Как подключиться к своим ресурсам в облачных средах

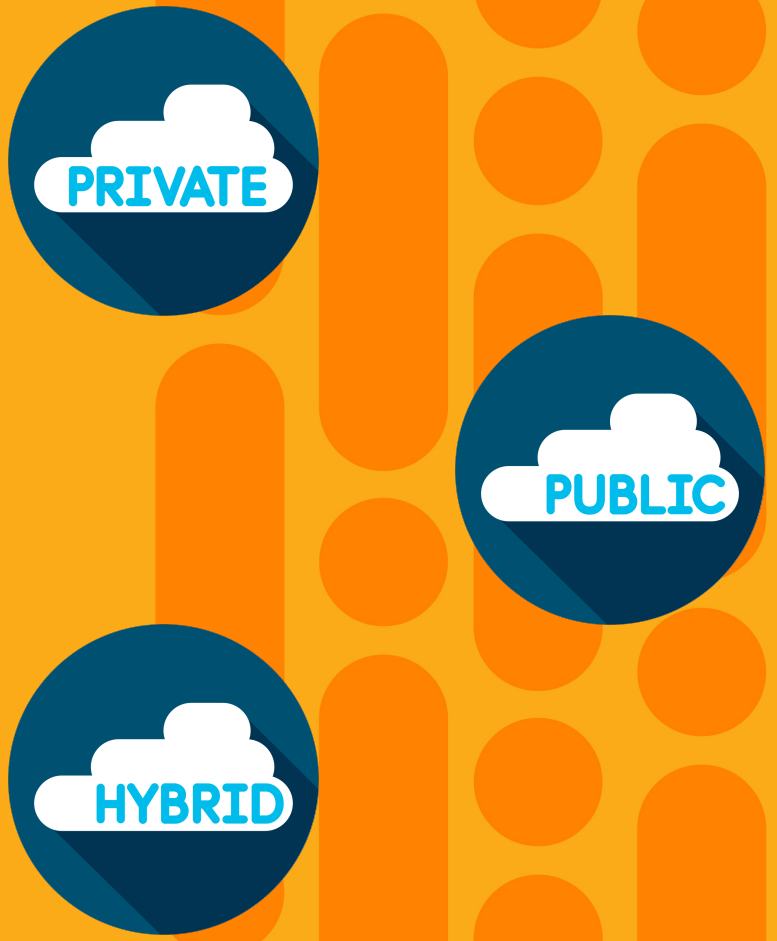
План доклада

Немного про облака

Как соединить свою инфраструктуру с публичным облаком/облаками

Инструментарий

Облака???



Давайте определимся с понятиями

- Пользователь имеет эксклюзивный доступ к выделенным ресурсам ЦОД (физическим или виртуализированным)
- Ресурсы – локальные или в ЦОД co-location провайдера
- Потребление ресурсов – в любом удобном формате

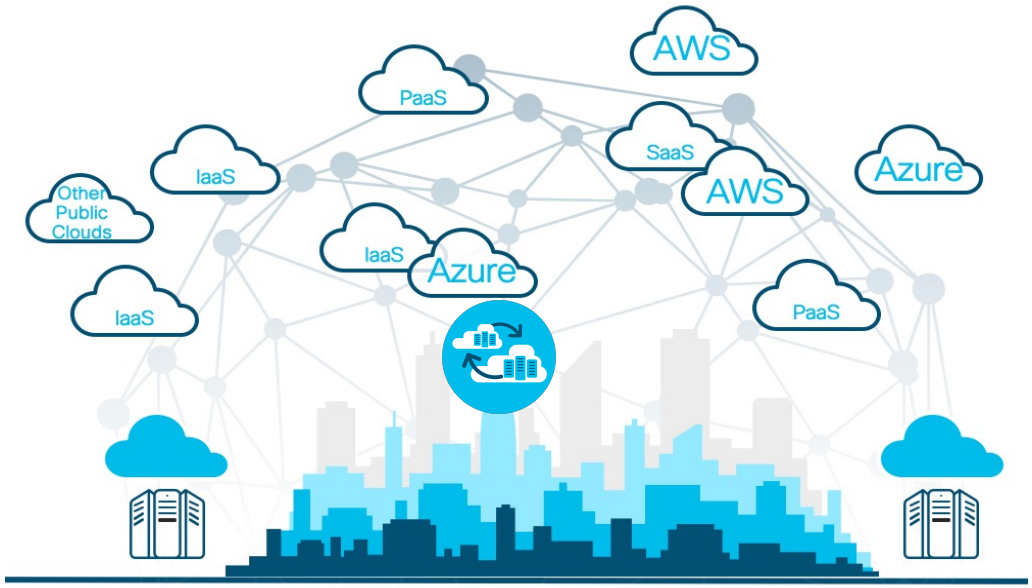
- Пользователь не владеет собственной инфраструктурой ЦОД (сеть, вычислительные ресурсы, ресурсы хранения).
- Модель потребления XaaS (IaaS/SaaS/DRaaS и так далее)

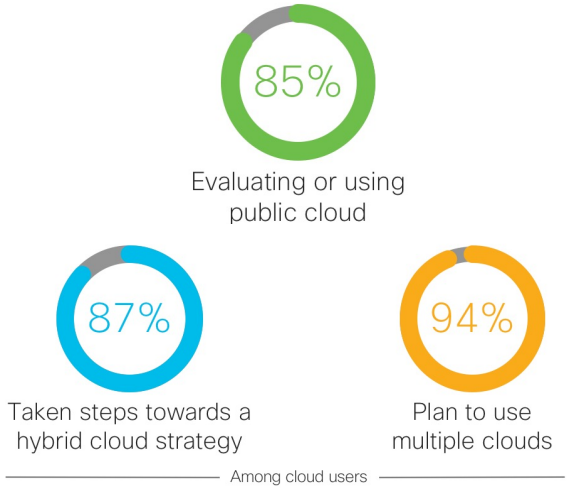
- Реальность…
- Пользователь одновременно использует ресурсы частных и публичных облачных сред

***

Смена вектора

Движение в сторону публичных облаков





Трудности

- Visibility and Control
- Layer 2 Abstraction
- Security Model
- Cloud Services

Достоинства

- Application Agility
- Ease of Deployment
- HA, Scalability and Low Cost

Data Center (Private Cloud – Hypervisors)	Public Cloud	Hybrid Cloud	Multi Cloud

Как соединить свою сетевую инфраструктуру с облаком

Еще немного определений
Hybrid vs Multicloud Networking

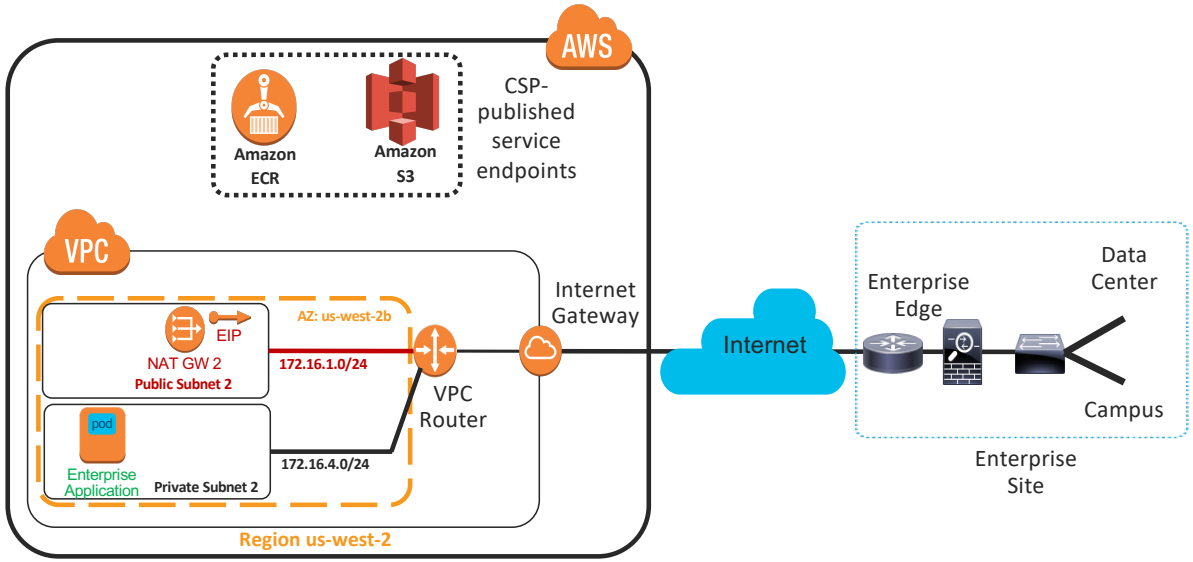
- **Hybrid Cloud Networking = Сетевой транспорт между on-prem инфраструктурой и единственным облачным провайдером**
- **Multicloud Networking = Сетевой транспорт между on-prem инфраструктурой и несколькими облачными провайдерами, а также между несколькими различными облачными провайдерами**
- Технологии могут быть идентичными для всех соединений или различаться в зависимости от провайдера, региона, проекта и т.д.
- Общие ингредиенты для создания транспорта для hybrid и multicloud:
  - **Encryption** (IPsec/IKEv1/IKEv2, SSL, PKI)
  - **Routing** (Static, BGP и OSPF, EIGRP)
  - **Tunneling** (IPsec tunnel mode, GRE, mGRE, MPLS, segment routing..)
- Общий набор вариантов оконечных устройств:
  - **Native VPN** (IPsec over Internet) –сервис от провайдера публичного облака для соединения с on-prem МСЭ/маршрутизатором пользователя
  - **Коммерческая/Open Source VPN** платформа, расположенная в облаке, соединяемая с on-prem МСЭ/маршрутизатором пользователя
  - **Colocation/Direct Peering**: сервис от провайдера публичного облака к on-prem инфраструктуре через colo-площадки 3-их компаний
    - Google Cloud Platform Dedicated Interconnect/Direct Peering/Carrier Peering: https://cloud.google.com/interconnect/
    - Amazon Web Services Direct Connect/PrivateLink: https://aws.amazon.com/directconnect/
    - Microsoft Azure ExpressRoute: https://azure.microsoft.com/en-us/services/expressroute/

Зачем покупать сервис от нескольких облачных провайдеров?

- **Обеспечение высокой доступности - резервирование облачных сервисов**
- Различия в региональном присутствии облачных провайдеров
- Различия в номенклатуре доступных сервисов в конкретных регионах
- Специфичные проектные требования
- **Преференции по бизнес-причинам (M&A)**

Вариант Internet Over-the-Top (OTT)

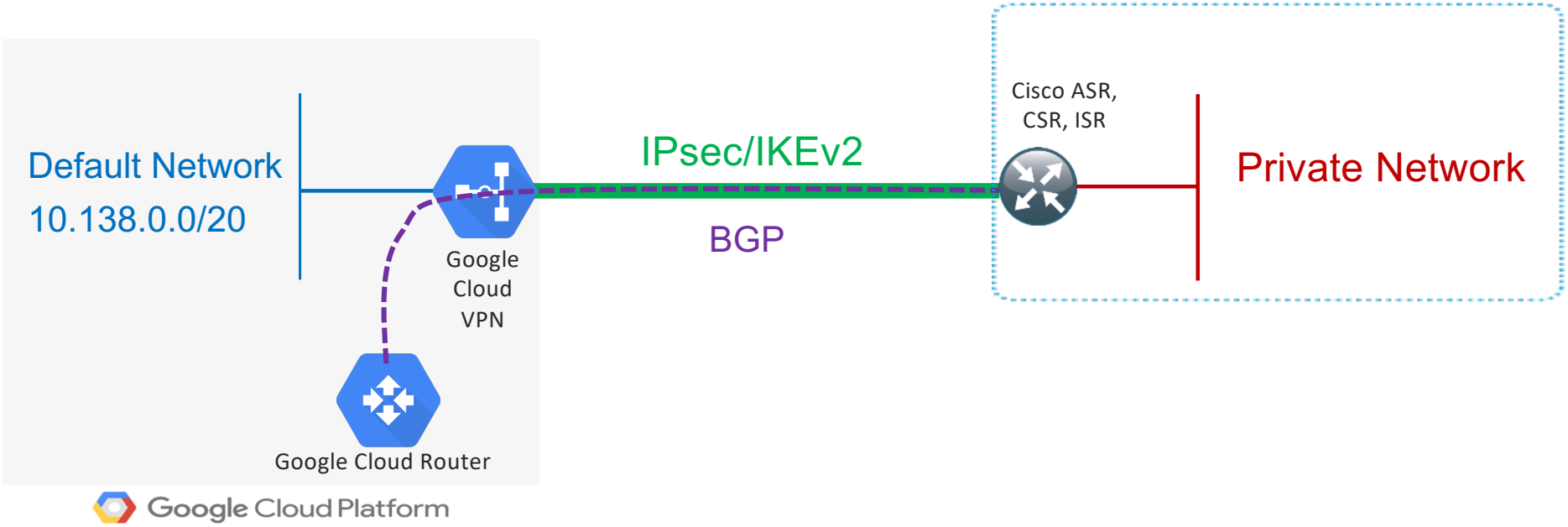
- Корпоративные пользователи/приложения присоединяются к публичным IP приложений или публичным адресам шлюзов провайдера облачных услуг (Cloud Service Provider, CSP)
- Без ‘традиционного’ S2S IPsec VPN
- Поддержка TLS
- **Может противоречить политикам ИБ заказчика**



VPN over the Internet vs Direct Connect/ExpressRoute/Dedicated Interconnect

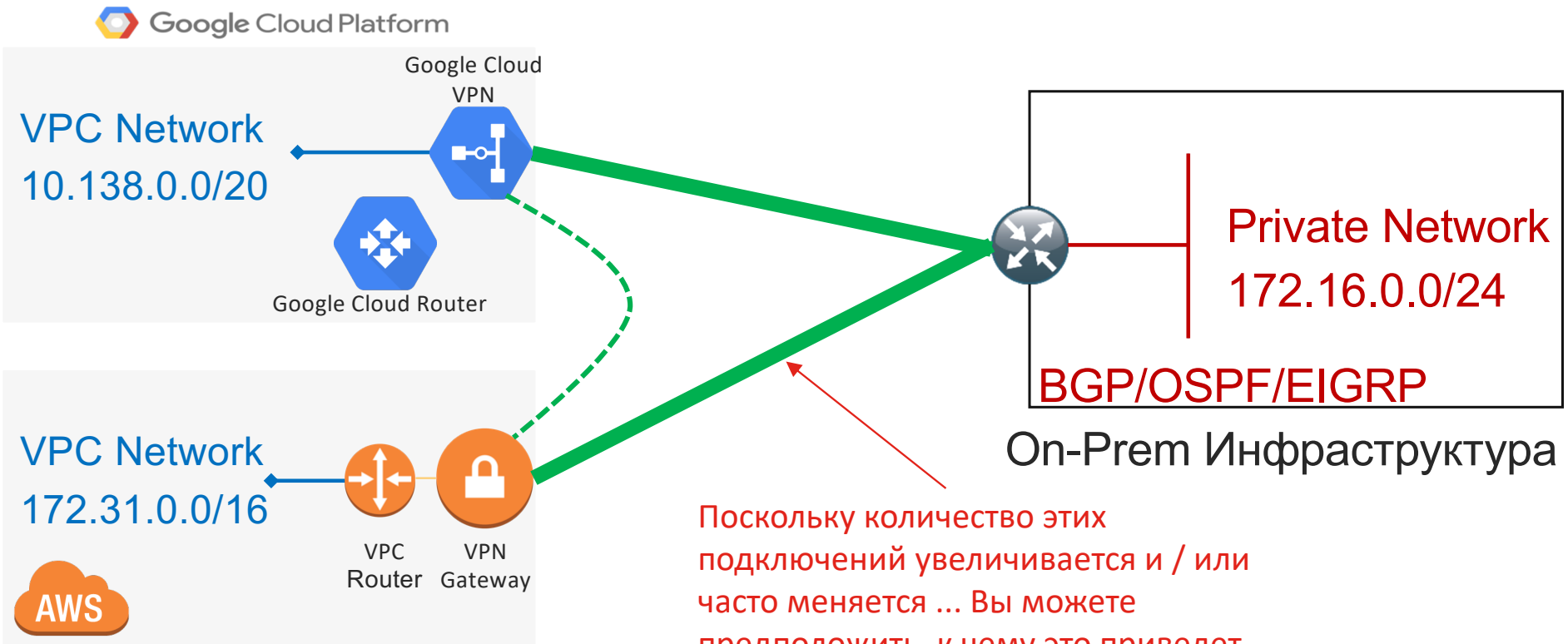
	VPN over the Internet	Direct/Express/Dedicated
Throughput		Winner
QoS		Winner
Latency		Winner
Inline Services		Winner
Managed Services		Winner
Cost	Winner	
Time to Provision	Winner	
Flexibility	Winner	
Location Availability	Winner	

Сервис Native IPsec VPN



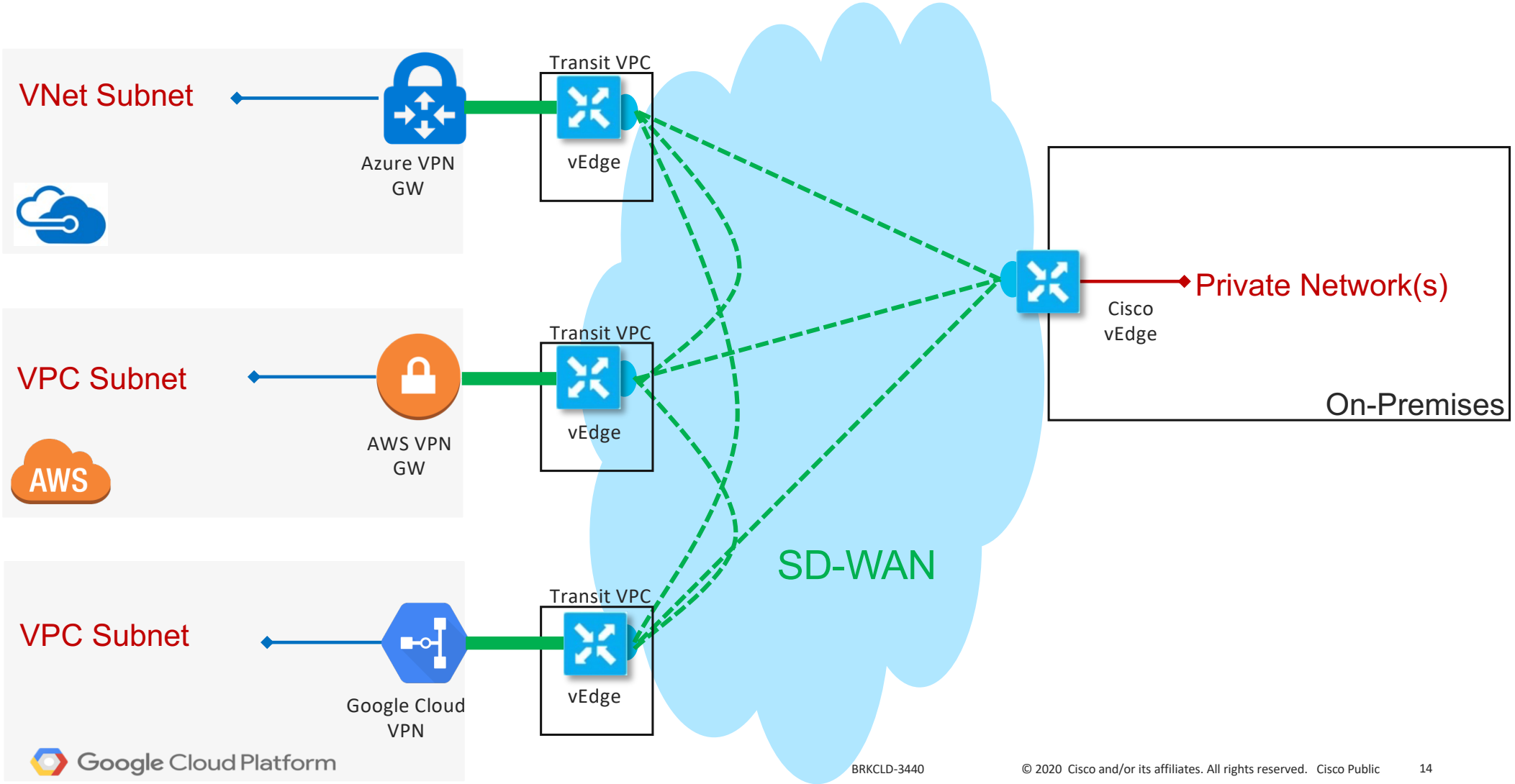
Переходим к Multicloud Networking

Множество различных сервисов Native IPsec VPN

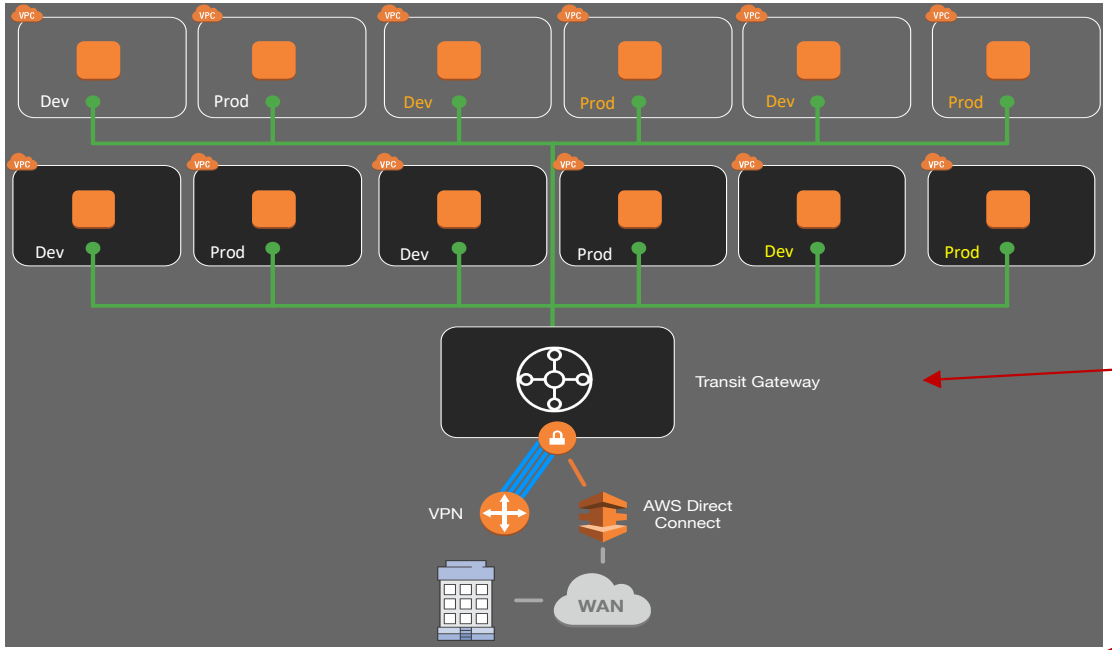


Поскольку количество этих подключений увеличивается и / или часто меняется ... Вы можете предположить, к чему это приведет

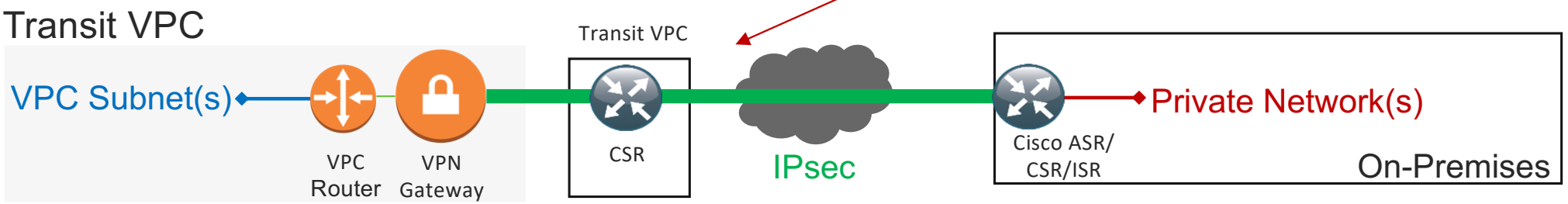
Multicloud with Transit VPC



AWS – Transit Gateway (TGW)

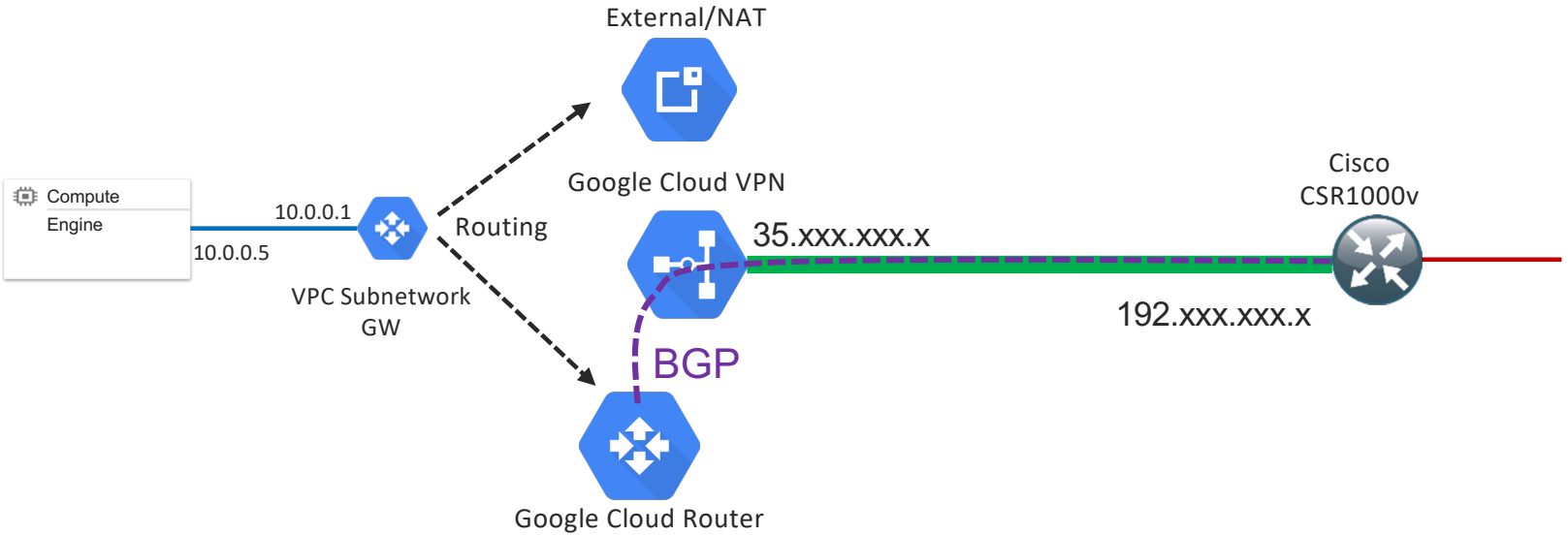


TGW ‘can’ replace transit VPC -



Опции маршрутизации и поддержка Split-Tunnel

- AWS/Azure/GCP допускают использование split-tunneling или forced/direct маршрутизацию
- Split-tunneling:
  - Ресурсы публичного облака (instances/VMs, container clusters) будут использовать шлюз по умолчанию в своем VPC для всех маршрутов non-On-Premises
  - Ресурсы публичного облака будут использовать специфичные маршруты к On-Premise инфраструктуре, анонсируемые CSR
- Forced/Direct маршрутизация – Все ресурсы публичного облака будут использовать VPN соединения как маршрут по умолчанию для всего трафика (весь трафик -> в сторону On-Premise)



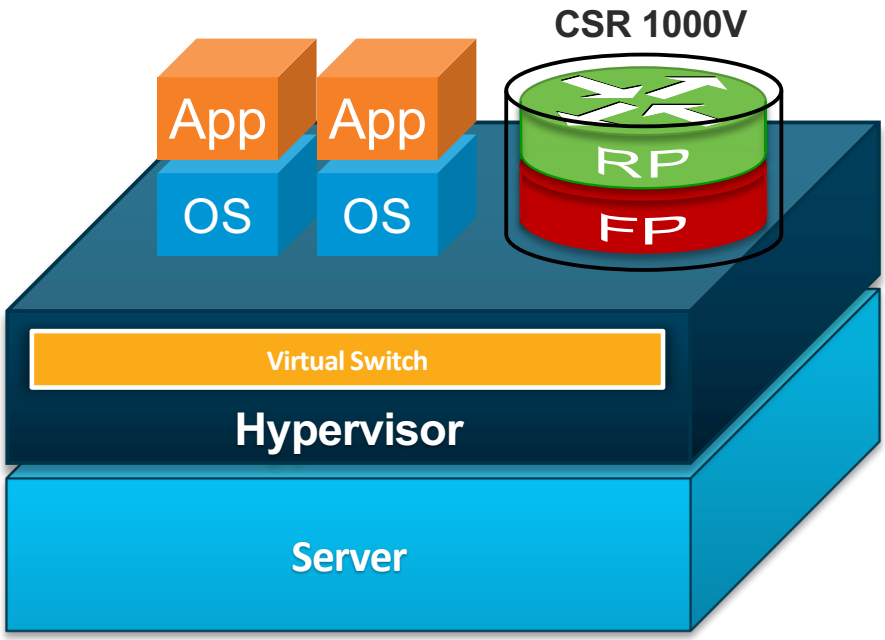
Отказ от использования сервисов Native VPN

Каковы причины изменения дизайна?

- **Если ваша on-prem инфраструктура находится за NAT провайдера – и нет NAT-T**
- **Вам нужно распространить применяемый на вашей площадке протокол маршрутизации (OSPF/EIGRP) на публичное облако**
- **Согласованность процессов эксплуатации**
- Вам нужны конфигурации IPsec/IKE, которые не поддерживает ваш провайдер облачных услуг
- Вы хотите использовать SSL VPN
- Вам нужен MPLS VPN
- Нужна поддержка QoS, IP SLA, NetFlow, корпоративного инструментария для настройки и мониторинга
- Производительность Native VPN сервисов недостаточна

Маршрутизатор для размещения в инфраструктуре провайдера облачных услуг Cisco Cloud Services Router (CSR) 1000V

Cisco IOS XE



https://www.youtube.com/playlist?list=PLCiTBLSYkcoTUS6b4MFthdvhDrseo6MeN

Программное обеспечение

- Знакомая по ASR1000 и ISR4000 операционная система IOS XE

Универсальное решение

- Работает на платформах x86
- Поддерживаемые гипервизоры и платформы: VMware ESXi, Linux KVM, Citrix Xen, Microsoft Hyper-V, Cisco NFVIS и CSP2100
- Поддерживаемые облачные платформы: Amazon AWS, Microsoft Azure, Google Cloud Platform

Гибкое управление производительностью

- Лицензии от 10 Mbps до 10 Gbps
- Использование от 1vCPU до 8vCPU

Варианты лицензирования

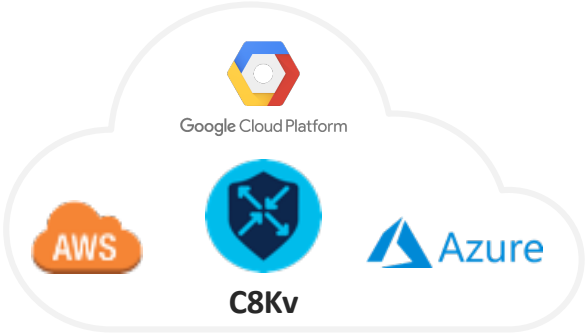
- 1-3-5 лет
- Smart License

Автоматизация и программируемость

- NetConf/Yang, RESTConf, Guest Shell, SSH/Telnet

Новинка – Catalyst 8000v Edge

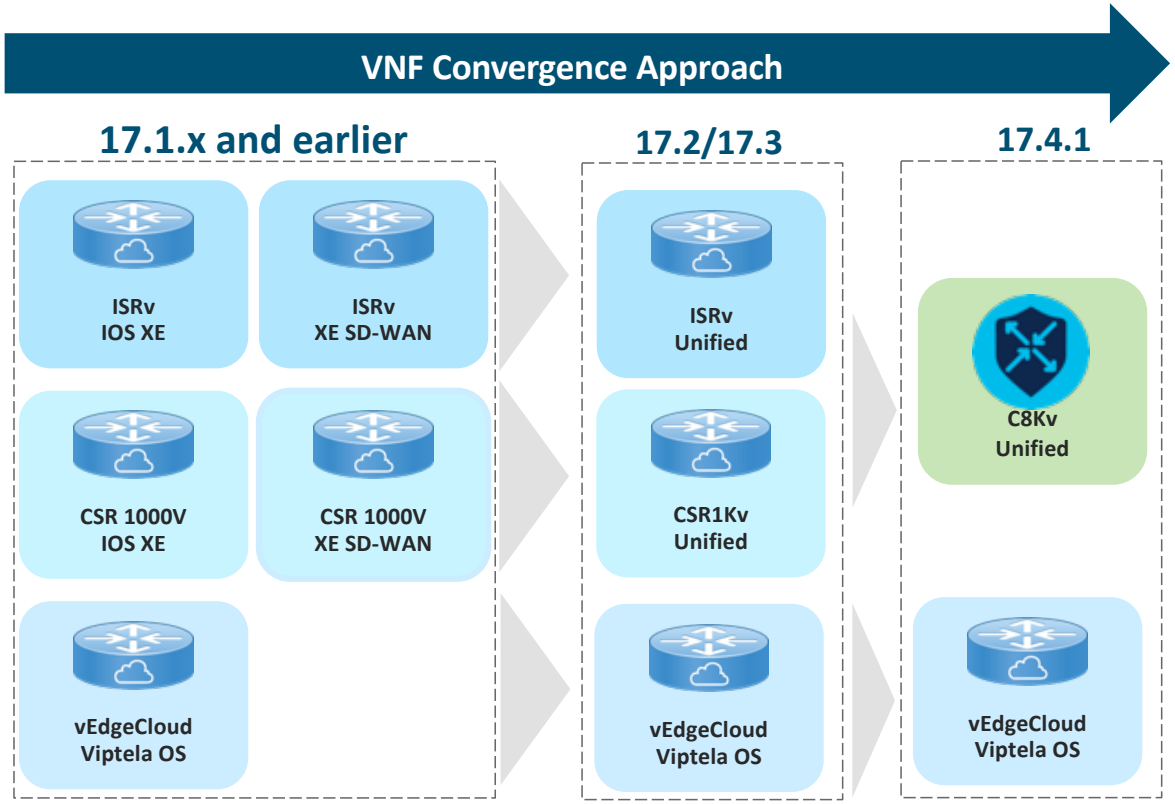
- Работает на платформах x86, ENCS или CSP в public/private облаках.
  - VMWare, RH KVM
  - Hyper-V/XenServer/KVM Ubuntu/SUSE Linux - позже
- Поддерживается в AWS, Azure, Google Cloud
- Основные варианты применения в облачных задачах:
  - Шлюз для route-based IPSec VPN (DMVPN, FlexVPN, GetVPN)
  - MPLS WAN endpoint
  - VXLAN шлюз
  - SD-WAN Headend
  - Точка контроля сетевых сервисов (AppNav/ZBFW/NAT/AVC и т.д.)
- Лицензирование:
  - Полоса (10 Mbps – 10 Gbps), уровень лицензии, срок действия
  - Модель PAYG (AWS/Azure marketplaces)



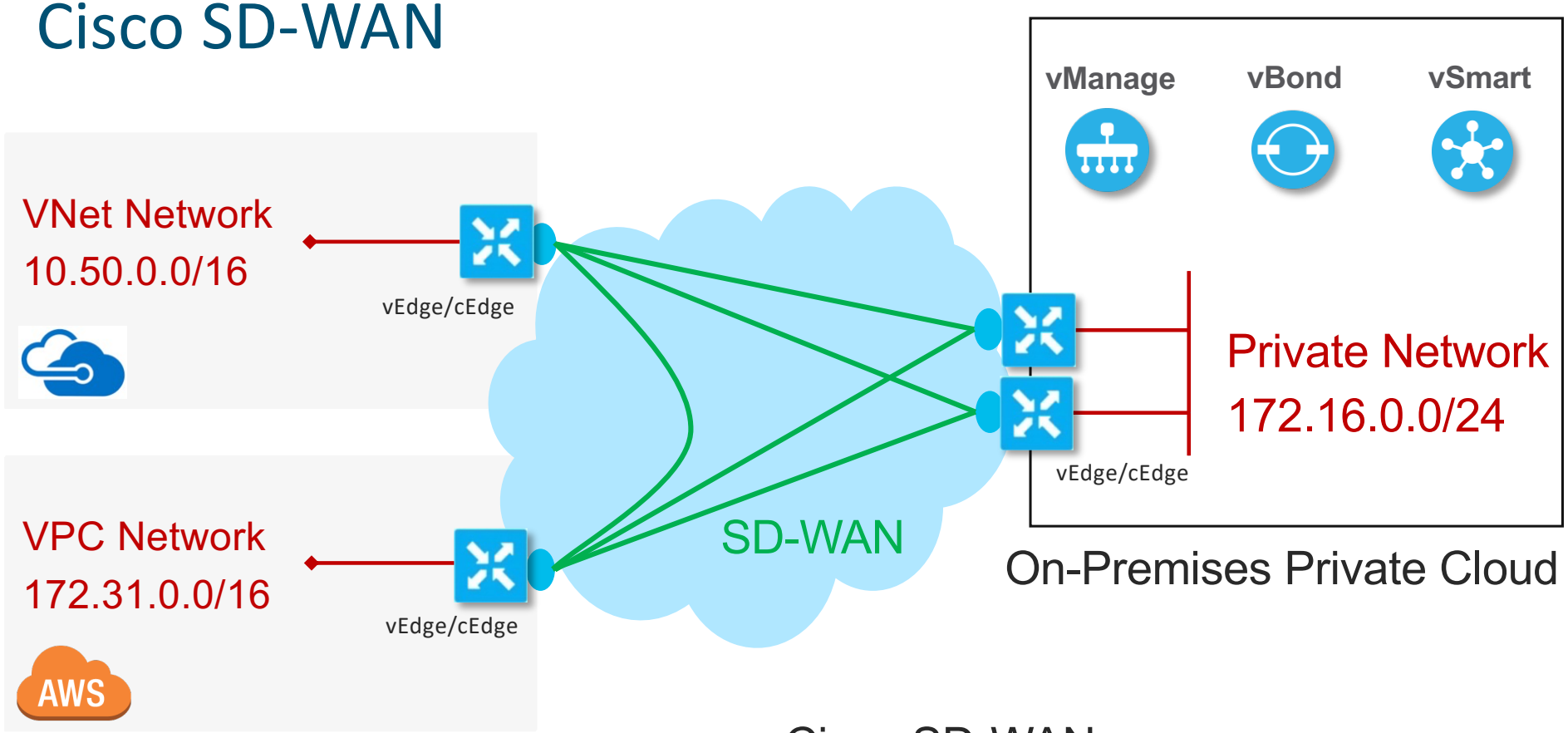
https://www.cisco.com/go/cloudrouter

***

Развитие виртуальных маршрутизаторов

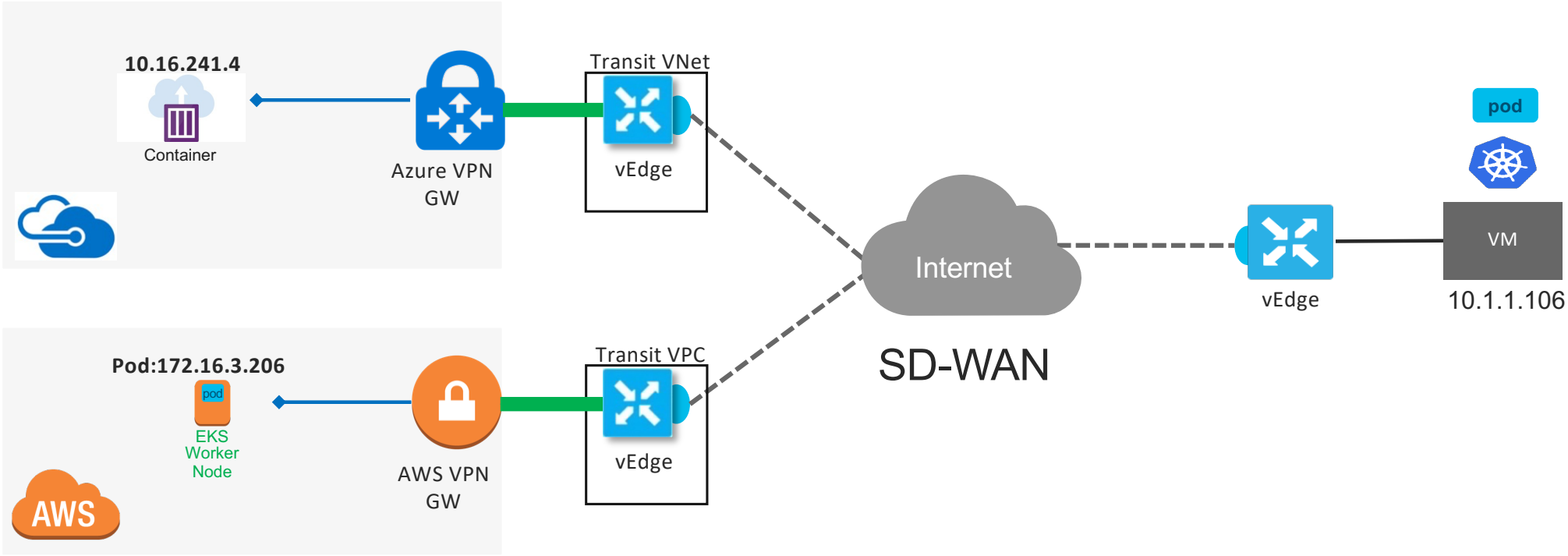


Cisco SD-WAN



Cisco SD-WAN:
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

Cisco SD-WAN and Multicloud

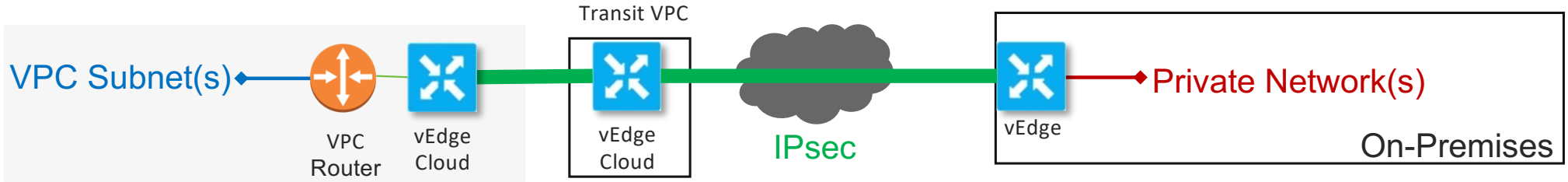


IPsec VPN – на примере Cisco SD-WAN

Per-VPC Cisco vEdge

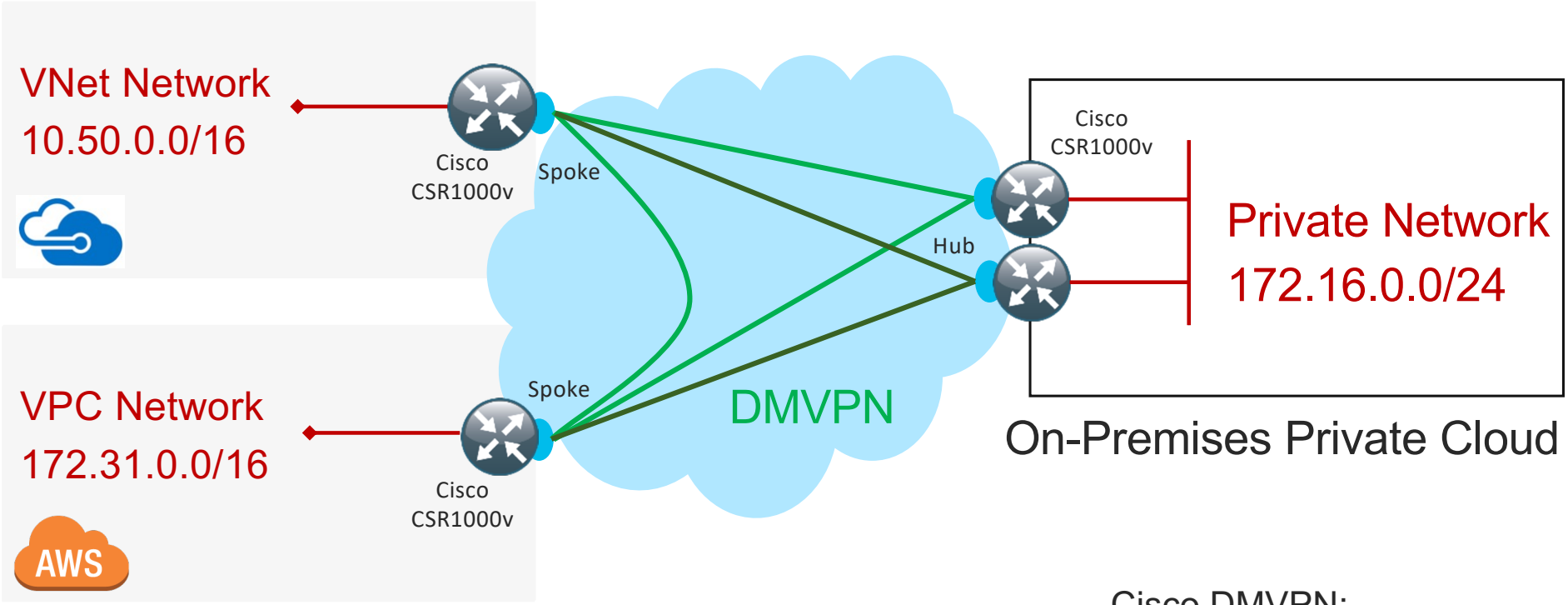
Transit VPC: Cisco vEdge + CSP VPN

Transit VPC: Cisco vEdge + Per-VPC vEdge



DMVPN – классика в применении к multicloud

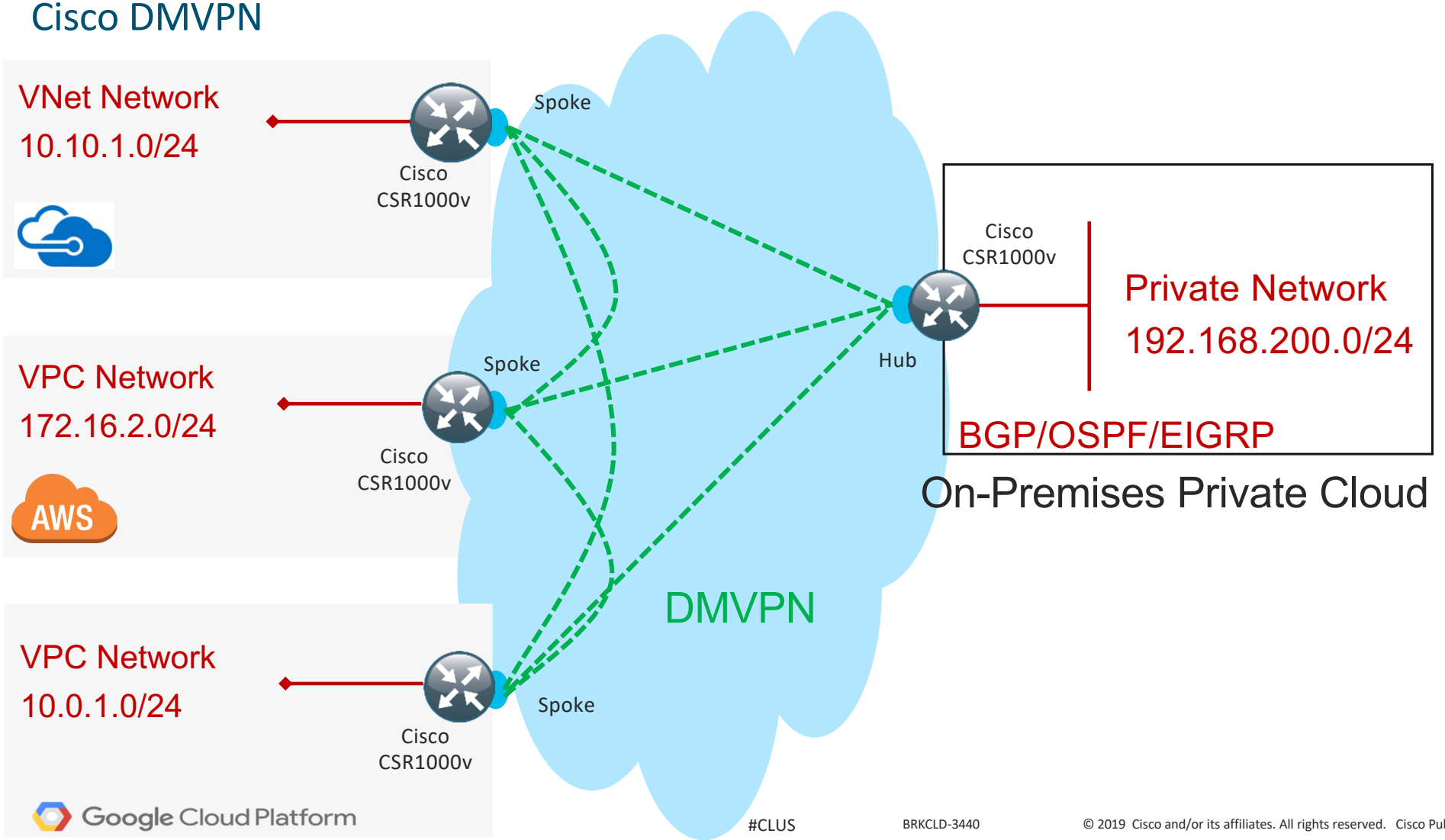
Cisco DMVPN – простое в настройке решение



Cisco DMVPN:
https://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn/index.html

DMVPN – Enable Dynamic Multicloud Networking

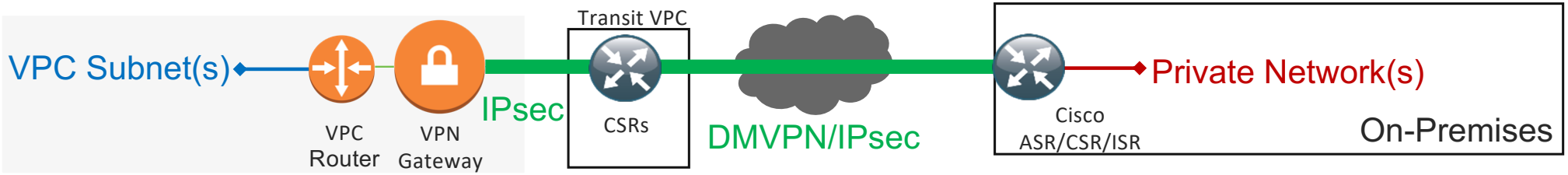
Cisco DMVPN



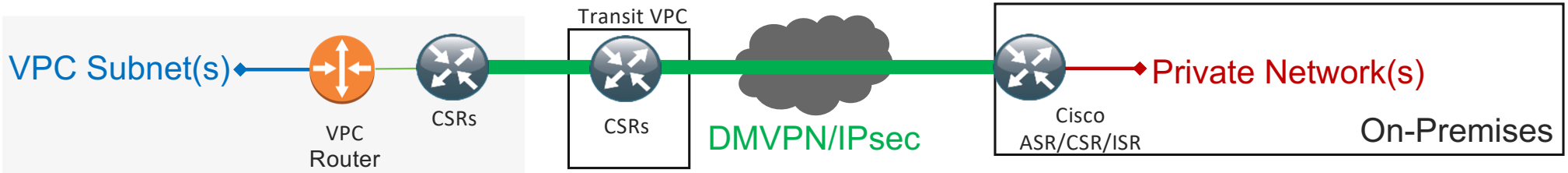
IPsec VPN - Cisco CSR 1000v Example

Per-VPC Cisco CSR 1000v

Transit VPC: Cisco CSR + CSP VPN



Transit VPC: Cisco CSR + Per-VPC CSR



A Note On MTU

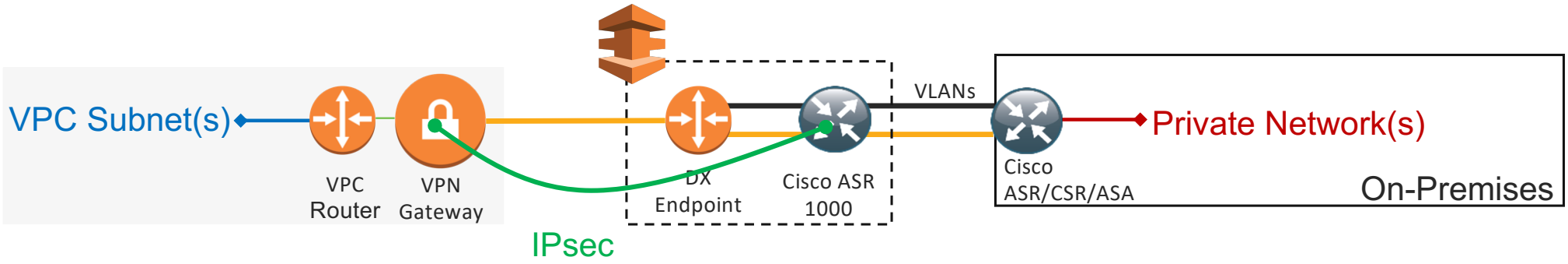
- All three providers recommend a different size interface MTU for the IPsec tunnel interface:
  - Google recommends 1460 on the tunnel: https://cloud.google.com/vpn/docs/concepts/advanced#mtu
  - AWS recommends 1399 on the tunnel: https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html
  - Azure recommends 1400 on the tunnel: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices
- In addition to MTU, you need to set and test your TCP MSS values
- In real world testing, an IP MTU of 1400 and TCP MSS of 1360 worked for all sites but this may need to change based on your applications and if you are adding other encaps like MPLS

Public Cloud Provider – CSR High-Availability

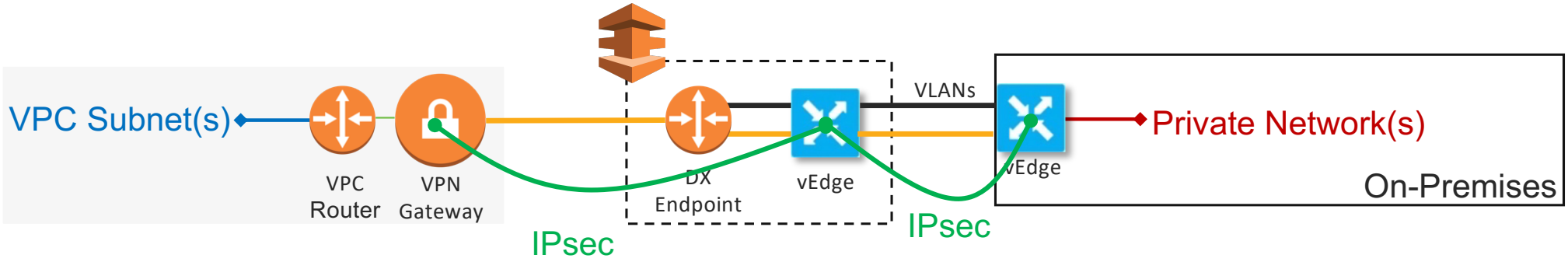
- Common challenge with all public cloud provider is that there is not true layer 2 support on a VPC subnet – this prevents FHRPs from working properly
- Must setup a monitoring/tracking feature to watch for CSR interface/instance failure and adjust the VPC route table to point to 2nd CSR inside interface
- AWS CSR High-Availability:
  - https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/aws/b_csraws/b_csraws_chapter_0100.pdf
- Azure CSR High-Availability:
  - https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/azu/b_csr1000config-azure/b_csr1000config-azure_chapter_0110.html

Colocation - With or Without VPN

Cisco Routers or Firewalls + Some Combo of Colocation/peering



Cisco SD-WAN + Some Combo of Colocation/peering



AWS Direct Connect (DX)

Cisco SD-WAN

Public Cloud Support

- Cisco SD-WAN (vEdge) on AWS: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/07Deploy_the_vEdge_Routers/01Create_vEdge_Cloud_VM_Instance_on_AWS
- AWS Marketplace: https://aws.amazon.com/marketplace/pp/B07BZ53FJT
- Cisco SD-WAN on Microsoft Azure: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/07Deploy_the_vEdge_Routers/02Create_vEdge_Cloud_VM_Instance_on_Azure
- Microsoft Azure Marketplace: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco_cloud_vedge_4_nics?tab=Overview
- Cisco SD-WAN Design/Deployment Guides: https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/branch-wan-edge.html
- Cisco SD-WAN Cloud OnRamp for Colocation: https://www.cisco.com/c/en/us/td/docs/routers/sdwan-cloud-onramp-for-colocation/solution-user-guide/cisco-sdwan-cloud-onramp-colocation-solution-guide-19_1.html

DMVPN (Dynamic Multipoint VPN)

- Cisco DMVPN
  - https://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn/index.html
- Cisco Live DMVPN
  - https://www.ciscolive.com/global/on-demand-library/?search=dmvpn#/
- Cisco IWAN CVD
  - https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/branch-wan-edge.html
- DMVPN is a Cisco innovation for building GRE/mGRE + IPsec VPN connections in a dynamic and scalable manner

Automation Challenges

"You can't possibly be successful automating something you don't understand the design for"

- Dumb, bald, loud guy

Automating the Multicloud Network

- Challenges:
  - **Different toolsets** for **different jobs** (Ansible, Python, Bash scripts, Terraform, etc..)
  - **Different toolsets** for **different clouds** (Heat for OpenStack, CloudFormation for AWS, Deployment Manager for GCP, Azure Automation)
  - **Different toolsets** for **different vendor** products (Cisco NSO, CloudCenter Suite, YANG development kit, etc..)
- There is no silver bullet - Start simple:
  - Use what your team knows – Perform a gap analysis on what you have against what you need
  - Initially, automate the things that hurt a lot to do by hand and that change frequently – I use free tools but that doesn't mean the process is free ☺
  - **Native Tools**: It's safe to use the cloud provider's native automation toolset (e.g., AWS CloudFormation) when that is the only provider you need to deal with
  - **Abstracted Tools**: When you are dealing with multiple providers to include on-premises providers (e.g., VMware vSphere or Microsoft Azure Stack), it makes life easier to abstract away from native cloud provider tool sets and use something like Terraform and/or combo of tools
  - **Full Stack Tools**: When you want to stop pulling your hair out and you want to build full 'stacks' in nearly any environment, move to something that can treat the environment as a whole
    - Cisco CloudCenter Suite: https://www.cisco.com/c/en/us/products/cloud-systems-management/cloudcenter/index.html
    - Cisco Managed Services Accelerator: https://www.cisco.com/c/en/us/products/cloud-systems-management/managed-services-accelerator/index.html

Amazon CloudFormation

- https://aws.amazon.com/cloudformation/
- Template-based (JSON/YAML) – Build a stack(s) from a template file
- Sometimes you need to run more than one stack (in order) to get what you need
  - Example template: https://github.com/shmcfarl/multicloud/tree/master/aws/cloudformation

Google Cloud Platform – Deployment Manager

- https://cloud.google.com/deployment-manager/
- Configuration files (YAML), Templates (Python/Jinja2), Schema files (JSON)
- Sometimes you need to run more than one stack (in order) to get what you need
  - Example templates: https://github.com/shmcfarl/multicloud/tree/master/gcp/deployment-manager

Microsoft Azure Automation/Resource Manager

- https://azure.microsoft.com/en-us/services/automation/
- Runbooks (create graphically, PowerShell, Python)
  - Read and select these carefully: https://docs.microsoft.com/en-us/azure/automation/automation-runbook-types
- Resource Manager: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview
  - https://github.com/Azure/azure-quickstart-templates/tree/master/cisco-csr-1000v
- Example template: https://github.com/shmcfarl/multicloud/blob/master/azure/resource-manager/az-arm-csr-cleaned.json

Call APIs Directly

- Cisco SD-WAN APIs: https://developer.cisco.com/sdwan/
- Google Cloud Platform: https://cloud.google.com/compute/docs/reference/latest/
- Amazon Web Services: https://docs.aws.amazon.com/AWSEC2/latest/APIReference/Welcome.html
- Microsoft Azure: https://docs.microsoft.com/en-us/rest/api/

HashiCorp Terraform - Abstracted Model

https://github.com/terraform-providers

https://github.com/terraform-providers/terraform-provider-aws

Providers

https://github.com/terraform-providers/terraform-provider-azurerm

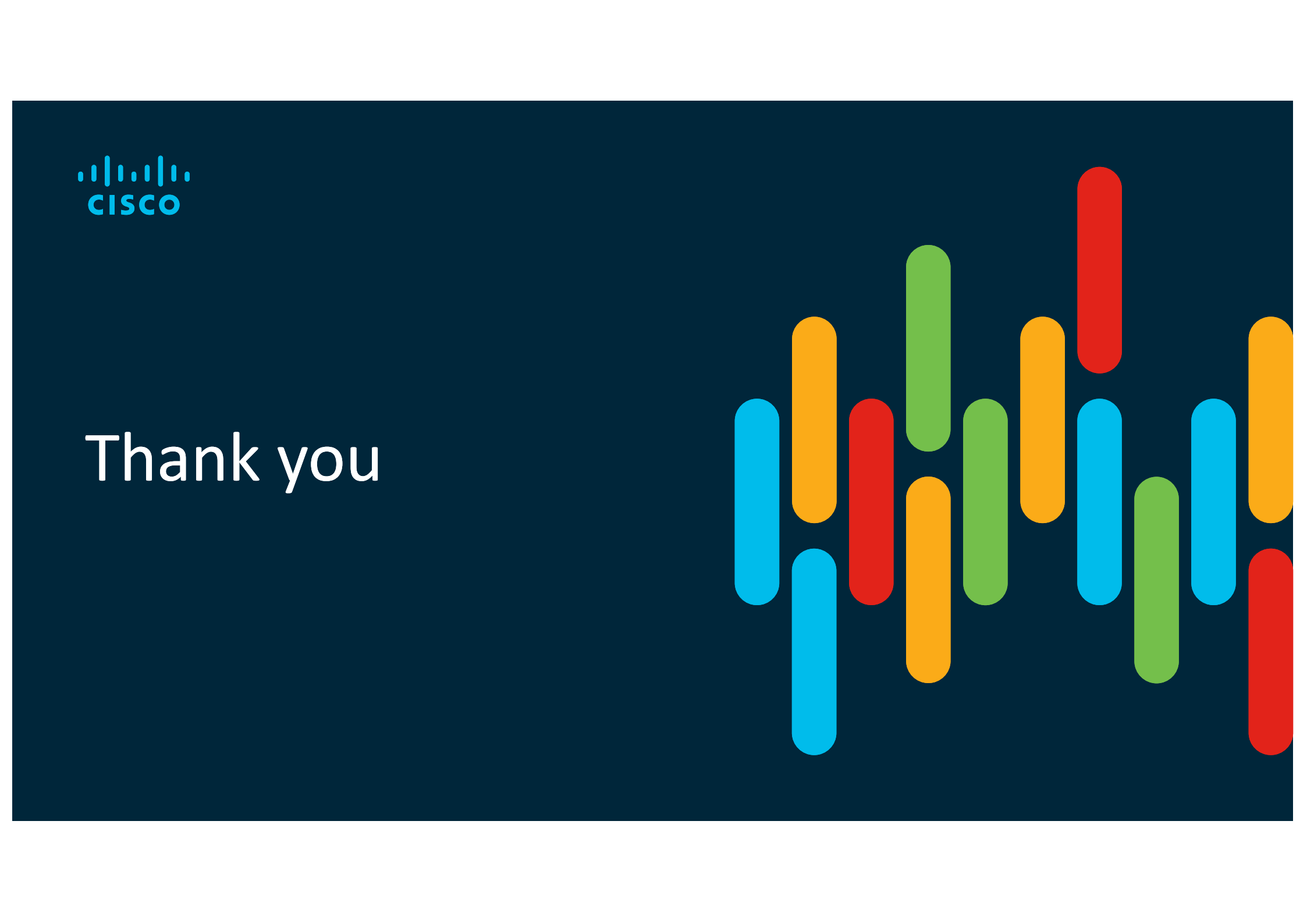
https://github.com/terraform-providers/terraform-provider-kubernetes

https://github.com/terraform-providers/terraform-provider-google

https://github.com/CiscoDevNet/terraform-sdwan

Summary

- Cisco Multicloud Solutions: https://www.cisco.com/c/en/us/solutions/cloud/multicloud-portfolio.html
- Public cloud native IPsec VPN support is good, but it is always point-to-point, does not have consistent support and lacks network-rich features - It may be good enough for your initial use case(s)
- If you have deployed or want to deploy SD-WAN, adding in your public cloud sites into your overall SD-WAN design can reap many operational and cost benefits
- If you have an existing WAN/Branch deployment of DMVPN, adding spokes at public cloud site(s) can help optimize traffic flow (no hair-pinning), enable rich network features at the public cloud site and allow for a consistent technical and operation experience
- Keep an eye out for ACI Anywhere (Cisco Cloud ACI): https://aws.amazon.com/blogs/apn/extending-on-premises-cisco-cloud-aci-network-security-segmentation-to-aws/
- Multicloud between multiple public cloud providers and on-premises look like distinctly separate hybrid cloud deployments but..
    - You have to take into consideration:
        - Team knowledge of public cloud operations, tools, automation
        - Cross cloud tools and automation
        - Diversity of network designs, protocols, security
        - Multi-region designs
        - Availability zones within and across providers


Thank you