Multicloud Networking: An Overview

Shannon McFarland
CCIE #5245
Distinguished Engineer
@eyepv6

Agenda

- Hybrid Cloud Networking vs Multicloud Networking - A Level Set
- Extending on-premises private cloud to public cloud
- Add more public clouds to the mix
- Automation challenges

Hybrid Cloud Networking vs Multicloud Networking – A Level Set

Hybrid vs Multicloud Networking

- Hybrid Cloud Networking == Network transport from on-premises to a single public cloud provider
- Multicloud Networking == Network transport from on-premises to multiple public cloud providers and/or between multiple public cloud providers
- The technologies used can be identical for every connection or they can be per-provider, per-region, per-project, etc..
- Common network transport ingredients for Hybrid and Multicloud:
  - Encryption (IPsec/IKEv2/IKEv2, SSL, PKI)
  - Routing (Static, BGP and with supported public cloud-hosted routers: OSPF, EIGRP)
  - Tunneling (IPsec tunnel mode, GRE, mGRE, MPLS, VPLS, VXLAN, L2TPv3, etc..)
- Common network endpoint options:
  - Native VPN (IPsec over Internet) using public cloud provider services that connect to on-premises router/firewall
  - Commercial/Open Source VPN platform hosted on the public cloud provider connecting to an on-premises router/firewall
  - Colocation Peering: Service from public cloud provider to on-premises via a 3rd party colo facility

Why Would You Use Multiple Cloud Providers?

- **Cloud provider high availability**
- **M&A may dictate public cloud provider preference (for a time)**
- Regional cloud provider access
- Feature disparity between providers, regions and/or services
- Per-project service requirements

Extending On-Premises Private Cloud to a Public Cloud

Reference

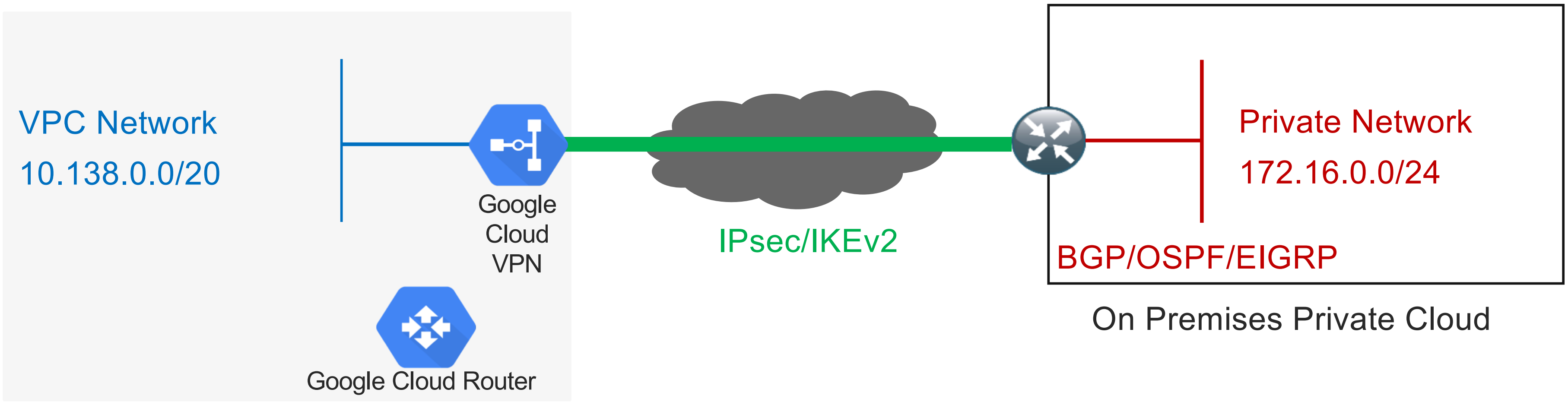
Public Cloud Provider Native VPN Services

The Big Three

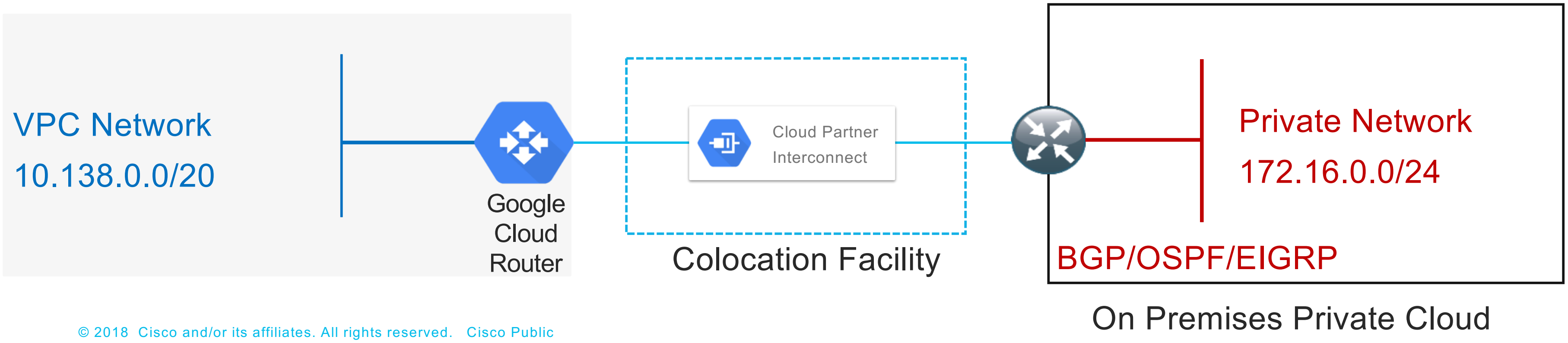
- Amazon Web Services (AWS):
  - VPN: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html
  - Direct Connect: https://aws.amazon.com/directconnect/
- Google Cloud Platform (GCP):
  - VPN: https://cloud.google.com/compute/docs/vpn/overview
  - Dedicated Interconnect: https://cloud.google.com/interconnect/
- Microsoft Azure:
  - VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/
  - ExpressRoute: https://azure.microsoft.com/en-us/services/expressroute/
- OpenStack public cloud goodness: https://www.openstack.org/passport

Options – IPsec-over-the-Internet or Dedicated Connections

IPsec VPN + Internet

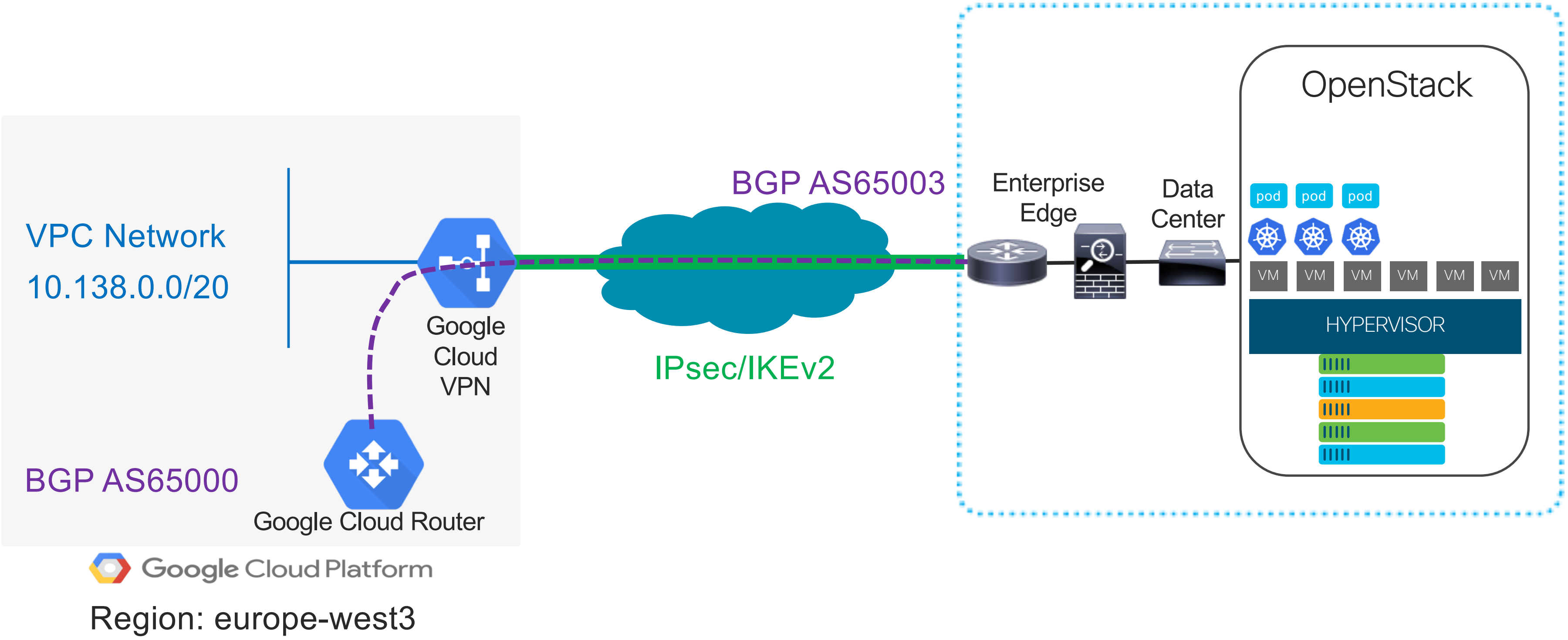


Colocation



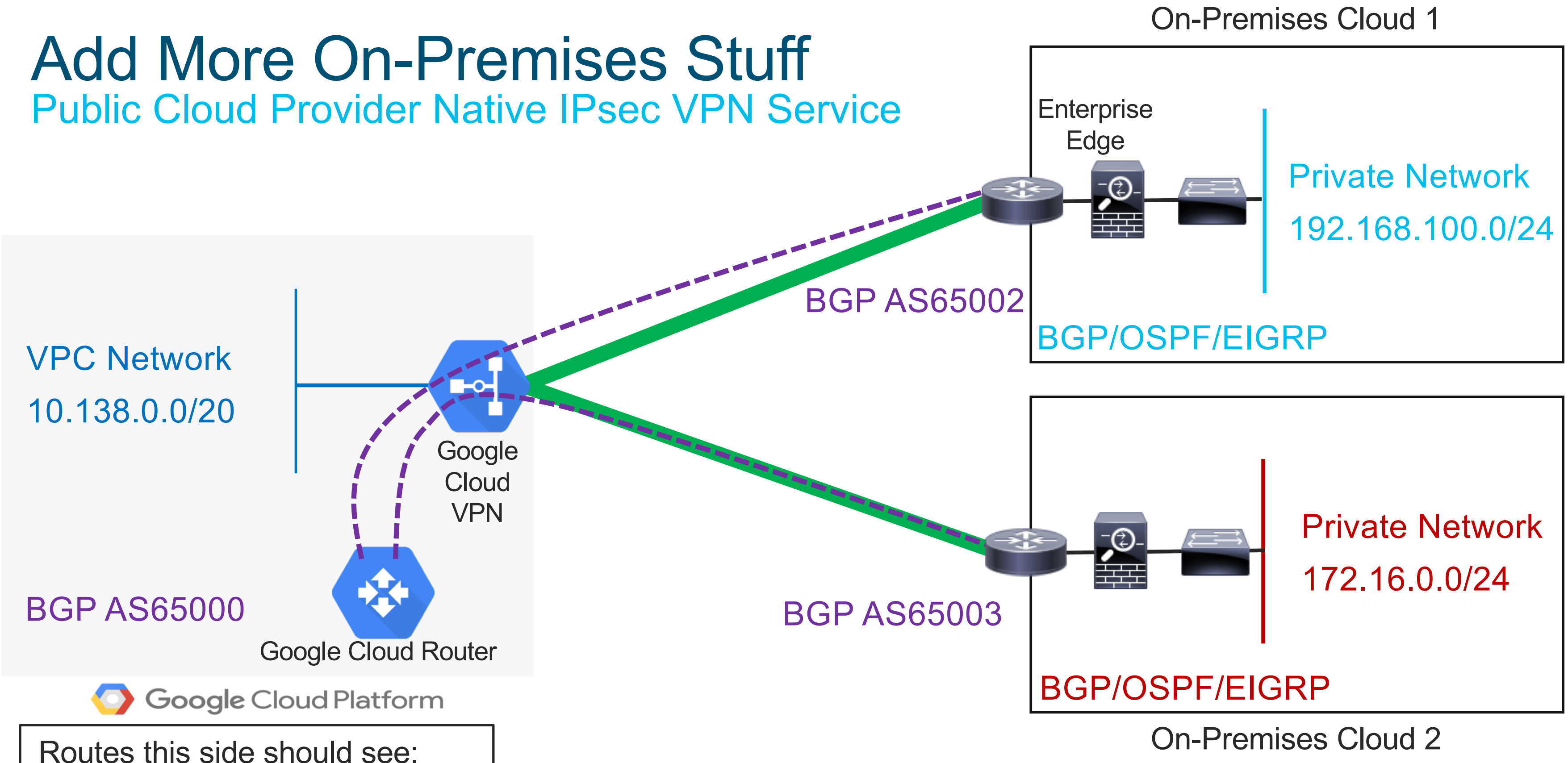
Starting Simple

Public Cloud Provider Native IPsec VPN Service



Add More On-Premises Stuff

Public Cloud Provider Native IPsec VPN Service

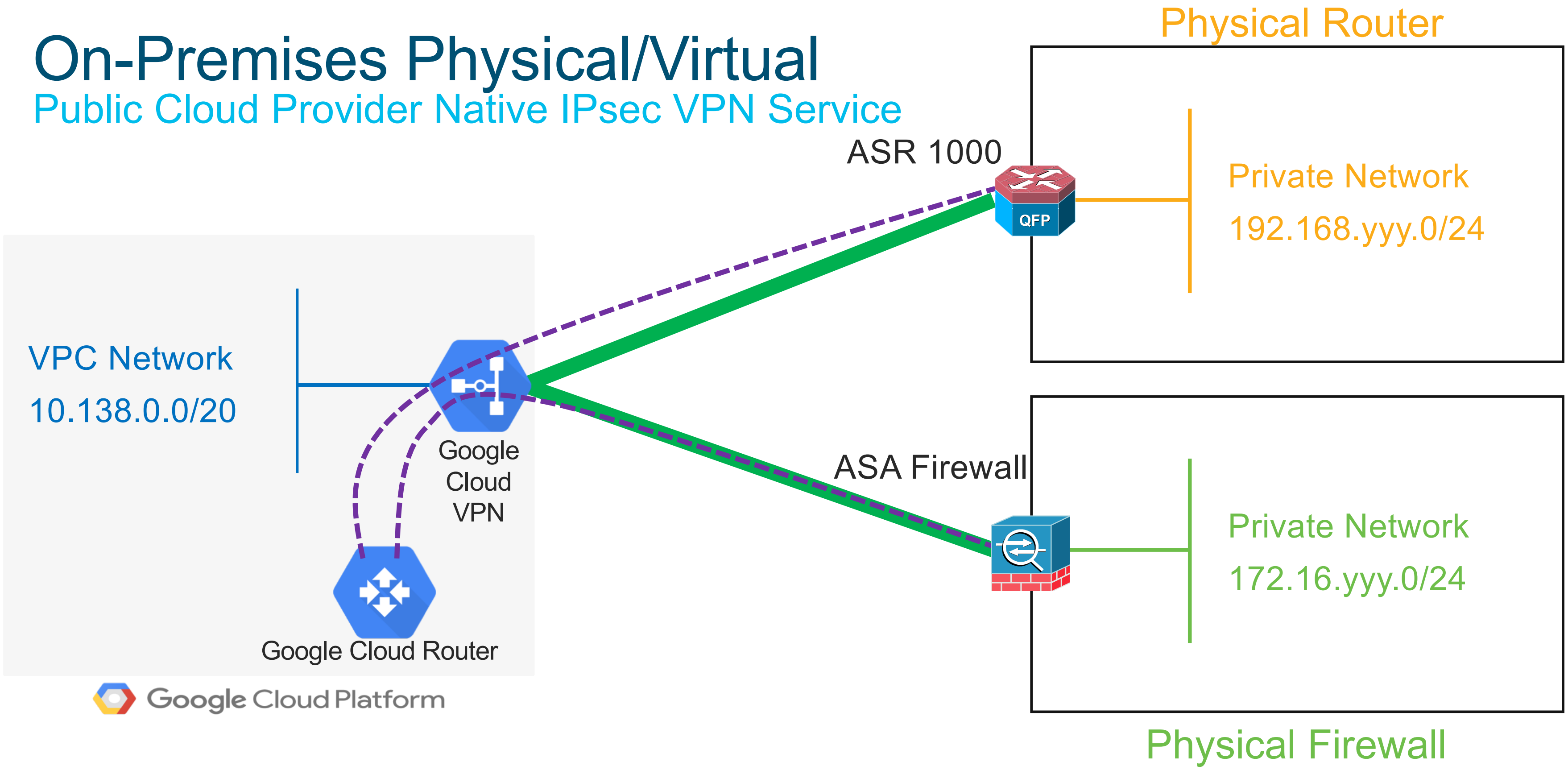


Routes this side should see:
172.16.0.0/24
192.168.100.0/24

Routes this side should see:
10.138.0.0/20

On-Premises Physical/Virtual

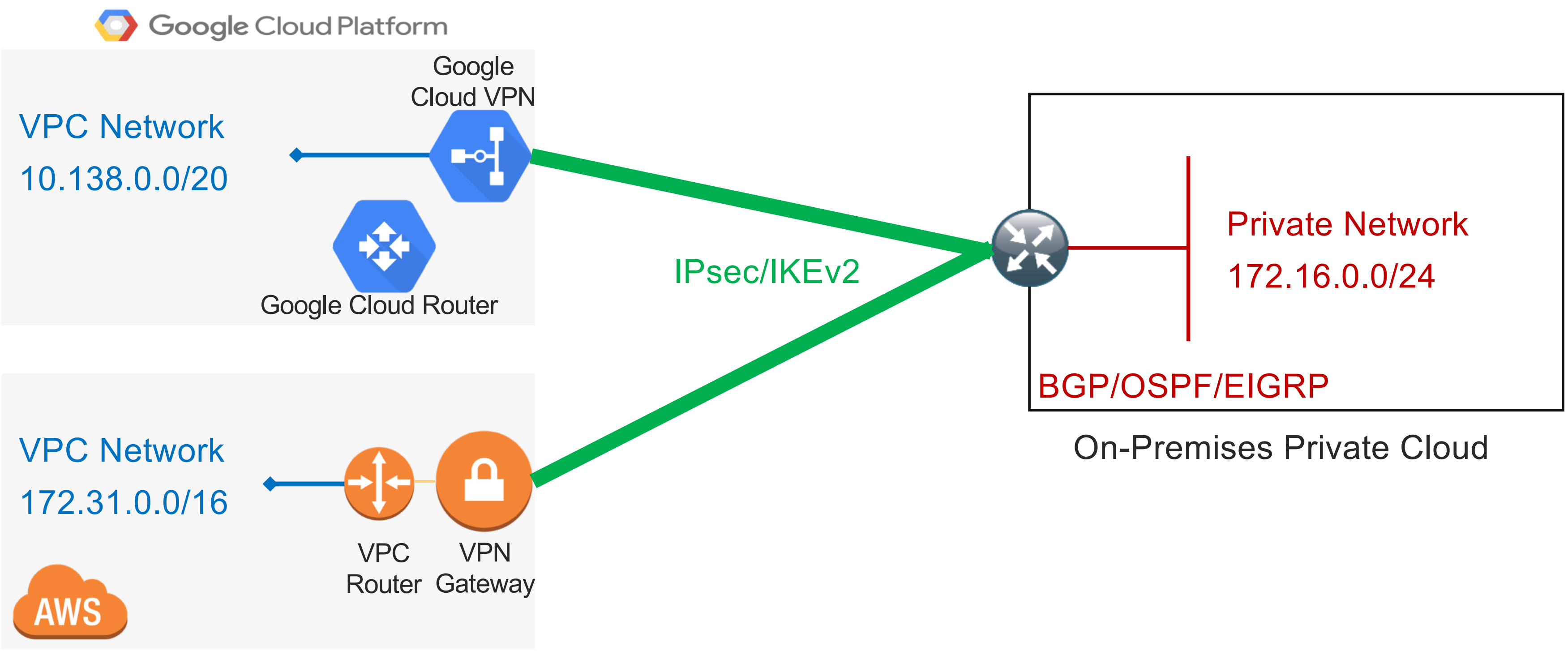
Public Cloud Provider Native IPsec VPN Service



Add More Public Cloud Providers to the Mix

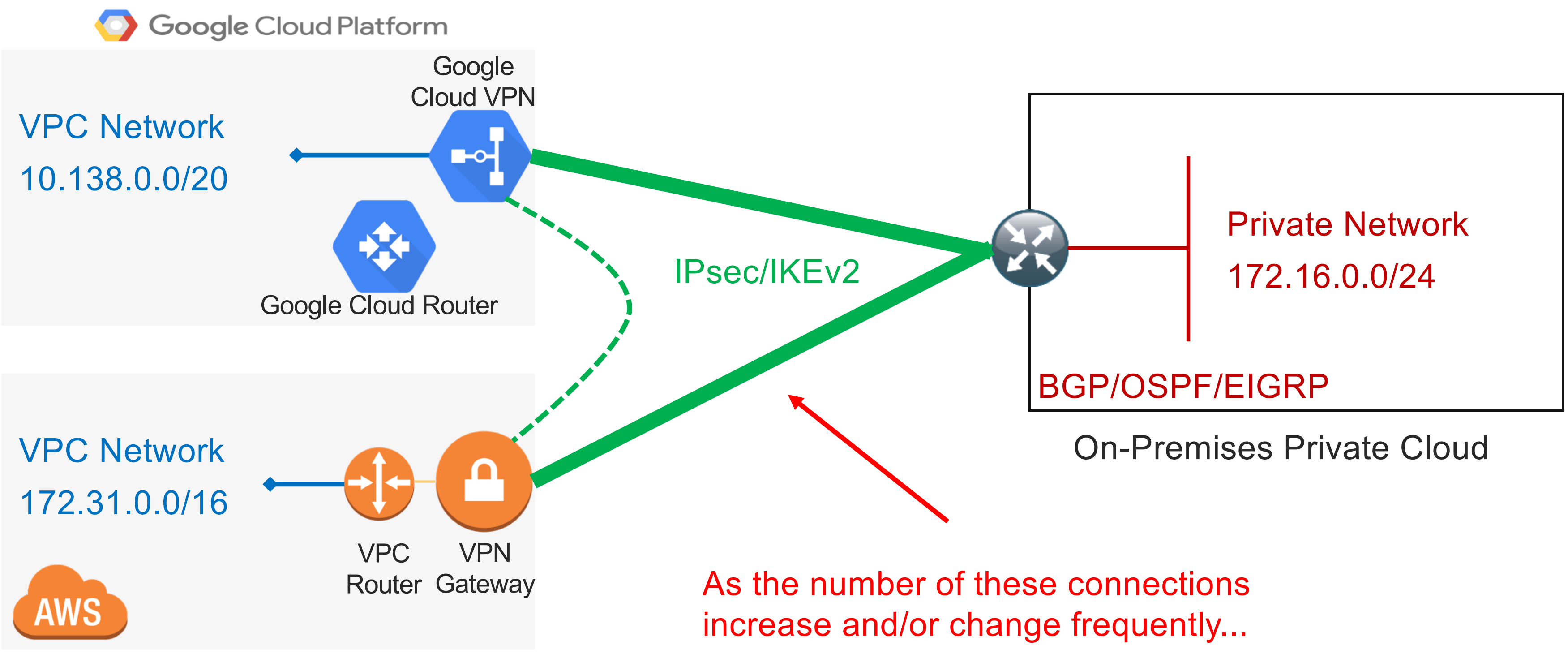
Stepping into Multicloud Networking

Multiple Native IPsec VPN Services



Stepping into Multicloud Networking

Multiple Native IPsec VPN Services



As the number of these connections increase and/or change frequently...
You can see where this is going

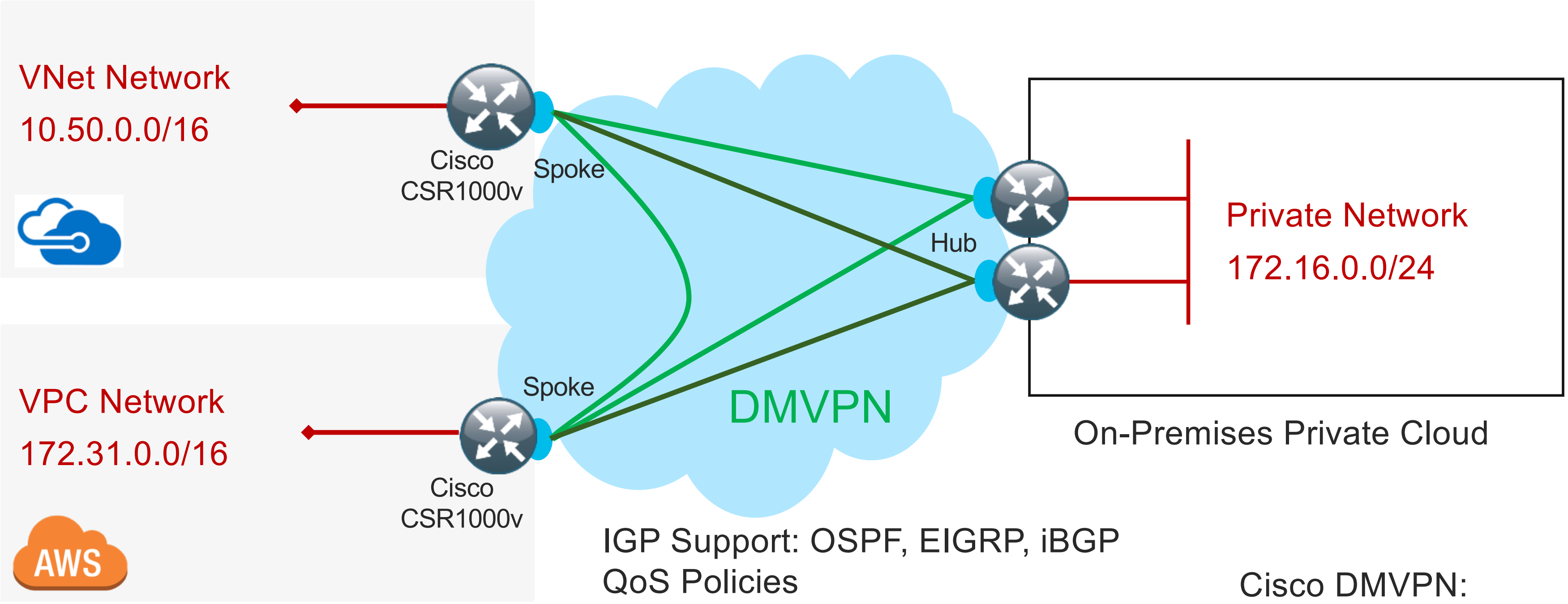
Moving Away From Native VPN Services

What Conditions Cause a Change in Design?

- If on-premises routers/firewalls are behind NAT – Check for provider support of NAT-T
- You need different IPsec/IKE configurations than what the provider offers
- You need to extend your on-premises IGP (OSPF/EIGRP) into the public cloud
- You need MPLS VPN
- QoS, specific network monitoring (IP SLA, NetFlow), Enterprise toolsets for configuration and monitoring
- Operational consistency

DMVPN – Enable Dynamic Multicloud Networking

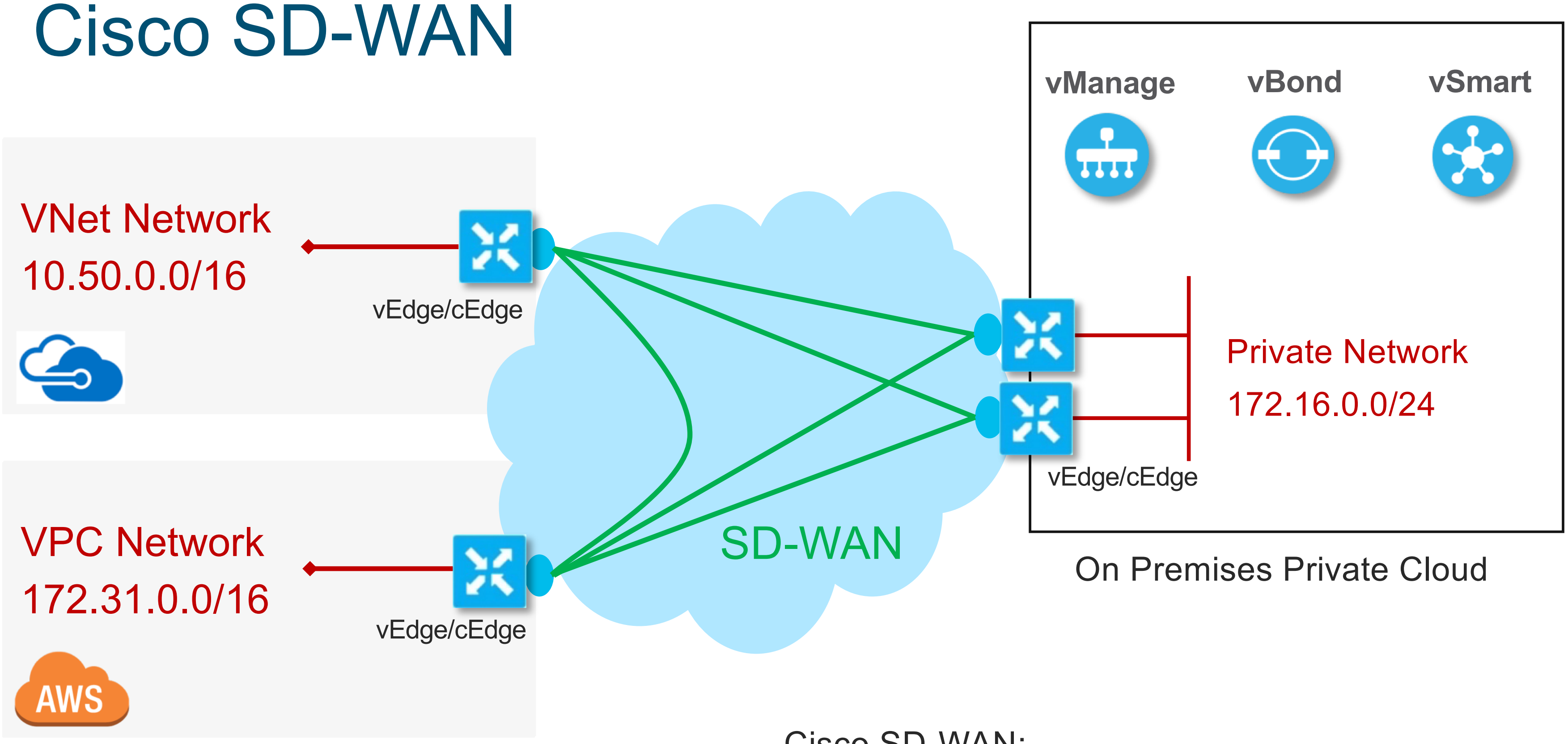
Cisco DMVPN



IGP Support: OSPF, EIGRP, iBGP
QoS Policies
IP SLA, NetFlow
NAT-T (Transparency)
MPLS
etc...

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

Cisco SD-WAN



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

Automation Challenges

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 Resource Manager)
  - Different toolsets for different vendor products (Cisco NSO, Cloud Center, Prime, 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 ☺
    - I use public cloud clients (gcloud CLI, aws CLI, azure CLI) for services that don't change frequently or that need very unique/non-repeatable configurations
    - I use public cloud provider automation tools (e.g., GCP Deployment Manager) for in-project work (new instances with new networks for a GCP-only project)
    - I use REST for things that change a lot, especially if driven from another dashboard
  - When you want to stop pulling your hair out, move to something that can front-end each API that you need to talk to and treat the environment as a whole – Cisco CloudCenter: https://www.cisco.com/c/en/us/products/cloud-systems-management/cloudcenter/index.html

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 for NAT and lacks network-rich features
- DMVPN with Cisco CSR, ASR, ISR can greatly improve the deployment, HA, scalability and operations of the VPN connections
- If you have deployed or want to deploy an SD-WAN, adding in your public cloud sites into your overall SD-WAN design can reap many operational and cost benefits
- 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

cisco