Cisco Multicloud Portfolio:
Cloud Connect

Design considerations and overview

August 2018
Contents

Introduction .............................................................................................................................................3
Cisco Multicloud Portfolio: overview ..................................................................................................3
Cloud Connect: Overview .....................................................................................................................4
Cloud Connect: Use cases ......................................................................................................................4
Cloud Connect: Benefits .......................................................................................................................5
Cloud Connect design considerations: overview ................................................................................5
Cloud to private data center designs ..................................................................................................6
Cloud to private data center via IPsec VPN ..........................................................................................6
Cloud to private data center via dedicated network connection ............................................................10
Advantages and disadvantages of IPsec VPN vs. dedicated network connection ....................................11
Cloud-to-cloud transit VPC design ....................................................................................................12
Scalable dedicated network connection designs ................................................................................14
Branch-to-cloud designs ......................................................................................................................16
Additional considerations ................................................................................................................18
Path isolation ........................................................................................................................................18
Application visibility ...........................................................................................................................18
Summary .............................................................................................................................................19
Additional resources ..........................................................................................................................19
**Introduction**

This guide provides a high-level overview of various design considerations and methods for providing network connectivity to cloud provider networks – in particular, Infrastructure-as-a-Service (IaaS) and/or Platform-as-a-Service (PaaS) cloud-provider Virtual Private Clouds (VPCs). The following designs are discussed:

- Cloud to private data center
- Cloud to cloud
- Branch to cloud

The audience for this document includes network design engineers, network operations personnel, and security operations personnel who wish to implement connectivity from their organization’s networks to one or more cloud provider VPCs.

**Technical note:** For this document, “VPC” means any generic cloud provider network, such as an Amazon Virtual Private Cloud, a Google Virtual Private Cloud Network, or a Microsoft Azure Virtual Network.

**Cisco Multicloud Portfolio: overview**

In a multicloud world, growing complexity is driving a cloud gap between what your customers require and what your people, processes, and tools can support. With the Cisco Multicloud Portfolio, we make it simple: simple to connect, simple to protect, and simple to consume.

The Cisco Multicloud Portfolio is a set of essential products, software, and services supported with simplified ordering and design deployment guides to help you when it comes to multicloud adoption. It consists of four component portfolios (Figure 1):

- **Cloud Advisory:** Helps you design, plan, accelerate, and remove risk from your multicloud migration
- **Cloud Connect:** Securely extends your private networks into public clouds and helps ensure the appropriate application experience
- **Cloud Protect:** Protects your multicloud identities, direct-to-cloud connectivity, data, and applications, including Software as a Service (SaaS), and detects infrastructure and application threats on-premises and in public clouds
- **Cloud Consume:** Helps you deploy, monitor, and optimize applications in multicloud and container environments
Cloud Connect: Overview
Cloud Connect consists of essential products that help securely extend your private networks – including data center, branches, and campuses – to public clouds and to help ensure an optimal application experience:

- Cisco Cloud Services Router (CSR) 1000V Series
- Cisco vEdge Router with Cisco Umbrella™
- Cisco Aggregation Services Router (ASR) 1000 Series

For detailed use cases, see the section about Cloud Connect on the portfolio’s solution page at https://www.cisco.com/go/multicloud. Cisco partners can find more information about this on the Cisco partner sites like Cisco Salesconnect.

Cloud Connect: Use cases
Cloud Connect delivers value in the following use cases:

- Securely extending a private network to single or multiple public cloud environments. Includes multiple clouds (for example, multiple Amazon Web Services [AWS] and Azure), multiple regions in a cloud, or multiple VPCs in a cloud; VPN; multicloud and multi-VPC connectivity; scaling; and performance optimization of transit VPC. Also supports extending data centers into the cloud (through Cisco ASR 1000 Series or Cisco CSR 1000V Series routers) and enabling direct branch-to-cloud connectivity (when a branch has a Cisco 4000 Series Integrated Services Router [ISR] and wants to connect the clouds or a branch has vEdge and requires a software-defined WAN [SD-WAN] extension to the cloud).
- Optimizing data center and branch connectivity performance to cloud IaaS and SaaS. Includes best path to destination (SD-WAN), cloud segmentation, monitoring to assure best performance, visibility into traffic going to applications, and traffic shaping/Quality of Service (QoS). Also supports extending data centers into the cloud and enabling direct branch-to-cloud connectivity (when a branch has a 4000 Series ISR and wants to connect the clouds or a branch has vEdge and requires an SD-WAN extension to the cloud).
- Securing access to the Internet and SaaS from the branch. Includes connecting and protecting branch office users directly to the multicloud environment using Direct Internet Access (DIA), SD-WAN (vEdge), and secure Internet gateways (Cisco Umbrella).
Cloud Connect: Benefits

Cloud Connect benefits include the ability to:

- Extend a private network to a multicloud environment while leveraging existing investments
- Apply consistent security policies across a private and public cloud footprint
- Enhance and secure the app experience on a cloud network by enabling visibility, path selection and optimization
- Centralize management in a manner that is intuitive, fast, and easy to design, provision, and apply policies across the entire network
- Achieve faster and simpler adoption of cloud
- Improve TCO
- Access a richer networking security feature set and higher performance
- Improve ease of use through consistency of management tools for both on-premises and cloud
- Simplify implementation through increased visibility into the public cloud network

Cloud Connect design considerations: overview

In a multicloud world, IT managers are quickly realizing the benefits of cloud computing services such as IaaS, PaaS, and SaaS. Organizations can simply leverage existing Internet connectivity to access applications provided by SaaS providers instead of taking months to develop their own custom applications. This allows the organization to focus its resources on its core business, rather than on the development of applications, such as Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP), that are common across all organizations. IaaS and PaaS cloud providers allow organizations to prototype new applications more rapidly and cost-effectively. Instead of procuring, installing, and managing hardware, which could take months to accomplish, network administrators can easily use the on-demand and scalable compute services within an IaaS or PaaS provider. This allows the organization to focus its resources on applications rather than on managing the data center and physical infrastructure. With the use of IaaS and PaaS cloud services, expenses shift from fixed costs for hardware, software, and data center infrastructure to variable costs based on the usage of compute resources and the amount of data transferred between the private data center and the cloud provider.

This design guide discusses various designs for providing network connectivity to IaaS and PaaS cloud-provider VPCs. The following types of designs are discussed:

- Cloud to private data center
- Cloud to cloud
- Branch to cloud
Cloud to private data center designs

This section discusses designs for connecting private data center networks to one or more VPCs provided by one or more cloud providers. These cloud providers are typically IaaS or PaaS providers, such as AWS, Google Cloud Platform (GCP), or Microsoft Azure.

**Technical note:** For this document, the term "private data center" will be used interchangeably with the terms "on-premises private cloud" and "private network."

The most basic design is the connection of a private data center network to a single VPC provided by a single cloud provider. Technically, since only one cloud provider is involved, this is considered to be a hybrid cloud deployment and not a multicloud deployment. Even with this most basic design, the network administrator has the choice of how to provide network connectivity from the private network to the cloud provider – either via IP Security (IPsec) VPN or by directly connecting to the cloud provider.

**Cloud to private data center via IPsec VPN**

The simplest design for providing connectivity from a private data center to a single VPC is through an IPsec VPN connection that uses the Internet. Figure 2 shows an example of a high-availability design.

**Figure 2.** Private network to cloud provider – IPsec VPN connection to single VPC with high availability

At the private network, high availability is accomplished by having two VPN gateways, each of which establishes one or more IPsec VPN tunnels to the cloud provider VPN gateway. The network administrator must be careful to identify all the areas within the design that require resiliency. This may include connectivity to the Internet via multiple Internet service providers using separate entrance facilities to the private network, or possibly connectivity to the VPC from separate physical private network locations.
The network administrator has considerable choice for the platform that provides the IPsec VPN gateway functionality at the private network. Some of the choices are as follows:

- Dedicated (IPsec VPN only) physical appliances, such as the Cisco ASR 1000 Series Routers
- Dedicated (IPsec VPN only) Virtual Network Functions (VNFs), such as the Cisco CSR 1000V Series Routers
- Integrated (IPsec VPN, firewall, etc.) physical appliances, such as the Cisco Adaptive Security Appliance (ASA) or Cisco Firepower® firewalls
- Integrated (IPsec VPN, firewall, etc.) VNFs, such as the Cisco Adaptive Security Virtual Appliance (ASAv) firewall

With dedicated devices (appliances or VNFs), additional services need to be provided by deploying additional devices within a service chain. The security policy of the organization will often determine the additional services that need to be deployed. Separate devices, each with a single function, provide a clear separation of functionality within the overall service chain (IPsec VPN, firewalling, intrusion prevention and detection, Digital Loss Prevention (DLP), etc.), but may result in additional appliances and/or VNFs being deployed. The requirements for performance and/or ease of deployment may guide the decision as to whether to deploy a hardware appliance or VNF. Hardware appliances generally have greater performance per device (not including the horizontal scalability of deploying multiple VNFs), while VNFs tend to provide more flexibility and easier deployment.

The cloud provider VPN gateway is typically a logical construct within the cloud provider VPC for terminating VPN connections. Multiple VPN connections can be provisioned between the cloud provider VPN gateway and the customer VPN gateways. Specific implementations, such as the AWS virtual private gateway, support resilience by automatically provisioning multiple IPsec tunnels per VPN connection.

Routing between the private network and the cloud provider VPC can be done via either static routes or dynamic routing, typically using the Border Gateway Protocol (BGP) between autonomous systems. Static routing may be sufficient for single VPCs in a non-high-availability design. However, for designs with redundant customer VPN gateways, BGP routing provides automatic failover in the event of a failure of one of the customer VPN gateways or IPsec VPN tunnels.

The network administrator should note that having multiple paths does not necessarily mean load-balancing of traffic across both customer VPN gateways, or across the IPsec VPN connections, when using BGP. BGP routing will select a single path between autonomous systems (in each direction) unless BGP multipath is supported and configured. A single path does not necessarily mean symmetric routing, either: as shown in Figure 3, traffic to the VPC could pass through one customer VPN gateway while return traffic from the VPC could pass through the other customer VPN gateway.
Asymmetric routing can also be considered. However, there are some situations in which it is undesirable. In particular, if stateful firewalling is implemented on the customer VPN gateways, it may not function correctly unless return traffic from the VPC passes through the same customer VPN gateway interface as the traffic that was sent to the VPC. Also, Cisco Application Visibility and Control (AVC) running on the customer VPN gateways may not function correctly with asymmetric routing. In order to correctly classify some applications, AVC must have visibility into the first few packets of the flow in both directions.

The network administrator can ensure symmetric routing via several methods. For example, when redistributing routes learned through BGP into an Interior Gateway Protocol (IGP), the network administrator can modify the routing metrics to make one of the customer VPN gateways more favorable from the viewpoint of the IGP. All internal routers will then send traffic destined to the VPC to only one of the customer VPN gateways. To make one of the customer VPN gateways more favorable from a BGP perspective to the cloud provider’s VPN gateways, techniques such as autonomous system prepending can be implemented on the customer VPN gateways. Both of the above methods assume that both the customer VPN gateways are active. Another alternative is to simply deploy a set of VPN gateways in an active/standby configuration, as is often done with stateful firewalls that have VPN functionality. In this case, the choice of the customer VPN gateway platform helps guide the method by which symmetric routing between the private network and the VPC is achieved.
When implementing connectivity to cloud provider services deployed within VPCs, the network administrator must also take into account the network security policies of the organization. For example, the security policy of some organizations may require that all traffic that exits a physical site of the organization toward the Internet be sent through a stateful firewall that implements Network Address Translation (NAT). This may require a stateful firewall to be placed in front of any dedicated VPN gateways that establish IPsec connections to cloud provider VPCs. A benefit of this design is that the stateful firewall can be configured to block all connections initiated from the Internet inbound toward the VPN gateways – essentially allowing the VPN gateways at the private network to establish connections only out to the VPC. However, it also may force the use of NAT between the private network and the VPC. In such scenarios, the network administrator must ensure that the VPN gateways support features such as NAT Traversal (NAT-T), and that the stateful firewall in front of the VPN gateways is configured for NAT. This could mean 1:1 static NAT translations from publicly routable IP addresses to the internal private IP addresses of the VPN gateways. Alternatively, it may be possible to implement Port Address Translation (PAT) to the outside publicly routable IP address of the firewall in some designs.

The single VPC design shown in Figure 3 above can easily be extended to support a small number of VPCs, either from the same or from multiple cloud providers. An example is shown in Figure 4.

Figure 4. Private network to cloud provider: IPsec VPN connection to a small number of VPCs
As can be seen from the above figure, when the number of VPCs increases, the number of IPsec VPN tunnels also increases, increasing the complexity of the configuration of the VPN gateways deployed at the customer network as well as decreasing the overall scalability of the design. Another disadvantage of this design is that all cloud-to-cloud traffic (traffic between VPCs) must be sent through the private network. This may be suboptimal from a latency perspective, if the private network site is geographically distant from the VPC locations. It may also be suboptimal from a bandwidth perspective, because the bandwidth of the private network is unnecessarily being used for traffic that does not originate or terminate at the private network.

An alternative to supporting cloud-to-cloud traffic is to implement a transit VPC design. This will be discussed further in the Cloud to Cloud Transit VPC Design section below.

**Cloud to private data center via dedicated network connection**

Although an IPsec VPN connection provides the ability to rapidly deploy connectivity to a VPC, it does not provide much, if any, ability to control key parameters such as bandwidth, latency, jitter, and packet loss between the private network and the cloud provider network. An alternative design is to deploy dedicated network connectivity between the private network and the VPC. An example of a single VPC deployment using a dedicated network connection is shown in Figure 5.

**Figure 5.** Private network to cloud provider: dedicated network connection to single VPC with high availability

The design in the figure shows a high-availability design. At the private network, high availability is accomplished by having two customer routers, each of which has a separate physical circuit from a partner or network carrier to a partner colocation site. The carrier can be a local partner, regional partner, or national carrier. Even with dedicated connectivity to the VPC, depending upon the security policy of the organization, a set of stateful firewalls (and possibly other security services) may be required at the private network, directly behind the routers that terminate the physical circuits to the colocation site.

Equipment within the colocation site must also be designed for resiliency, both within the customer-controlled cage and within the cloud provider-controlled cage. As discussed earlier, the network administrator must be careful to identify all areas within the design that require resiliency. This may include using separate entrance facilities at both the private network and the colocation site for each circuit, or possibly connectivity from separate physical private network locations. Note that an even greater level of high availability could be achieved by having each circuit terminate at a separate colocation site.
Within the colocation site, the physical circuits terminate on equipment (generally routers and/or switches) within the customer cage. Typically 1-Gbps or 10-Gbps cross-connects are established between the equipment within the customer cage and the equipment within the cloud provider cage. Some colocation partners offer an exchange service that allows them to groom connections from multiple cloud providers into a single high-availability pair of connections to the customer cage. This saves the costs associated with pulling individual fiber-optic cross-connects from each cloud provider cage to the customer cage. This approach may give the colocation partner the ability to offer sub-line-rate services below 1-Gbps or 10-Gbps connectivity as well. An example of such an exchange service is the Equinix Cloud Exchange Fabric. Figure 6 shows an example of a high-availability design with an exchange service.

Figure 6. Private network to cloud provider: dedicated network connection through colocation partner single VPC with high availability

Dynamic routing, using External BGP (EBGP) peering and 802.1q tagged VLANs (generally one per VPC), is implemented between the equipment within the customer cage and the equipment within the cloud provider cage. Connectivity between the cloud provider cage and the actual VPCs is through the cloud provider’s network. This may involve configuring logical virtual connections through the cloud provider’s web-based console, Command-Line Interface (CLI), or APIs.

Advantages and disadvantages of IPsec VPN vs. dedicated network connection
Table 1 summarizes, at a high level, the advantages and disadvantages of each of the methods of connectivity to the cloud provider.

<table>
<thead>
<tr>
<th>IPsec VPN over the Internet</th>
<th>Dedicated network connection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td><strong>Advantages</strong></td>
</tr>
<tr>
<td>● Generally lower cost</td>
<td>● Ability to control key SLA parameters of latency, jitter, bandwidth, and packet loss over a dedicated connection</td>
</tr>
<tr>
<td>● Greater flexibility and more rapid deployment</td>
<td></td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td><strong>Disadvantages</strong></td>
</tr>
<tr>
<td>● Little to no ability to control key SLA parameters of latency, jitter, bandwidth, and packet loss over the Internet</td>
<td>● Generally higher cost</td>
</tr>
<tr>
<td></td>
<td>● Less flexibility and longer deployment times</td>
</tr>
</tbody>
</table>
The customer use case behind the provisioning of cloud connectivity will often guide the network administrator as to which connectivity option is the better choice. For example, if rapid deployment and teardown of VPCs are required for prototyping new applications, where the performance of the network connectivity is less of a concern, then IPsec VPN connectivity may be the better option. However, if deployment of the VPC is for housing long-term internal production applications, in which performance degradation will result in productivity loss within the organization, dedicated connectivity may be the better option.

**Cloud-to-cloud transit VPC design**

As discussed in the above Cloud to Private Data Center via IPsec VPN section, backhauling all cloud-to-cloud traffic (traffic between VPCs) through the private network may be a suboptimal design from a latency and bandwidth perspective. An alternative to supporting cloud-to-cloud traffic, when implementing IPsec VPN connectivity to VPCs, is to implement a transit VPC design. An example of a transit VPC design with high availability is shown in Figure 7.

**Figure 7.** Cloud to cloud: IPsec VPN connectivity with transit VPC design

**Technical note:** Although the VPN connectivity is established based on publicly routable IP addresses, traffic does not necessarily traverse the Internet. For a transit VPC design involving a single cloud provider, the traffic may ride over the cloud provider’s private network.

Most cloud providers allow traffic between different VPCs within a single region – and recently, for some cloud providers, between regions. However, most cloud providers do not allow traffic to transit a VPC; meaning that traffic must originate or terminate within a VPC, not simply pass through it. This means that as the number of VPCs increases, the amount of peering between the VPCs increases dramatically, if full connectivity between VPCs is desired.
A transit VPC is designed to ease this issue. With a transit VPC design, a pair of redundant Cisco CSR 1000V Routers is implemented within a VPC dedicated to function simply as a transit point for traffic between other VPCs. The cloud provider VPN gateway at each nontransit VPC establishes a VPN connection to each CSR 1000V router within the transit VPC.

**Technical note:** Depending upon the specific cloud provider implementation, each VPN connection can consist of two IPsec tunnels, as is done with the AWS VPN connection and AWS virtual private gateway (VGW).

Another advantage of the transit VPC design is that it is fully automated for some cloud providers. For example, with the transit VPC design of AWS, the network administrator simply configures a tag within the spoke VPC, indicating that the spoke is to be connected to a transit VPC. AWS will then automatically provision the VPN connectivity between the spoke VPC and the transit VPC.

Although the transit VPC design allows cloud-to-cloud traffic flows, most organizations also require connectivity into their private networks. The transit VPC design can be extended by manually configuring additional IPsec VPN connections between the CSR 1000V routers within the transit VPC and the customer VPN gateways deployed within the private network. An example of a transit VPC with high-availability private network connectivity is shown in Figure 8.

**Figure 8.** Cloud to cloud: IPsec VPN transit VPC design with private network

The transit VPC can also serve as a centralized location for controlling access between VPCs, both within a single cloud provider and between different cloud providers. Additional cloud provider VPC IPsec VPN connections can be manually configured on the transit VPC Cisco CSR 1000V Routers, similar to the private network connections.
Access to and from the private network can also be controlled at the transit VPC. As with the direct-access designs discussed earlier, access control can take various forms:

- Simple route leaking, which provides a very coarse subnet-level access control
- Implementing Cisco TrustSec® on the Cisco CSR 1000V Routers, which provides group-based policy and more granular access control
- Implementing stateful firewalls within the Cisco CSR 1000V Routers, which provides very granular access control
- Implementing network virtualization techniques, which provides both network and path isolation of traffic. Network virtualization techniques may need to be extended all the way back into the private network locations

If stateful firewalls are implemented within the transit VPC, the network administrator must ensure that routing of traffic is symmetrical through one of the two Cisco CSR 1000V Routers within the transit VPC. For AWS, this can be done automatically through a setting that configures autonomous system path prepending on the Cisco CSR 1000V Routers through the use of route-map statements.

**Scalable dedicated network connection designs**

As with IPsec VPN designs, the single VPC dedicated network connection design, discussed in the “Cloud to private data center via dedicated network connection” section, can be extended to support multiple VPCs from the same cloud provider or from multiple cloud providers, and to cloud-to-cloud as well as cloud-to-private data center connectivity. An example of a more complex dedicated network connection design is shown in Figure 9.

*Figure 9. Dedicated network connection: multiple private network sites to multiple VPCs with high availability*
Multiple VPCs from the same cloud provider can be accommodated simply by adding additional 802.1q tagged VLANs between the equipment within the customer cage and the equipment within the cloud provider cage and configuring additional logical virtual connections to the VPCs.

Additional cloud provider VPCs can be accommodated by provisioning cross-connects between the other cloud provider’s cage and the existing customer cage, without necessarily having to deploy more equipment within the colocation site. Alternatively, as shown in the figure above, the colocation partner exchange service can groom the various cloud provider connections into a single set of redundant connections to the customer cage.

In some scenarios, the private network may have multiple sites that require dedicated network connections into cloud provider networks. Such sites may be geographically dispersed. Each private network site can use local, regional, or national carrier networks to connect to the most optimal (depending upon available bandwidth, cost, etc.) colocation facility. A dedicated network connection from that colocation facility into one cloud provider’s network may be provisioned. However, existing connectivity into other cloud providers’ networks may use high-speed connectivity between the colocation partner sites, as shown in the figure above. This provides an alternative to provisioning additional dedicated network connections into existing cloud provider networks at each colocation site. Private network sites can also use high-speed, low-cost local, or regional carrier networks to connect into colocation sites that do not have dedicated network connections into cloud provider networks, and use the high-speed backbone of the colocation network to connect to sites that do have dedicated network connections into cloud provider networks. This can potentially provide an alternative to national carrier networks.

Since traffic between VPCs from the same cloud provider, or between different cloud providers, passes through the equipment within the customer cage of the colocation site, cloud-to-cloud traffic (traffic between VPCs) does not have to be sent through the private network. This may be more optimal from a latency perspective, particularly if the private network site is geographically distant from the VPC locations. It is also more optimal from a bandwidth perspective, because the bandwidth of the private network is not being used unnecessarily for traffic that does not originate or terminate at the private network.

Finally, the customer cage provides a centralized location for controlling access between VPCs, both within a single cloud provider and between different cloud providers. Access to and from the private network can also be controlled within the customer cage at the colocation site. Access control can take various forms:

- Simple route leaking, which provides a very coarse subnet level access control
- Implementing stateful firewalls, which provides very granular access control
- Implementing network virtualization techniques, which provides both network and path isolation of traffic.

Network virtualization techniques may need to be extended all the way back into the private network locations.
Branch-to-cloud designs

Dedicated network connectivity to a small number of private network locations, such as data centers and large regional sites, might be necessary to ensure that the key parameters such as bandwidth, latency, jitter, and packet loss between the private network and the cloud provider network are met. However, dedicated network connectivity may not be a cost-effective solution for connecting hundreds, or potentially thousands, of small branch locations to cloud provider VPCs. Transit VPC designs still result in the need to establish multiple IPsec VPN tunnels from each branch (in a high-availability design) to a transit VPC location. As the number of branches increases, the number of IPsec VPN tunnels that need to be configured on the transit VPC Cisco CSR 1000V routers becomes unmanageable and potentially not scalable. Also, all traffic has to pass through the transit VPC. With potentially thousands of branch locations, the transit VPC itself could become a bandwidth bottleneck for access to the cloud provider networks.

An alternative is to deploy technologies that dynamically provide site-to-site connectivity between branch locations and VPCs. Such technologies include the use of dynamic multipoint VPN (DMVPN) or the SD-WAN solution. Figure 10 provides an example of branch-to-cloud provider connectivity to a single VPC.

Figure 10. Branch to cloud provider: DMVPN or SD-WAN connectivity to a single VPC
With DMVPN, existing Cisco 4000 Series ISRs at branch locations can dynamically establish direct IPsec VPN connections to Cisco CSR 1000V Routers deployed on virtual machine instances within the cloud provider VPCs. With the SD-WAN solution, Cisco vEdge Routers at branch locations can dynamically establish direct IPsec VPN connections to Cisco vEdge Cloud routers deployed on virtual machine instances within the cloud provider VPCs. Connectivity to multiple VPCs can be accomplished by dynamically establishing additional direct IPsec VPN connections from the branch locations, as shown in Figure 11.

Figure 11. Branch to cloud provider – DMVPN or SD-WAN connectivity to multiple VPCs

There can be several advantages to implementing VNFs such as the Cisco CSR 1000V and/or vEdge Cloud router at the VPC, instead of using the native IPsec VPN service of the cloud provider gateway. In particular, feature support and flexibility are, generally, where VNFs provide a clear advantage over a cloud provider’s native IPsec VPN service. Most cloud provider native IPsec VPN services do not support DMVPN functionality. This means the ability to dynamically establish IPsec tunnels directly between endpoints as needed. Each cloud provider’s native IPsec VPN service offering is slightly different, so it is important to understand what is and is not supported before implementing either a native IPsec VPN service or a VNF. Some of the additional advantages and disadvantages of implementing a VNF over a cloud provider’s native IPsec VPN service are shown in Table 2.
Table 2. Advantages and disadvantages of VNF over a cloud provider native IPsec VPN service

<table>
<thead>
<tr>
<th>Third-party VNF such as Cisco CSR 1000V or vEdge Cloud router</th>
<th>Cloud provider native IPsec VPN service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages</td>
<td></td>
</tr>
<tr>
<td>• Site-to-site direct connectivity.</td>
<td>• The native IPsec VPN service of each cloud provider is always supported.</td>
</tr>
<tr>
<td>• Ability to support both IPv4 and IPv6 over IPsec VPN connections.</td>
<td>• Generally, the recurring cost of implementing the cloud provider native IPsec VPN service is slightly lower.</td>
</tr>
<tr>
<td>• More control over the deployment.</td>
<td>• Automation and orchestration of the cloud provider IPsec VPN service is generally provided by the cloud provider.</td>
</tr>
<tr>
<td>• The same technical knowledge can be extended to multiple public cloud providers (multiclouds) without an additional learning curve, especially if Cisco products are already in use within the private data center or branch offices.</td>
<td></td>
</tr>
<tr>
<td>Disadvantages</td>
<td></td>
</tr>
<tr>
<td>• Support for a particular third-party VNF, such as the Cisco CSR 1000V or vEdge Cloud router, depends on the particular cloud provider.</td>
<td>• May not support all IPsec VPN cipher suites (IKEv1 vs. IKEv2, etc.).</td>
</tr>
<tr>
<td>• Generally, the recurring cost of implementing the third-party VNF is slightly higher due to additional licensing costs for the use of the VNF software, as well as the costs of standing up and running the underlying virtual machine instance upon which the VNF runs.</td>
<td>• May support only IPv4 across the IPsec VPN connections.</td>
</tr>
<tr>
<td>• Although the deployment of a third-party VNF can be automated, it may require learning a different set of automation and/or orchestration tools built around the APIs supported by the particular VNF.</td>
<td>• Supports only static routing and dynamic routing using BGP.</td>
</tr>
</tbody>
</table>

## Additional considerations

This section discusses additional design considerations with regard to deploying multicloud designs.

### Path isolation

Whether or not path isolation of the traffic to and from VPCs is required within the private network depends on the business use case for deploying the VPCs, and the applications running on the virtual machine instances within each VPC. Depending upon where the end users of the applications that reside on the virtual machine instances within the VPC sit within the private network, this could mean extending the virtual network to the data center, to the building distribution modules, or even across the WAN to branch locations. Achieving this extension could involve the deployment of VLANs, VRFs, VRF-Lite, MPLS, Cisco Software-Defined Access (SD-Access), SD-WAN, or Cisco Application Centric Infrastructure (Cisco ACI™) technologies throughout the private network.

### Application visibility

With the increased use of cloud computing services, expenses shift from fixed costs for hardware, software, and data center infrastructure to variable costs based on the usage of compute resources and the amount of data transferred between the private data center and the cloud provider. Applications running on virtual machine instances within cloud provider networks are not usually under the administrative control of network operations personnel. However, the network administrator may need to monitor the usage of such resources for cost tracking and/or internal billing purposes.

Technologies such as AVC running on Cisco ASR 1000 Series, 4000 Series ISRs, or CSR 1000V Routers, which make use of the Cisco Next-Generation Network-Based Application Recognition (NBAR2) engine, provide visibility into which application flows are using the VPN or dedicated network connection between the private network and the VPC, as well as how much data is being sent. This visibility can prove valuable in managing the overall costs of the cloud computing service, and potentially simplify internal billing of the cost of the service back to the various internal organizations.
Export of flow information and telemetry to partner applications such as the LiveAction LiveNX network performance and analytics platform, or to Cisco DNA™ Analytics and Assurance, running on Cisco DNA Center™, can be used not only to monitor performance of the overall cloud computing service, but also to apply advanced analytics algorithms to uncover correlations and suggest remediation when issues arise.

Summary

This design guide has provided a high-level overview of various designs and methods for implementing connectivity to cloud provider networks. Private data center to cloud providers can be implemented using IPsec VPN, when flexibility and speed of deployment are of primary concern. When application performance is the primary concern, and key SLA parameters such as bandwidth, latency, jitter, and packet loss must be controlled, dedicated network connections to cloud providers may prove to be the better choice. Cloud-to-cloud designs can be scaled by implementing a transit VPC IPsec VPN design. With this design, all spoke-to-spoke VPC traffic passes through a dedicated transit VPC. The transit VPC design can easily be extended to the private network by configuring the private data center as another spoke of the transit VPC.

Colocation partner facilities, which also serve as dedicated network connection locations for cloud providers, can help scale and simplify dedicated network connection designs. Branch-to-cloud provider connectivity can be scaled by providing dynamic site-to-site connectivity from each branch to the cloud provider VPC, using technologies such as DMVPN or SD-WAN. Finally, the network administrator must take into account additional considerations such as requirements for access control and path isolation, as well as visibility into traffic to and from the cloud providers, when designing multicloud networks.

Additional resources

If you have further questions, refer to the following additional resources:

- LiveAction: https://www.liveaction.com
- Equinix: https://equinix.com
- Amazon Web Services: https://aws.amazon.com
● Google Cloud Platform:  
https://cloud.google.com  

● Microsoft Azure:  
https://azure.microsoft.com

For a complete list of all of our design and deployment guides for the Cisco Multicloud Portfolio, including Cloud Protect and Cloud Consume, visit http://www.cisco.com/go/clouddesignguides.

About Cisco design considerations and overview guides

Cisco design considerations and overview guides consist of design considerations and best practices of systems and/or solutions to facilitate optimal design selections and implementation approaches. For more information visit: https://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS, OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco Stadium Vision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDa, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, Giga Drive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2018 Cisco Systems, Inc. All rights reserved.