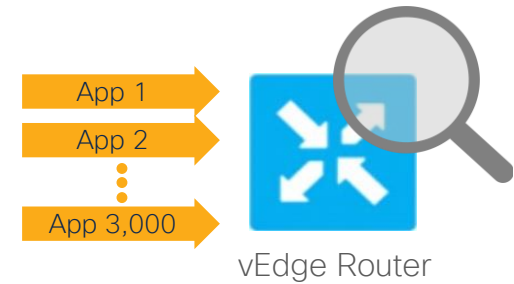
\* Factory default config

# Application-Aware Routing

# Visibilidade e reconhecimento de aplicações



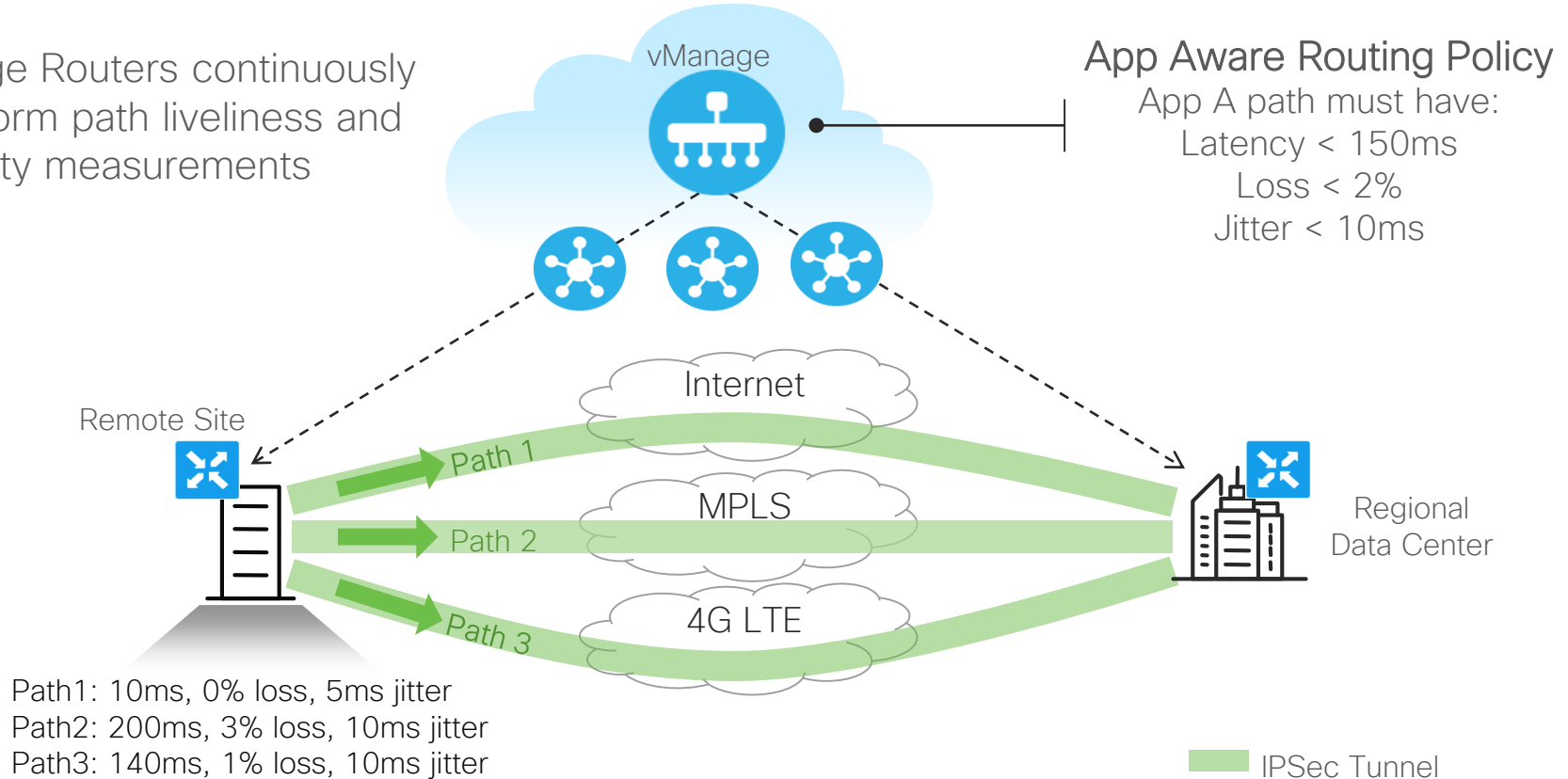
## Deep Packet Inspection



- ✓ App Firewall
- ✓ Traffic prioritization
- ✓ Transport selection

# SLA para as aplicações críticas

- vEdge Routers continuously perform path liveliness and quality measurements

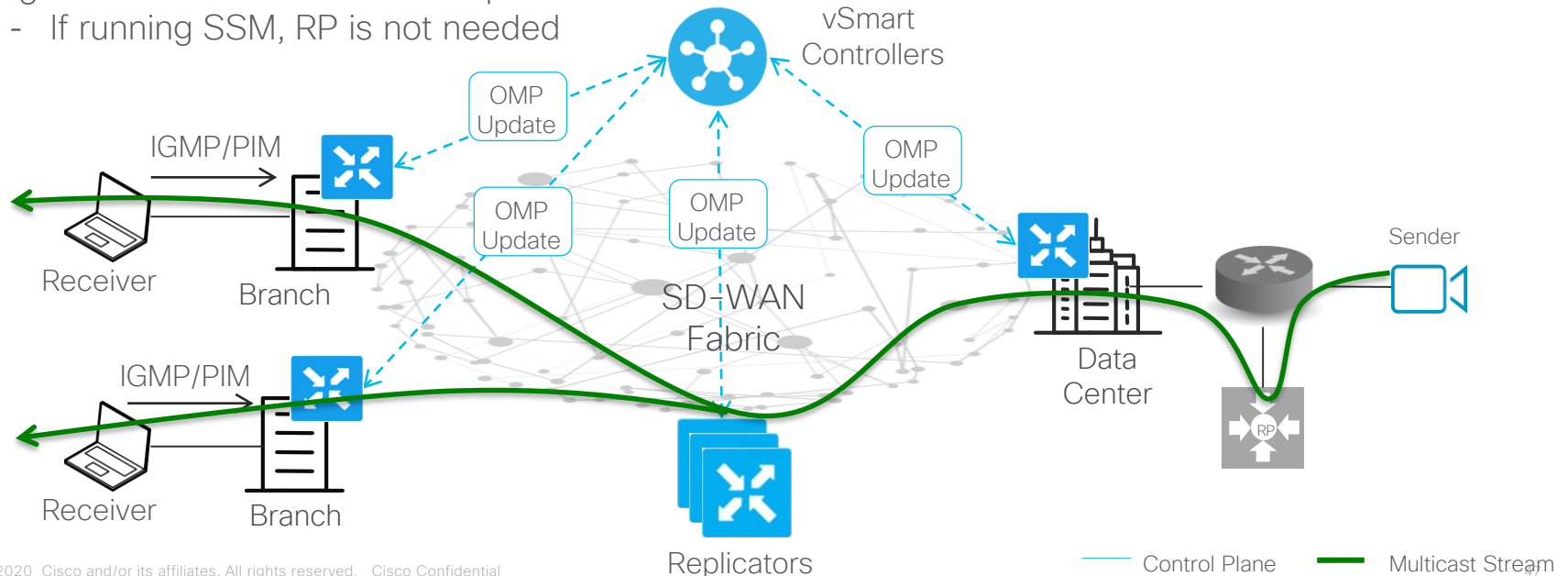


Multicast

# Fluxo de tráfego Multicast

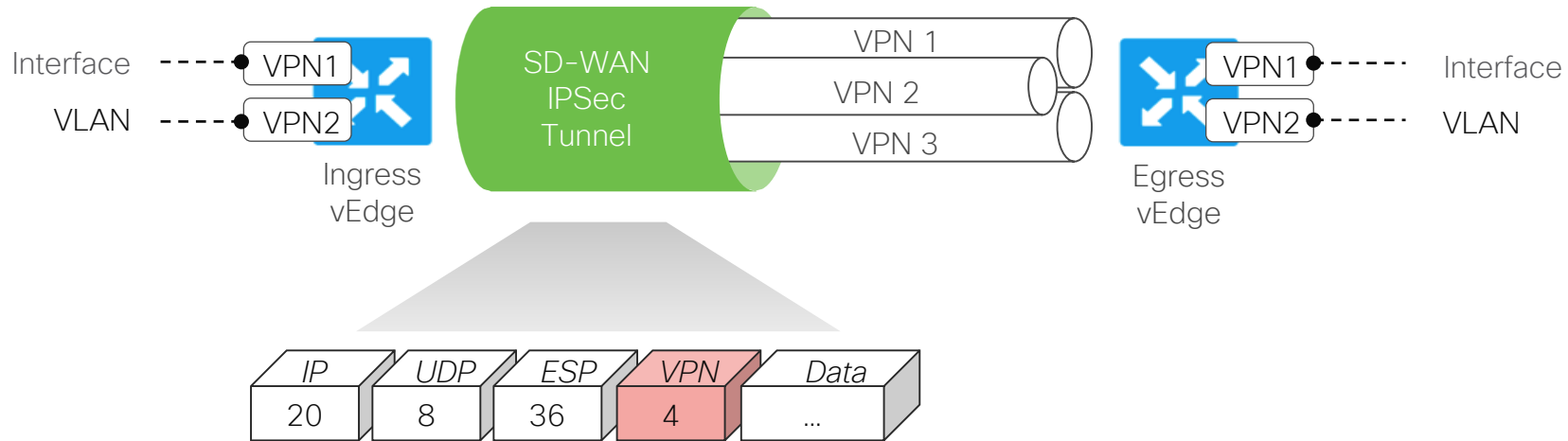
- vEdges interoperare with IGMP v1/v2 and PIM on the service side
- vEdges advertise receiver multicast groups using OMP
- vEdge cannot be RP. Router is required.
  - If running SSM, RP is not needed

- Replicators advertise themselves using OMP
- Replicators replicate multicast stream to receivers as learnt through OMP



# Segurança no transporte de dados

# Segmentação Fim-a-Fim

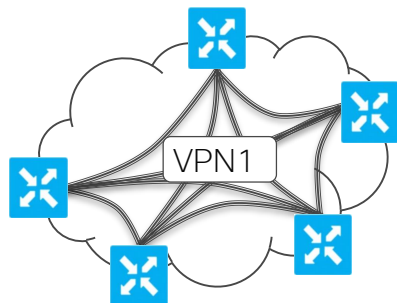


- Segment connectivity across fabric w/o reliance on underlay transport
- vEdge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs

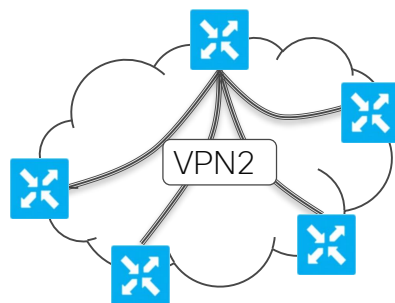


# Topologias arbitrárias por VPN

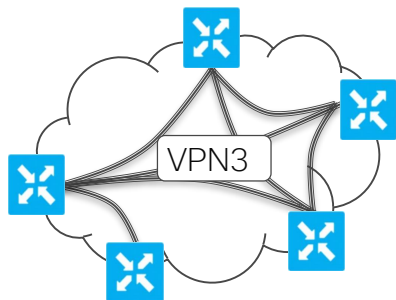
Full-Mesh



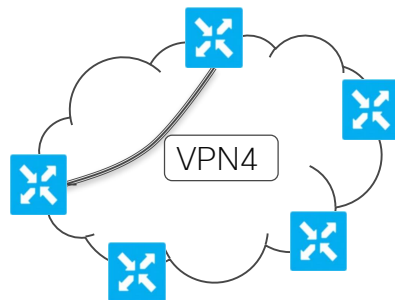
Hub-and-Spoke



Partial Mesh

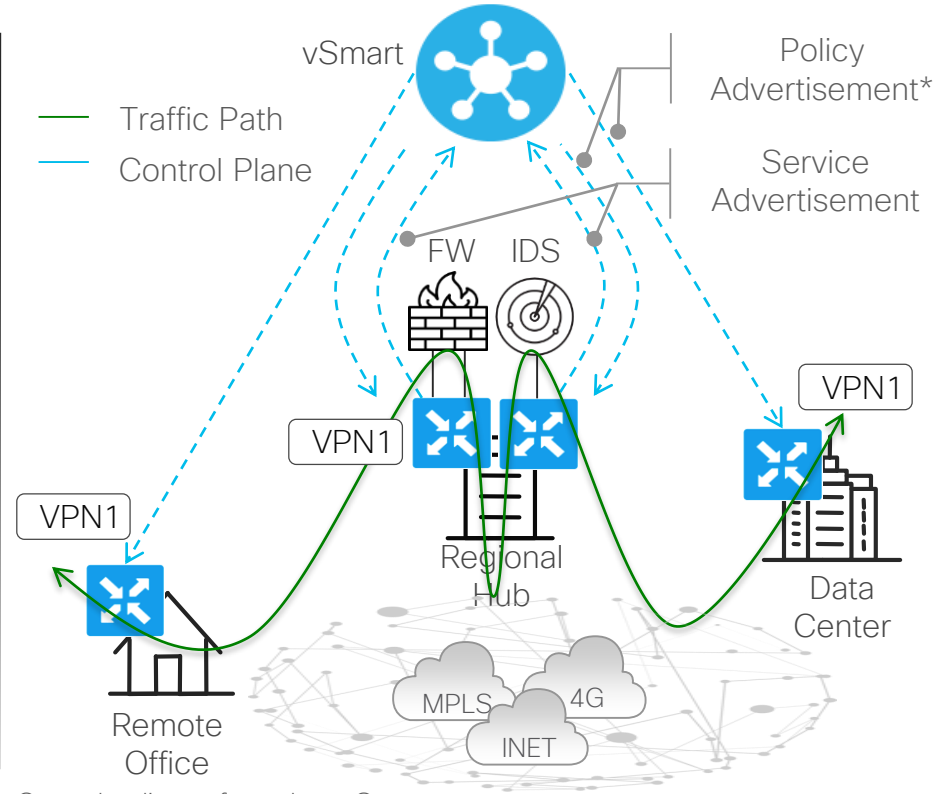
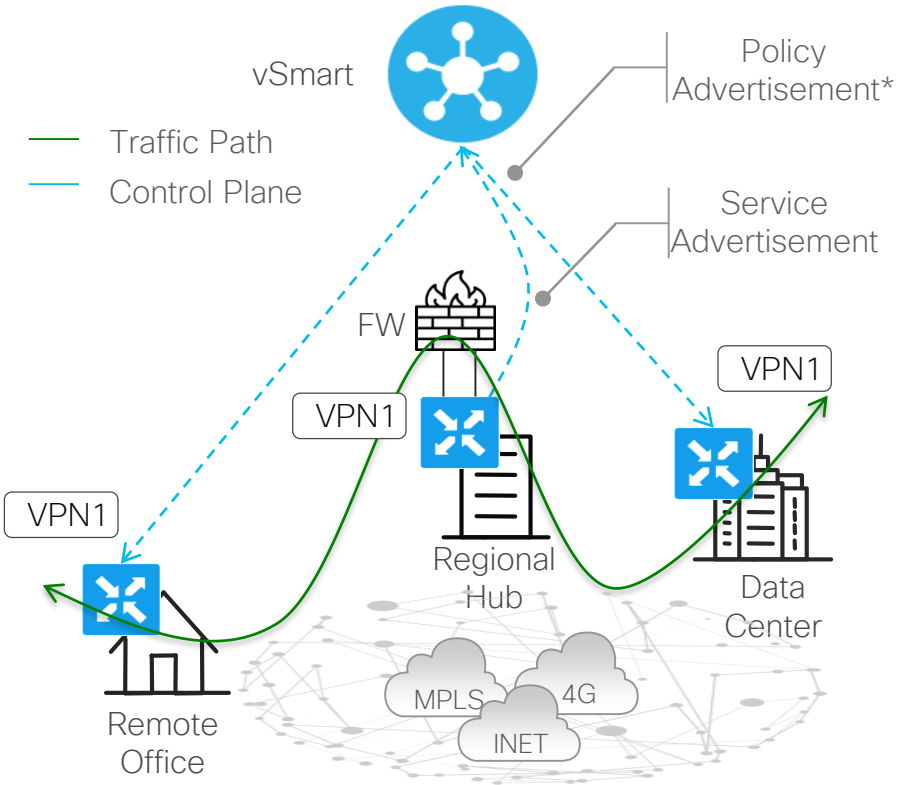


Point-to-Point



- Cada VPN pode utilizar um tipo de topologia
- As topologias podem ser definidas através de Control Policies
- Tráfego de voz vão se beneficiar em topologias full-mesh
- Questões de segurança ou compliance podem exigir topologias Hub-and-Spoke

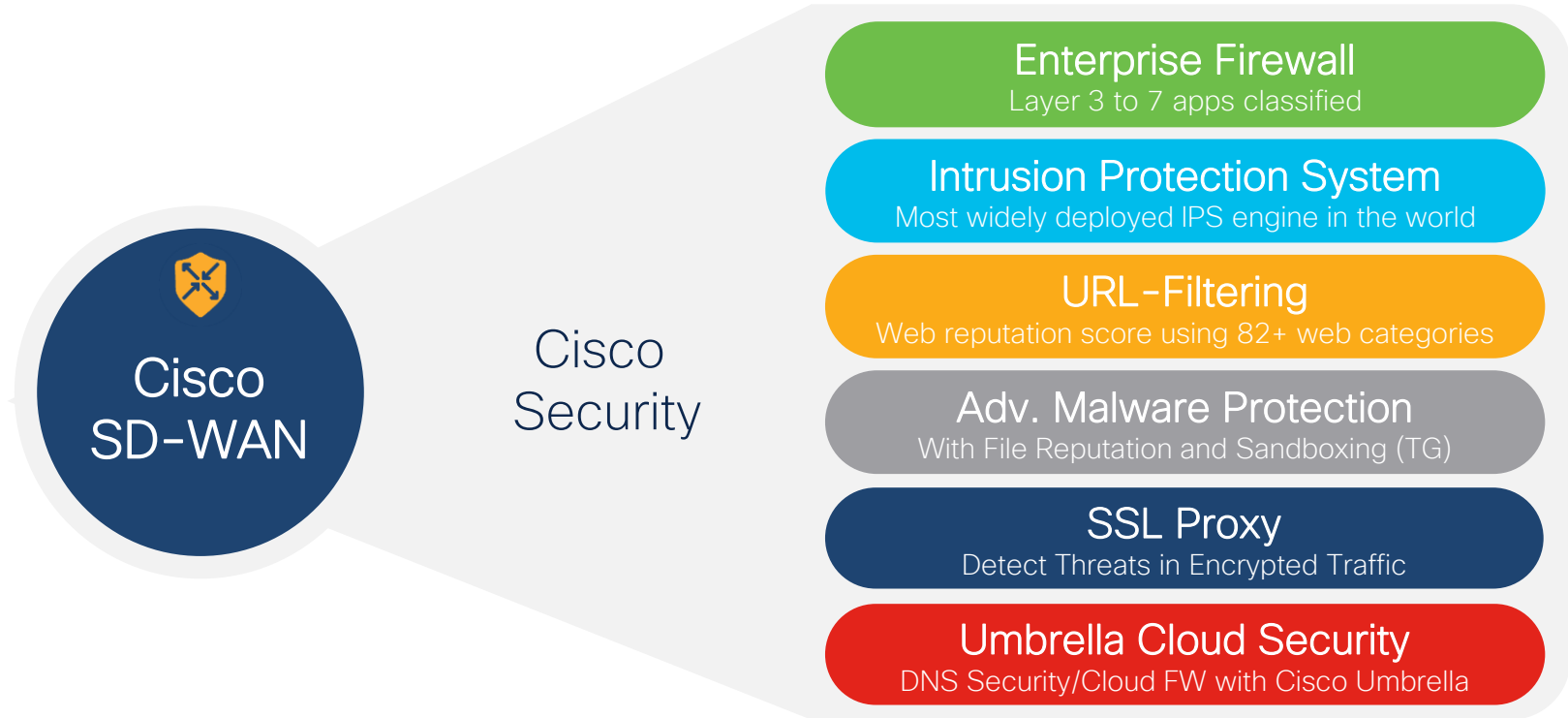
# Service Chaining



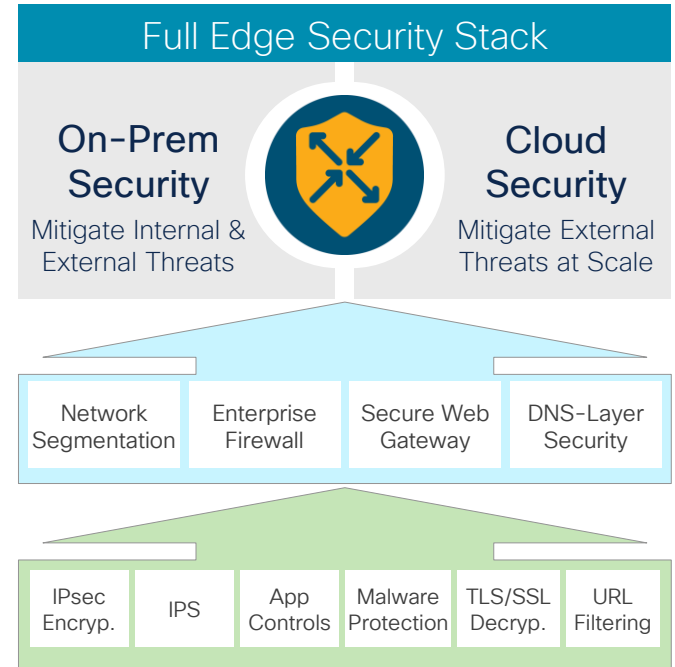
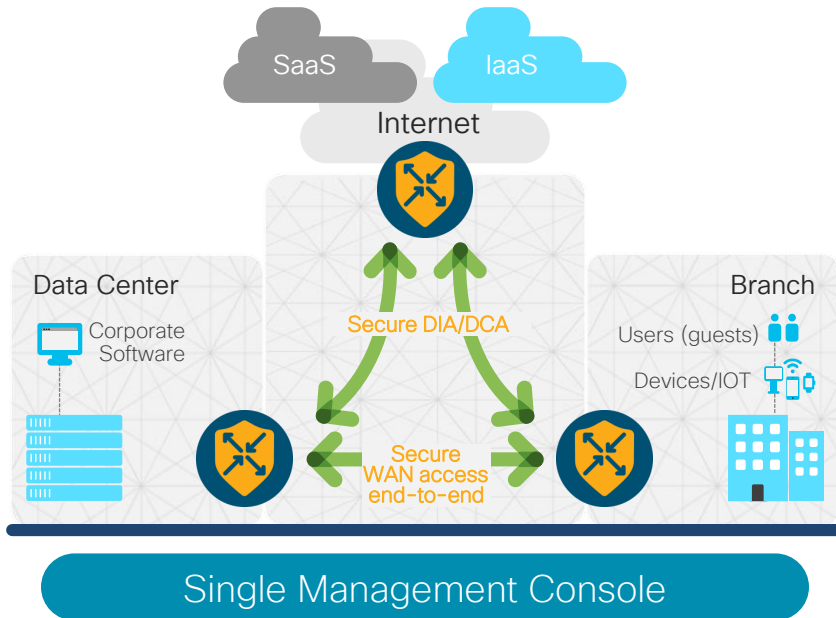
\* For data policy only. Control policy enforced on vSmart.

Cloud & SASE

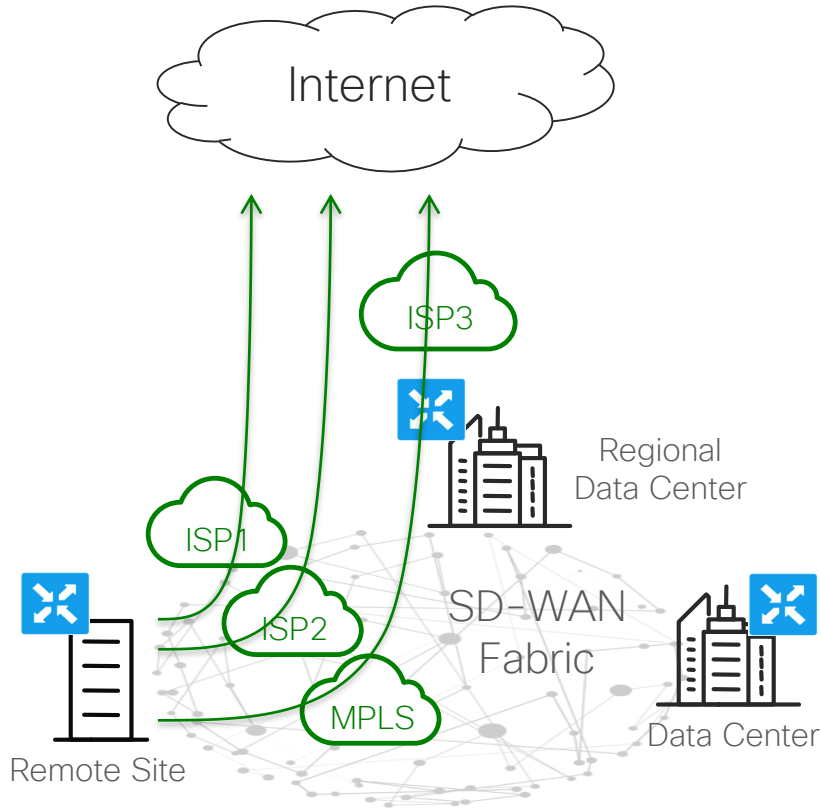
# Cisco SD-WAN & SASE



# Segurança certa, no lugar certo

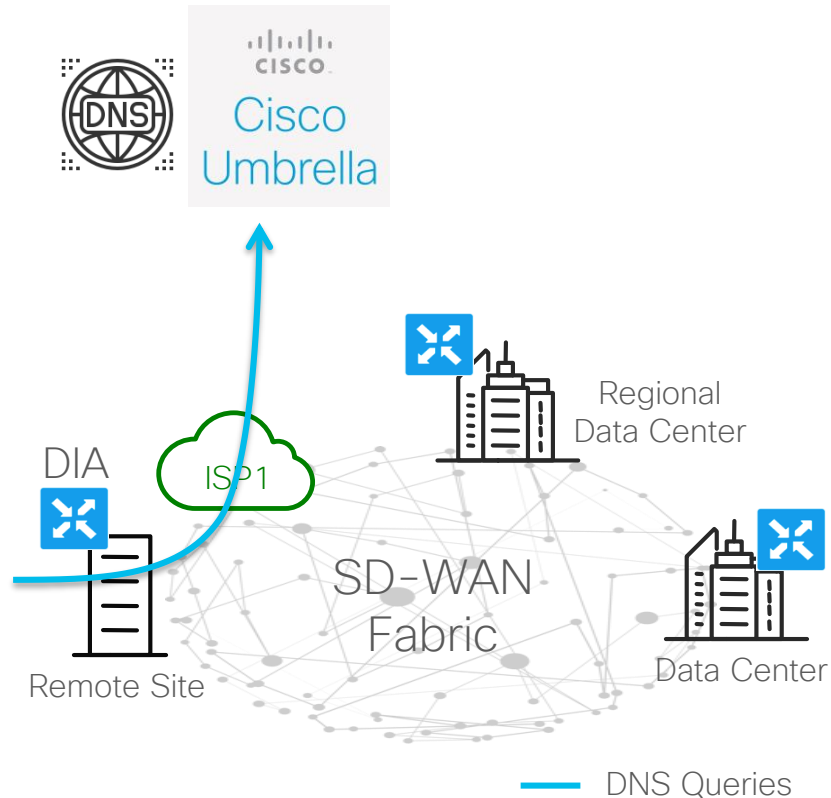


# Direct Internet Access (DIA)



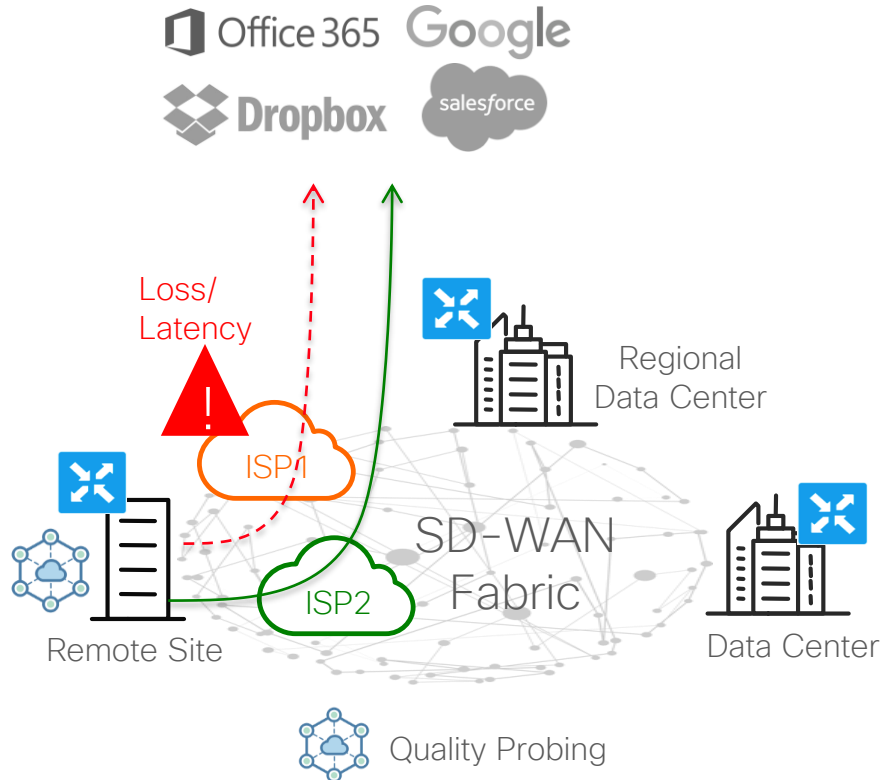
- Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
  - Per-VPN behavior enforcement
- VPN default route for all traffic DIA or data policy for selective traffic DIA
- Network Address Translation (NAT) on the vEdge router only allows response traffic back
  - Any unsolicited Internet traffic will be blocked by IP table filters
- For performance based routing toward SaaS applications use Cloud onRamp

# Cloud Security with Cisco Umbrella



- vEdge router intercepts client DNS queries
  - Deep Packet Inspection
- DNS queries are forwarded to Cisco Umbrella DNS servers based on the data or application aware routing policies centrally defined on vManage
  - Target DNS servers list is defined under the service side VPN
  - Policy can pin DNS query for specific application (DPI based) to specific DNS server from the list
- Cisco Umbrella enforces security policy compliance based on DNS resolution

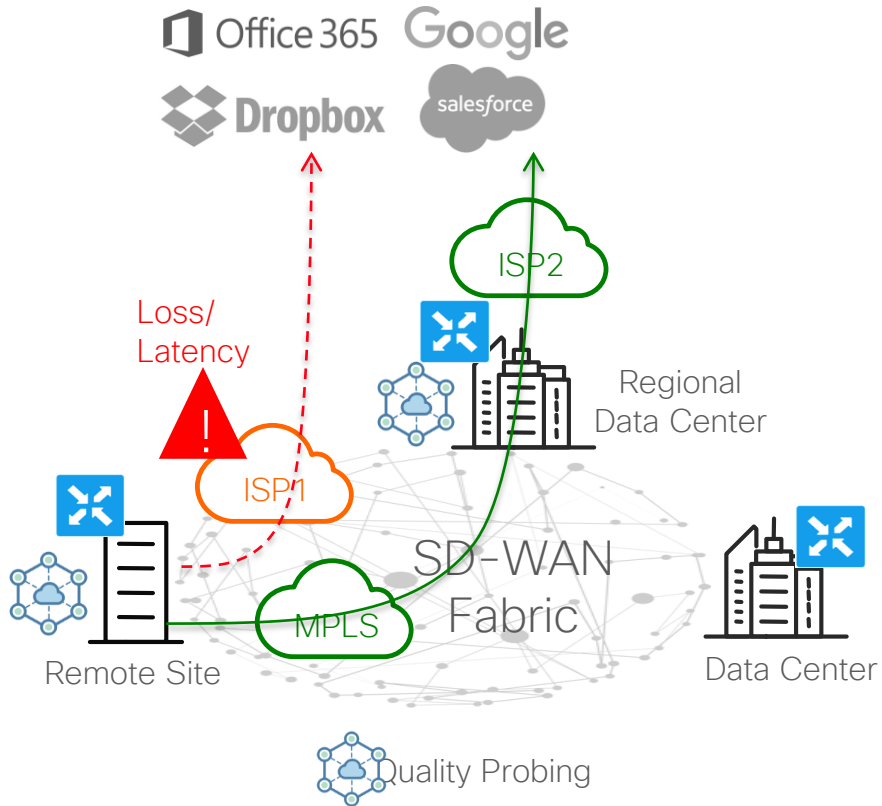
# Cloud onRamp for SaaS – Internet DIA



- vEdge router at the remote site performs quality probing for selected SaaS applications across each local DIA exit
  - Simulates client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
- Local DIA exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

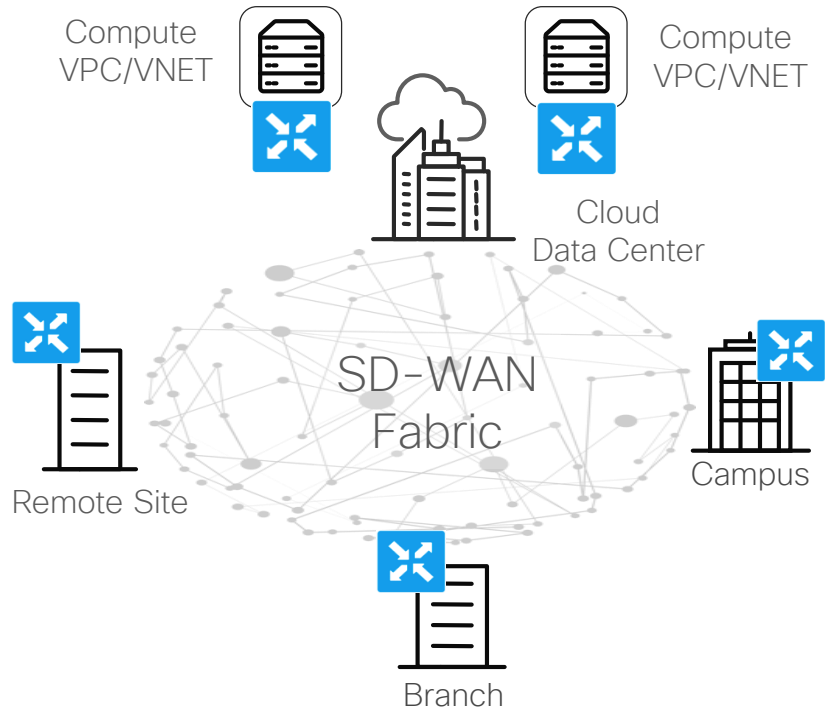


# Cloud onRamp for SaaS – Regional Gateway



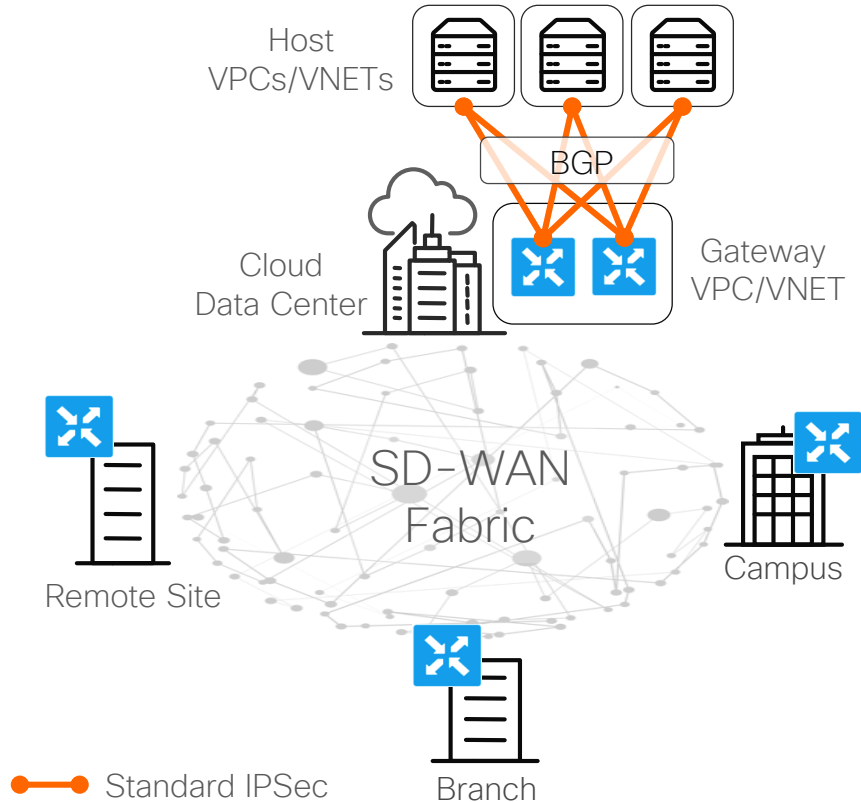
- vEdge routers at the remote site and regional hub perform quality probing for selected SaaS applications across their local Internet exits
  - Simulate client connection using HTTP ping
- Results of quality probing are quantified as vQoE score (combination of loss and latency)
  - HTTP ping for local DIA and App-Route+HTTP ping for regional Internet exit
- Internet exit with better vQoE score is chosen to carry the traffic for the selected SaaS application
  - Initial application flow may choose sub-optimal path until DPI identification is complete and cache table is populated

# Cloud onRamp for IaaS – Attached Compute



- vEdge Cloud routers are instantiated in Amazon VPCs or Microsoft Azure VNets
  - Posted in marketplace
  - Use Cloud-Init for ZTP
- One vEdge Cloud router per VPC/VNET
  - No multicast support, can't form VRRP
  - No router redundancy
- vEdge Cloud routers join the fabric, all fabric services are extended to the IaaS instances, e.g. multipathing, segmentation and QoS
  - For multipathing, can combine AWS Direct Connect or Azure ExpressRoute with direct internet connectivity

# Cloud onRamp for IaaS – Gateway VPC/VNET

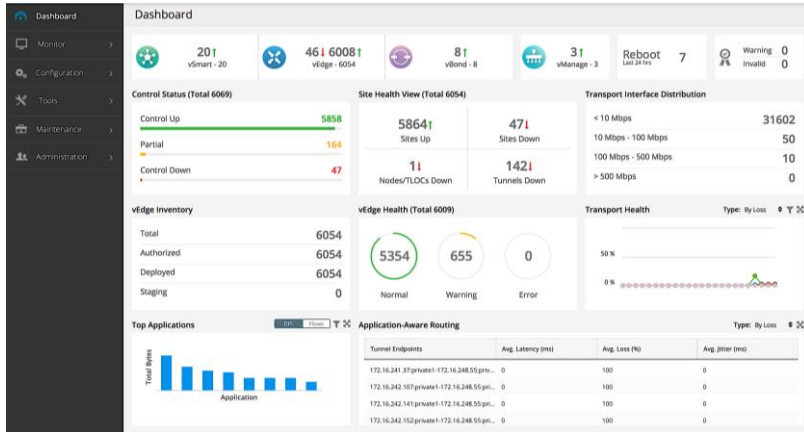


- A pair of vEdge routers is instantiated in Amazon VPC or Microsoft Azure VNET
  - Gateway VPC/VNET
- A pair of standard based IPsec tunnels is stretched from gateway VPC/VNET to each host VPCs/VNETs
  - Connectivity redundancy
- BGP is established across IPsec tunnels for route advertisement
  - Bi-directional BGP/OMP redistribution on the gateway VPC/VNET vEdge routers
  - Active/active forwarding
- Entire process is automated through intuitive vManage workflow

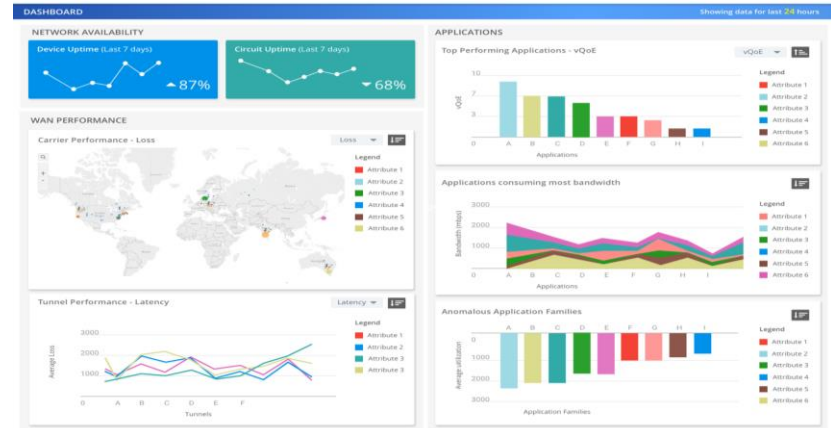
Analytics

# Gerenciamento e visibilidade simplificados

## Cisco vManage



## Cisco vAnalytics



REST



NETCONF



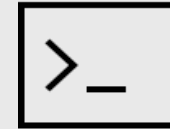
Syslog



SNMP



Flow Export



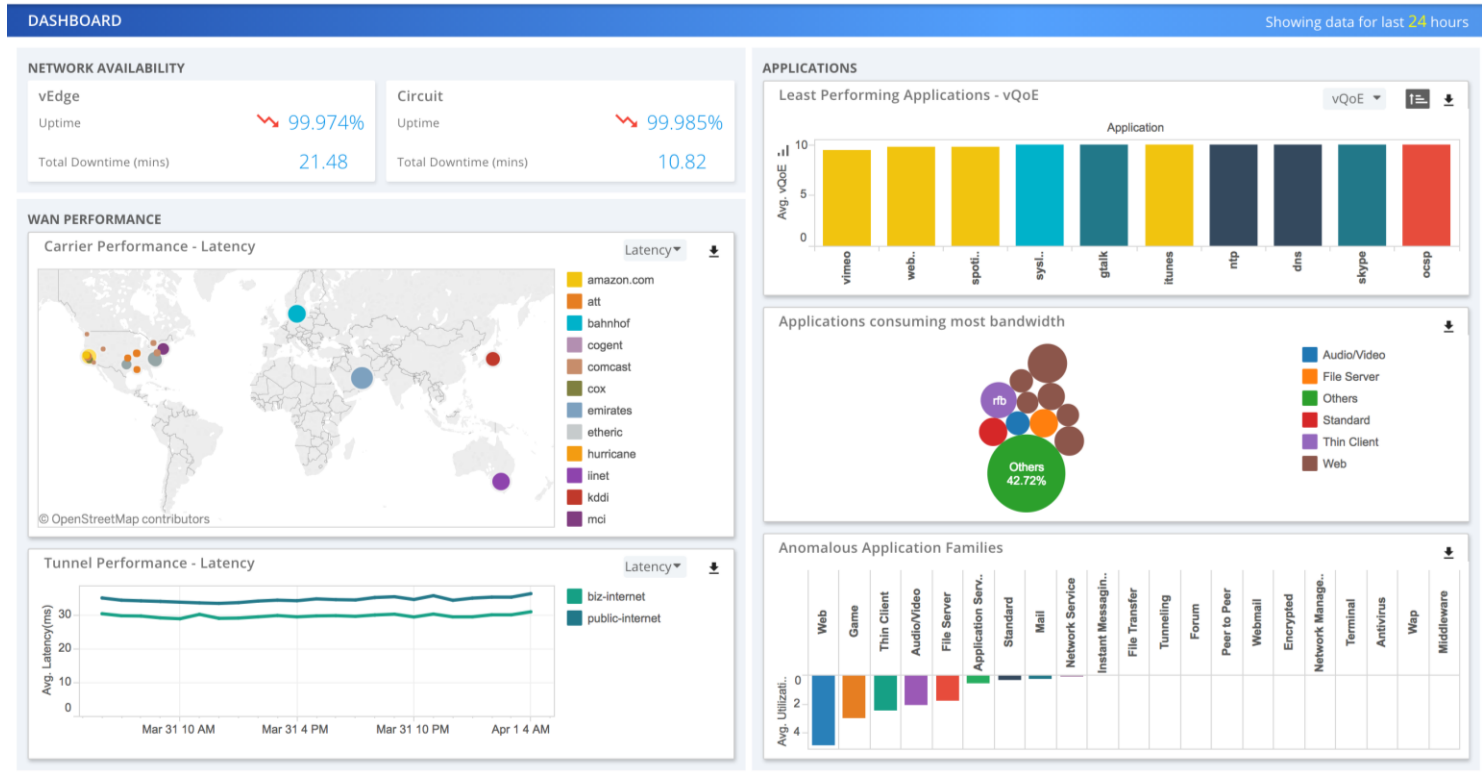
CLI



Linux Shell

## Power Tools

# vAnalytics



## Polling Question 3

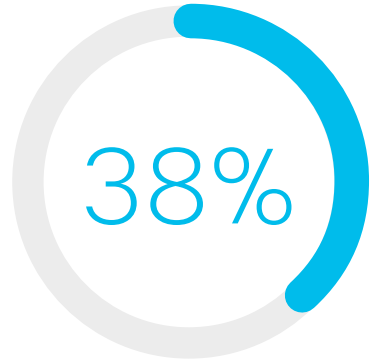
Quais benefícios a solução SD-WAN pode fornecer para a sua rede?

- a) Encaminhamento do tráfego com base nas características de delay, jitter e packet loss dos links de transporte.
- b) Automação de tarefas repetitivas.
- c) Visibilidade e monitoramento do ambiente.
- d) Gerenciamento e operação de forma centralizada, em uma única console.
- e) Todas as alternativas.

Como o Cisco SD-WAN  
pode ajudar minha  
empresa?



# Resultados com Cisco SD-WAN



Redução no custo de operação de WAN (5Y)



Mais ágil para criar novas políticas e realizar mudanças

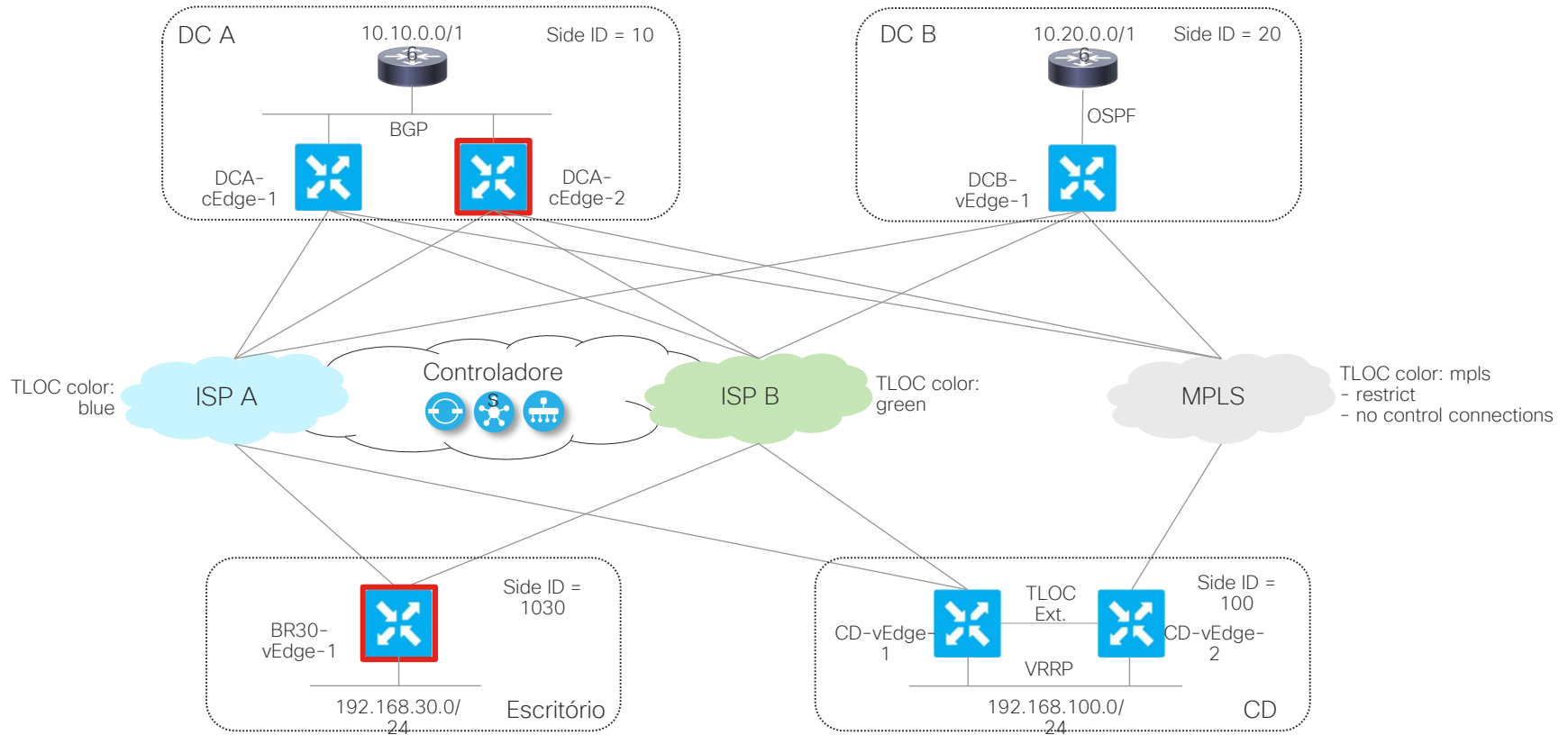


Redução de Downtime não planejado

Fonte: [IDC white paper-Business Value of Cisco SD-WAN Solutions: Studying the Results of Deployed Organizations, IDC, April 2019.](#)

Demonstração

# Topologia - Demo





Faça suas  
perguntas agora!



Use o painel  
Perguntas e Respostas ou Q&A  
para enviar suas perguntas.

Nosso especialista responderá ao vivo <sup>70</sup>

# Ask me Anything

Até a próxima sexta-feira, 20 de Novembro de 2020.

Link para o evento: <https://bit.ly/cl-amaNov12>



Guilherme Lyra



Lucas Borges



# Participe em nossas Redes sociais



## Twitter

- @Cisco\_Support
- @CiscoDoBrasil

## Facebook

- Hey Cisco  
<http://bit.ly/csc-facebook>
- Cisco Do Brasil  
<https://www.facebook.com/CiscoDoBrasil/>
- Cisco Portugal  
<https://www.facebook.com/ciscoporugal/>

Saiba mais sobre os próximos eventos

# Convidamos você a visitar nossos canais

## YouTube

- Cisco Comunity
- <http://bit.ly/csc-youtube>



## App

- Cisco Technical Support



## LinkedIn

- Cisco-Community
- <http://bit.ly/csc-linked-in>



Saiba mais sobre os próximos eventos



# A Cisco também tem Comunidades em outros idiomas!

Se você fala Inglês, Espanhol, Francês, Japonês, Russo ou Chinês, lhe convidamos a conhecer nossas Comunidades



[Cisco Community](#)  
Inglês

[Comunidad de Cisco](#)  
Espanhol

[Communauté Cisco](#)  
Francês

[思科社区](#)  
Chinês

[Сообщество](#)  
[Cisco](#)  
Russo

[シスコのコミュニティ](#)  
Japonês

Por favor, tome 10 segundos  
para responder nossa enquete de  
múltipla escolha ao finalizar o evento!

Sua opinião é muito importante para  
continuar melhorando!



*Obrigado por ser parte dessa  
experiência!*

