Amazon Virtual Private Cloud Connectivity Options

Steve Morad

July 2014

Contents

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 as well as 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 will be 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:

User Network–to–Amazon VPC Connectivity Options	
Hardware VPN	Describes establishing a hardware VPN connection from your network equipment on a remote network to AWS-managed network equipment attached to your Amazon VPC.
AWS Direct Connect	Describes establishing a private, logical connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
AWS Direct Connect + VPN	Describes establishing a private, encrypted connection from your remote network to Amazon VPC, leveraging AWS Direct Connect.
AWS VPN CloudHub	Describes establishing a hub-and-spoke model for connecting remote branch offices.
Software VPN	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	
VPC Peering	Describes the AWS-recommended approach for connecting multiple Amazon VPCs within a region using the Amazon VPC peering feature.
Software VPN	Describes connecting multiple Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
Software-to-Hardware VPN	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.
Hardware VPN	Describes connecting multiple Amazon VPCs, leveraging multiple hardware VPN connections between your remote network and each of your Amazon VPCs.
AWS Direct Connect	Describes connecting multiple Amazon VPCs, leveraging logical connections on customer-managed AWS Direct Connect routers.
Internal User-to-Amazon VPC Connectivity Options	
Software Remote Access VPN	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 (e.g., 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 AWS hosted resources just like any other internally facing resource.

VPC connectivity to remote customer networks is best achieved when using nonoverlapping 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, nonoverlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions.[1]

Option	Use Case	Advantages	Limitations
Hardware VPN	Hardware-based, IPsec VPN connection over the Internet	Reuse existing VPN equipment and processes Reuse existing Internet connections AWS-managed endpoint includes multidata 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)
AWS Direct Connect	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

[1] http://aws.amazon.com/vpc/faqs/

Option	Use Case	Advantages	Limitations
AWS Direct Connect + VPN	Hardware-based, 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
AWS VPN CloudHub	Connect remote branch offices in a hub-and-spoke model for primary or backup connectivity	Reuse existing Internet connections and AWS VPN connections (e.g., use AWS VPN CloudHub as backup connectivity to a third-party MPLS network) AWS-managed virtual private gateway includes multidata center redundancy and automated failover Supports BGP for exchanging routes and routing priorities (e.g., 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)
Software VPN	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)

Hardware VPN

Amazon VPC provides the option of creating an IPsec, hardware VPN connection between remote customer networks and their Amazon VPC over the Internet, as shown in Figure 1. 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 (VGW) represents two distinct VPN endpoints, physically located in separate data centers to increase the availability of your VPN connection.

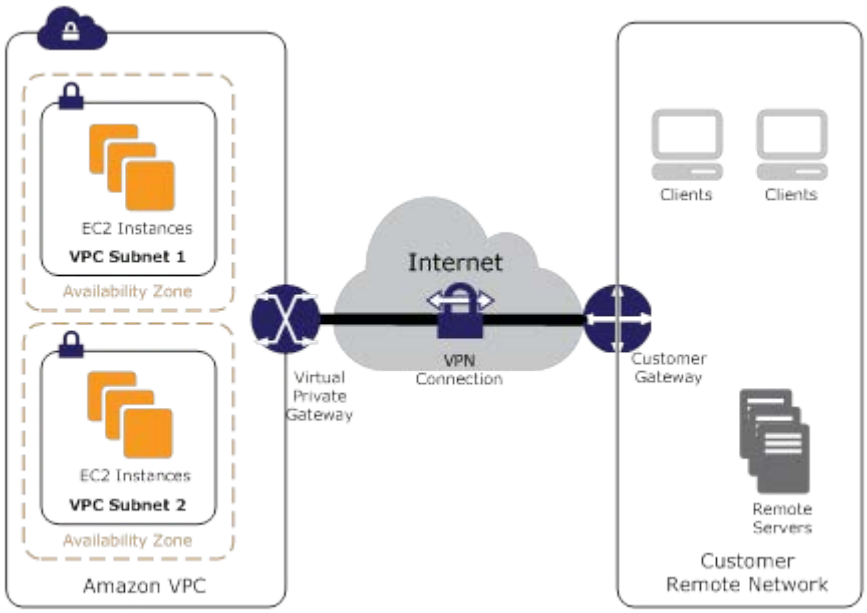

Figure 1: Hardware VPN

The VGW 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 Figure 2. Both dynamic and static routing options are provided to give you flexibility in your routing configuration. Dynamic routing leverages 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 network(s) and AWS.

It is important to note that when BGP is used, 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.

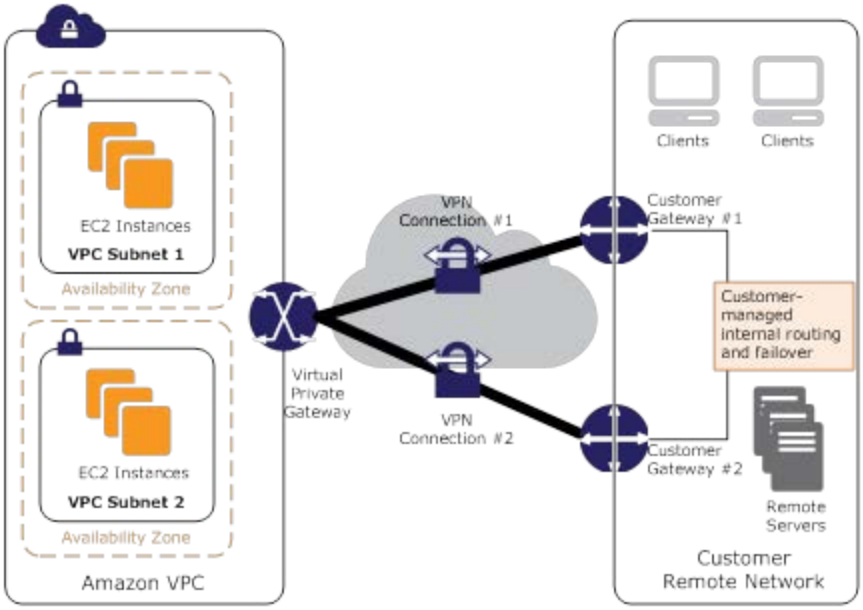

Figure 2: Redundant Hardware VPN Connections

Additional Resources

- Adding a Hardware Virtual Private Gateway to Your VPC[2]
- Customer Gateway device minimum requirements[3]
- Customer Gateway devices known to work with Amazon VPC[4]

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

[2] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

[3] http://aws.amazon.com/vpc/faqs/#C8

[4] http://aws.amazon.com/vpc/faqs/#C9

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. Figure 3 illustrates this pattern.

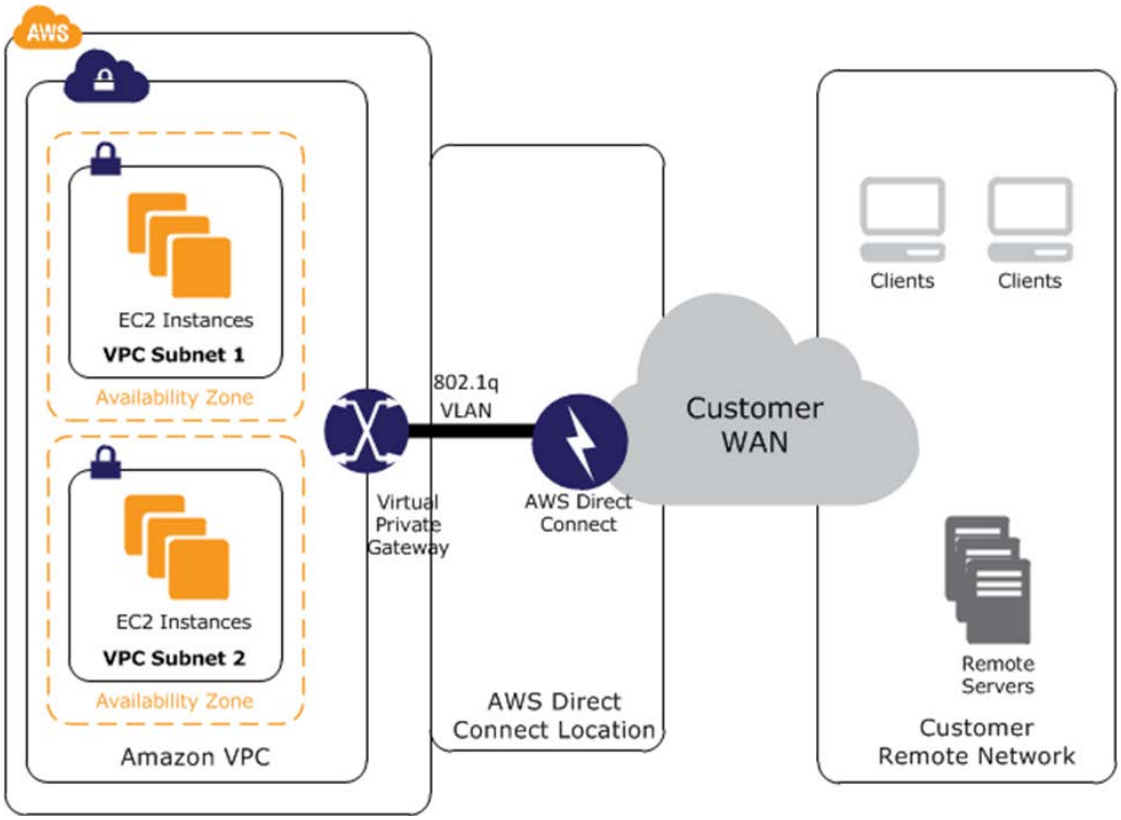

Figure 3: AWS Direct Connect

Additional Resources

- AWS Direct Connect product page[5]
- AWS Direct Connect locations[6]
- AWS Direct Connect FAQs[7]
- Getting Started with AWS Direct Connect[8]

[5] http://aws.amazon.com/directconnect/

[6] http://aws.amazon.com/directconnect/#details

[7] http://aws.amazon.com/directconnect/faqs/

[8] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

AWS Direct Connect + VPN

With AWS Direct Connect + VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC hardware 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 VGW IPsec endpoint. This solution combines the AWS-managed benefits of the hardware VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Figure 4 shows this option.

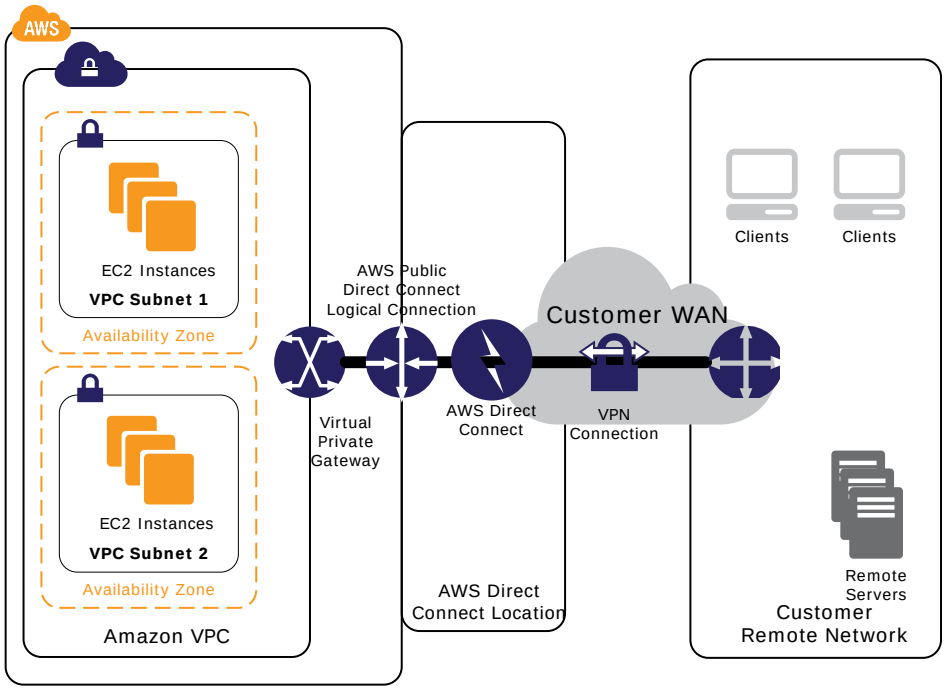

Figure 4: AWS Direct Connect + VPN

Additional Resources

- AWS Direct Connect product page[9]
- AWS Direct Connect FAQs[10]
- Adding a Hardware Virtual Private Gateway to Your VPC

[9] http://aws.amazon.com/directconnect/

[10] http://aws.amazon.com/directconnect/faqs/

AWS VPN CloudHub

Building on the hardware VPN and AWS Direct Connect 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.

Figure 5 depicts the AWS VPN CloudHub architecture, with blue dashed lines indicating network traffic between remote sites being routed over their AWS VPN connections.

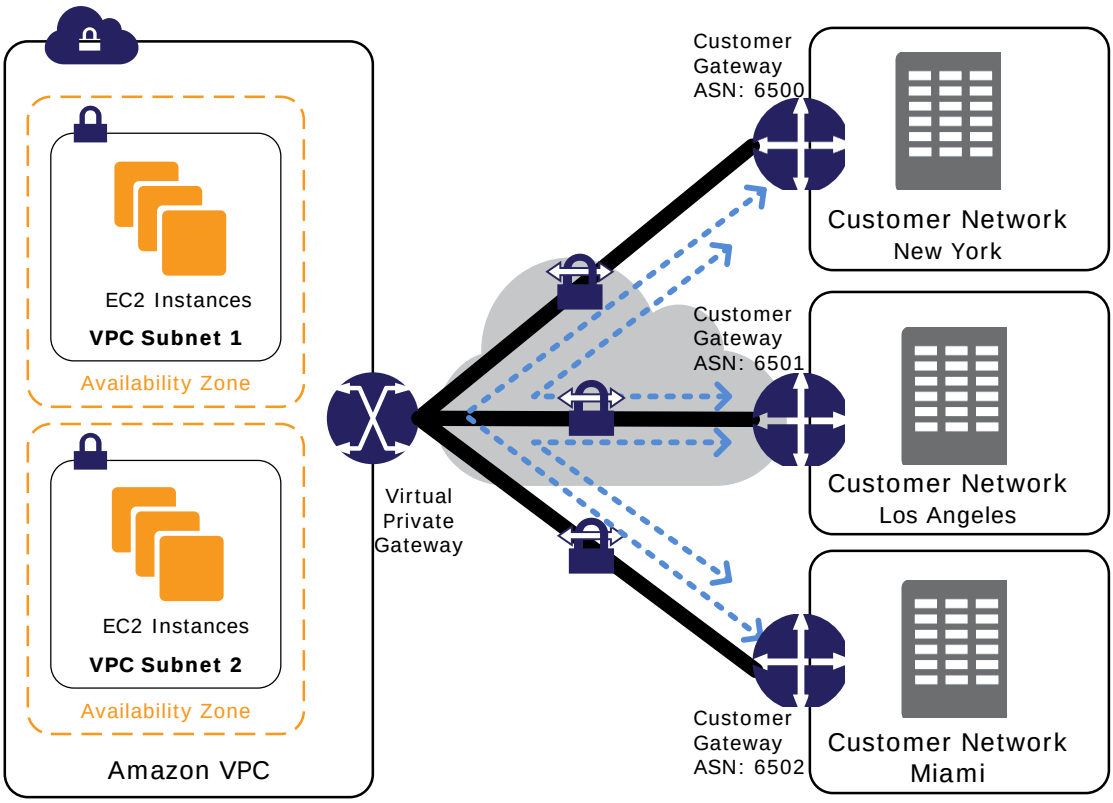

Figure 5: AWS VPN CloudHub

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 hardware VPN options (e.g., multiple gateways per site for redundancy or backbone routing that you provide) depending on your requirements.

Additional Resources

- AWS VPN CloudHub[11]
- Amazon VPC VPN Guide
- Customer Gateway device minimum requirements[12]
- Customer Gateway devices known to work with Amazon VPC[13]
- AWS Direct Connect product page[14]

[11] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

[12] http://aws.amazon.com/vpc/faqs/#C8

[13] http://aws.amazon.com/vpc/faqs/#C9

[14] http://aws.amazon.com/directconnect/

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 hardware VPN solution. Figure 6 shows this option.

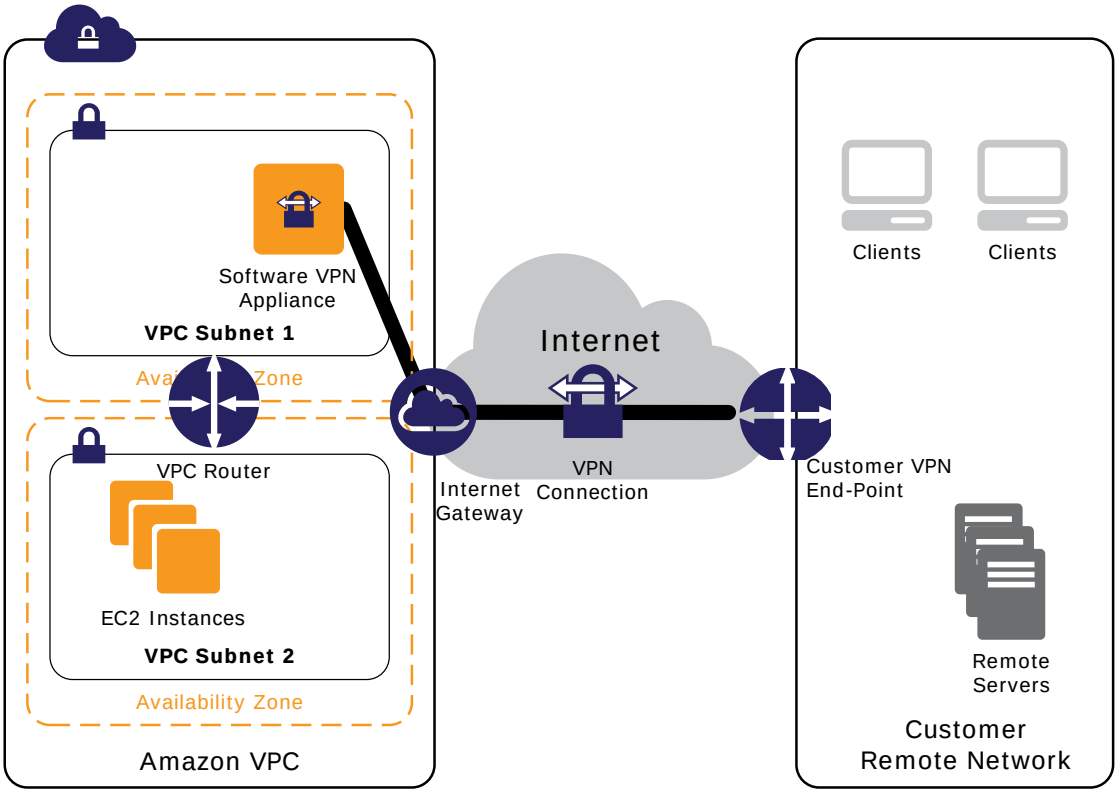

Figure 6: Software VPN

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 as the software VPN appliance runs on a single Amazon EC2 instance. See "Appendix A: High-Level HA Architecture for Software VPN Instances" for additional information.

Additional Resources

- VPN Appliances from the AWS Marketplace[15]
- Tech Brief - Connecting Cisco ASA to VPC EC2 Instance (IPSec)[16]
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPSec)[17]
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)[18]

[15] https://aws.amazon.com/marketplace/search/results/ref=brs_navgno_search_box?searchTerms=vpn

[16] http://aws.amazon.com/articles/8800869755706543

[17] Although these guides specifically address connecting multiple Amazon VPCs, they are easily adaptable to support this network configuration by substituting one of the VPCs with an on-premises VPN device connecting to an IPsec or SSL software VPN appliance running in an Amazon VPC.

[18] http://aws.amazon.com/articles/0639686206802544

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 UsCustomer 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 nonoverlapping 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, nonoverlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions: http://aws.amazon.com/vpc/faqs/.

Option	Use Case	Advantages	Limitations
VPC peering	AWS-provided network connectivity between two VPCs within a single region.	• Leverages AWS networking infrastructure within a region • Does not rely on VPN instances or a separate piece of physical hardware • No single point of failure • No bandwidth bottleneck	• Peering connections are currently only supported within an AWS region
Software VPN	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
Software-to-hardware VPN	Software appliance to Hardware VPN connection between VPCs	• Leverages AWS networking equipment in-region and Internet pipes between regions • AWS-managed endpoint includes multidata center redundancy and automated failover	• 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
Hardware VPN	VPC-to-VPC routing managed by you over hardware-based, IPsec VPN connections using your equipment and the Internet	• Reuse existing Amazon VPC VPN connections • AWS-managed endpoint includes multidata 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)
AWS Direct Connect	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

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 within a region. VPC peering connections can be created between your own VPCs or with a VPC in another AWS account within the same AWS region.

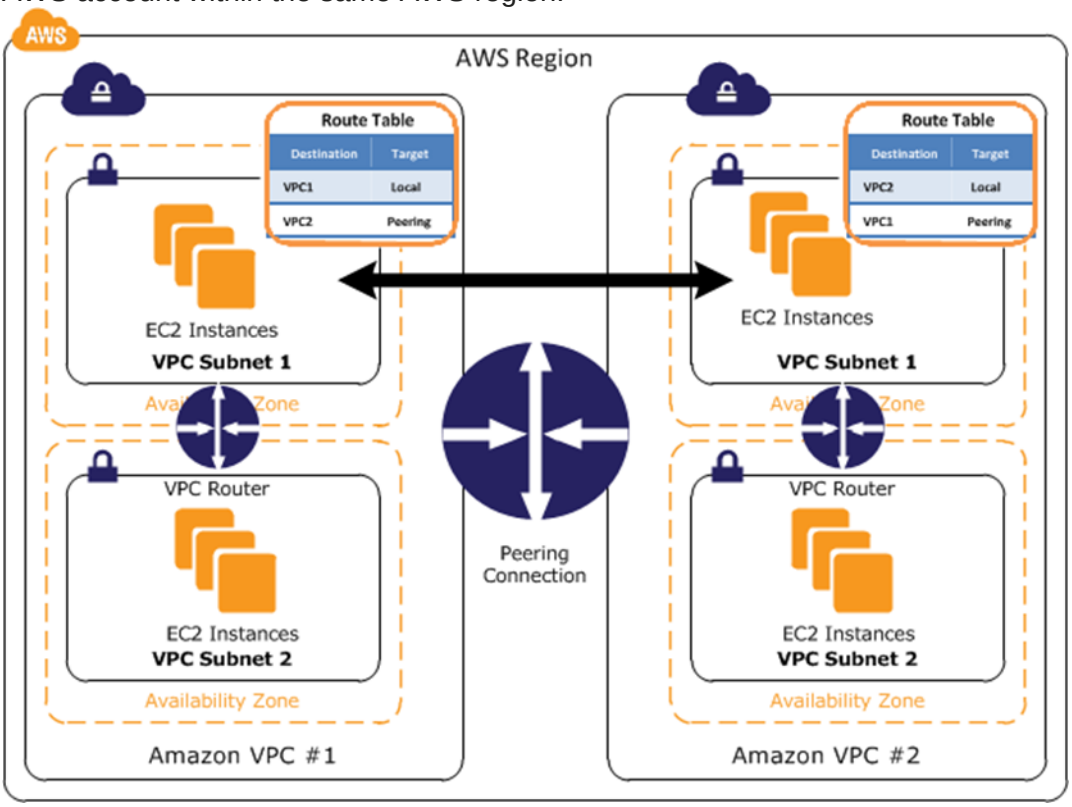

Figure 7: VPC-to-VPC Peering

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.[19]

Additional Resources

- Amazon VPC User Guide[20]
- Amazon VPC Peering Guide

[19] http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/

[20] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

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.

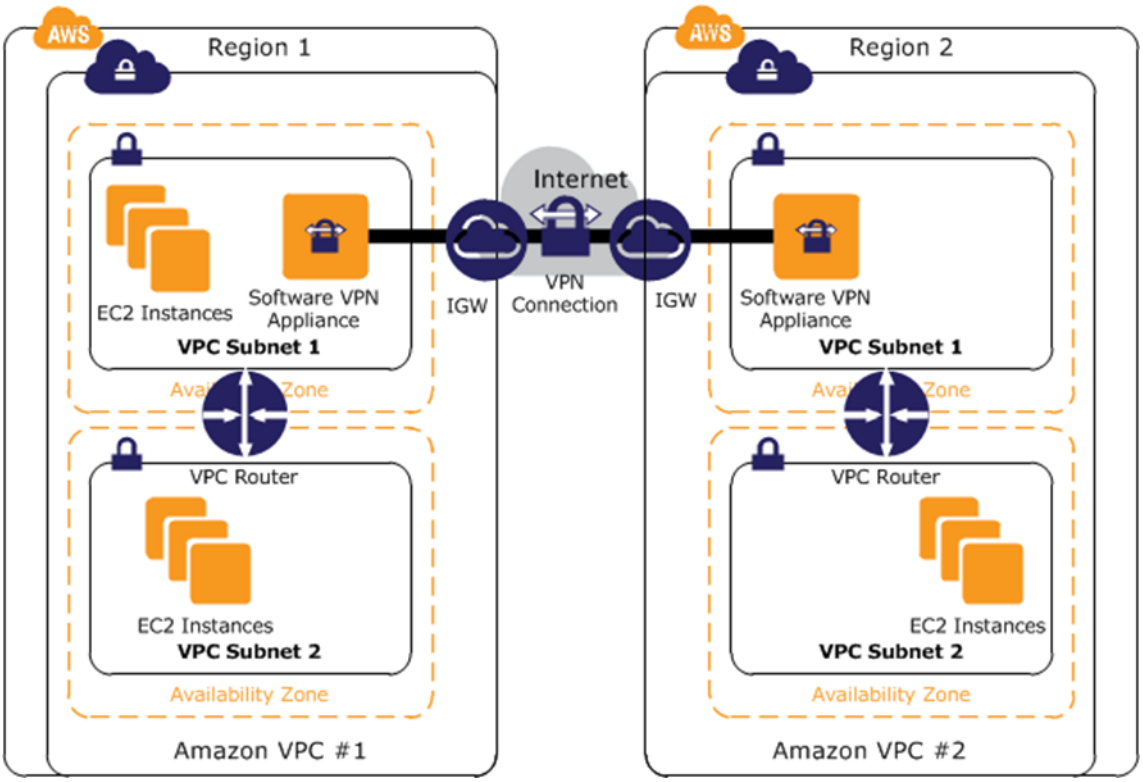

Figure 8: Interregion VPC-to-VPC Routing

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. See “Appendix A: High-Level HA Architecture for Software VPN Instances” for additional information.

Additional Resources

- VPN Appliances from the AWS Marketplace
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPSec)[21]
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)[22]

Software-to-Hardware VPN

Amazon VPC provides the flexibility to combine the hardware 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 hardware VPN endpoint including automated multidata center redundancy and failover built into the VGW 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 Figure 9.

[21] http://aws.amazon.com/articles/5472675506466066

[22] http://aws.amazon.com/articles/0639686206802544

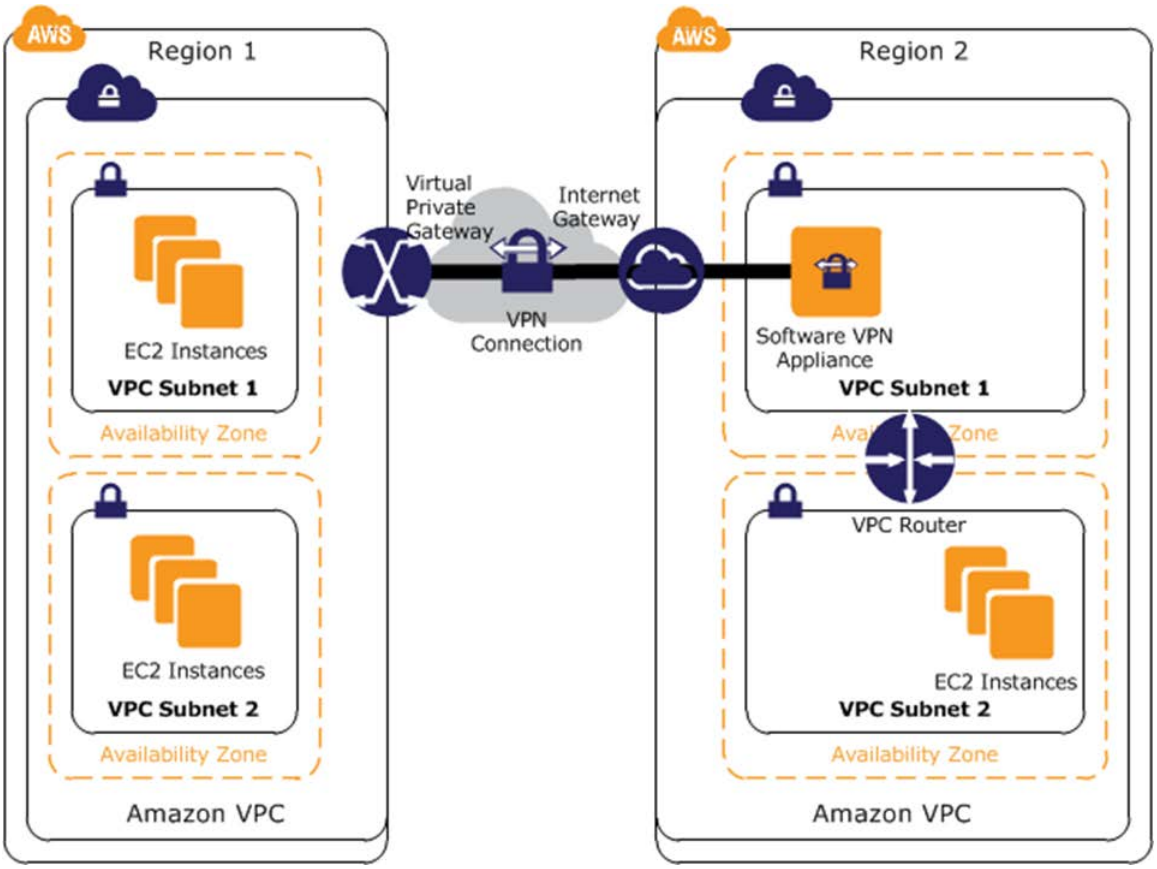

Figure 9: Intraregion VPC-to-VPC Routing

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. Please see "Appendix A: High-Level HA Architecture for Software VPN Instances" for additional information.

Additional Resources

- Tech Brief - Connecting Multiple VPCs with Sophos Security Gateway[23]
- Configuring Windows Server 2008 R2 as a Customer Gateway for Amazon Virtual Private Cloud[24]

[23] http://aws.amazon.com/articles/1909971399457482

[24] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/CustomerGateway-Windows.html

Hardware VPN

Amazon VPC provides the option of creating a hardware IPsec VPN to connect your remote networks with your Amazon VPCs over the Internet. You can leverage multiple hardware VPN connections to route traffic between your Amazon VPCs as shown in Figure 10.

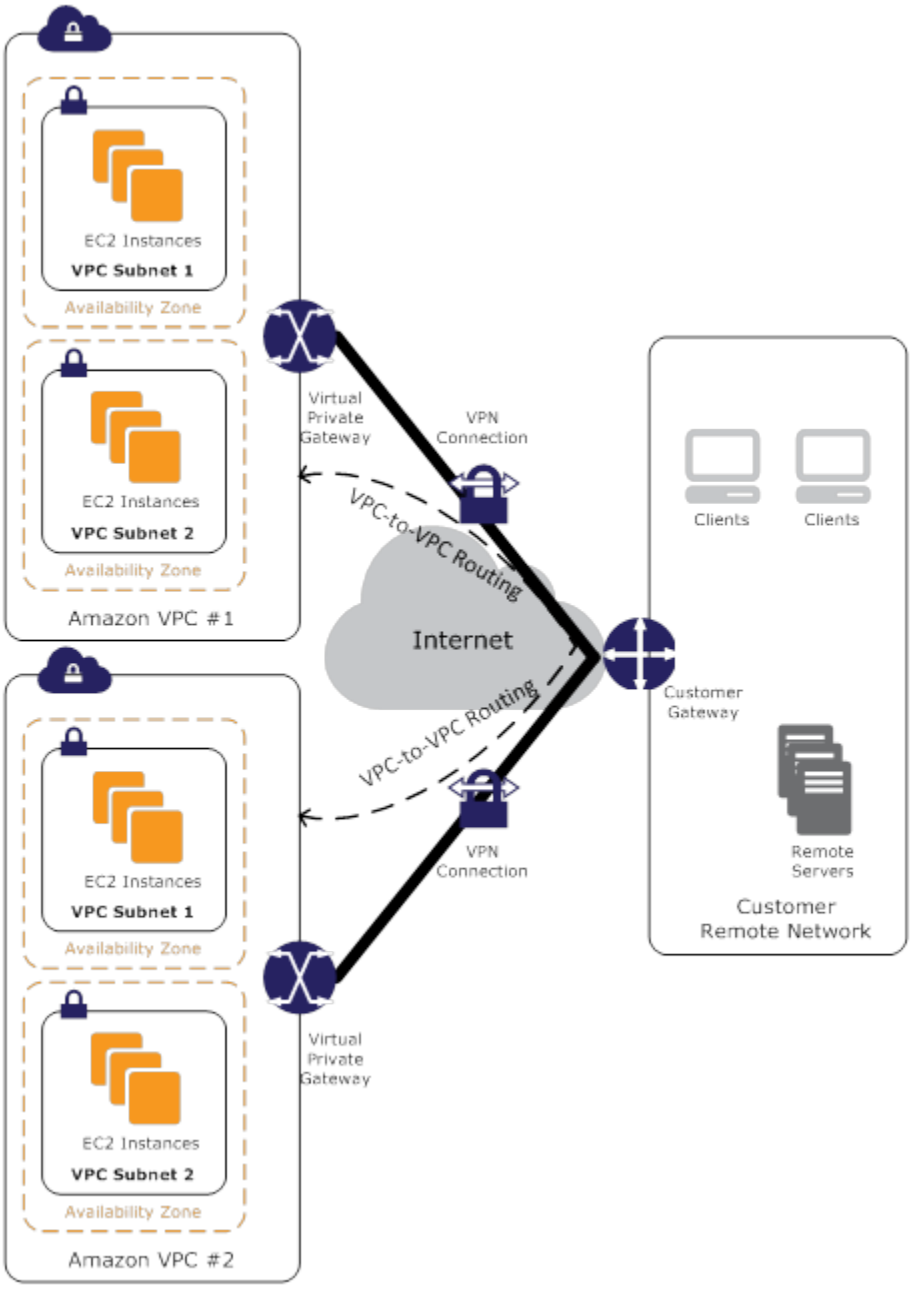

Figure 10: Routing Traffic between VPCs

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

Amazon VGW also supports multiple customer gateway connections (as described in the "Customer Network–to–Amazon VPC Options" and "Hardware VPN" sections and shown in Figure 2), 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 network(s) 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, as well as the potential ability to reuse hardware VPN connections.

Additional Resources

- Amazon VPC Users Guide
- Customer Gateway device minimum requirements
- Customer Gateway devices known to work with Amazon VPC
- Tech Brief - Connecting a Single Router to Multiple VPCs[25]

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 Figure 11. In addition to intraregion 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.

[25] http://aws.amazon.com/articles/5458758371599914

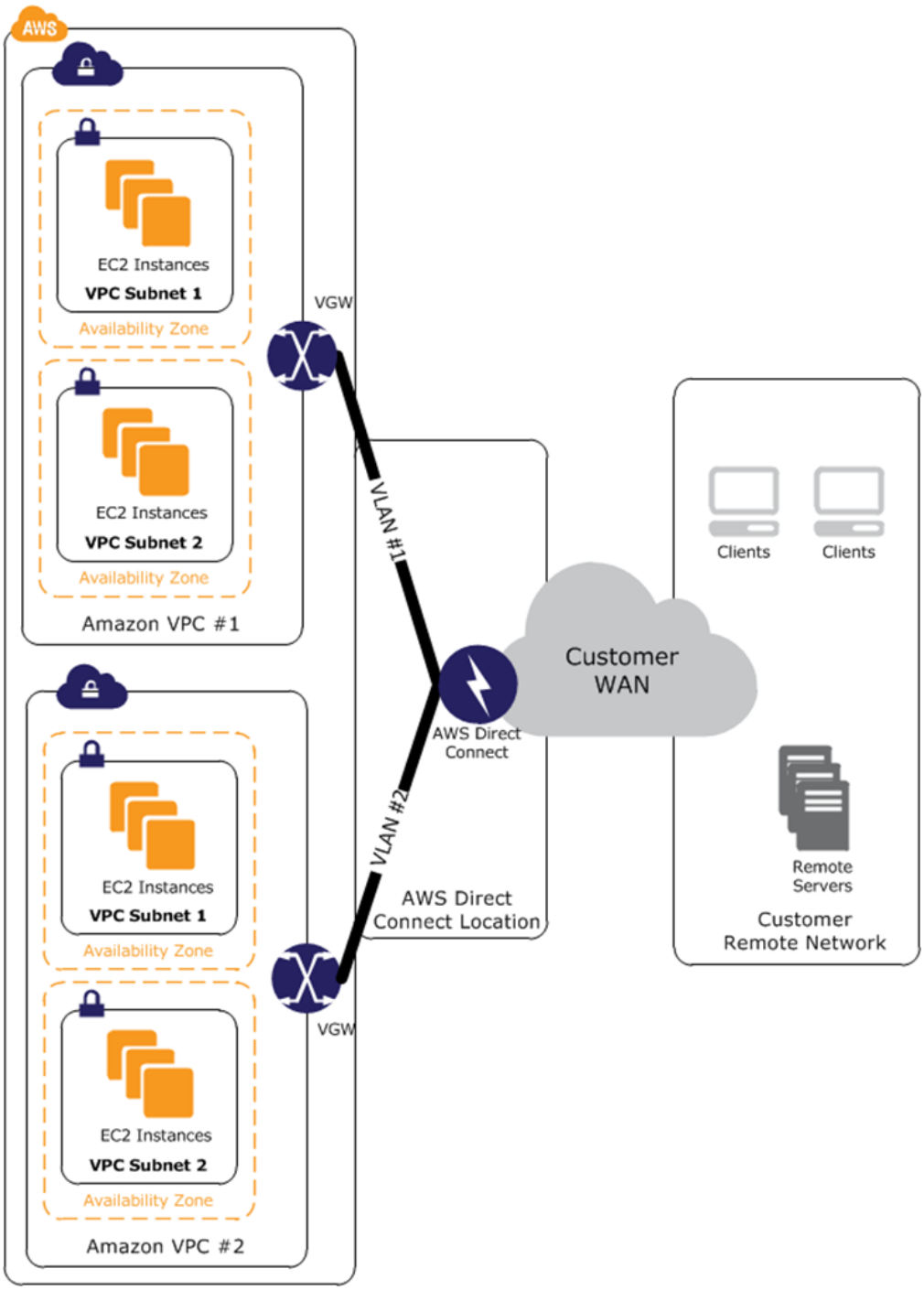

Figure 11: Intraregion VPC-to-VPC Routing with AWS Direct Connect

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[26]
- AWS Direct Connect locations[27]
- AWS Direct Connect FAQs[28]
- Get Started with AWS Direct Connect[29]

[26] http://aws.amazon.com/directconnect/

[27] http://aws.amazon.com/directconnect/#details

[28] http://aws.amazon.com/directconnect/faqs/

[29] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

Internal User-to-Amazon VPC Connectivity Options

Internal user access to Amazon VPC resources is typically accomplished either through your network–to-Amazon VPC options 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 “Customer Network–to–Amazon VPC Options” is beyond the scope of this document.

With software remote-access VPN, you can leverage low cost, elastic, and secure Amazon Web 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.

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

Option	Use Case	Advantages	Limitations
User Network-to-Amazon VPC 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. Figure 12 shows a simple remote-access solution leveraging an internal remote user database.

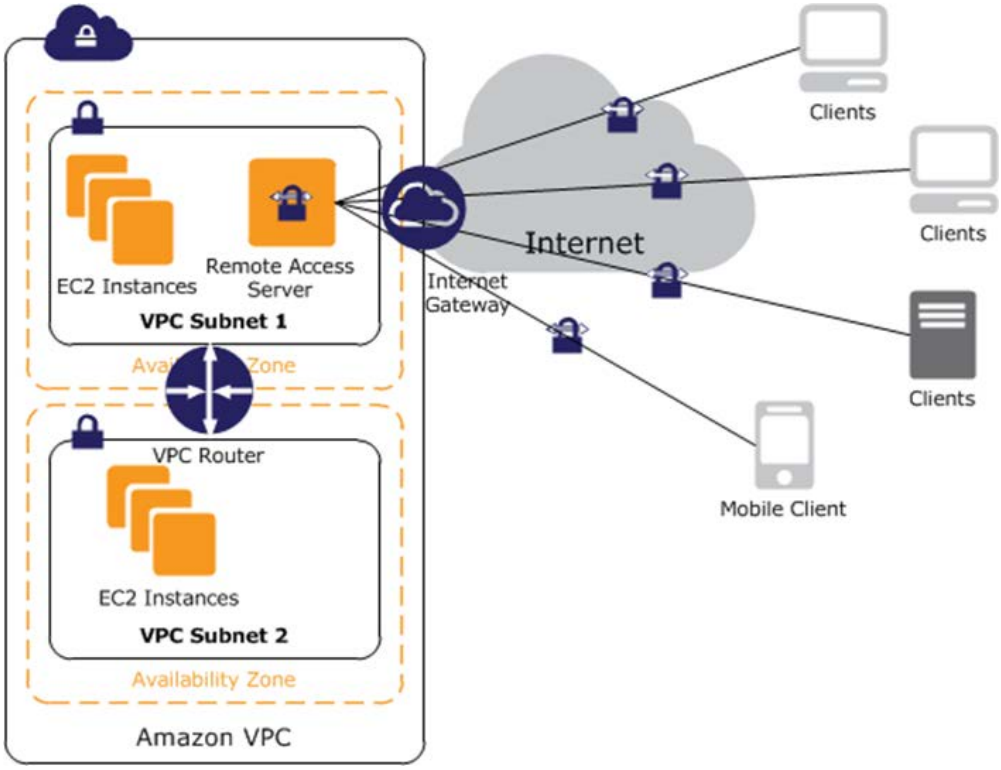

Figure 12: Remote-access Solution

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. Figure 13 shows this combination, allowing the remote-access server to leverage internal access management solutions if desired.

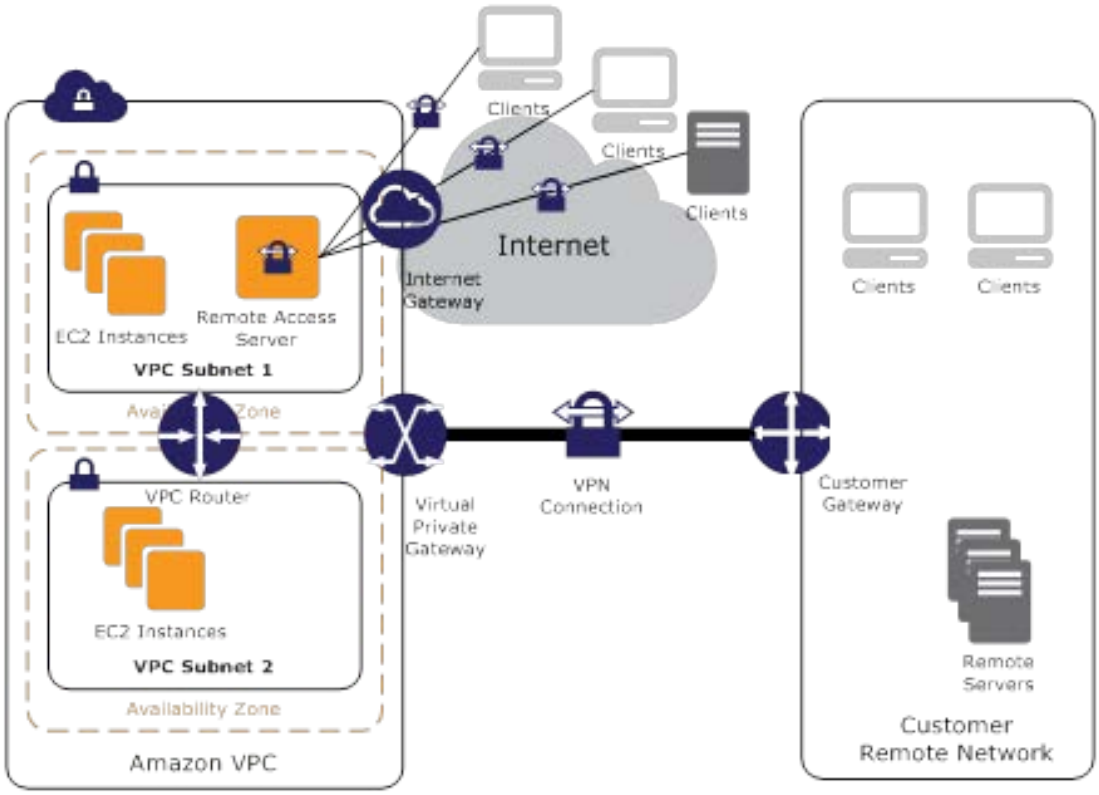

Figure 13: Combination Remote-access Solution

As with the software VPN options, the customer is responsible for managing the remote access software including user management, configuration, patches and upgrades. Additionally, please note 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. Please see "Appendix A: High-Level HA Architecture for Software VPN Instances" for additional information.

Additional Resources

- VPN Appliances from the AWS Marketplace
- OpenVPN Access Server Quick Start Guide[30]

[30] http://docs.openvpn.net/how-to-tutorialsguides/virtual-platforms/amazon-ec2-appliance-ami-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 others have leveraged to successfully integrate their remote networks or multiple Amazon VPC networks. We hope that these options will help you 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.

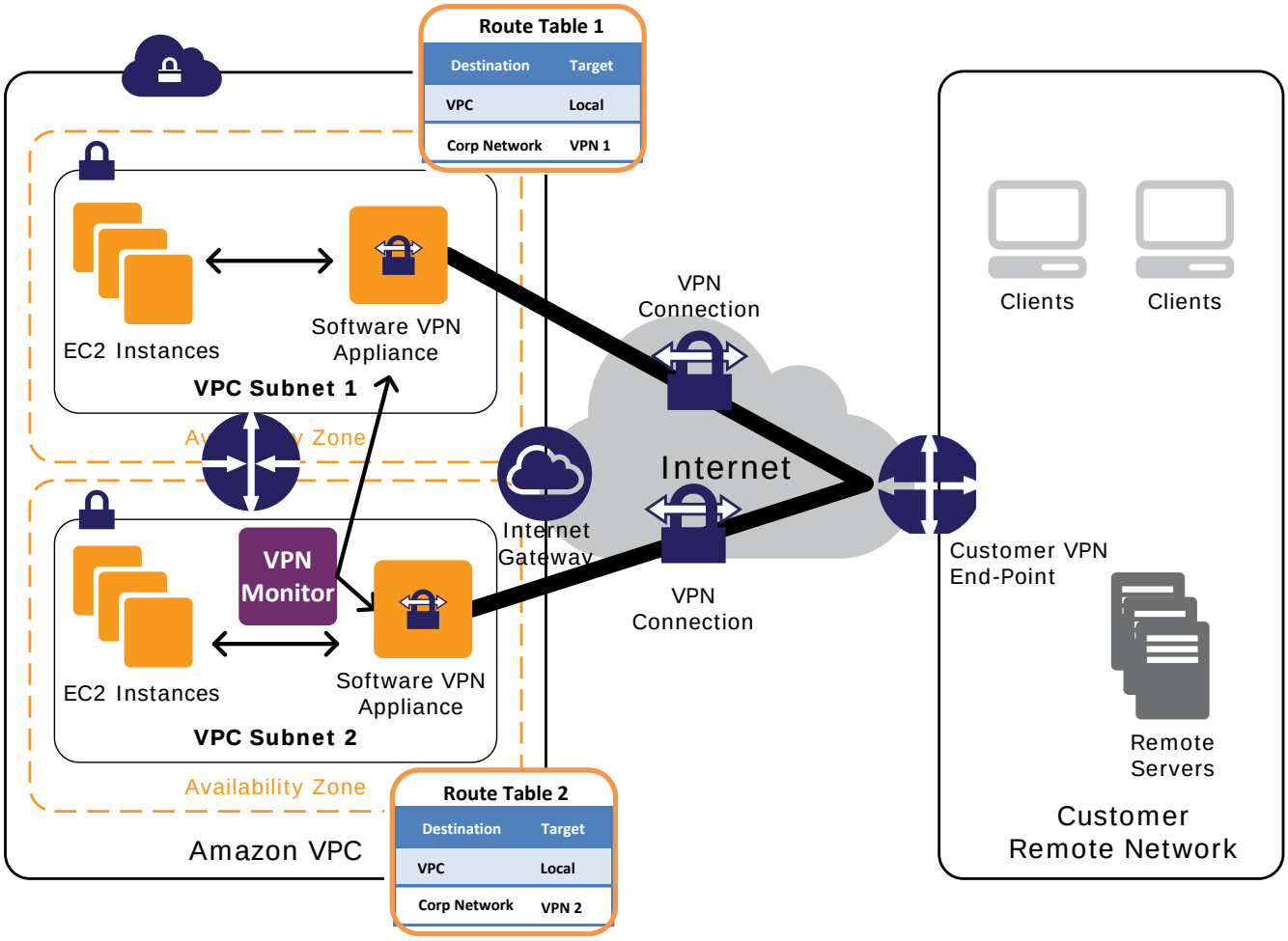

Figure 14: High-Level HA Design

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 will then provide VPN connectivity for instances that share the same Availability Zone.

VPN Monitoring Instance(s)

The VPN monitor is a custom instance that you will need to create and develop monitoring scripts to run on. 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. Please think through the necessary business logic to provide notification and/or attempt to automatically repair network connectivity in the event of a VPN connection failure.