Amazon Virtual Private Cloud Connectivity Options

AWS Whitepaper

Amazon Virtual Private Cloud Connectivity Options: AWS Whitepaper

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Amazon Virtual Private Cloud Connectivity Options

Publication date: **June 6, 2020** (*Document revisions* (p. 35))

Abstract

Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the Amazon Web Services (AWS) Cloud where they can launch AWS resources in a virtual network using customer-defined IP address ranges. Amazon VPC provides customers with several options for connecting their AWS virtual networks with other remote networks. This document describes several common network connectivity options available to our customers. These include connectivity options for integrating remote customer networks with Amazon VPC and connecting multiple Amazon VPCs into a contiguous virtual network.

This whitepaper is intended for corporate network architects and engineers or Amazon VPC administrators who would like to review the available connectivity options. It provides an overview of the various options to facilitate network connectivity discussions as well as pointers to additional documentation and resources with more detailed information or examples.

Introduction

Amazon VPC provides multiple network connectivity options for you to use, depending on your current network designs and requirements. These connectivity options include using either the internet or an AWS Direct Connect connection as the network backbone and terminating the connection into AWS or user-managed network endpoints. Additionally, with AWS, you can choose how network routing is delivered between Amazon VPC and your networks, leveraging either AWS services or user-managed network equipment and routes. This whitepaper considers the following options with an overview and a high-level comparison of each:

- Network-to-Amazon VPC connectivity options (p. 4)
  - AWS Managed VPN (p. 6) – Describes establishing a VPN connection from your network equipment on a remote network to AWS managed service attached to your Amazon VPC.
  - AWS Transit Gateway + VPN (p. 7) – Describes establishing a VPN connection from your network equipment on a remote network to a regional network hub for Amazon VPCs, using AWS Transit Gateway.
  - AWS Direct Connect (p. 9) - Describes establishing a private, logical connection from your remote network to Amazon VPC, using AWS Direct Connect.
  - AWS Direct Connect + AWS Transit Gateway (p. 11) – Describes establishing a private, logical connect from your remote network to a regional network hub for Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
  - AWS Direct Connect + VPN (p. 12) – Describes establishing a private, encrypted connection from your remote network to Amazon VPC, using AWS Direct Connect.
  - AWS Direct Connect + AWS Transit Gateway + VPN (p. 13) – Describes establishing a private, encrypted connection from your remote network to a regional network hub for Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
  - AWS VPN CloudHub (p. 14) – Describes establishing a hub-and-spoke model for connecting remote branch offices.
  - Software Site-to-Site VPN (p. 15) – Describes establishing a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC.
- Amazon VPC-to-Amazon VPC connectivity options (p. 17)
  - VPC peering (p. 18) – Describes connecting Amazon VPCs within and across regions using the Amazon VPC peering feature.
  - AWS Transit Gateway (p. 20) – Describes connecting Amazon VPCs within and across regions using AWS Transit Gateway in a hub-and-spoke model.
  - Software Site-to-Site VPN (p. 21) – Describes connecting Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
  - Software VPN-to-AWS Managed VPN (p. 22) – Describes connecting Amazon VPCs with a VPN connection established between a user-managed software VPN appliance in one Amazon VPC and AWS managed VPN attached to the other Amazon VPC.
  - AWS Managed VPN (p. 22) – Describes connecting Amazon VPCs with VPN connections between your remote network and each of your Amazon VPCs.
  - AWS PrivateLink (p. 24) – Describes connecting Amazon VPCs with VPC interface endpoints and VPC endpoint services.
- Software remote access-to-Amazon VPC connectivity options (p. 25)
  - AWS Client VPN (p. 25) – Describes connecting software remote access to Amazon VPC, leveraging AWS Client VPN.

    - Software client VPN (p. 26) – Describes connecting software remote access to Amazon VPC, leveraging user-managed software VPN appliances.

- Transit VPC option (p. 28)
    - Describes establishing a global transit network on AWS using a software VPN in conjunction with an AWS-managed VPN.

Network-to-Amazon VPC connectivity options

This section provides design patterns for connecting remote networks with your Amazon VPC environment. These options are useful for integrating AWS resources with your existing on-site services (for example, monitoring, authentication, security, data or other systems) by extending your internal networks into the AWS Cloud. This network extension also allows your internal users to seamlessly connect to resources hosted on AWS just like any other internally facing resource.

VPC connectivity to remote customer networks is best achieved when using non-overlapping IP ranges for each network being connected. For example, if you'd like to connect one or more VPCs to your home network, make sure they are configured with unique Classless Inter-Domain Routing (CIDR) ranges. We recommend allocating a single, contiguous, non-overlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions.

Option	Use Case	Advantages	Limitations
AWS Managed VPN (p. 6)	AWS managed IPsec VPN connection over the internet to individual VPC	Reuse existing VPN equipment and processes Reuse existing internet connections AWS managed high availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies	Network latency, variability, and availability are dependent on internet conditions Customer managed endpoint is responsible for implementing redundancy and failover (if required) Customer device must support single-hop BGP (when leveraging BGP for dynamic routing)
AWS Transit Gateway + VPN (p. 7)	AWS managed IPsec VPN connection over the internet to regional router for multiple VPCs	Same as the previous option AWS managed high availability and scalability regional network hub for up to 5,000 attachments	Same as the previous option
AWS Direct Connect (p. 9)	Dedicated network connection over private lines	More predictable network performance Reduced bandwidth costs Supports BGP peering and routing policies	May require additional telecom and hosting provider relationships or new network circuits to be provisioned

Option	Use Case	Advantages	Limitations
AWS Direct Connect + AWS Transit Gateway (p. 11)	Dedicated network connection over private lines to regional router for multiple VPCs	Same as the previous option AWS managed high availability and scalability regional network hub for up to 5,000 attachments	Same as previous option
AWS Direct Connect + VPN (p. 12)	IPsec VPN connection over private lines	More predictable network performance Reduced bandwidth costs Supports BGP peering and routing policies on AWS Direct Connect Reuse existing VPN equipment and processes AWS managed high availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies on VPN connection	May require additional telecom and hosting provider relationships or new network circuits to be provisioned Customer managed endpoint is responsible for implementing redundancy and failover (if required) Customer device must support single-hop BGP (when leveraging BGP for dynamic routing)
AWS Direct Connect + AWS Transit Gateway + VPN (p. 13)	IPSec VPN connection over private lines to regional router for multiple VPCs	Same as previous option AWS managed high availability and scalability regional network hub for up to 5,000 attachments	Same as previous option
AWS VPN CloudHub (p. 14)	Connect remote branch offices in a hub-and-spoke model for primary or backup connectivity	Reuse existing internet connections and AWS VPN connections AWS managed high availability VPN service Supports BGP for exchanging routes and routing priorities	Network latency, variability, and availability are dependent on the internet User managed branch office endpoints are responsible for implementing redundancy and failover (if required)

Option	Use Case	Advantages	Limitations
Software Site-to-Site VPN (p. 15)	Software appliance-based VPN connection over the internet	Supports a wider array of VPN vendors, products, and protocols Fully customer-managed solution	Customer is responsible for implementing HA (high availability) solutions for all VPN endpoints (if required)

AWS Managed VPN

Amazon VPC provides the option of creating an IPsec VPN connection between your remote networks and Amazon VPC over the internet, as shown in the following figure.

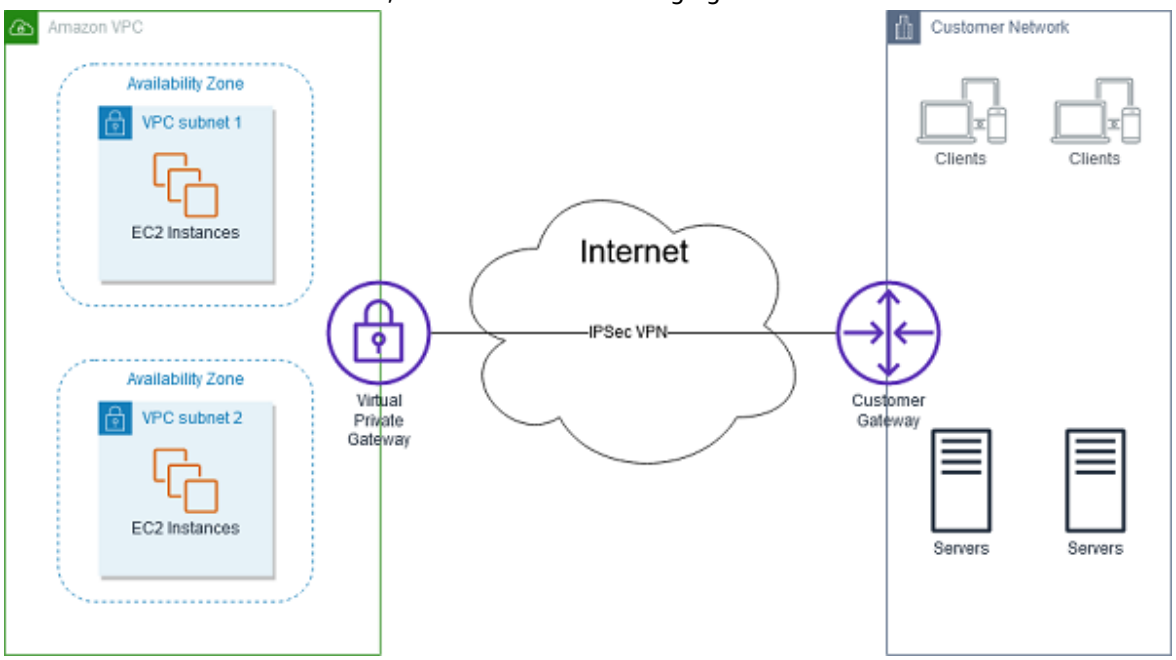

Figure 1 - AWS Managed VPN

Consider taking this approach when you want to take advantage of an AWS-managed VPN endpoint that includes automated redundancy and failover built into the AWS side of the VPN connection.

The virtual private gateway also supports and encourages multiple user gateway connections so that you can implement redundancy and failover on your side of the VPN connection, as shown in the following figure.

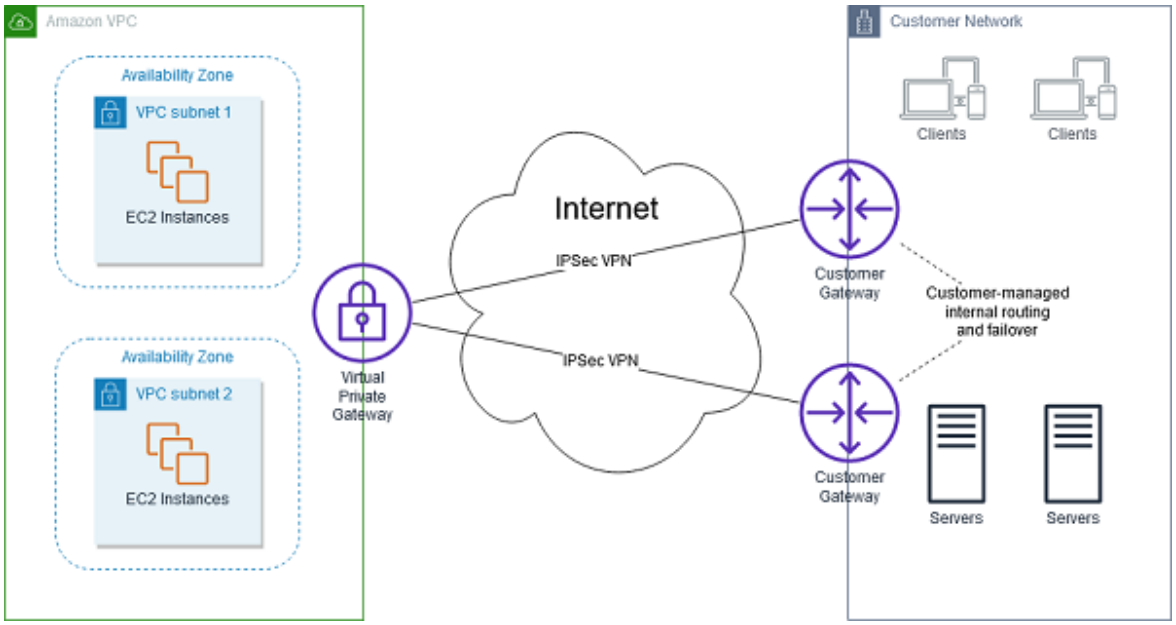

Figure 2 - Redundant AWS Managed VPN Connections

Both dynamic and static routing options are provided to give you flexibility in your routing configuration. Dynamic routing uses BGP peering to exchange routing information between AWS and these remote endpoints. With dynamic routing, you can also specify routing priorities, policies, and weights (metrics) in your BGP advertisements and influence the network path between your networks and AWS. It's important to note that when you use BGP, both the IPSec and the BGP connections must be terminated on the same user gateway device, so it must be capable of terminating both IPSec and BGP connections.

Additional resources

- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

AWS Transit Gateway + VPN

AWS Transit Gateway is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks. AWS Transit Gateway + VPN, using the Transit Gateway VPN attachment, provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet, as shown in the following figure.

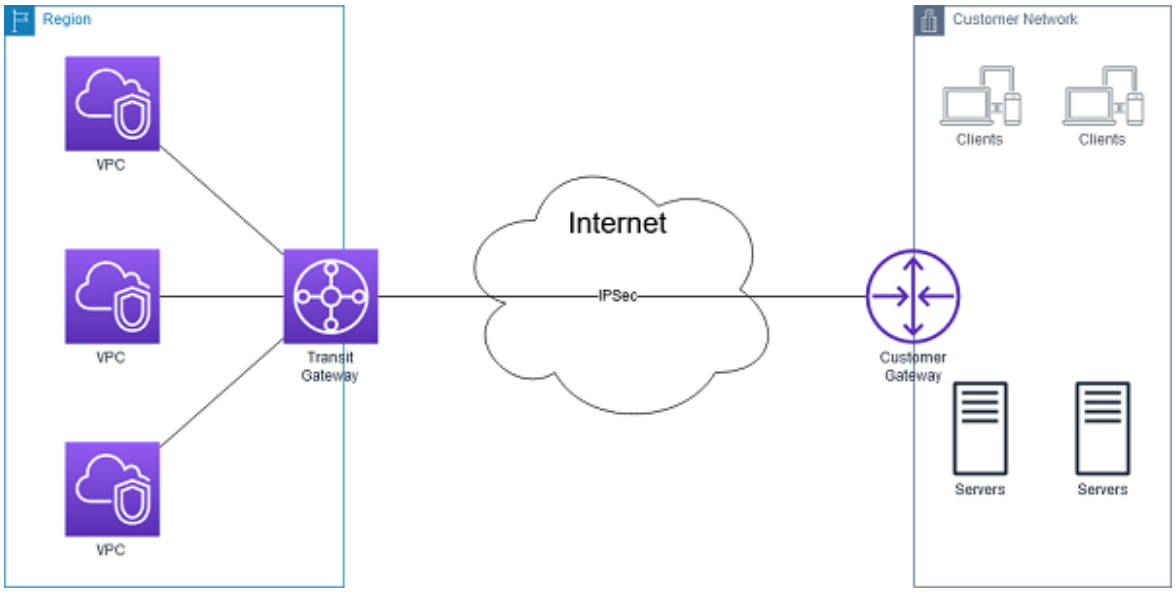

Figure 3 - AWS Transit Gateway and VPN

Consider using this approach when you want to take advantage of an AWS-managed VPN endpoint for connecting to multiple VPCs in the same region without the additional cost and management of multiple IPSec VPN connections to multiple Amazon VPCs.

AWS Transit Gateway also supports and encourages multiple user gateway connections so that you can implement redundancy and failover on your side of the VPN connection as shown in the following figure.

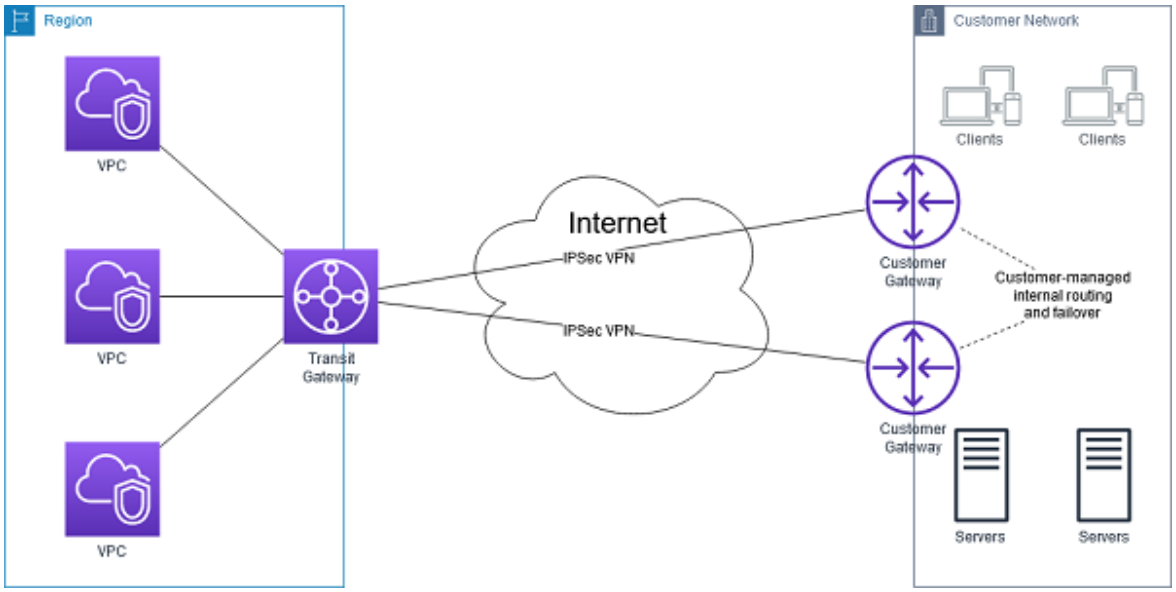

Figure 4 - AWS Transit Gateway and Redundant VPN

Both dynamic and static routing options are provided to give you flexibility in your routing configuration on the Transit Gateway VPN IPSec attachment. Dynamic routing uses BGP peering to exchange routing information between AWS and these remote endpoints. With dynamic routing, you can also specify routing priorities, policies, and weights (metrics) in your BGP advertisements and influence the network path between your networks and AWS. It's important to note that when you use BGP, both the IPSec

and the BGP connections must be terminated on the same user gateway device, so it must be capable of terminating both IPSec and BGP connections.

Additional resources

- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more VPCs in the same region. Using private VIF on AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, as shown in the following figure.

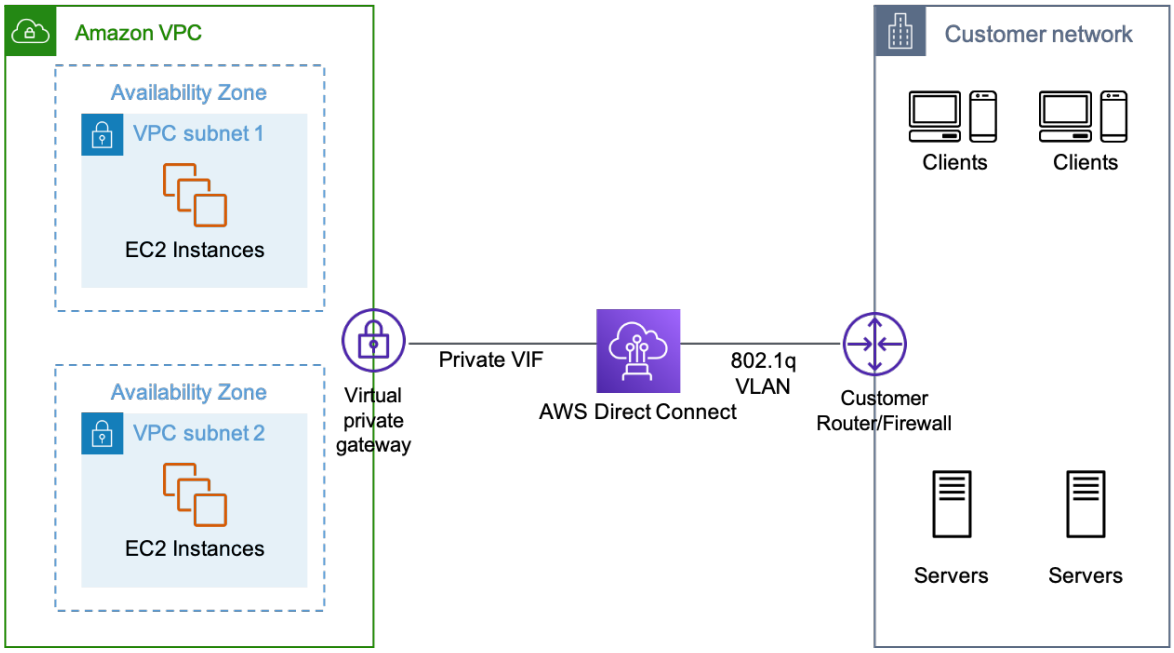

Figure 5 - AWS Direct Connect

Multiple dynamically routed AWS Direct Connect connections are necessary to support high availability, as shown in the following figure.

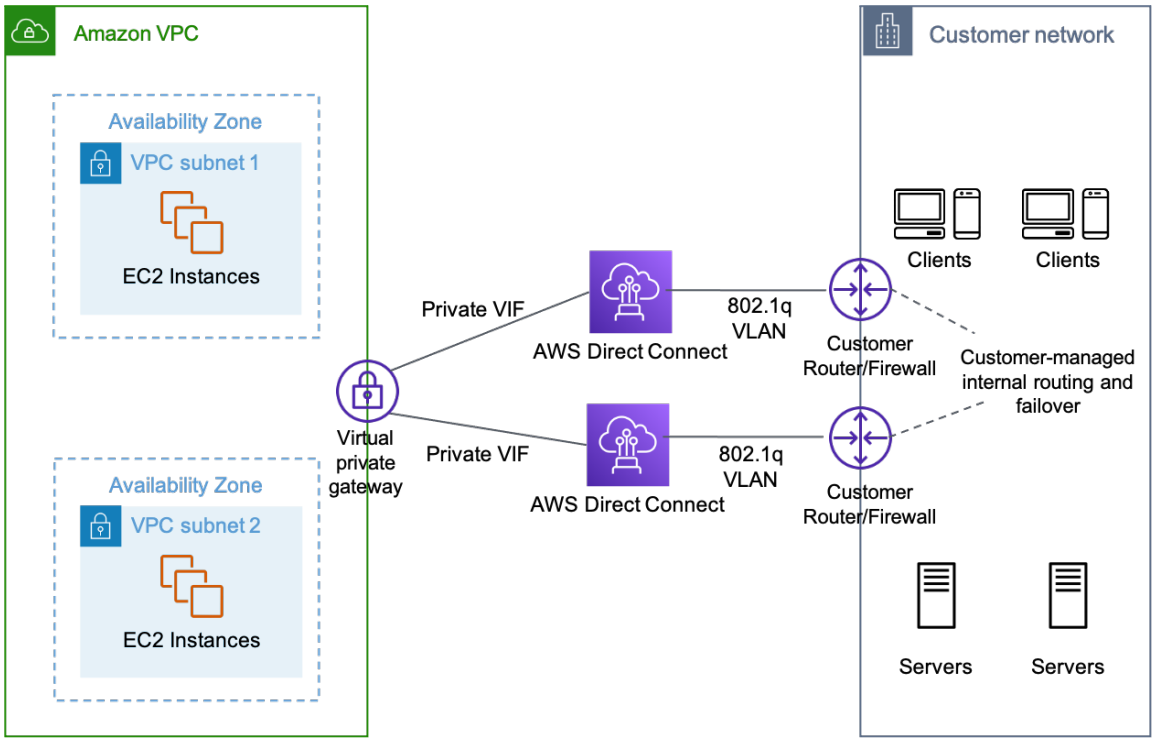

Figure 6 - Redundant AWS Direct Connect

AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. It uses industry-standard 802.1q VLANs to connect to Amazon VPC using private IP addresses. You can choose from an ecosystem of WAN service providers for integrating your AWS Direct Connect endpoint in an AWS Direct Connect location with your remote networks. AWS Direct Connect lets you establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations. You can also work with your provider to create sub-1G connection or use link aggregation group (LAG) to aggregate multiple 1 gigabit or 10 gigabit connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

A Direct Connect gateway is a globally available resource to enable connections to multiple Amazon VPCs across different regions or AWS accounts. This feature also allows you to connect to any participating VPCs from one private VIF, reducing AWS Direct Connect management, as shown in the following figure.

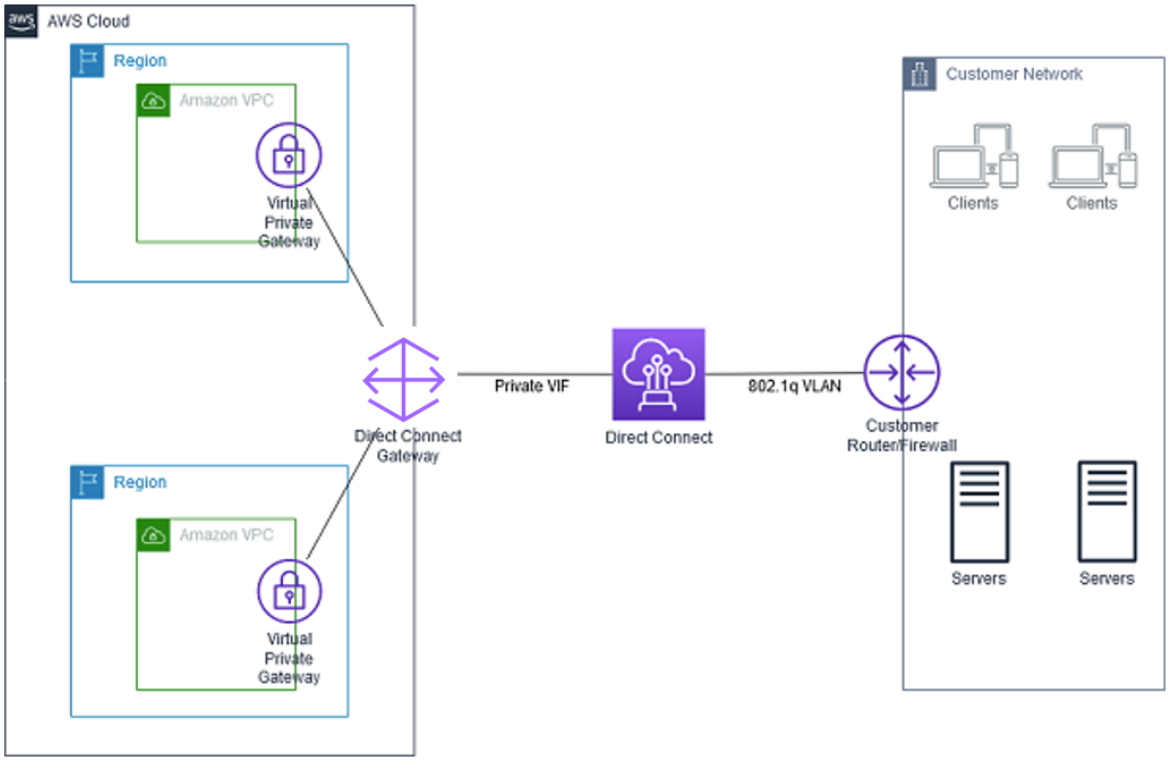

Figure 7 - AWS Direct Connect Gateway

Additional resources

- AWS Direct Connect User Guide
- AWS Direct Connect virtual interfaces

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect + AWS Transit Gateway, using transit VIF attachment to Direct Connect gateway, enables your network to connect up to three regional centralized routers over a private dedicated connection, as shown in the following diagram.

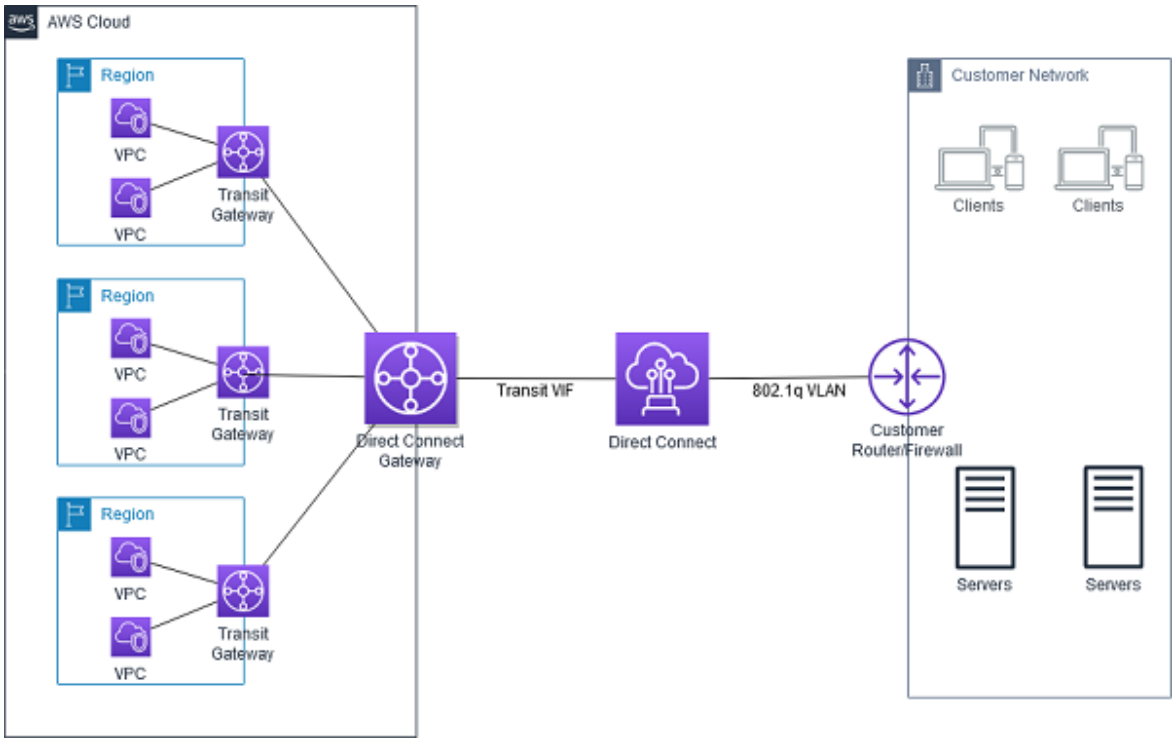

Figure 8 - AWS Direct Connect and AWS Transit Gateway

Each AWS Transit Gateway is a network transit hub to interconnect VPCs in the same region, consolidating Amazon VPC routing configuration in one place. This solution simplifies management of connections between an Amazon VPC and your networks over a private connection that can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

Additional resources

- AWS Direct Connect User Guide
- Link aggregation groups in AWS Direct Connect
- Blog post: Integrating sub-1 Gbps hosted connections with AWS Transit Gateway

AWS Direct Connect + VPN

With AWS Direct Connect + VPN, you can combine AWS Direct Connect dedicated network connections with the Amazon VPC VPN. AWS Direct Connect public VIF establishes a dedicated network connection between your network to public AWS resources, such as an Amazon virtual private gateway IPsec endpoint. The following figure illustrates this option.

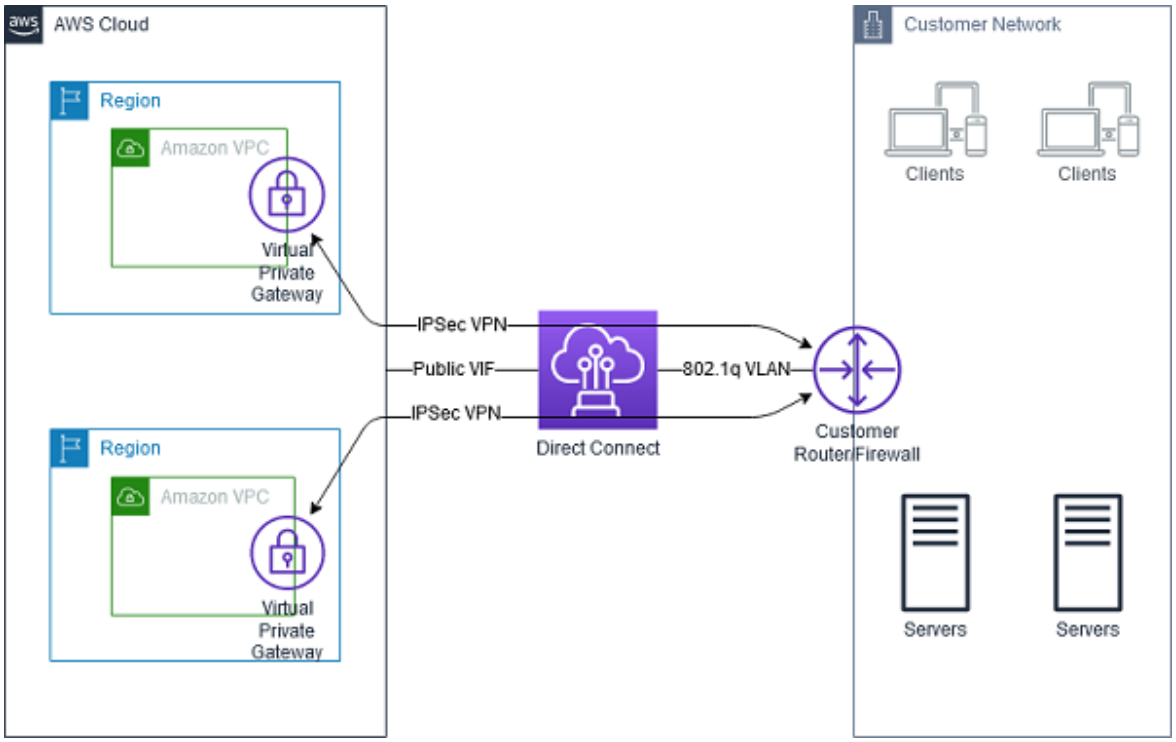

Figure 9 - AWS Direct Connect and VPN

This solution combines the benefits of the end-to-end secure IPSec connection with low latency and increased bandwidth of the AWS Direct Connect to provide a more consistent network experience than internet-based VPN connections. A BGP connection is established between the AWS Direct Connect and your router on the public VIF. Another BGP session or a static router will be established between the virtual private gateway and your router on the IPSec VPN tunnel.

Additional resources

- AWS Direct Connect
- AWS Direct Connect virtual interfaces
- AWS Site-to-Site VPN User Guide

AWS Direct Connect + AWS Transit Gateway + VPN

With AWS Direct Connect + AWS Transit Gateway + VPN, using public VIF on AWS Direct Connect, enables end-to-end IPSec-encrypted connections between your networks and a regional centralized router for Amazon VPCs over a private dedicated connection, as shown in the following figure.

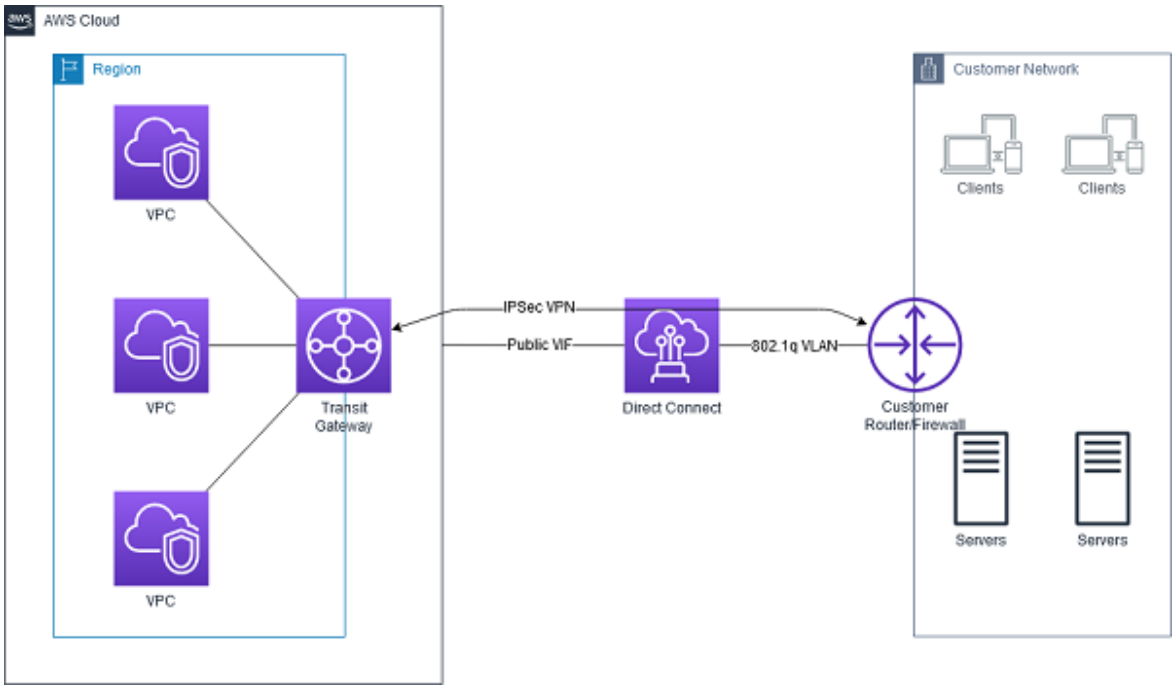

Figure 10 - AWS Direct Connect and AWS Transit Gateway and VPN

Consider taking this approach when you want to simplify management and minimize the cost of IPSec VPN connections to multiple Amazon VPCs in the same region, with the low latency and consistent network experience benefits of a private dedicated connection over an internet-based VPN. A BGP connection is established between the AWS Direct Connect and your router on the public VIF. Another BGP session or a static router will be established between the AWS Transit Gateway and your router on the IPSec VPN tunnel.

Additional resources

- AWS Direct Connect virtual interfaces
- Transit gateway VPN attachments
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

AWS VPN CloudHub

Building on the AWS managed VPN options described previously, you can securely communicate from one site to another using the AWS VPN CloudHub. The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. Use this approach if you have multiple branch offices and existing internet connections and would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

The following figure shows the AWS VPN CloudHub architecture, with dashed lines indicating network traffic between remote sites being routed over their AWS VPN connections.

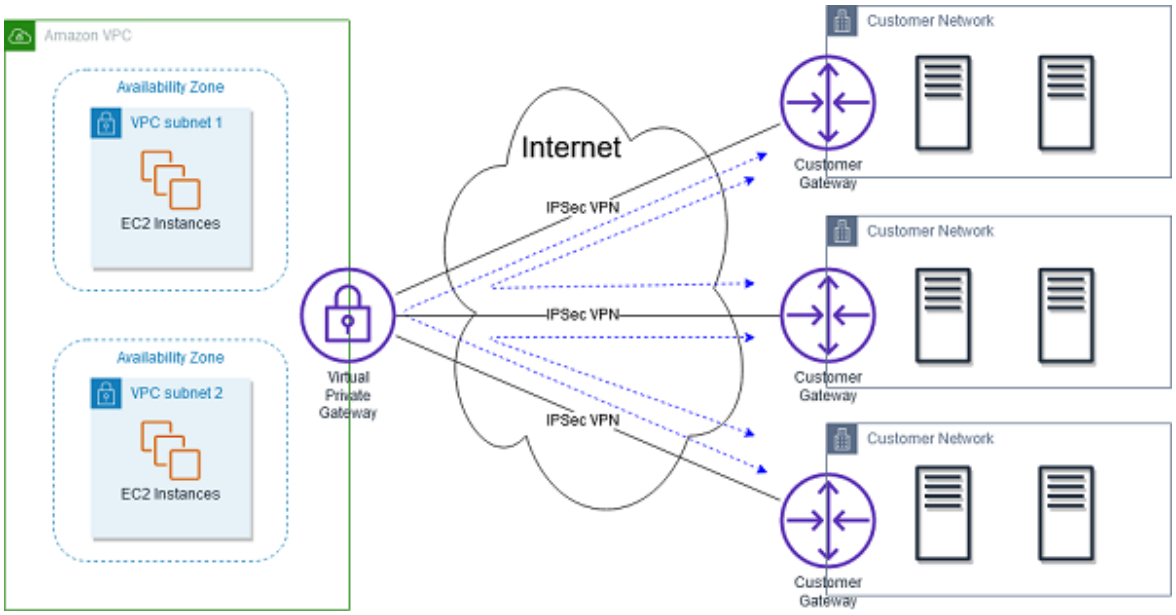

Figure 11 - AWS VPN CloudHub

AWS VPN CloudHub uses an Amazon VPC virtual private gateway with multiple customer gateways, each using unique BGP autonomous system numbers (ASNs). Your gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and re-advertised to each BGP peer so that each site can send data to and receive data from the other sites. The remote network prefixes for each spoke must have unique ASNs, and the sites must not have overlapping IP ranges.

Additional resources

- Providing secure communication between sites using VPN CloudHub
- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

Software Site-to-Site VPN

Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection, either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's VPN solution. The following figure shows this option.

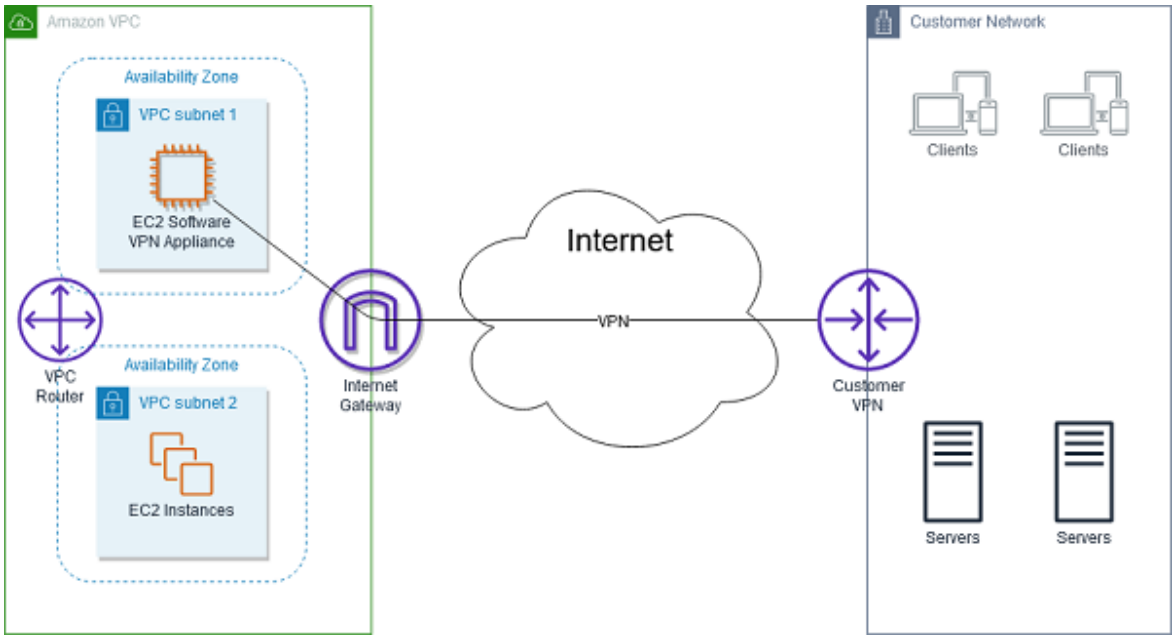

Figure 12 - Software Site-to-Site VPN

You can choose from an ecosystem of multiple partners and open source communities that have produced software VPN appliances that run on Amazon EC2. Along with this choice comes the responsibility that you must manage the software appliance, including configuration, patches, and upgrades.

Note that this design introduces a potential single point of failure into the network design because the software VPN appliance runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances (p. 31) Architecture for Software VPN Instances.

Additional resources

- VPN appliances available in the AWS Marketplace
- Tech Brief - Connecting Cisco ASA to VPC EC2 Instance (IPSec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPSec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

Amazon VPC-to-Amazon VPC connectivity options

Use these design patterns when you want to integrate multiple Amazon VPCs into a larger virtual network. This is useful if you require multiple VPCs due to security, billing, presence in multiple regions, or internal charge-back requirements, to more easily integrate AWS resources between Amazon VPCs. You can also combine these patterns with the Network–to–Amazon VPC connectivity options for creating a corporate network that spans remote networks and multiple VPCs.

VPC connectivity between VPCs is best achieved when using non-overlapping IP ranges for each VPC being connected. For example, if you'd like to connect multiple VPCs, make sure each VPC is configured with unique Classless Inter-Domain Routing (CIDR) ranges. Therefore, we advise you to allocate a single, contiguous, non-overlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions.

Option	Use Case	Advantages	Limitations
VPC peering (p. 18)	AWS-provided network connectivity between two VPCs.	Leverages AWS managed scalable networking infrastructure	VPC peering does not support transitive peering relationships Difficult to manage at scale
AWS Transit Gateway (p. 20)	AWS-provided regional router connectivity for VPCs	AWS managed high availability and scalability service Regional network hub for up to 5,000 attachments	
Software Site-to-Site VPN (p. 21)	Software appliance-based VPN connections between VPCs	Supports a wide array of VPN vendors, products, and protocols Managed entirely by you	You are responsible for implementing HA solutions for all VPN endpoints (if required) VPN instances could become a network bottleneck
Software VPN-to-AWS Managed VPN (p. 22)	Software appliance to VPN connection between VPCs	AWS managed high availability VPC VPN connection Supports a wide array of VPN vendors and products managed by you	You are responsible for implementing HA solutions for the software appliance VPN endpoints (if required) VPN instances could become a network bottleneck

Option	Use Case	Advantages	Limitations
		Supports static routes and dynamic BGP peering and routing policies	IPSec VPN protocol only to AWS Managed VPN
AWS Managed VPN (p. 22)	VPC-to-VPC routing managed by you over IPsec VPN connections using your equipment	Amazon managed high availability VPC VPN connections Supports static routes and dynamic BGP peering and routing policies	The endpoint you manage is responsible for implementing redundancy and failover (if required)
AWS PrivateLink (p. 24)	AWS-provided network connectivity between two VPCs using interface endpoints.	Leverages AWS managed scalable networking infrastructure	VPC Endpoint services only available in AWS region in which they are created.

VPC peering

A VPC peering connection is a networking connection between two VPCs that enables routing using each VPC's private IP addresses as if they were in the same network. VPC peering connections can be created between your own VPCs or with a VPC in another AWS account. VPC peering also supports inter-region peering.

Traffic using inter-region VPC Peering always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.

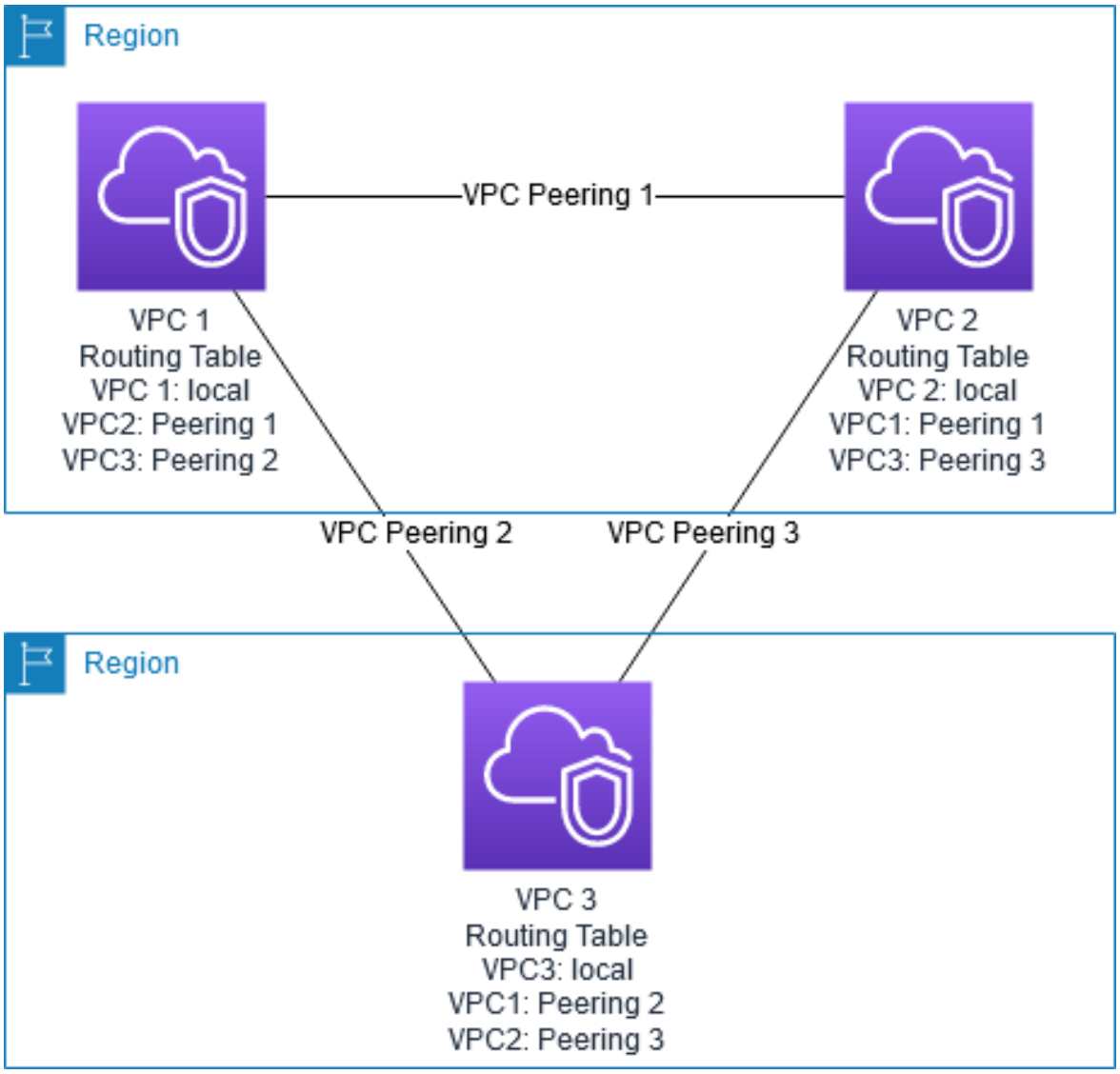

Figure 13 - VPC-to-VPC Peering

AWS uses the existing infrastructure of a VPC to create VPC peering connections and do not rely on a separate piece of physical hardware. Therefore, they do not introduce a potential single point of failure or network bandwidth bottleneck between VPCs. Additionally, VPC routing tables, security groups, and network access control lists can be leveraged to control which subnets or instances are able to utilize the VPC peering connection.

Additional resources

- Amazon VPC peering
- What is VPC peering?

AWS Transit Gateway

AWS Transit Gateway is a highly available and scalable service to consolidate the AWS VPC routing configuration for a region with a hub-and-spoke architecture. Each spoke VPC only needs to connect to the Transit Gateway to gain access to other connected VPCs. Transit Gateway across different regions can peer with each other to enable VPC communications across regions. With large number of VPCs, Transit Gateway provides simpler VPC-to-VPC communication management over VPC Peering, as shown in the following figure.

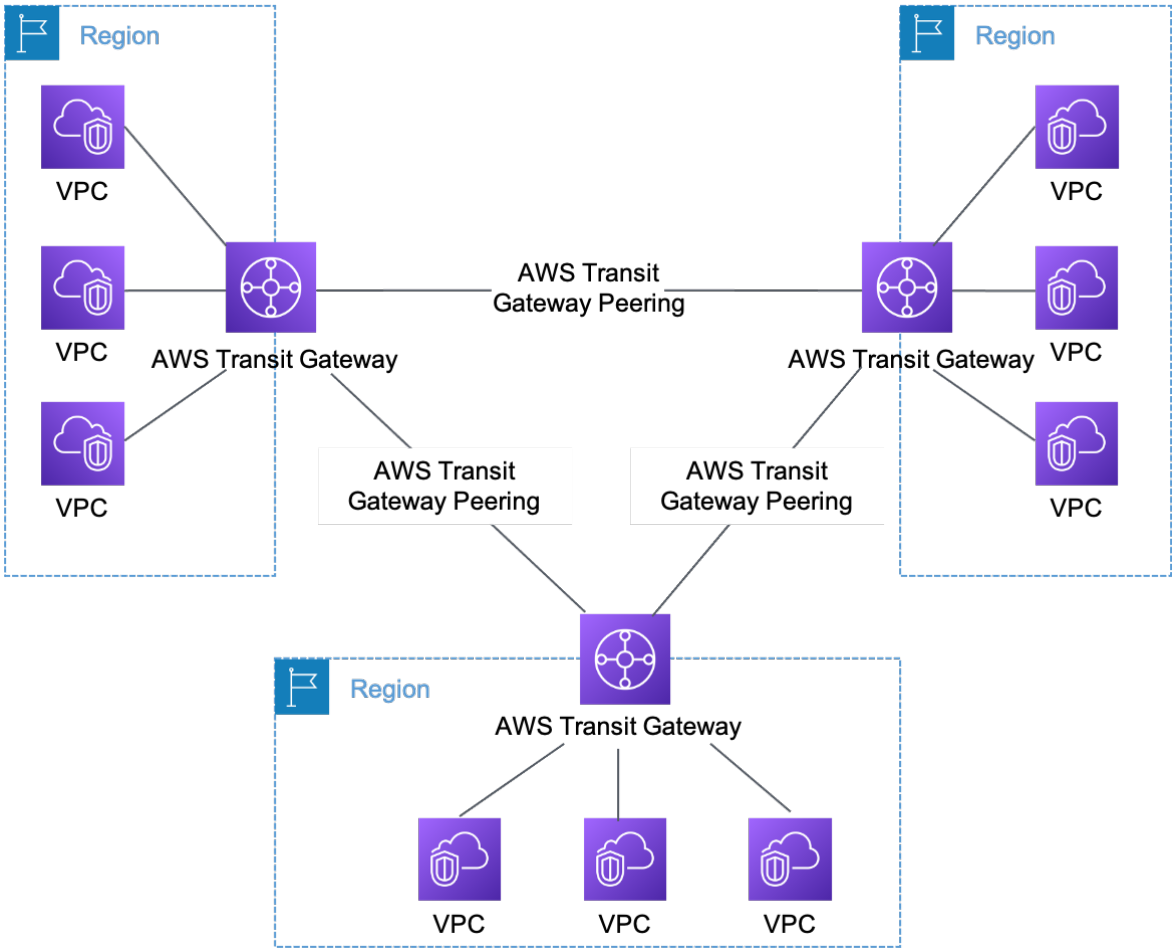

Figure 14 - AWS Transit Gateway

AWS Transit Gateway traffic always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.

Additional resources

- Amazon VPC transit gateway
- Transit gateway peering attachments

Software Site-to-Site VPN

Amazon VPC provides network routing flexibility. This includes the ability to create secure VPN tunnels between two or more software VPN appliances to connect multiple VPCs into a larger virtual private network so that instances in each VPC can seamlessly connect to each other using private IP addresses. This option is recommended when you want to manage both ends of the VPN connection using your preferred VPN software provider. This option uses an internet gateway attached to each VPC to facilitate communication between the software VPN appliances.

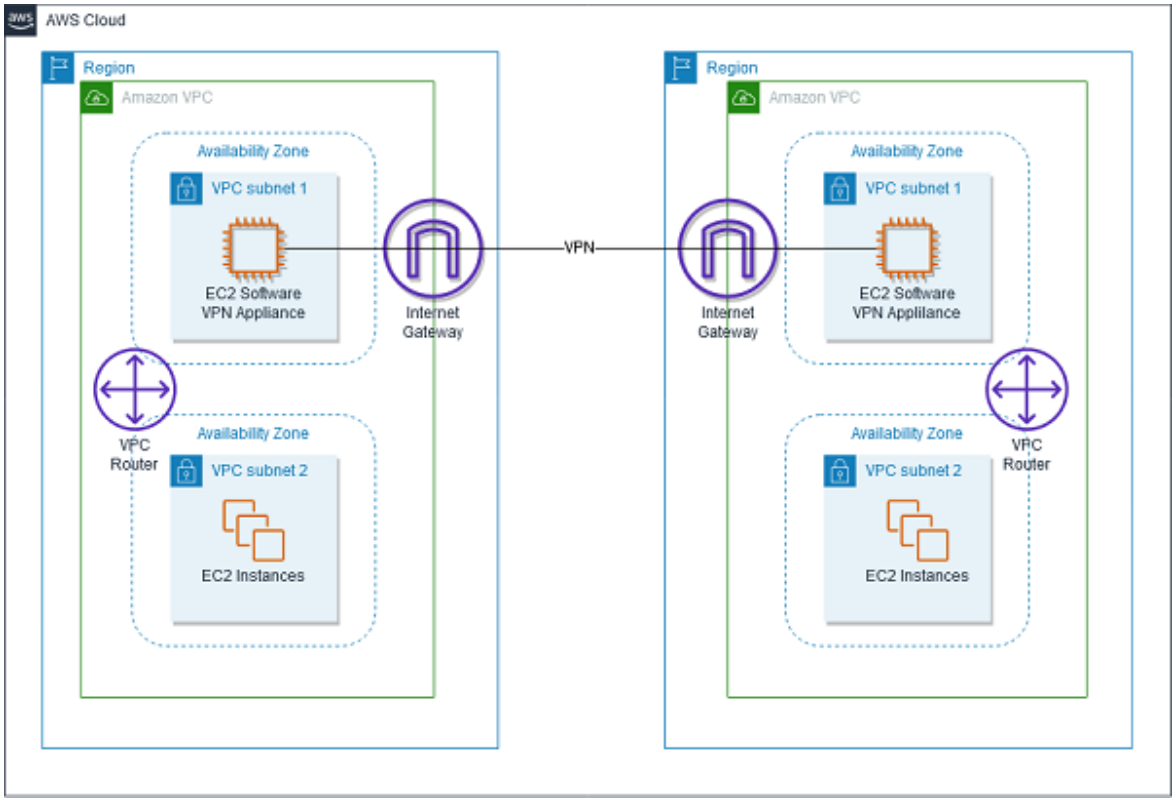

Figure 15 - Software Site-to-Site VPN VPC-to-VPC Routing

You can choose from an ecosystem of multiple partners and open source communities that have produced software VPN appliances that run on Amazon EC2. Along with this choice comes the responsibility for you to manage the software appliance including configuration, patches, and upgrades.

Note that this design introduces a potential single point of failure into the network design as the software VPN appliance runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances (p. 31).

Additional resources

- VPN appliances available from the AWS Marketplace
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPSec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

Software VPN-to-AWS Managed VPN

Amazon VPC provides the flexibility to combine the AWS managed VPN and software VPN options to connect multiple VPCs. With this design, you can create secure VPN tunnels between a software VPN appliance and a virtual private gateway, allowing instances in each VPC to seamlessly connect to each other using private IP addresses. This option uses a virtual private gateway in one Amazon VPC and a combination of an internet gateway and software VPN appliance in another Amazon VPC, as shown in the following figure.

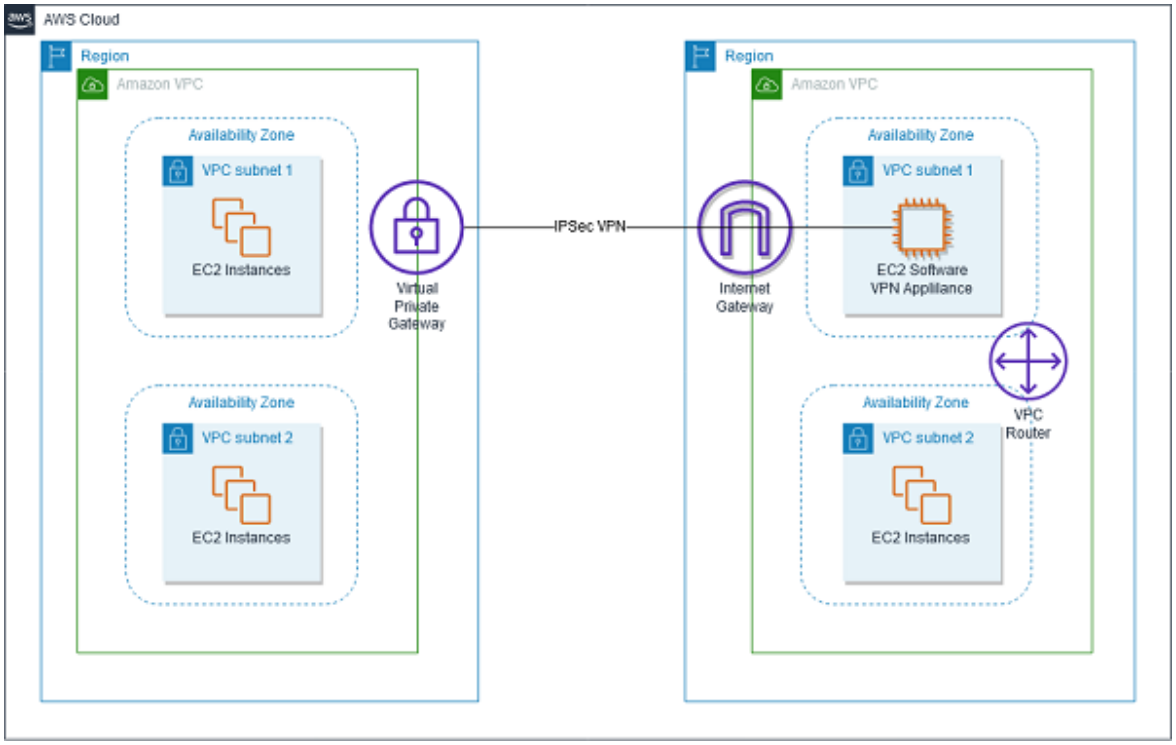

Figure 16 - Software VPN to AWS Managed VPN VPC-to-VPC Routing

Note that this design introduces a potential single point of failure into the network design. For additional information, see Appendix A: High-Level HA architecture for software VPN instances (p. 31).

Additional resources

- VPN appliances available from the AWS Marketplace
- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices

AWS Managed VPN

Amazon VPC provides the option of creating an IPsec VPN to connect your remote networks with your Amazon VPCs over the internet. You can take advantage of multiple VPN connections to route traffic, from your router, between your Amazon VPCs over the internet or AWS Direct Connect, as shown in the following figures.

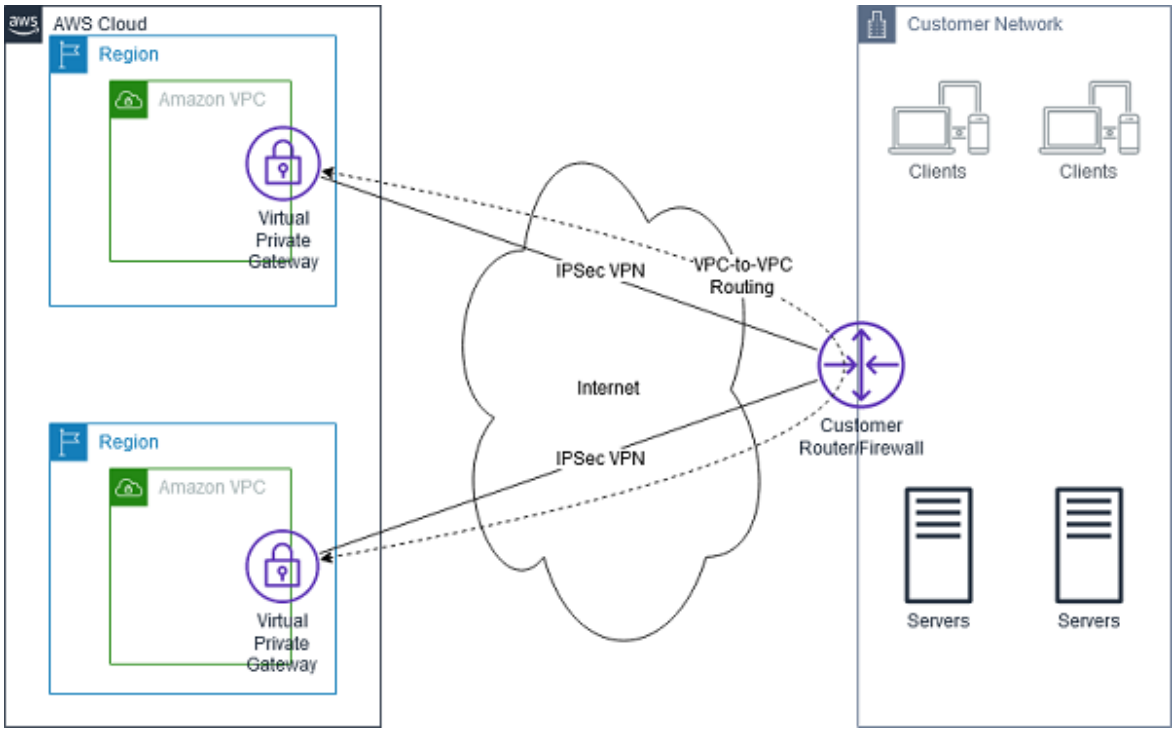

Figure 17 - AWS Managed VPN VPC-to-VPC Routing

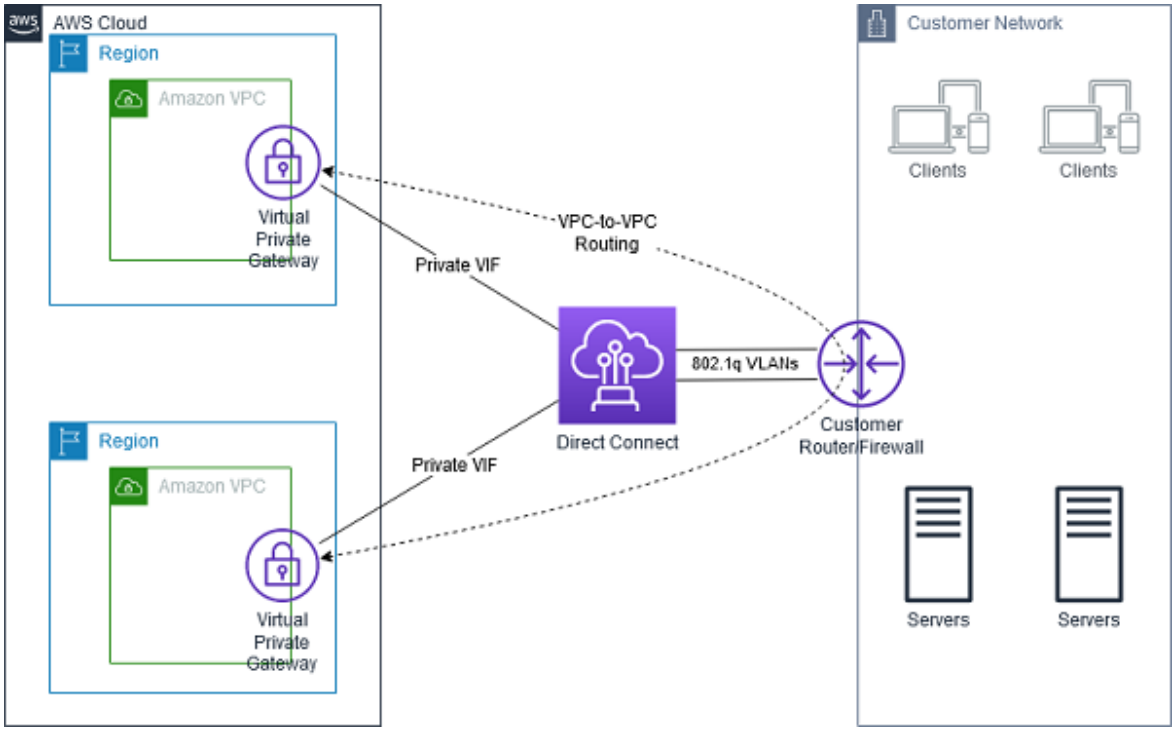

Figure 18 - AWS Direct Gateway VPC-to-VPC Routing

This approach is suboptimal from a routing perspective since the traffic must traverse to router on your network, but it gives you a lot of flexibility for controlling and managing routing on your local and remote networks, and the potential ability to reuse VPN connections.

Additional resources

- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC
- Tech Brief - Connecting a Single Customer Router to Multiple VPCs
- What is AWS Direct Connect?
- AWS Direct Connect virtual interfaces

AWS PrivateLink

AWS PrivateLink enables you to connect to some AWS services, services hosted by other AWS accounts (referred to as *endpoint services*), and supported AWS Marketplace partner services, via private IP addresses in your VPC. The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets. That means that VPC Security Groups can be used to manage access to the endpoints.

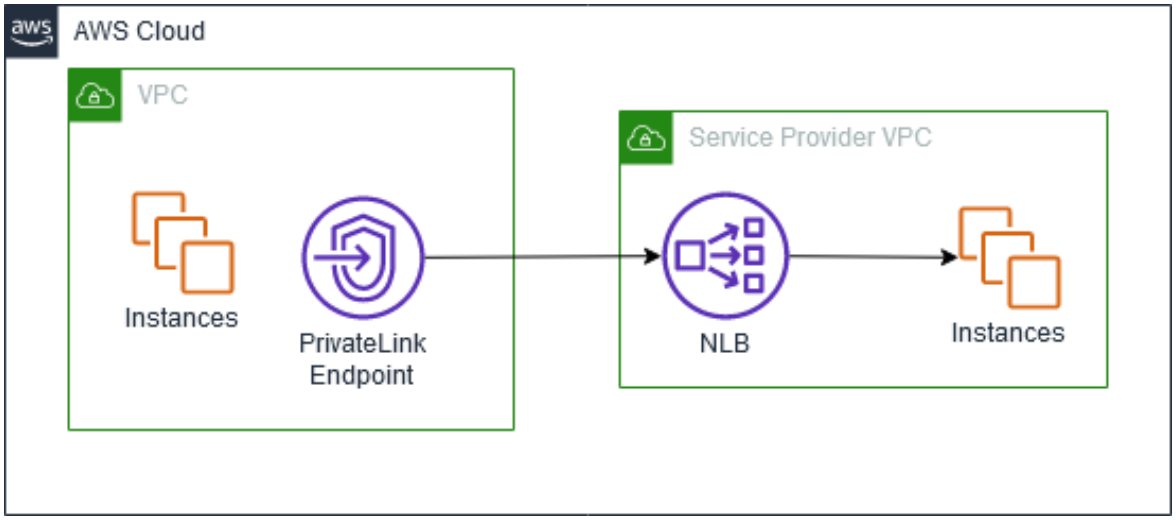

Figure 19 - AWS PrivateLink

We recommend this approach if you want to use services offered by another VPC securely within the AWS network, with all network traffic staying on the global AWS backbone and never traversing the public internet.

Additional resources

- Interface VPC endpoints (AWS PrivateLink)
- VPC endpoint services (AWS PrivateLink)

Software remote access-to-Amazon VPC connectivity options

With software remote access VPN, you can leverage low cost, elastic, and secure services to implement remote-access solutions while also providing a seamless experience connecting to AWS hosted resources. This option is typically preferred by smaller companies with less extensive remote networks or who have not already built and deployed remote access solutions for their employees.

You can combine these patterns with the Network-to-Amazon VPC connectivity options (p. 4) connectivity options and Amazon VPC-to-Amazon VPC connectivity options (p. 17) to create a network that spans remote networks and multiple VPCs.

The following table outlines the advantages and limitations of these options.

Option	Use Case	Advantages	Limitations
AWS Client VPN (p. 25)	AWS managed remote access solution to Amazon VPC and/or internal networks	AWS managed high availability and scalability service	OpenVPN clients only
Software client VPN (p. 26)	Software VPN appliance remote access solution to Amazon VPC and/or internal networks	Supports a wider array of VPN vendors, products, and protocols Fully customer-managed solution	You are responsible for implementing HA solutions

AWS Client VPN

AWS Client VPN is an AWS managed high availability and scalability service enabling secure software remote access. It provides the option of creating a secure TLS connection between remote clients and your Amazon VPCs, to securely access AWS resources and on-premises over the internet, as shown in the following figure.

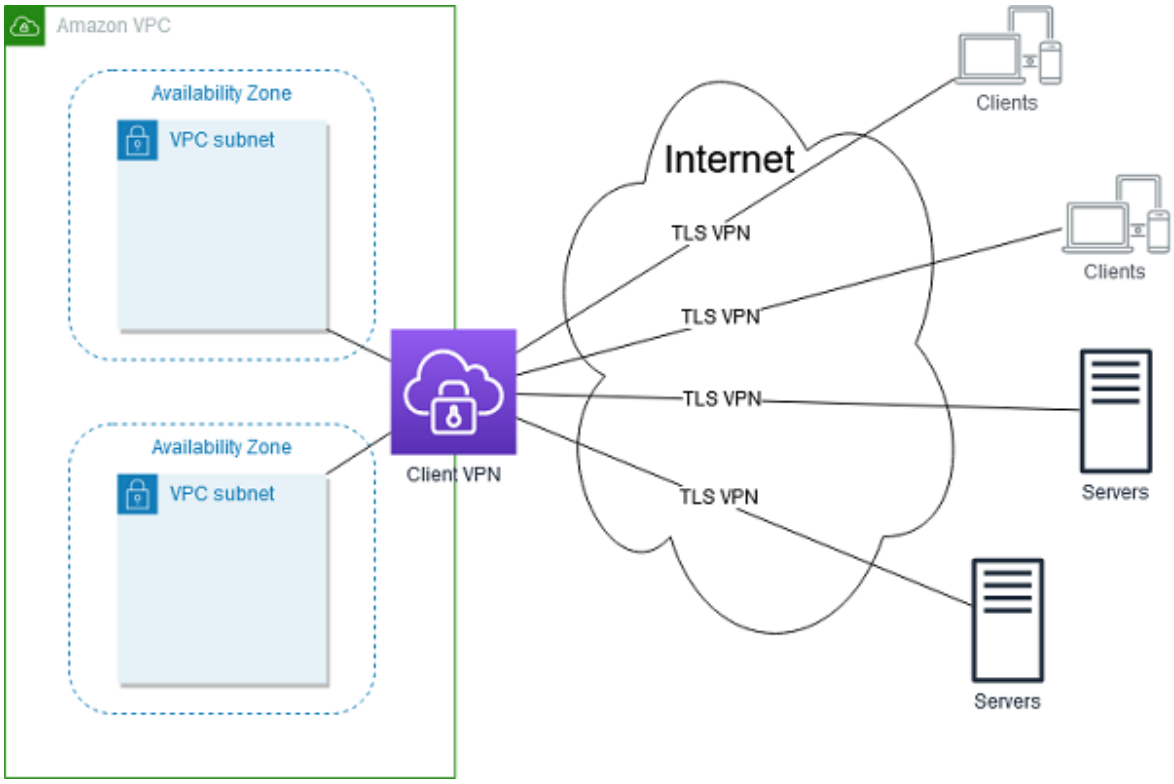

Figure 20 - AWS Client VPN Remote Access

The remote clients can be the AWS Client VPN for Desktop, or third-party OpenVPN VPN clients, with authentication by either Active Directory or mutual certificate authentication.

Additional resources

- AWS Client VPN Administrator Guide

Software client VPN

You can choose from an ecosystem of multiple partners and open source communities that have produced remote-access solutions that run on Amazon EC2. These solutions provide great flexibility on the security protocol use for remote-access into your Amazon VPCs, to securely access AWS resources and on-premises over the internet, as shown in the following figure.

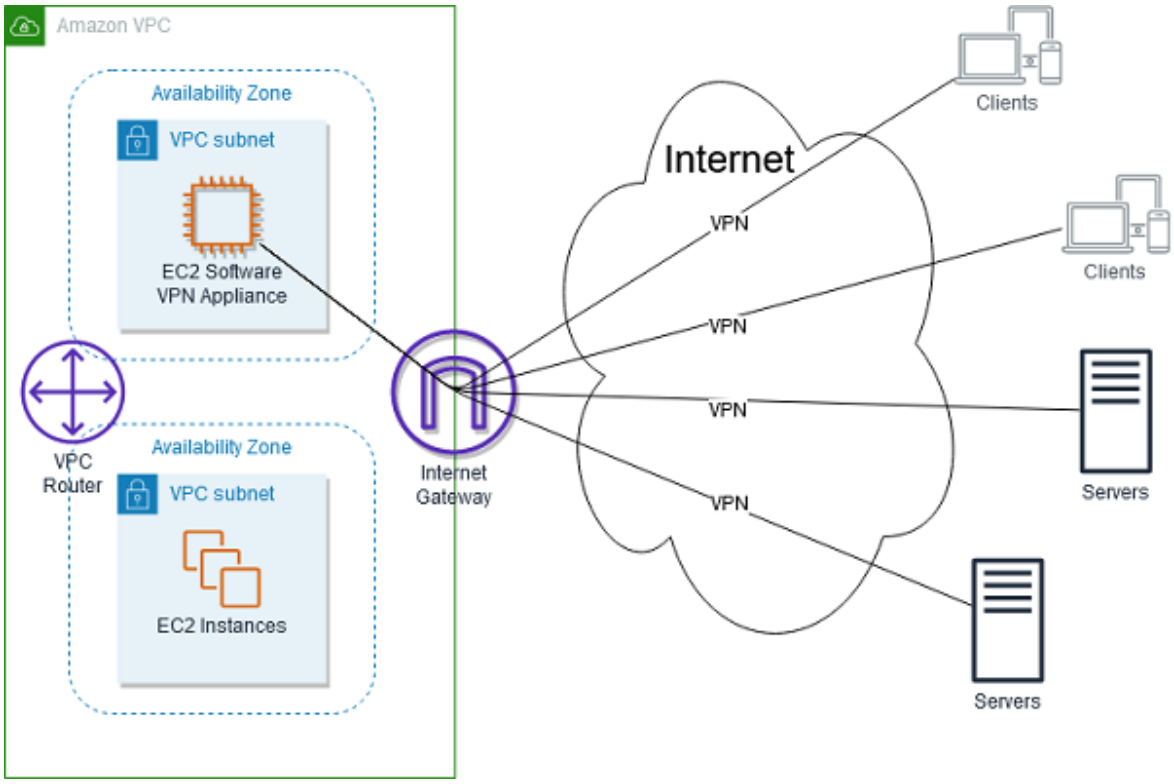

Figure 21 - Software Client VPN Remote Access

Remote-access solutions range in complexity, support multiple client authentication options (including multifactor authentication) and can be integrated with either Amazon VPC or remotely hosted identity and access management solutions (leveraging one of the network-to-Amazon VPC options) like Microsoft Active Directory or other LDAP/multifactor authentication solutions.

The customer is responsible for managing the remote access software including user management, configuration, patches and upgrades. This design introduces a potential single point of failure into the network design as the remote access server runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances.

Additional resources

- VPN appliances available from the AWS Marketplace
- OpenVPN Access Server Quick Start Guide

Transit VPC option

Building on the Software VPN designs mentioned above, you can create a global transit network on AWS. A transit VPC is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center. A transit VPC simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks. The following figure illustrates this design.

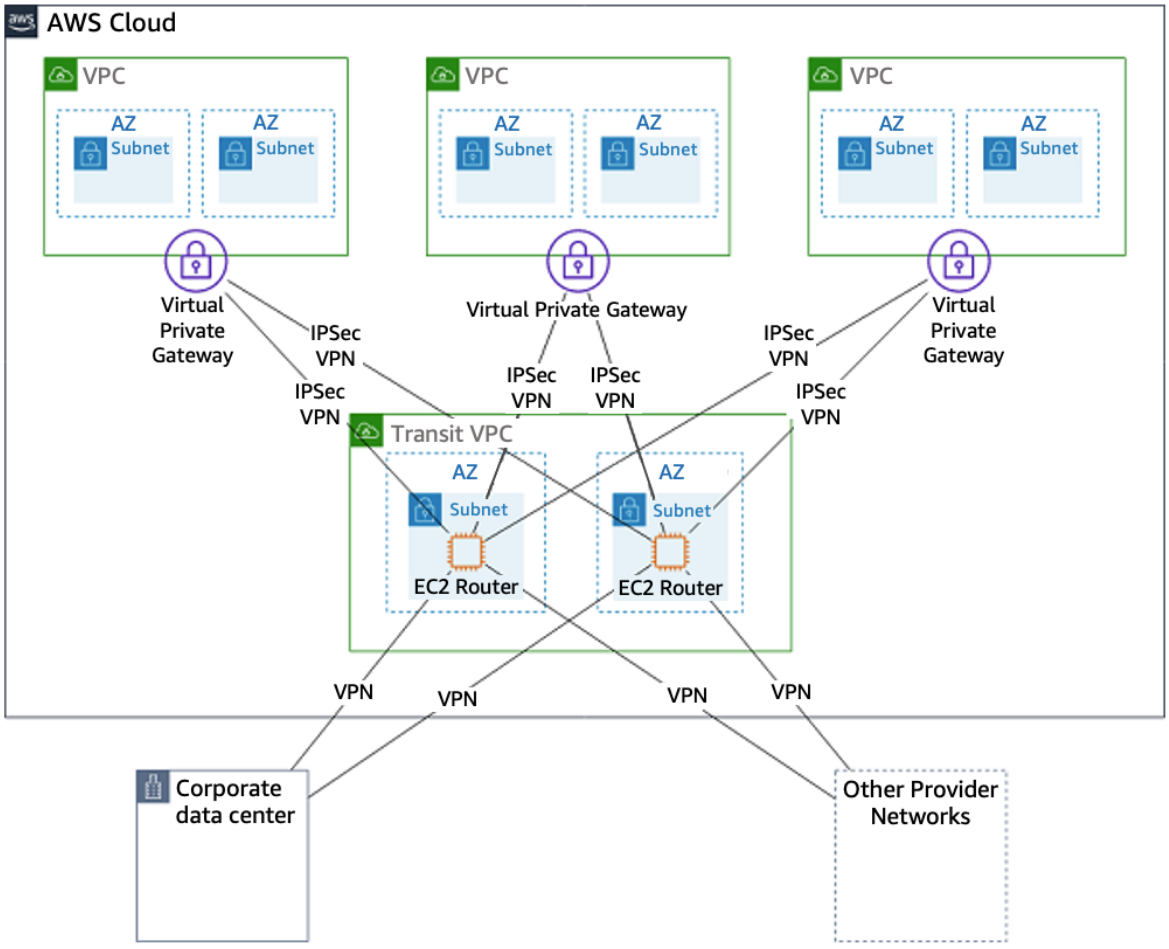

Figure 22 - Transit VPC

Along with providing direct network routing between VPCs and on-premises networks, this design also enables the transit VPC to implement more complex routing rules, such as network address translation between overlapping network ranges, or to add additional network-level packet filtering or inspection. The transit VPC design can be used to support important use cases like, private networking, shared connectivity and cross account AWS usage.

Additional resources

- AWS Transit Gateway

- Cisco CSR1000V- Transit VPC with Transit Gateway in AWS Marketplace

Conclusion

AWS provides a number of efficient, secure connectivity options to help you get the most out of AWS when integrating your remote networks with Amazon VPC. The options provided in this whitepaper highlight several of the connectivity options and patterns that customers have used to successfully integrate their remote networks or multiple Amazon VPC networks. You can use the information provided here to determine the most appropriate mechanism for connecting the infrastructure required to run your business regardless of where it is physically located or hosted.

Appendix A: High-Level HA architecture for software VPN instances

Creating a fully resilient VPC connection for software VPN instances requires the setup and configuration of multiple VPN instances and a monitoring instance to monitor the health of the VPN connections.

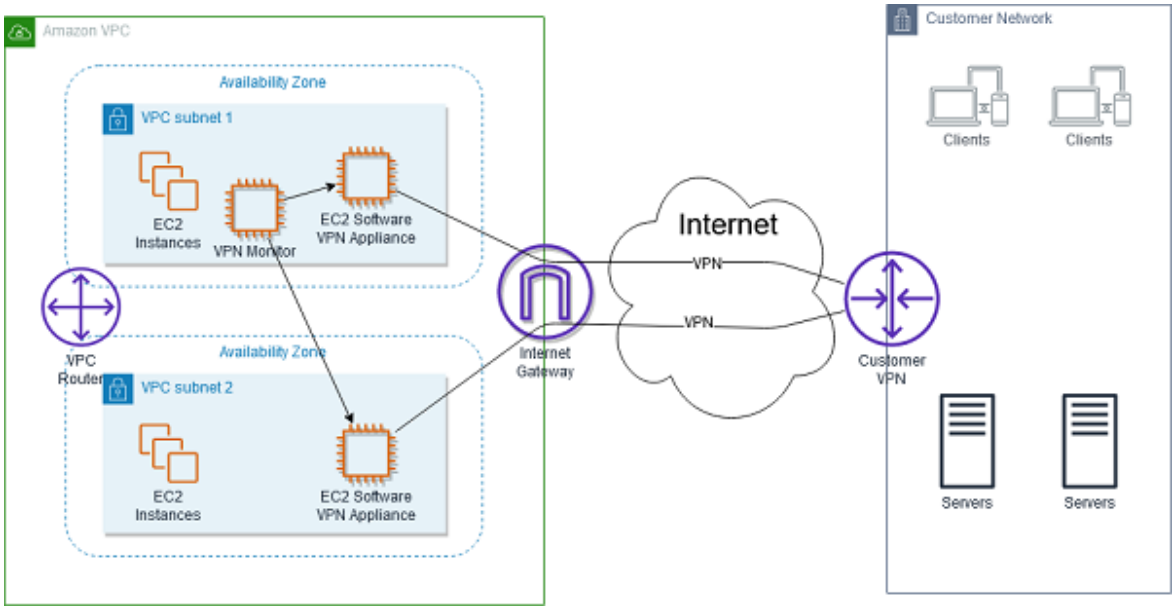

Figure 23 - High-Level Software VPN HA

We recommend configuring your VPC route tables to leverage all VPN instances simultaneously by directing traffic from all of the subnets in one Availability Zone through its respective VPN instances in the same Availability Zone. Each VPN instance then provides VPN connectivity for instances that share the same Availability Zone.

VPN monitoring

To monitor Software based VPN appliance you can create a VPN Monitor. The VPN monitor is a custom instance that you will need to run the VPN monitoring scripts. This instance is intended to run and monitor the state of VPN connection and VPN instances. If a VPN instance or connection goes down, the monitor needs to stop, terminate, or restart the VPN instance while also rerouting traffic from the affected subnets to the working VPN instance until both connections are functional again. Since customer requirements vary, AWS does not currently provide prescriptive guidance for setting up this monitoring instance. However, an example script for enabling HA between NAT instances could be used as a starting point for creating an HA solution for Software VPN instances. We recommend that you think through the necessary business logic to provide notification or attempt to automatically repair network connectivity in the event of a VPN connection failure.

Additionally, you can monitor the AWS Managed VPN tunnels using Amazon CloudWatch metrics, which collects data points from the VPN service into readable, near real-time metrics. Each VPN connection collects and publishes a variety of tunnel metrics to Amazon CloudWatch. These metrics allow you to monitor tunnel health, activity, and create automated actions.

Contributors

Contributors to this document include:

- Daniel Yu, Senior Technical Account Manager, AWS Enterprise Support
- Garvit Singh, Solutions Builder, AWS Solution Architecture
- Steve Morad, Senior Manager, Solution Builders, AWS Solution Architecture
- Sohaib Tahir, Solutions Architect, AWS Solution Architecture

Further reading

For additional information, refer to:

- AWS Solutions Implementation: AWS Global Transit Network

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

update-history-change	update-history-description	update-history-date
Whitepaper updated (p. 35)	Added AWS Transit Gateway and AWS Client VPN options, updated diagrams and information throughout.	June 6, 2020
Minor update (p. 35)	Minor change to fix reference to software VPN appliance.	May 20, 2020
Whitepaper updated (p. 35)	Updated information throughout. Focus on the following designs/features: transit VPC, Direct Connect gateway, and AWS PrivateLink.	January 1, 2018
Initial publication (p. 35)	Amazon Virtual Private Cloud Connectivity Options published.	July 1, 2014

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.