Amazon Virtual Private Cloud Connectivity Options

AWS Whitepaper

Amazon Virtual Private Cloud Connectivity Options: AWS Whitepaper

Table of Contents

Introduction

Publication date: **January 2018** (*Document Details* (p. 31))

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 leverage depending on your current network designs and requirements. These connectivity options include leveraging either the internet or an AWS Direct Connect connection as the network backbone and terminating the connection into either 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 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. 3)

- the section called "AWS Managed VPN" (p. 4) – Describes establishing a VPN connection from your network equipment on a remote network to AWS managed network equipment attached to your Amazon VPC.
- the section called "AWS Direct Connect" (p. 6) – Describes establishing a private, logical connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
- the section called "AWS Direct Connect Plus VPN" (p. 8) – Describes establishing a private, encrypted connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
- the section called "AWS VPN CloudHub" (p. 9) – Describes establishing a hub-and-spoke model for connecting remote branch offices.
- the section called "Software VPN" (p. 11) – Describes establishing a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC.
- the section called "Transit VPC" (p. 12) – Describes establishing a global transit network on AWS using Software VPN in conjunction with AWS managed VPN.

Amazon VPC-to-Amazon VPC Connectivity Options (p. 14)

- the section called "VPC Peering" (p. 15) – Describes the AWS-recommended approach for connecting multiple Amazon VPCs within and across regions using the Amazon VPC peering feature.
- the section called "Software VPN" (p. 17) – Describes connecting multiple Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
- the section called "Software-to-AWS Managed VPN" (p. 18) – Describes connecting multiple Amazon VPCs with a VPN connection established between a user-managed software VPN appliance in one Amazon VPC and AWS managed network equipment attached to the other Amazon VPC.
- the section called "AWS Managed VPN" (p. 19) – Describes connecting multiple Amazon VPCs, leveraging multiple VPN connections between your remote network and each of your Amazon VPCs.
- the section called "AWS Direct Connect" (p. 21) – Describes connecting multiple Amazon VPCs, leveraging logical connections on customer-managed AWS Direct Connect routers.
- the section called "AWS PrivateLink" (p. 23) – Describes connecting multiple Amazon VPCs, leveraging VPC interface endpoints and VPC endpoint services.

Internal User-to-Amazon VPC Connectivity Options (p. 24)

- the section called "Software Remote-Access VPN" (p. 24) – In addition to customer network–to–Amazon VPC connectivity options for connecting remote users to VPC resources, this section describes leveraging a remote-access solution for providing end-user VPN access into an Amazon VPC.

Network-to-Amazon VPC Connectivity Options

This section provides design patterns for you to connect 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 advise 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
the section called "AWS Managed VPN" (p. 4)	AWS managed IPsec VPN connection over the internet	Reuse existing VPN equipment and processes Reuse existing internet connections AWS managed endpoint includes multi-data center redundancy and automated failover 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)
the section called "AWS Direct Connect" (p. 21)	Dedicated network connection over private lines	More predictable network performance Reduced bandwidth costs 1 or 10 Gbps provisioned connections Supports BGP peering and routing policies	May require additional telecom and hosting provider relationships or new network circuits to be provisioned
the section called "AWS Direct Connect Plus VPN" (p. 8)	IPsec VPN connection over private lines	Same as the previous option with the addition of a secure IPsec VPN connection	Same as the previous option with a little additional VPN complexity

Option	Use Case	Advantages	Limitations
the section called "AWS VPN CloudHub" (p. 9)	Connect remote branch offices in a hub-and-spoke model for primary or backup connectivity	Reuse existing internet connections and AWS VPN connections (for example, use AWS VPN CloudHub as backup connectivity to a third-party MPLS network) AWS managed virtual private gateway includes multi-data center redundancy and automated failover Supports BGP for exchanging routes and routing priorities (for example, prefer MPLS connections over backup AWS VPN connections)	Network latency, variability, and availability are dependent on the internet User managed branch office endpoints are responsible for implementing redundancy and failover (if required)
the section called "Software VPN" (p. 11)	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)
the section called "Transit VPC" (p. 12)	Software appliance-based VPN connection with hub VPC AWS managed IPsec VPN connection for spoke VPC connection	Same as the previous option with the addition of AWS managed VPN connection between hub and spoke VPCs	Same as the previous section

AWS Managed VPN

Amazon VPC provides the option of creating an IPsec VPN connection between remote customer networks and their Amazon VPC over the internet, as shown in the following figure. Consider taking this approach when you want to take advantage of an AWS managed VPN endpoint that includes automated multi–data center redundancy and failover built into the AWS side of the VPN connection. Although not shown, the Amazon virtual private gateway represents two distinct VPN endpoints, physically located in separate data centers to increase the availability of your VPN connection.

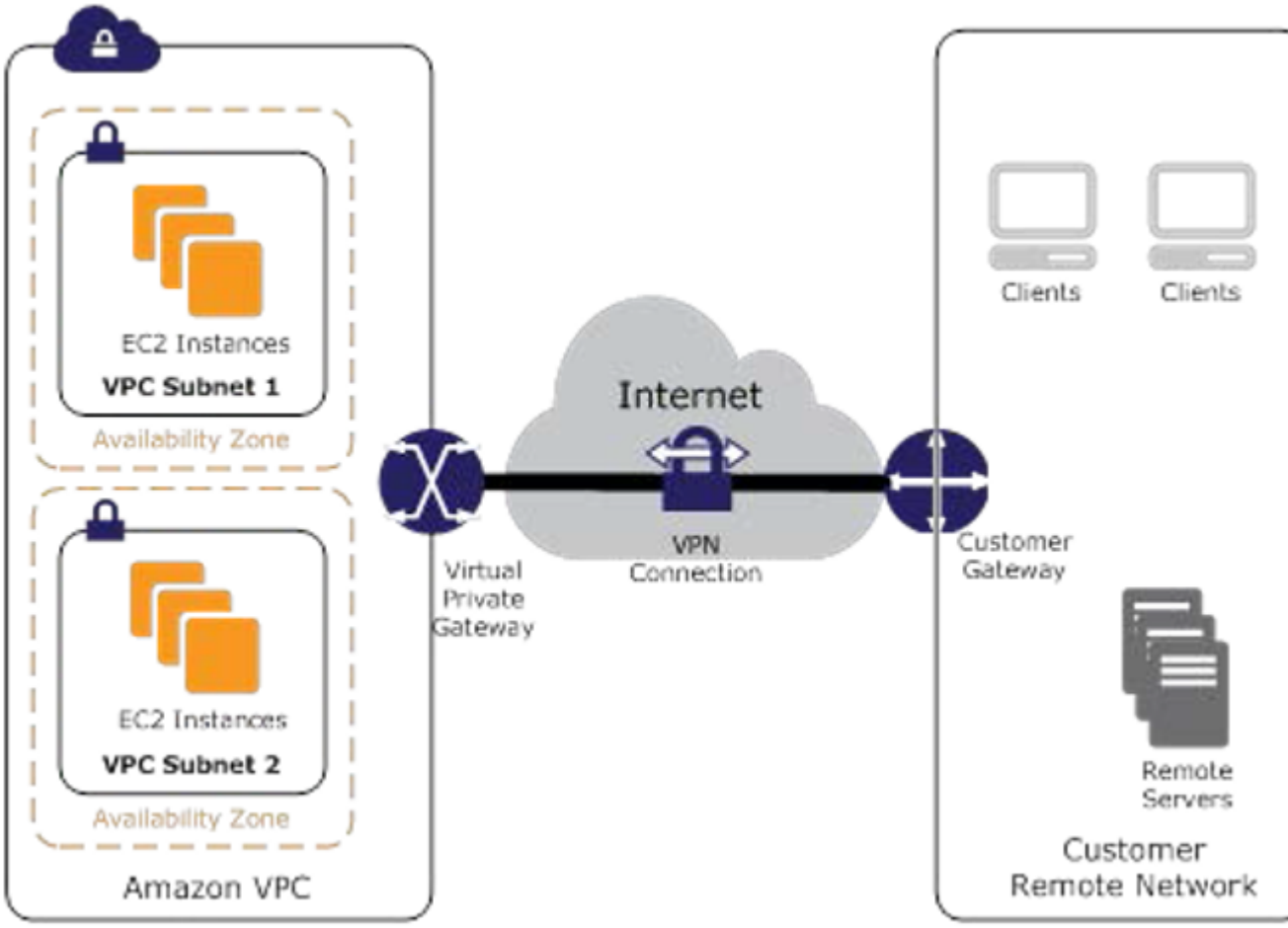

Figure: AWS managed VPN

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

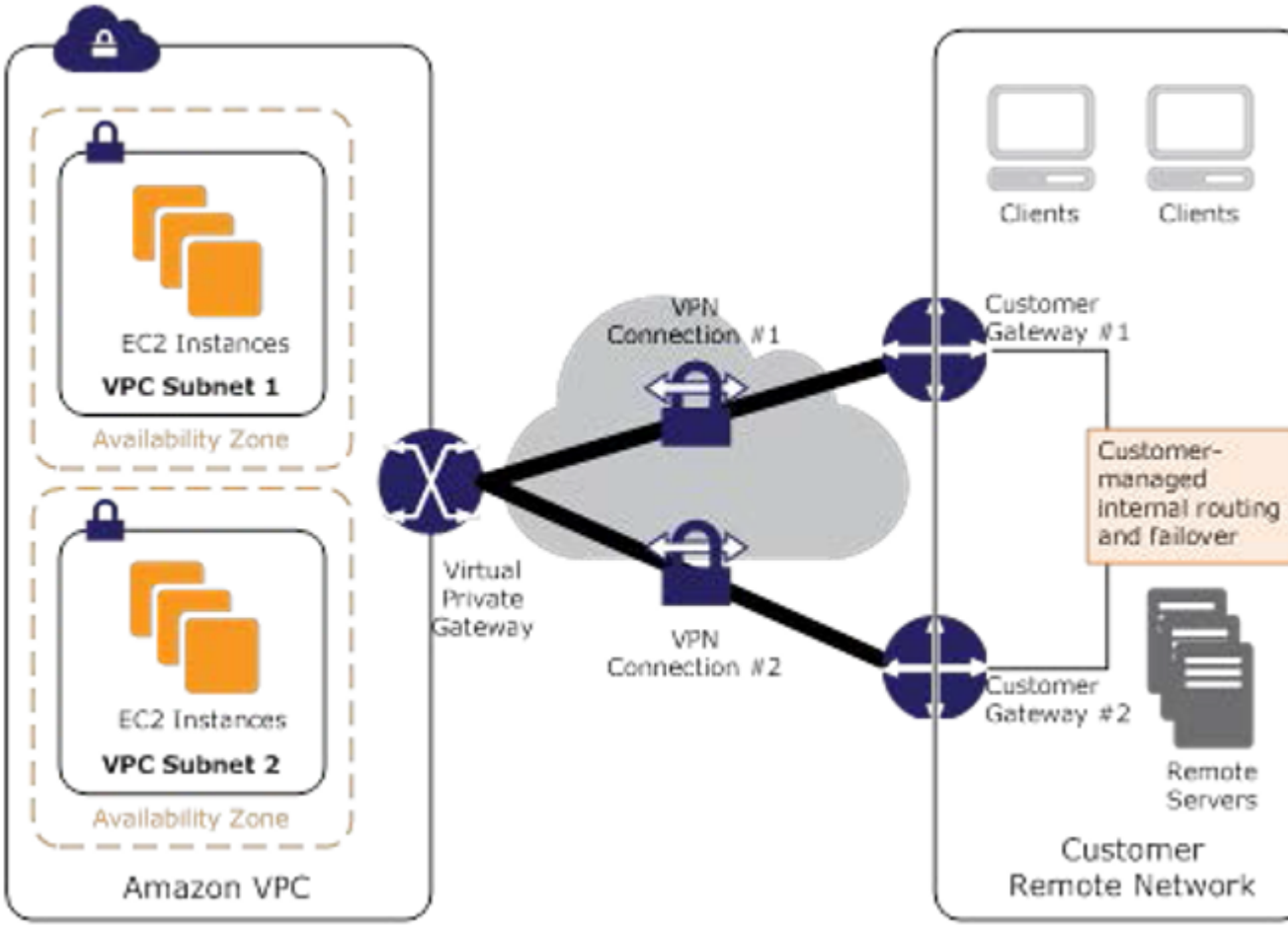

Figure: Redundant AWS managed VPN connections

Additional Resources

- Adding a Virtual Private Gateway to Your VPC
- Customer Gateway device minimum requirements
- Customer Gateway devices known to work with Amazon VPC

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to Amazon VPC. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment. This private connection can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

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. It uses industry-standard VLANs to access Amazon Elastic Compute Cloud (Amazon EC2) instances running within an 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. The following figure illustrates this pattern. 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.

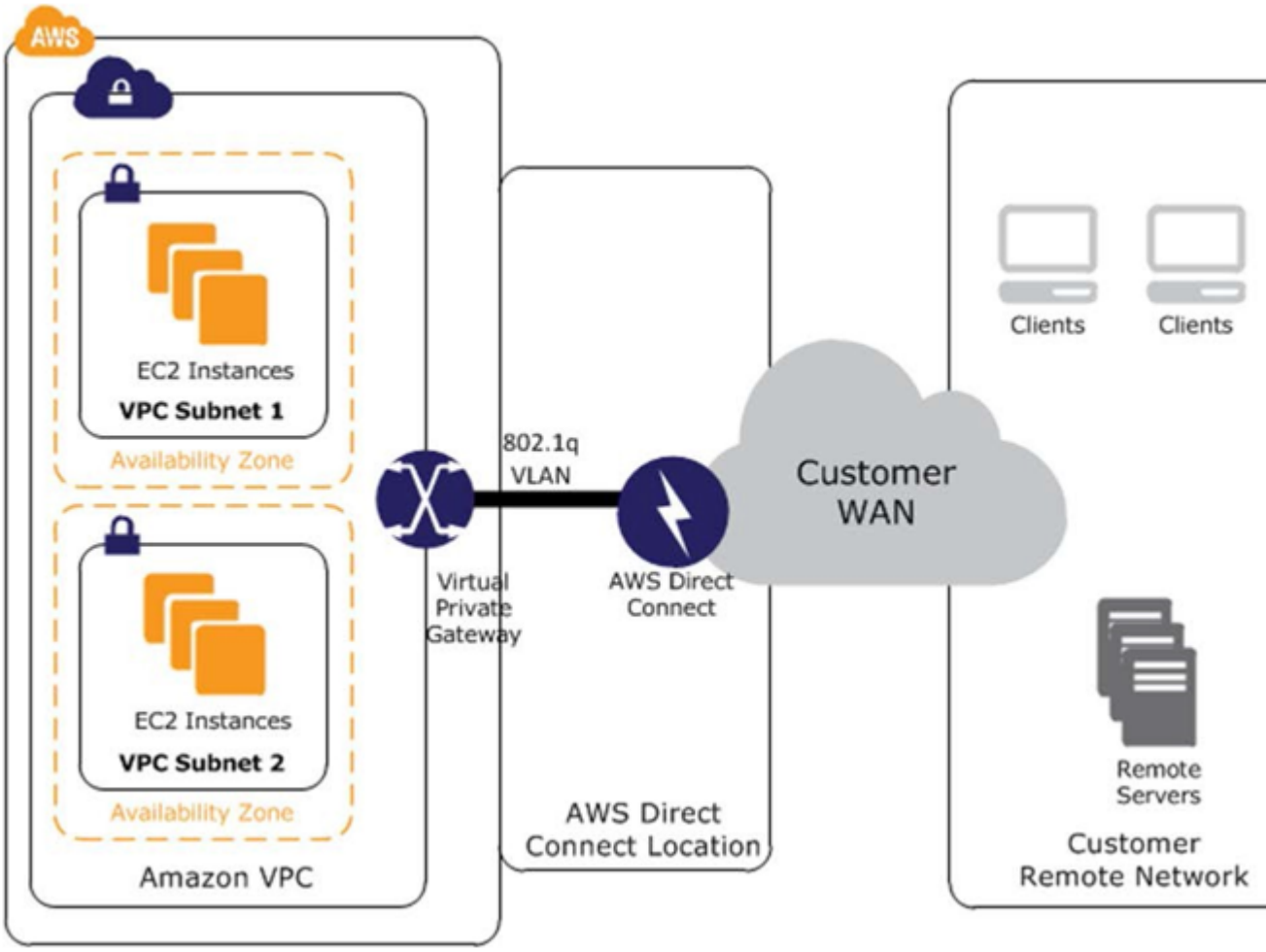

Figure: AWS Direct Connect

AWS Direct Connect allows you to connect your AWS Direct Connect connection to one or more VPCs in your account that are located in the same or different regions. You can use Direct Connect gateway to achieve this. A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any public region and access it from all other public regions.

This feature also allows you to connect to any of the participating VPCs from any Direct Connect location, further reducing your costs for using AWS services on a cross-region basis. The following figure illustrates this pattern.

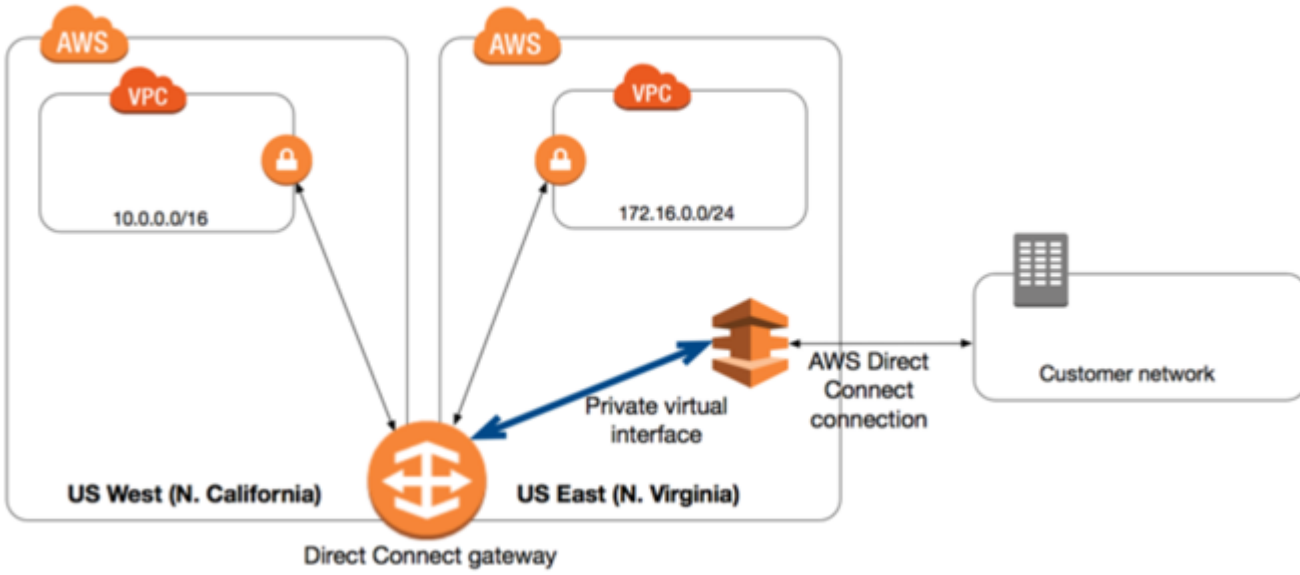

Figure: AWS Direct Connect Gateway

Additional Resources

- AWS Direct Connect product page
- AWS Direct Connect locations
- AWS Direct Connect FAQs
- AWS Direct Connect LAGs
- AWS Direct Connect Gateways
- Getting Started with AWS Direct Connect

AWS Direct Connect Plus VPN

With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

You can use AWS Direct Connect to establish a dedicated network connection between your network create a logical connection to public AWS resources, such as an Amazon virtual private gateway IPsec endpoint. This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection.

The following figure illustrates this option.

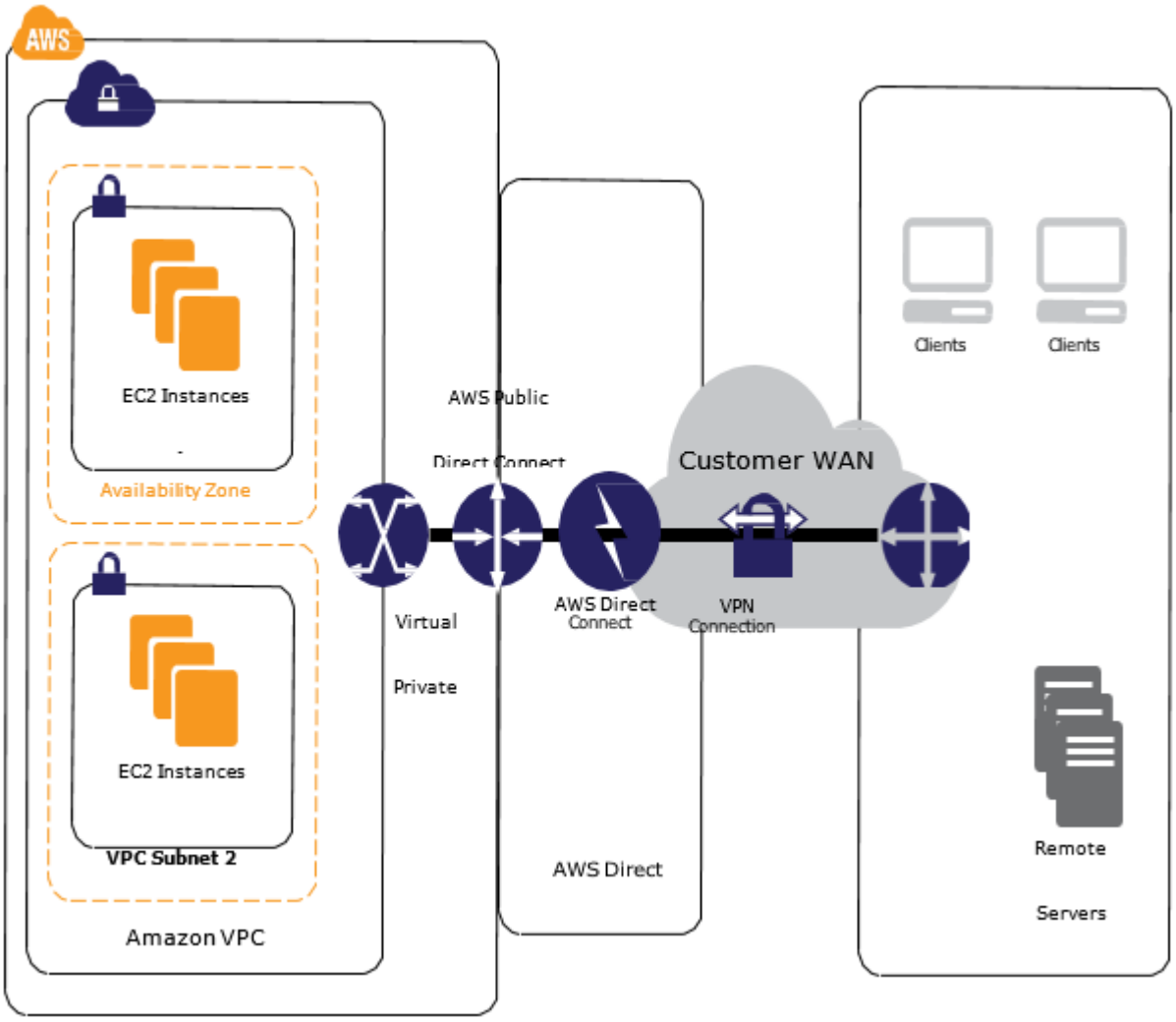

Figure: AWS Direct Connect and VPN

Additional Resources

- AWS Direct Connect product page
- AWS Direct Connect FAQs
- Adding a Virtual Private Gateway to Your VPC

AWS VPN CloudHub

Building on the AWS managed VPN and the section called "AWS Direct Connect" (p. 21) 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 design 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 depicts the AWS VPN CloudHub architecture, with blue dashed lines indicating network traffic between remote sites being routed over their AWS VPN connections.

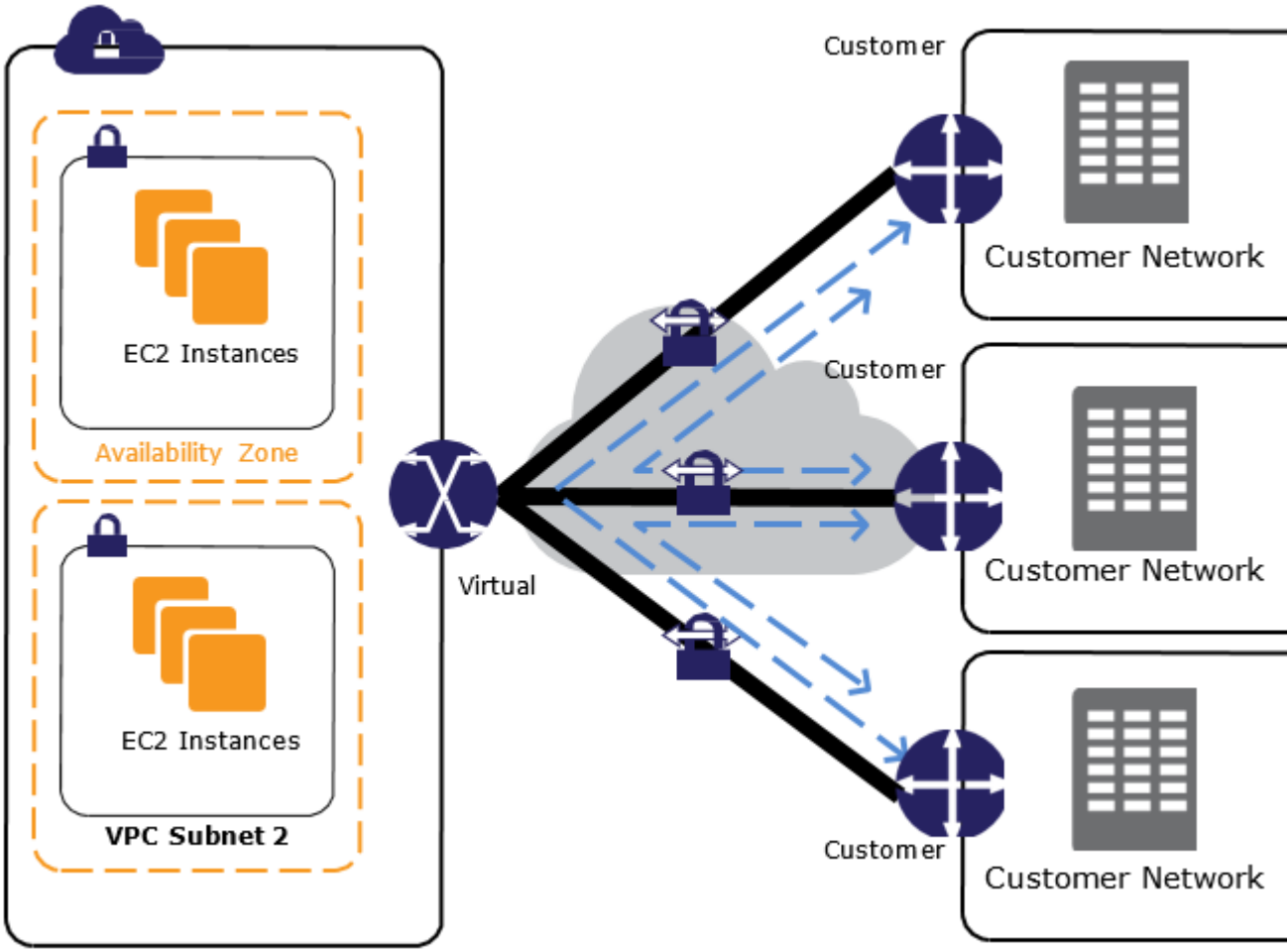

Figure: AWS VPN CloudHub

AWS VPN CloudHub leverages an Amazon VPC virtual private gateway with multiple 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 readvertised 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. Each site can also send and receive data from the VPC as if they were using a standard VPN connection.

This option can be combined with AWS Direct Connect or other VPN options (for example, multiple gateways per site for redundancy or backbone routing that you provide) depending on your requirements.

Additional Resources

- AWS VPN CloudHub
- Amazon VPC VPN Guide
- Customer Gateway device minimum requirements

- Customer Gateway devices known to work with Amazon VPC
- AWS Direct Connect product page

Software 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.

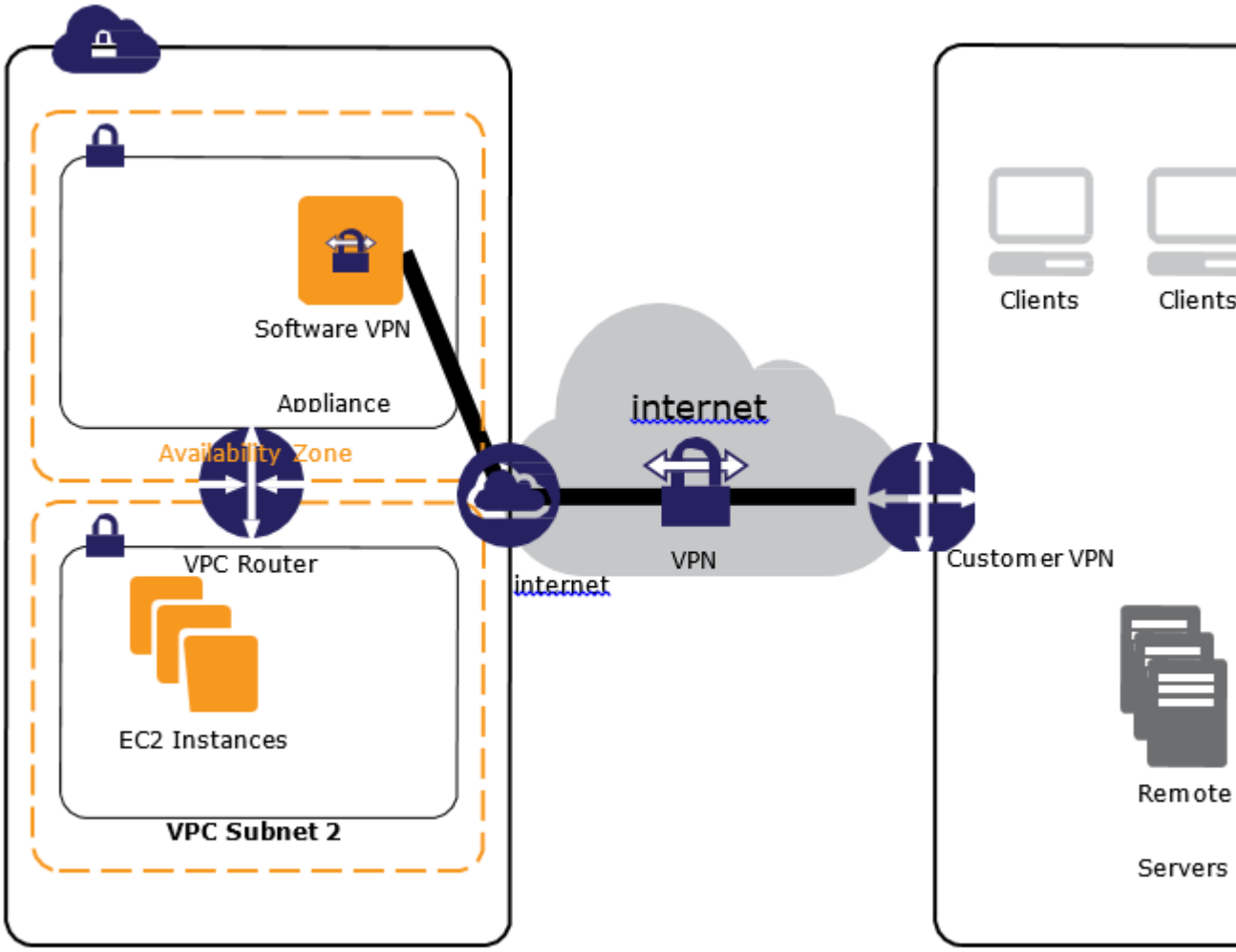

Figure: Software VPN

You can choose from an ecosystem of multiple partners and open source communities that have produced software VPN appliances that run on Amazon EC2. These include products from well-known security companies like Check Point, Astaro, OpenVPN Technologies, and Microsoft, as well as popular open source tools like OpenVPN, Openswan, and IPsec-Tools. 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 because the software VPN appliance runs on a single Amazon EC2 instance. For additional information, see *Appendix: High-Level HA Architecture for Software VPN Instances* (p. 28).

Additional Resources

- VPN Appliances from 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)

Transit VPC

Building on the Software VPN design 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.

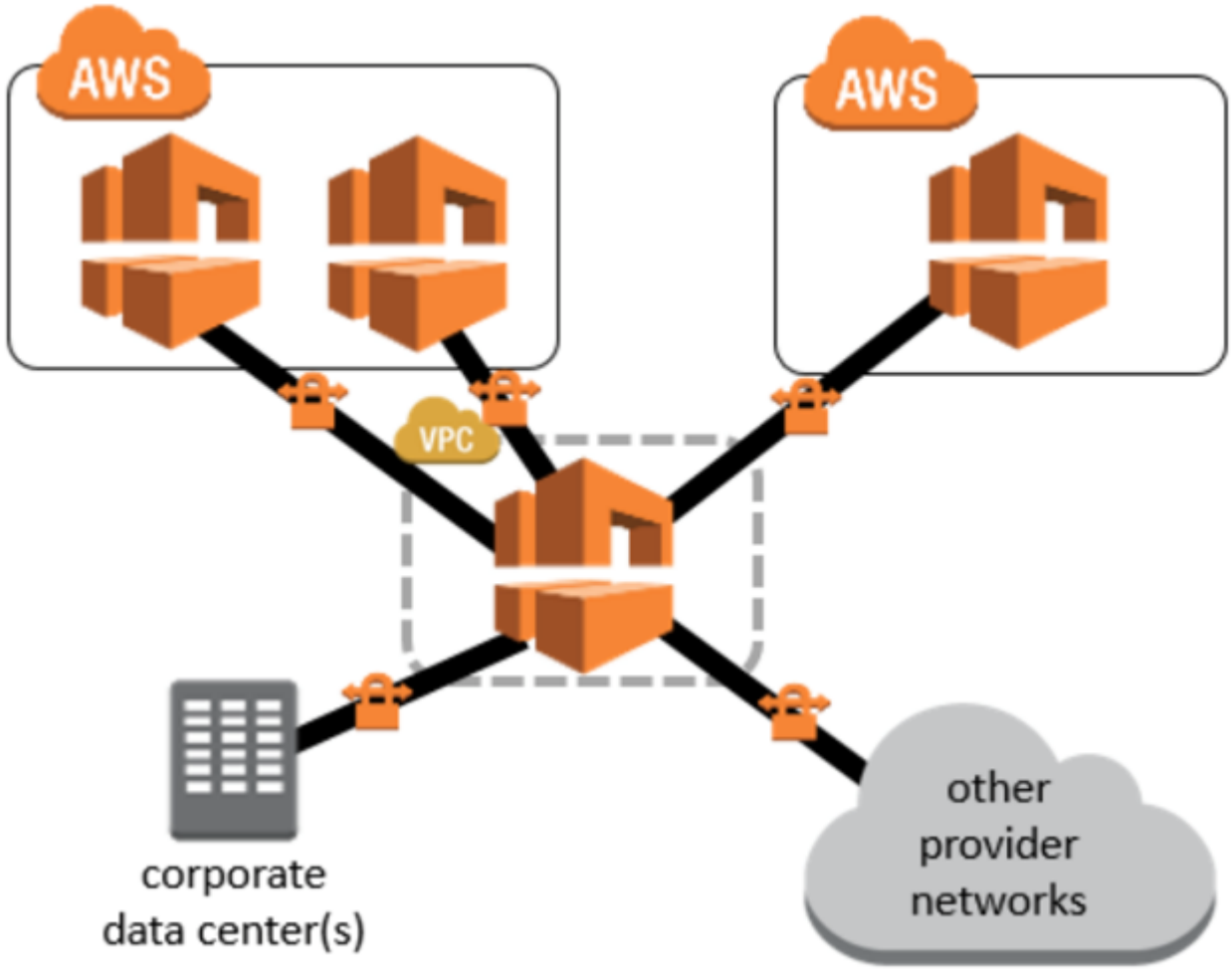

Figure: Software VPN and Transit VPC

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

- Tech Brief - Global Transit Network
- Solution - Transit VPC

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* (p. 3) 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
the section called "VPC Peering" (p. 15)	AWS-provided network connectivity between two VPCs.	Leverages AWS networking infrastructure Does not rely on VPN instances or a separate piece of physical hardware No single point of failure No bandwidth bottleneck	VPC peering does not support transitive peering relationships.
the section called "Software VPN" (p. 17)	Software appliance-based VPN connections between VPCs	Leverages AWS networking equipment in-region and internet pipes between regions Supports a wider 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
the section called "Software-to-AWS Managed VPN" (p. 18)	Software appliance to VPN connection between VPCs	Leverages AWS networking equipment in-region and internet pipes between regions AWS managed endpoint includes multi-data	You are responsible for implementing HA solutions for the software appliance VPN endpoints (if required)

Option	Use Case	Advantages	Limitations
		center redundancy and automated failover	VPN instances could become a network bottleneck
the section called "AWS Managed VPN" (p. 19)	VPC-to-VPC routing managed by you over IPsec VPN connections using your equipment and the internet	Reuse existing Amazon VPC VPN connections AWS managed endpoint includes multi-data center redundancy and automated failover Supports static routes and dynamic BGP peering and routing policies	Network latency, variability, and availability depend on internet conditions The endpoint you manage is responsible for implementing redundancy and failover (if required)
the section called "AWS Direct Connect" (p. 21)	VPC-to-VPC routing managed by you using your equipment in an AWS Direct Connect location and private lines	Consistent network performance Reduced bandwidth costs 1 or 10 Gbps provisioned connections Supports static routes and BGP peering and routing policies	May require additional telecom and hosting provider relationships
the section called "AWS PrivateLink" (p. 23)	AWS-provided network connectivity between two VPCs using interface endpoints.	Leverages AWS networking infrastructure No single point of failure	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. This is the AWS recommended method for connecting VPCs. 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.

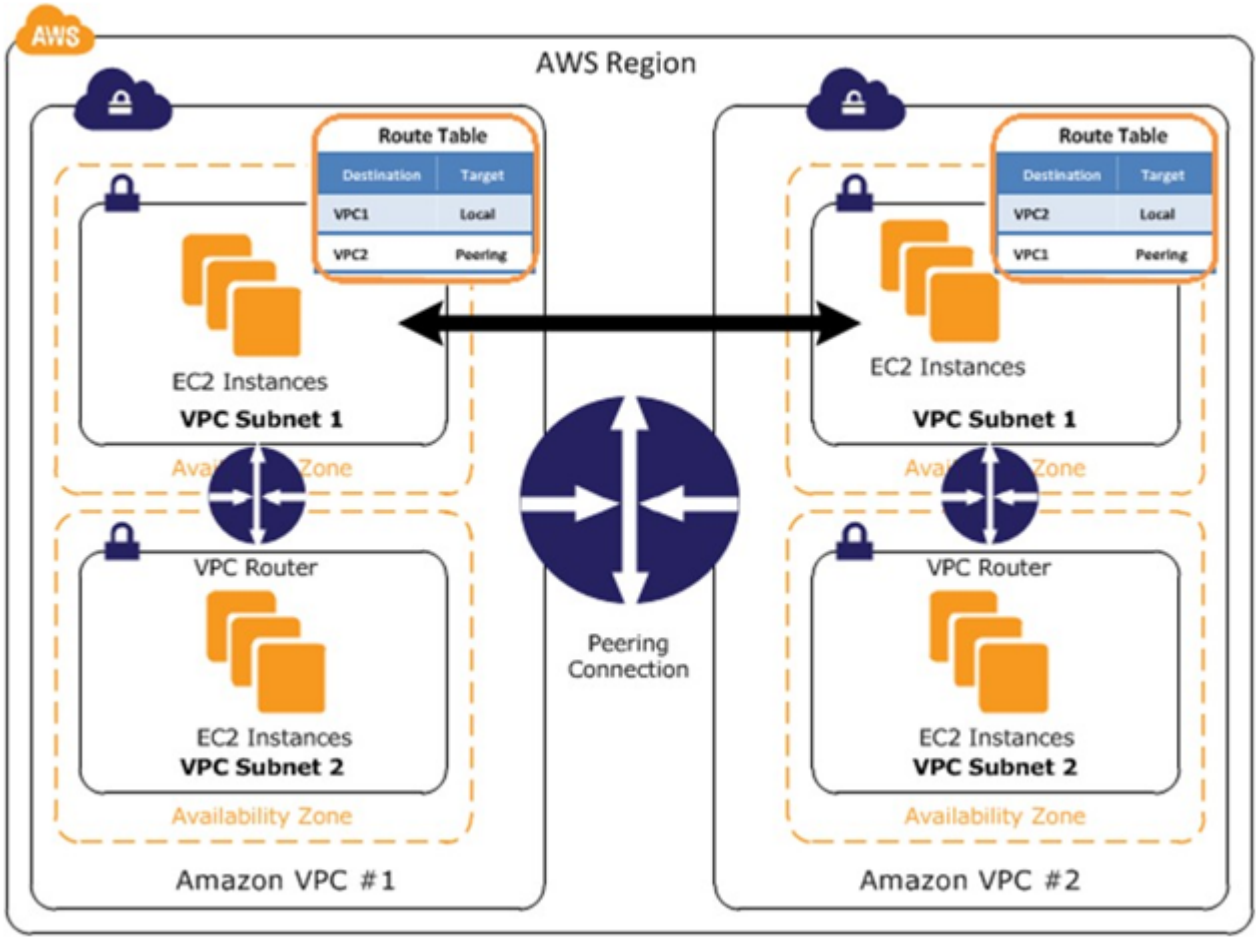

Figure: VPC-to-VPC peering

AWS uses the existing infrastructure of a VPC to create VPC peering connections. These connections are neither a gateway nor a VPN connection 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.

A VPC peering connection can help you to facilitate the transfer of data between VPCs. You can use them to connect VPCs when you have more than one AWS account, to connect a management or shared services VPC to application- or customer-specific VPCs, or to connect seamlessly with a partner's VPC. For more examples of scenarios in which you can use a VPC peering connection, see the Amazon VPC Peering Guide.

Additional Resources

- Amazon VPC User Guide
- Amazon VPC Peering Guide

Software 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 connect VPCs across multiple AWS Regions and 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.

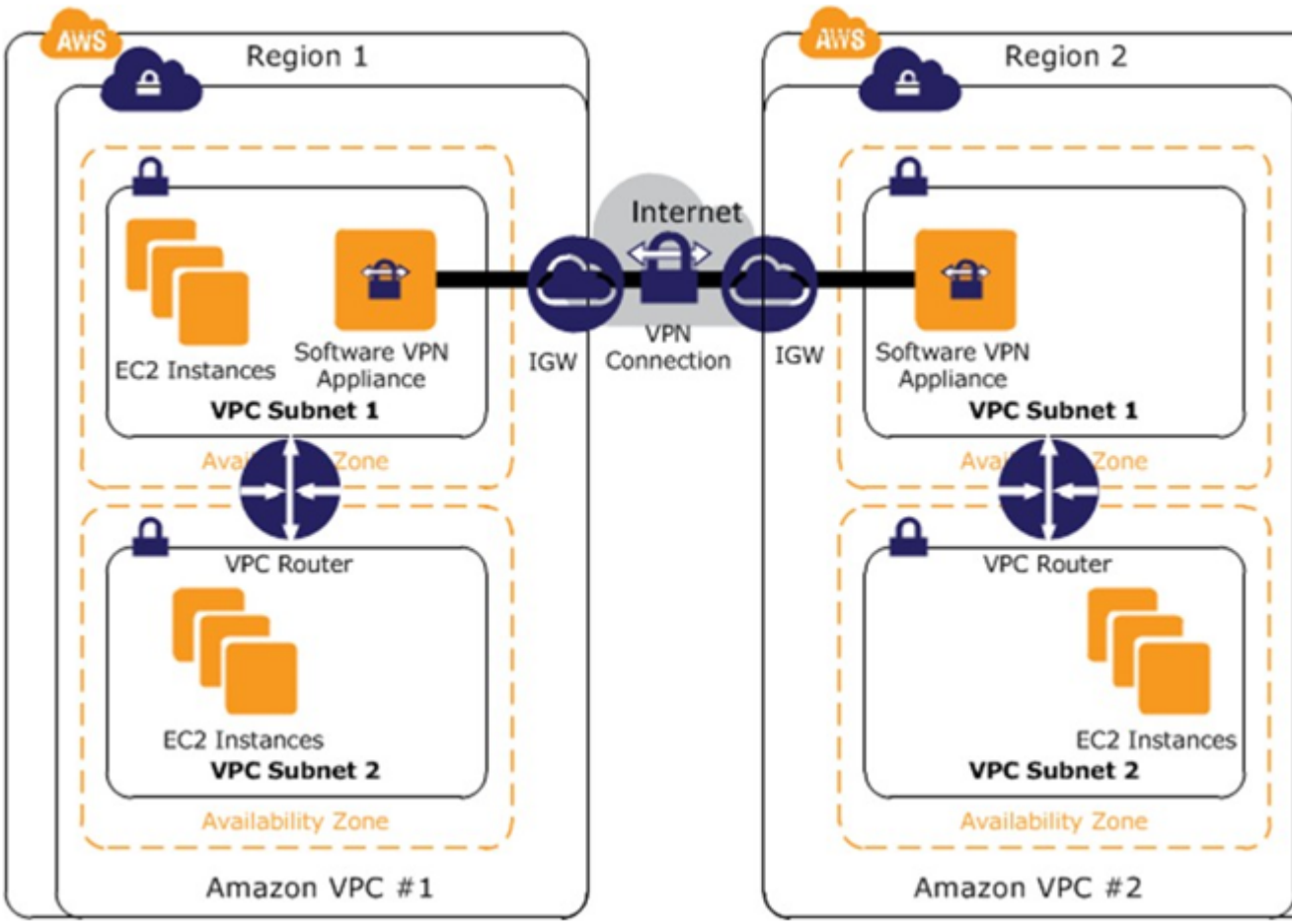

Figure: Inter-region VPC-to-VPC routing

You can choose from an ecosystem of multiple partners and open source communities that have produced software VPN appliances that run on Amazon EC2. These include products from well-known security companies like Check Point, Sophos, OpenVPN Technologies, and Microsoft, as well as popular open source tools like OpenVPN, Openswan, and IPsec-Tools. 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: High-Level HA Architecture for Software VPN Instances* (p. 28).

Additional Resources

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

Software-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 to connect multiple VPCs into a larger virtual private network, allowing instances in each VPC to seamlessly connect to each other using private IP addresses. This option is recommended when you want to connect VPCs across multiple AWS regions and would like to take advantage of the AWS managed VPN endpoint including automated multi-data center redundancy and failover built into the virtual private gateway side of the VPN connection. 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.

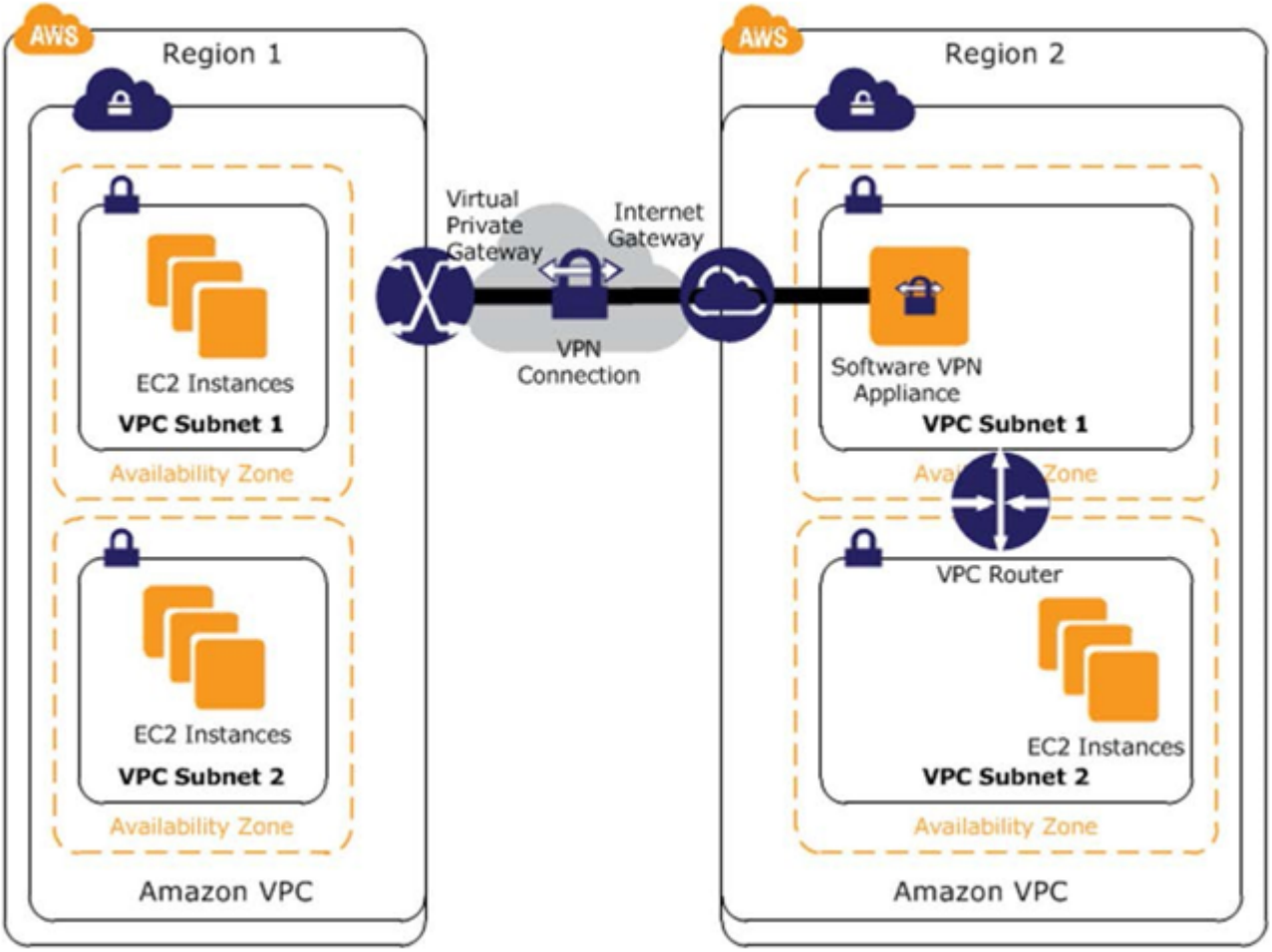

Figure: Intra-region VPC-to-VPC routing

Note that this design introduces a potential single point of failure into the network design as the Astaro Security Gateway appliance runs on a single Amazon EC2 instance. For additional information, see *Appendix: High-Level HA Architecture for Software VPN Instances* (p. 28).

Additional Resources

- Tech Brief - Connecting Multiple VPCs with Sophos Security Gateway
- Configuring Windows Server 2008 R2 as a Customer Gateway for Amazon Virtual Private Cloud

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 between your Amazon VPCs as shown in the following figure.

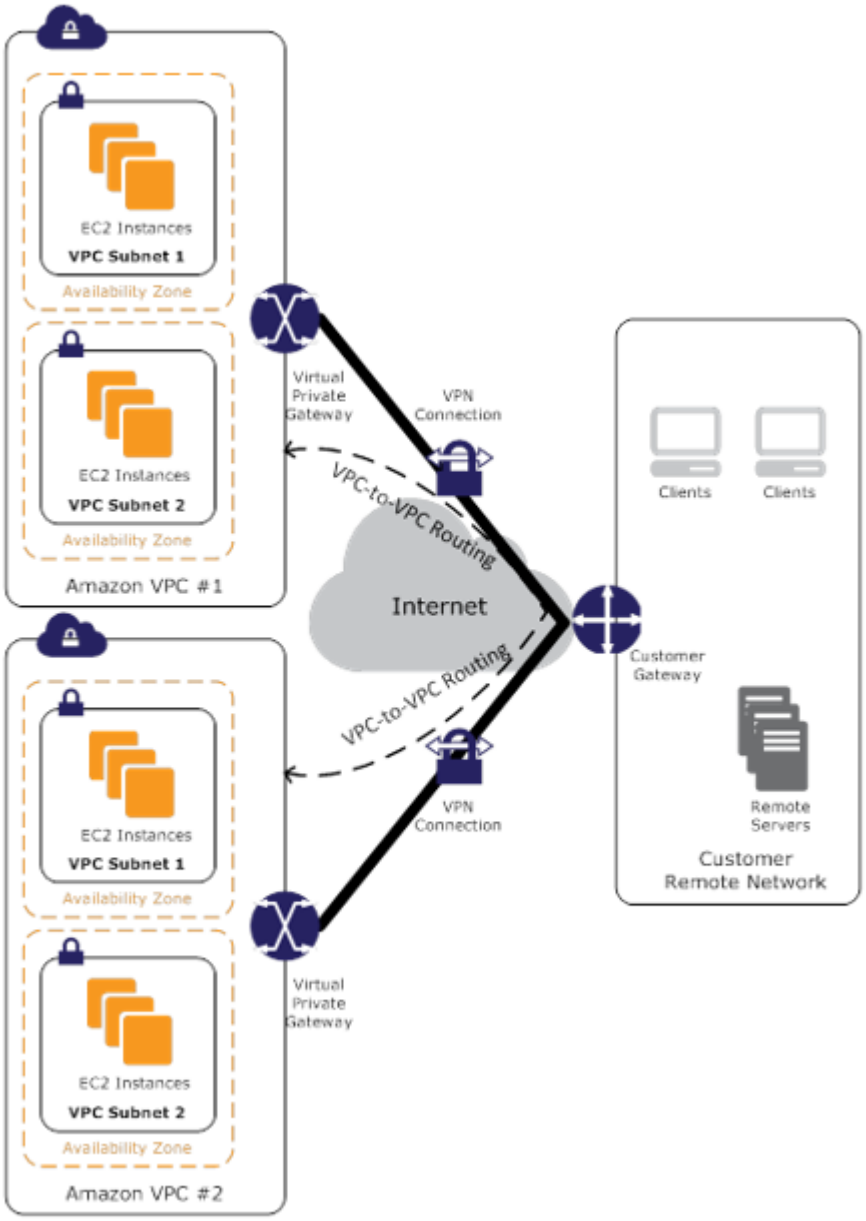

Figure Routing traffic between VPCs

We recommend this approach when you want to take advantage of AWS managed VPN endpoints including the automated multi-data center redundancy and failover built into the AWS side of each VPN connection. Although not shown, the Amazon virtual private gateway represents two distinct VPN endpoints, physically located in separate data centers to increase the availability of each VPN connection.

Amazon virtual private gateway also supports multiple customer gateway connections (as described in the *Network-to-Amazon VPC Connectivity Options* (p. 3) and AWS managed VPN sections and shown in the figure Redundant AWS managed VPN connections), allowing you to implement redundancy and failover on your side of the VPN connection. This solution can also leverage BGP peering to exchange routing information between AWS and these remote endpoints. You can specify routing priorities, policies, and weights (metrics) in your BGP advertisements to influence the network path traffic will take to and from your networks and AWS.

This approach is suboptimal from a routing perspective since the traffic must traverse the internet to get to and from 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

- Amazon VPC User Guide
- Customer Gateway device minimum requirements
- Customer Gateway devices known to work with Amazon VPC
- Tech Brief - Connecting a Single Router to Multiple VPCs

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to your Amazon VPC or among Amazon VPCs. This option can potentially reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than the other VPC-to-VPC connectivity options.

You can divide a physical AWS Direct Connect connection into multiple logical connections, one for each VPC. You can then use these logical connections for routing traffic between VPCs, as shown in the following figure. In addition to intra-region routing, you can connect AWS Direct Connect locations in other regions using your existing WAN providers and leverage AWS Direct Connect to route traffic between regions over your WAN backbone network.

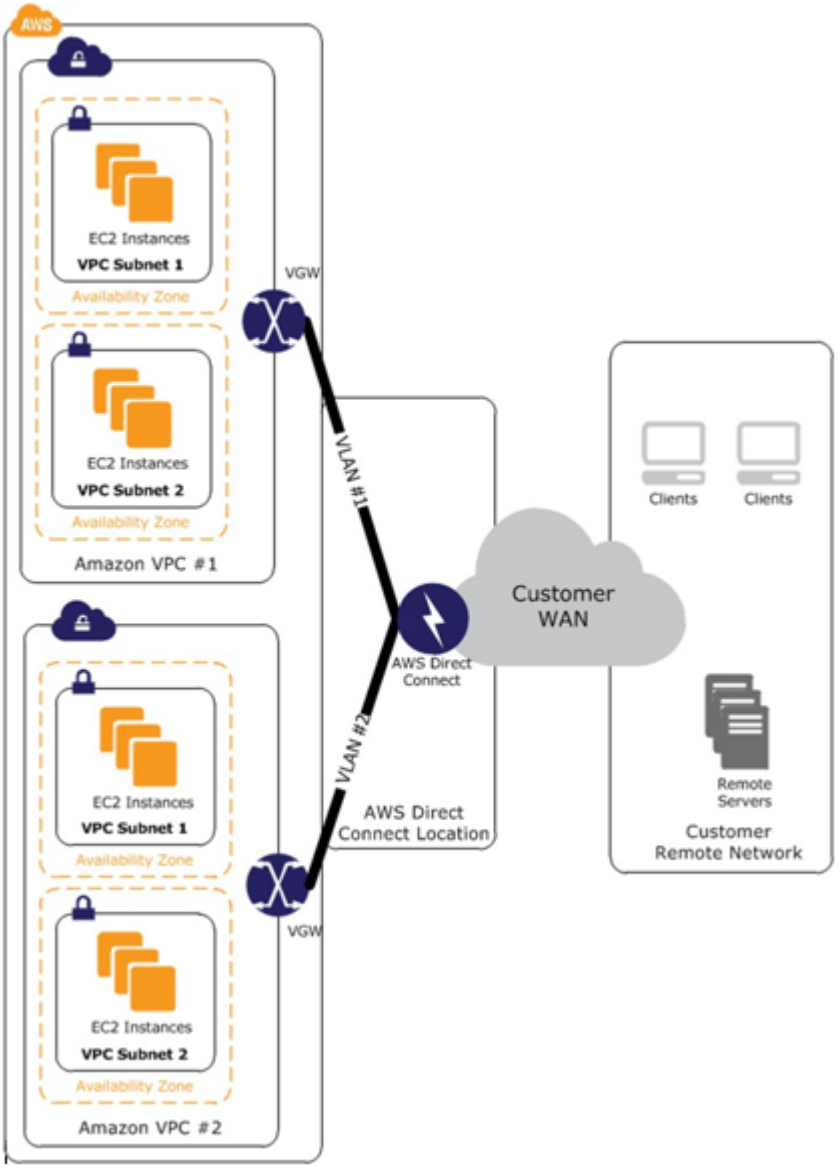

Figure: Intra-region VPC-to-VPC routing with AWS Direct Connect

We recommend this approach if you're already an AWS Direct Connect customer or would like to take advantage of AWS Direct Connect's reduced network costs, increased bandwidth throughput, and more consistent network experience. AWS Direct Connect can provide very efficient routing since traffic can take advantage of 1 GB or 10 GB fiber connections physically attached to the AWS network in each region. Additionally, this service gives you the most flexibility for controlling and managing routing on your local and remote networks, as well as the potential ability to reuse AWS Direct Connect connections.

Additional Resources

- AWS Direct Connect product page
- AWS Direct Connect locations
- AWS Direct Connect FAQs
- Get Started with AWS Direct Connect

AWS PrivateLink

An interface VPC endpoint (AWS PrivateLink) enables you to connect to services powered by AWS PrivateLink. These services include some AWS services, services hosted by other AWS accounts (referred to as *endpoint services*), and supported AWS Marketplace partner services. The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets. The service is now in your VPC, enabling connectivity to AWS services or AWS PrivateLink-powered service via private IP addresses. That means that VPC Security Groups can be used to manage access to the endpoints. Also, interface endpoint can be accessed from your premises via AWS Direct Connect.

In the following diagram, the account owner of VPC B is a service provider, and account owner of VPC A is service consumer.

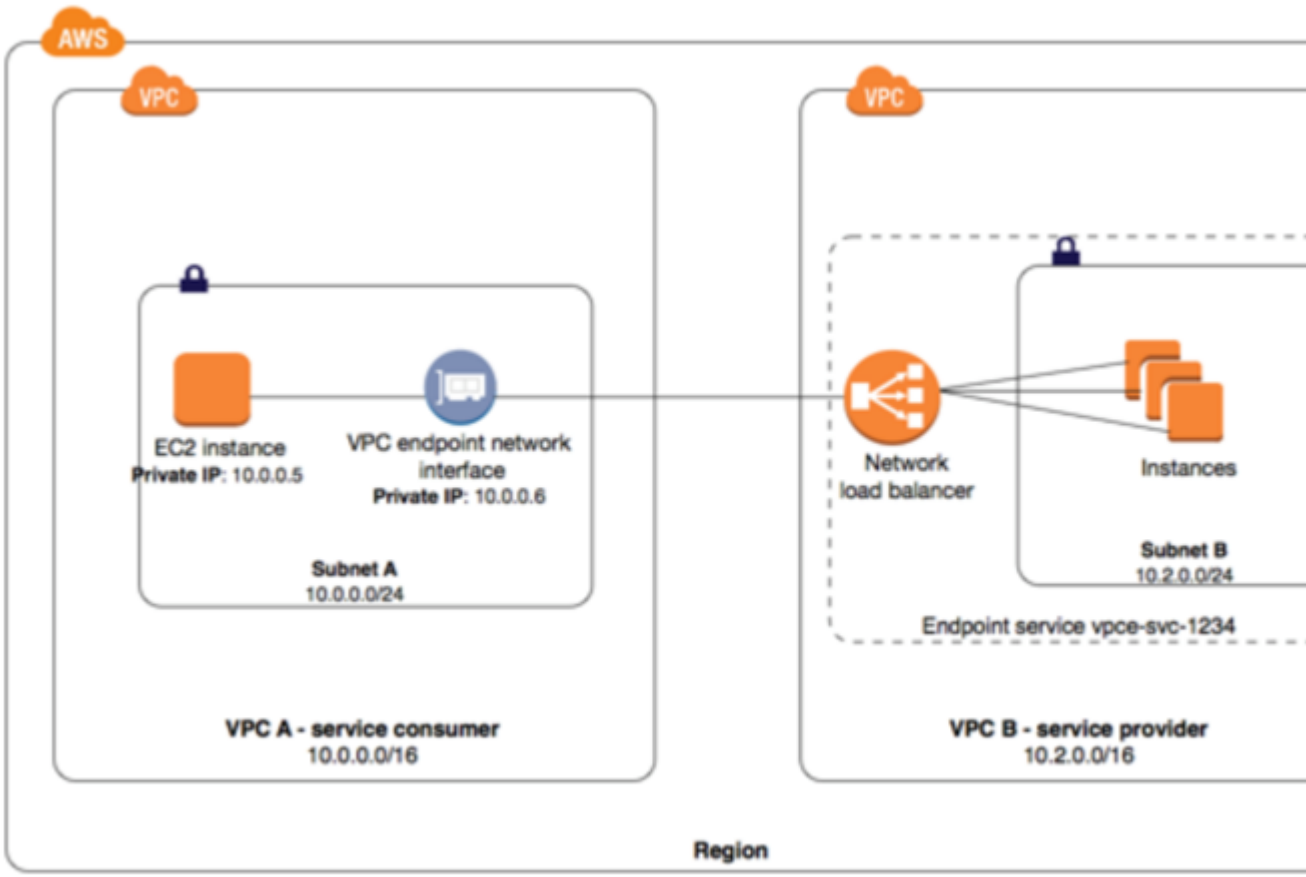

Figure: VPC-to-VPC routing with AWS PrivateLink

We recommend this approach if you want to use service offered by another VPC securely over private connection. You can create interface endpoint to keep all traffic within AWS network.

Additional Resources

- Interface VPC Endpoints
- VPC Endpoint Services

Internal User-to-Amazon VPC Connectivity Options

Internal user access to Amazon VPC resources is typically accomplished either through your *Network-to-Amazon VPC Connectivity Options* (p. 3) or the use of software remote-access VPNs to connect internal users to VPC resources. With the former option, you can reuse your existing on-premises and remote-access solutions for managing end-user access, while still providing a seamless experience connecting to AWS hosted resources. Describing on-premises internal and remote access solutions in any more detail than what has been described in *Network-to-Amazon VPC Connectivity Options* (p. 3) is beyond the scope of this document.

With software remote-access VPN, you can leverage low cost, elastic, and secure AWS services to implement remote-access solutions while also providing a seamless experience connecting to AWS hosted resources. In addition, you can combine software remote-access VPNs with your network-to-Amazon VPC options to provide remote access to internal networks if desired. 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. For more information, see the section called "Software Remote-Access VPN" (p. 24).

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

Option	Use Case	Advantages	Limitations
Network-to-Amazon VPC Connectivity Options	Virtual extension of your data center into AWS	Leverages existing end-user internal and remote-access policies and technologies	Requires existing end-user internal and remote access implementations
Software Remote-Access VPN	Cloud-based remote-access solution to Amazon VPC and/or internal networks	Leverages low-cost, elastic, and secure web services provided by AWS for implementing a remote access solution	Could be redundant if internal and remote access implementations already exist

Software Remote-Access 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 include products from well-known security companies like Check Point, Sophos, OpenVPN Technologies, and Microsoft. The following figure shows a simple remote-access solution leveraging an internal remote user database.

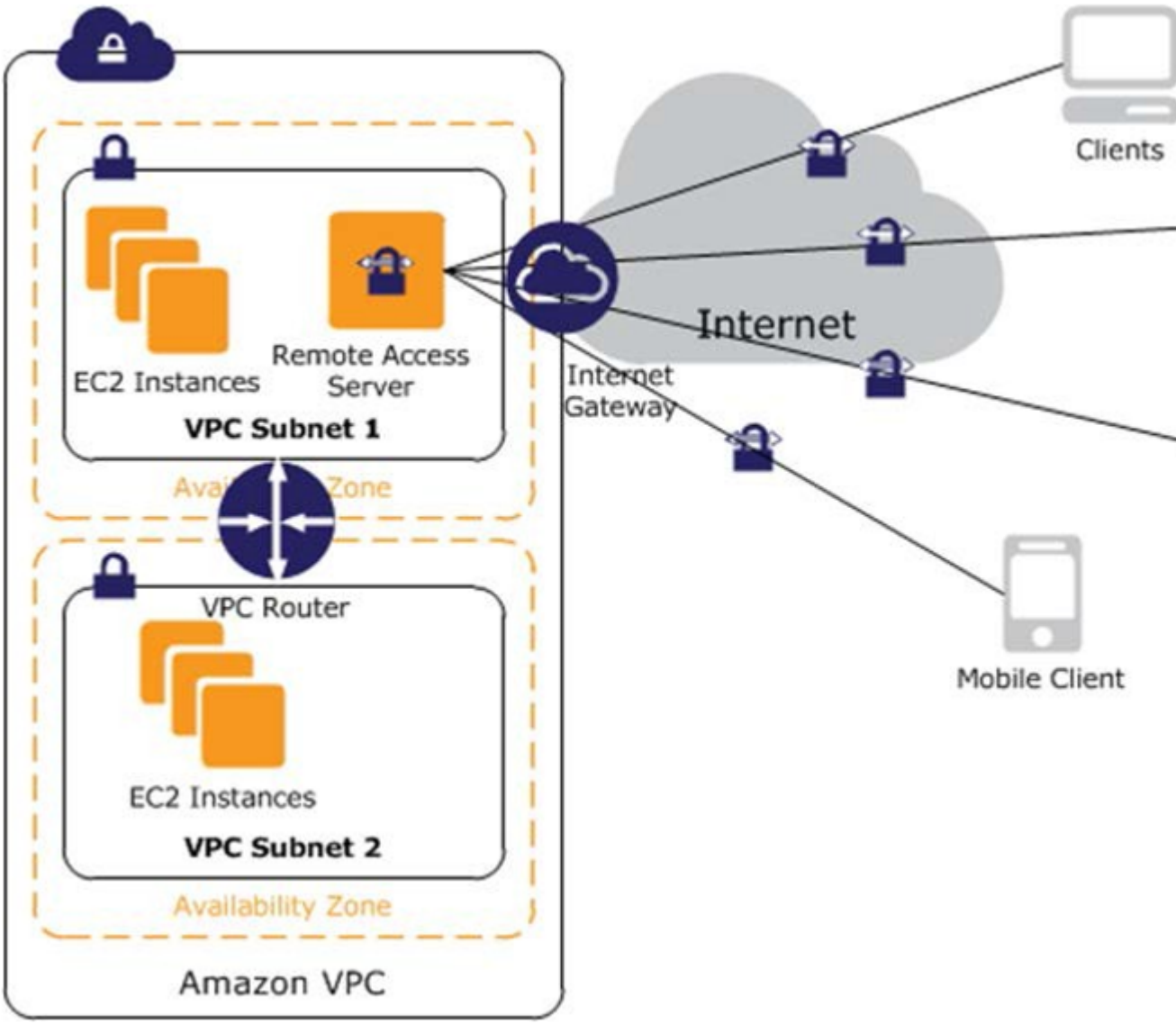

Figure: Remote-access solution

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 following figure shows this combination, allowing the remote-access server to leverage internal access management solutions if desired.

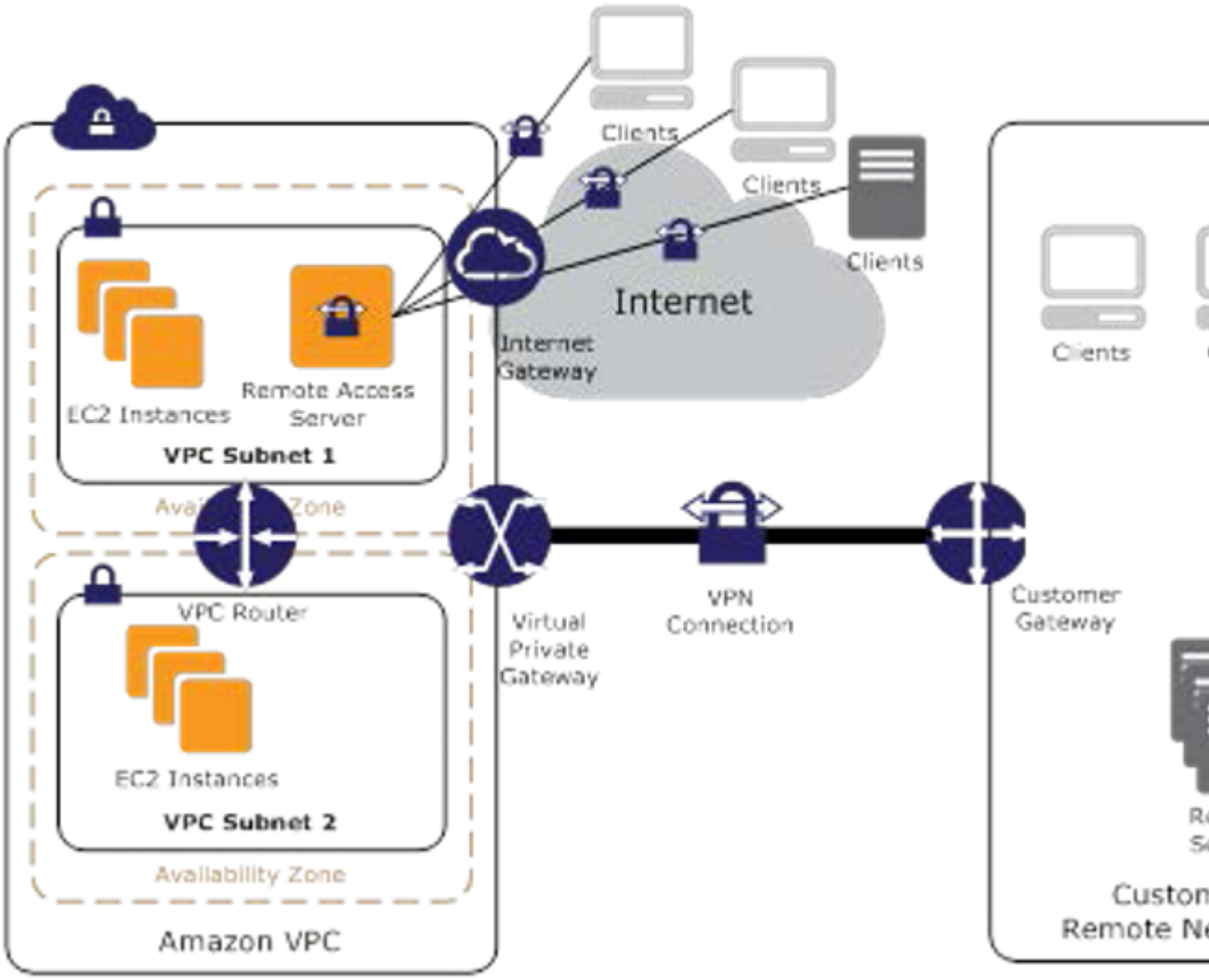

Figure: Combination remote-access solution

As with the software VPN options, the customer is responsible for managing the remote access software including user management, configuration, patches and upgrades.

Additionally, consider that 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: High-Level HA Architecture for Software VPN Instances* (p. 28).

Additional Resources

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

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: 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.

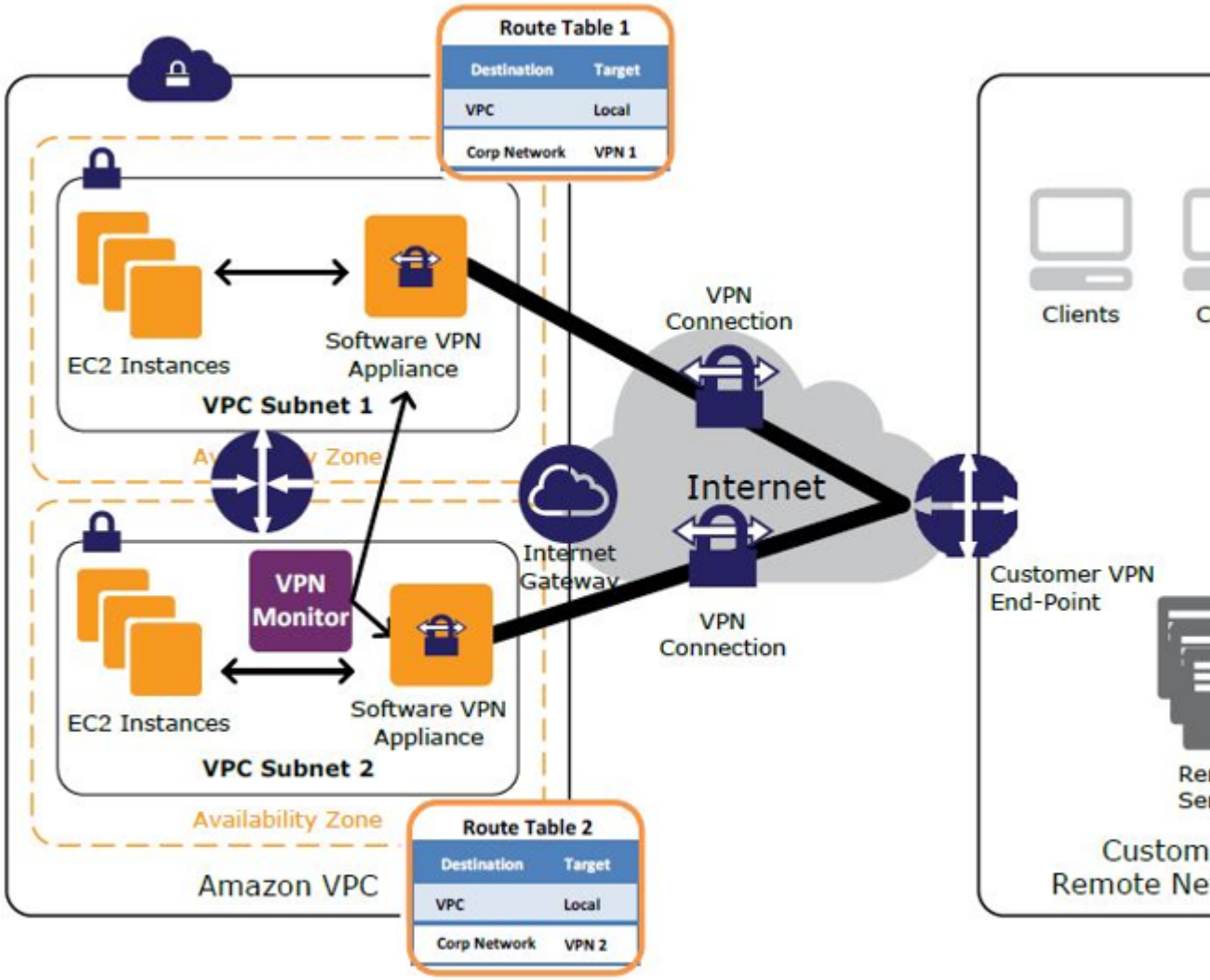

Figure: High-level HA design

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 will allow you to monitor tunnel health, activity, and create automated actions.

Resources

- AWS Architecture Center
- AWS Whitepapers
- AWS Architecture Monthly
- AWS Architecture Blog
- This Is My Architecture videos
- AWS Answers
- AWS Documentation

Document Details

Contributors

The following individuals and organizations contributed to this document:

- Garvit Singh, Solutions Builder , AWS Solution Architecture
- Steve Morad, Senior Manager, Solution Builders , AWS Solution Architecture
- Sohaib Tahir, Solutions Architect, AWS Solution Architecture

Document History

Date	Description
January 2018	Updated information throughout. Focus on the following designs/features: transit VPC, direct connect gateway, and private link.
July 2014	First publication

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the *AWS General Reference*.