Amazon Virtual Private Cloud Connectivity Options

Steve Morad
October 2012

(Please consult http://aws.amazon.com/whitepapers/ for the latest version of this paper)

Table of 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 interconnecting their AWS virtual networks with other remote networks. This document describes several common network connectivity options available to our customers. This includes connectivity options for integrating remote customer networks with Amazon VPC as well as interconnecting 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 is intended to provide an overview of the various options to facilitate network connectivity discussions as well as provide pointers to additional documentation and resources that provide more detailed information or examples.

Introduction

Amazon VPC provides multiple network connectivity options for our customers to leverage depending on their 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 customer-managed network endpoints. Additionally, AWS allows customers to choose how network routing will be delivered between Amazon VPC and customer networks leveraging either AWS or customer-managed network equipment and routes. This whitepaper breaks down these options into the following sections and subsections (each section starts with an overview, including a high-level comparison of each option):

Customer Network–to–Amazon VPC Connectivity Options	
Hardware VPN	Describes establishing a hardware VPN connection from a customer's network equipment on a remote network to AWS-managed network equipment attached to a customer's Amazon VPC.
AWS Direct Connect	Describes establishing a private, logical connection from a customer's remote network to Amazon VPC leveraging AWS Direct Connect.
AWS Direct Connect + VPN	Describes establishing a private, encrypted connection from a customer's 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 a customer's equipment on a remote network to a customer-managed software VPN appliance running inside an Amazon VPC.
Amazon VPC–to–Amazon VPC Connectivity Options	
Software VPN	Describes interconnecting multiple Amazon VPCs using VPN connections established between customer-managed software VPN appliances running inside of each Amazon VPC.
Software-to-Hardware VPN	Describes interconnecting multiple Amazon VPCs with a VPN connection established between a customer-managed software VPN appliance in one Amazon VPC and AWS-managed network equipment attached to the other Amazon VPC.
Hardware VPN	Describes interconnecting multiple Amazon VPCs leveraging multiple hardware VPN connections established between a customer's remote network and each of their Amazon VPCs.
AWS Direct Connect	Describes interconnecting 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.

Customer Network–to–Amazon VPC Connectivity Options

This section provides design patterns for customers who want to interconnect remote networks with their Amazon VPC environment. These options are useful for integrating AWS resources with a customer's 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 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 non-overlapping IP ranges for each network being interconnected. For example, if you'd like to interconnect one or more VPCs to your home network, make sure they are configured with unique Classless Inter-Domain Routing (CIDR) ranges. Therefore, we advise customers 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: http://aws.amazon.com/vpc/faqs/.

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 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)
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
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 CloudHub as backup connectivity to a 3rd party MPLS network) • AWS-managed virtual private gateway includes multi–data 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 • Customer-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 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. We recommend this approach for customers who would like to take advantage of an AWS-managed VPN endpoint that includes automated multi–datacenter 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.

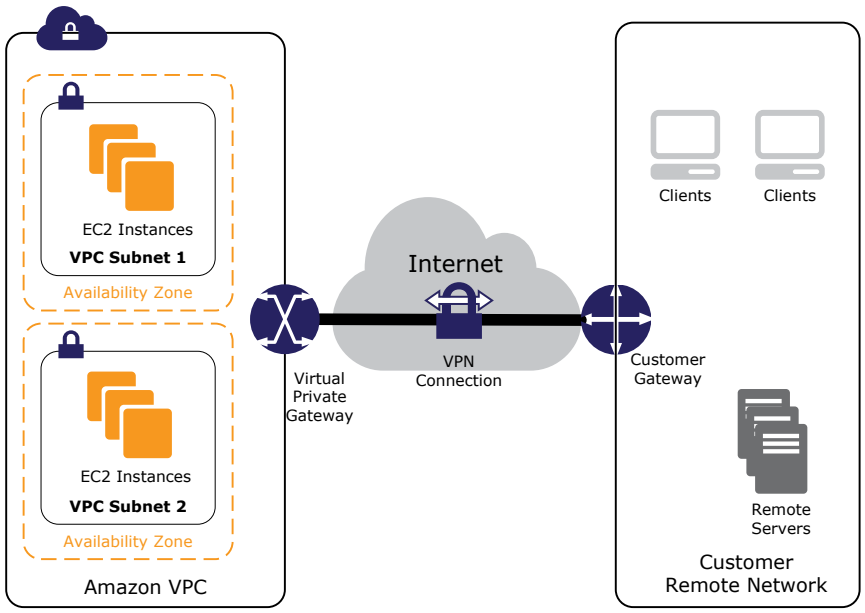

Figure 1 – Hardware VPN

Amazon VGW also supports and encourages multiple customer gateway connections so customers may implement redundancy and failover on their side of the VPN connection as shown in Figure 2. Both dynamic and static routing options are provided to give customers flexibility in their routing configuration. Dynamic routing leverages BGP peering to exchange routing information between AWS and these remote endpoints. Dynamic routing also allows customers to specify routing priorities, policies, and weights (metrics) in their BGP advertisements and to influence the network path between their 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 customer gateway device, so it must be capable of terminating both IPSec and BGP connections.

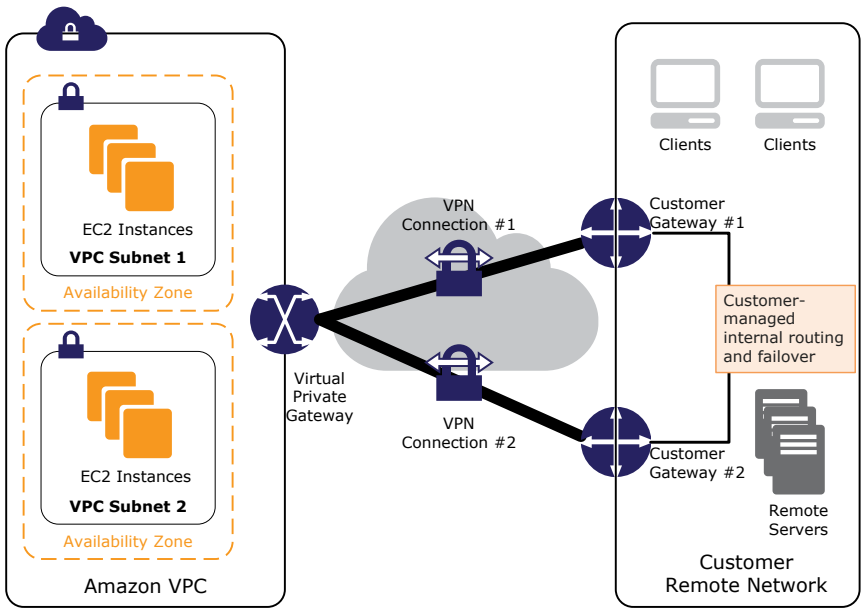

Figure 2 – Redundant Hardware VPN Connections

Additional Resources

- Adding a Hardware Virtual Private Gateway to Your VPC
- 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 network connection from on-premise to Amazon VPC. Using AWS Direct Connect, customers can establish private connectivity between AWS and their 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 customers establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations, and uses industry standard VLANs to access Amazon Elastic Compute Cloud (Amazon EC2) instances running within an Amazon VPC using private IP addresses. Customers may choose from an ecosystem of WAN service providers for integrating their AWS Direct Connect endpoint in an AWS Direct Connect location with their remote networks. Figure 3 illustrates this pattern.

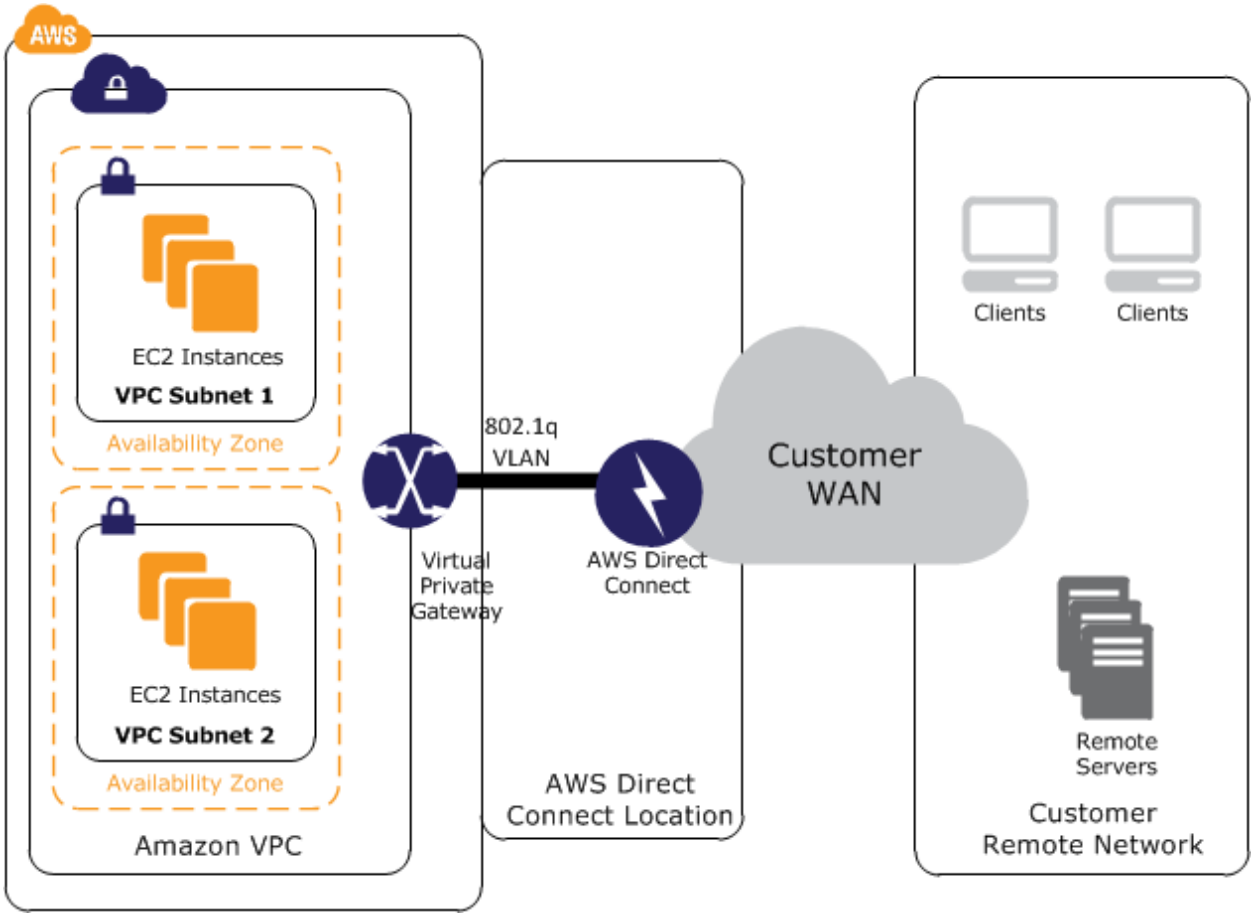

Figure 3 – AWS Direct Connect

Additional Resources

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

AWS Direct Connect + VPN

AWS Direct Connect + VPN allows customer to 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.

AWS Direct Connect lets customers establish a dedicated network connection between their network and one of the AWS Direct Connect locations and use an industry standard VLANs to 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 network experience benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Figure 4 shows this option.

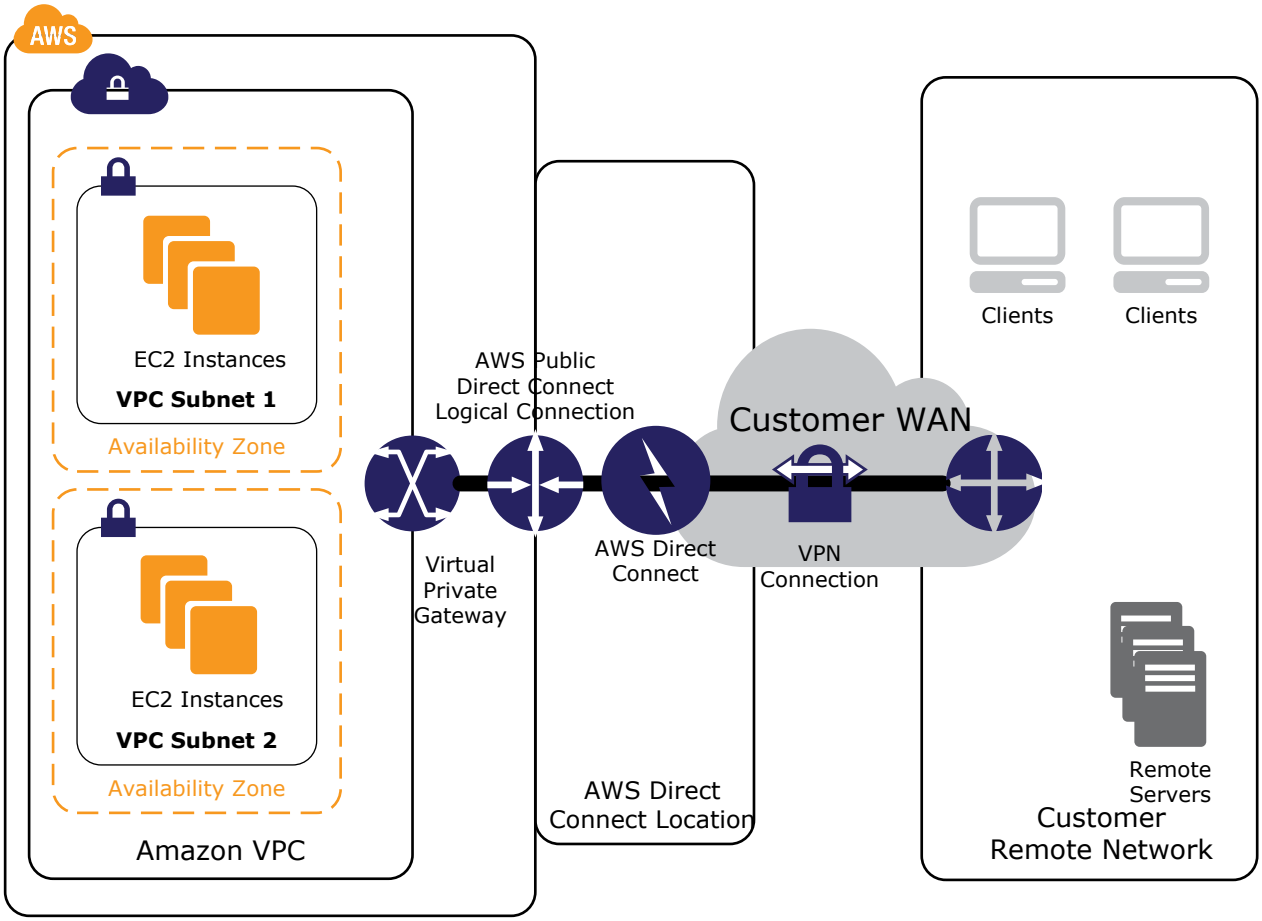

Figure 4 – AWS Direct Connect + VPN

Additional Resources

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

AWS VPN CloudHub

Building on the Hardware VPN and AWS Direct Connect options described previously, customers can securely communicate from one site to another using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who 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.

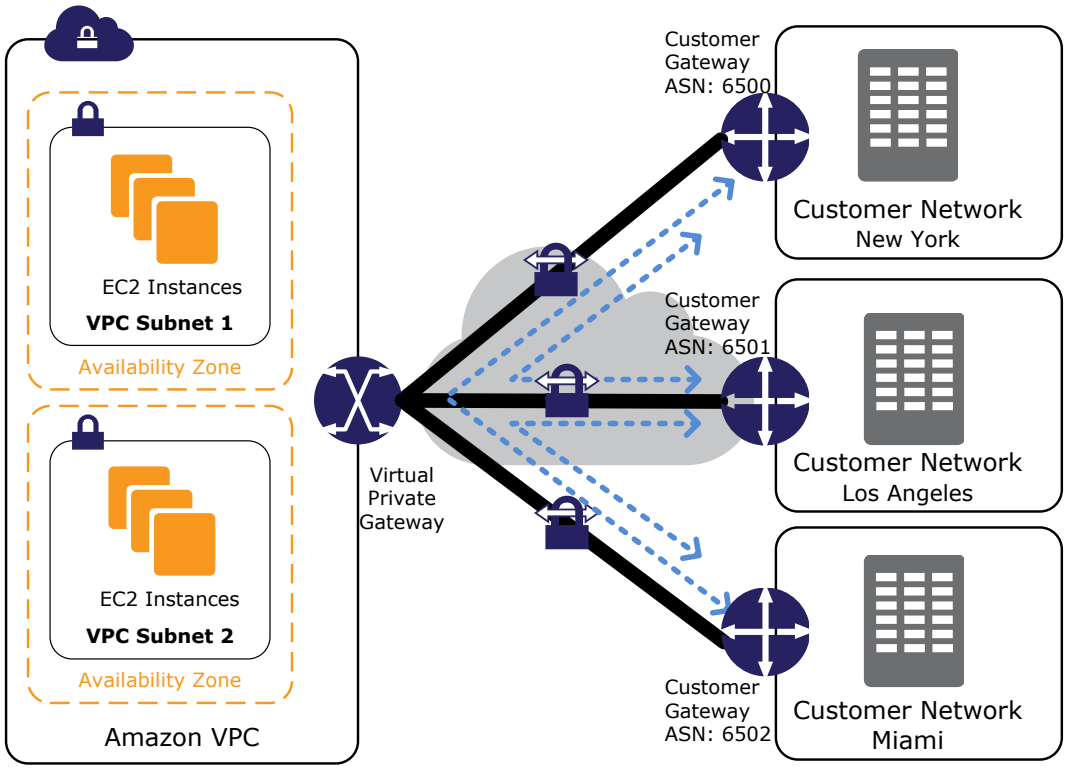

Figure 5 – AWS VPN CloudHub

AWS VPN CloudHub leverages an Amazon VPC Virtual Private Gateway with multiple customer gateways, each using unique BGP Autonomous System Numbers (ASNs). Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and re-advertised to each BGP peer, allowing each site to 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 customer gateways per site for customer-side redundancy or customer backbone routing) depending on customer 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 customers the flexibility to fully manage both sides of their Amazon VPC connectivity by creating a VPN connection between their remote network and a software VPN appliance running in their Amazon VPC network. This option is recommended for customers who must manage both ends of the VPN connection either for compliance purposes or for leveraging customer gateway devices that are not currently supported by Amazon VPC's hardware VPN solution. Figure 6 shows this option.

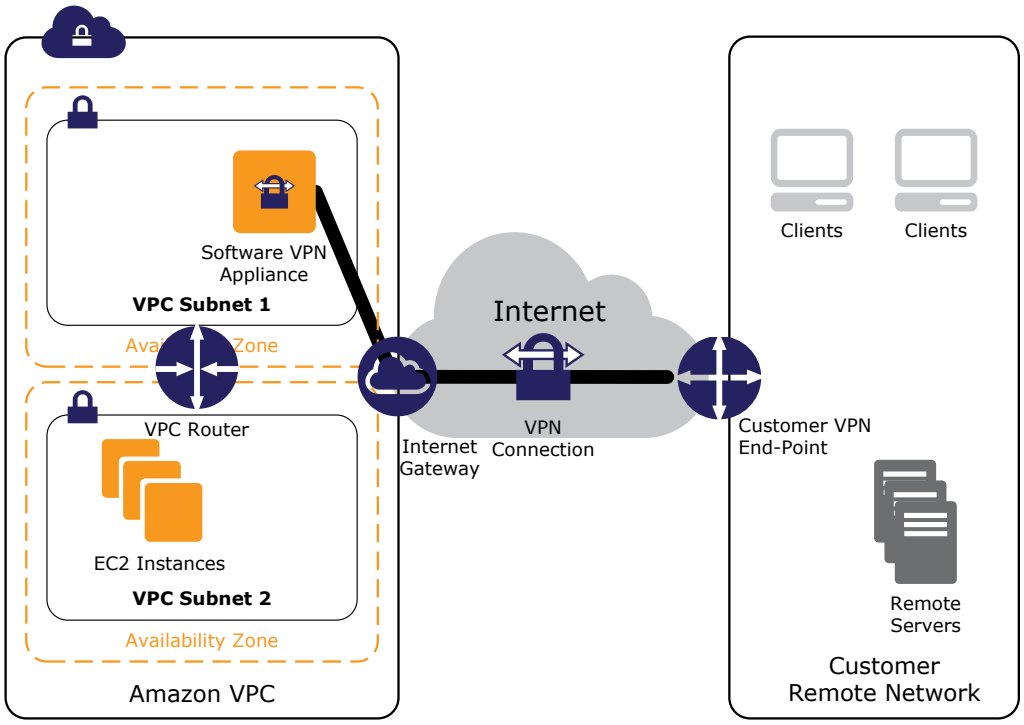

Figure 6 – Software VPN

AWS customers may 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 Checkpoint, 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 the customer to manage the software appliance including configuration, patches, and upgrades.

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

Additional Resources

- VPN Appliances from the AWS Marketplace
- Article - Connecting Cisco ASA to VPC EC2 Instance (IPSec)
- Article - Connecting Multiple VPCs with EC2 Instances (IPSec) [1]
- Article - Connecting Multiple VPCs with EC2 Instances (SSL) [1]

[1] 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-premise VPN device connecting to an IPsec or SSL Software VPN Appliance running in an Amazon VPC.

Amazon VPC–to–Amazon VPC Connectivity Options

These design patterns are applicable for customers who desire to integrate multiple Amazon VPCs into a larger virtual network. This is useful for customers who 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. These patterns can also be combined with the Customer 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 interconnected. For example, if you'd like to interconnect multiple VPCs, make sure each VPC is configured with unique Classless Inter-Domain Routing (CIDR) ranges. Therefore, we advise customers 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: http://aws.amazon.com/vpc/faqs/

Option	Use Case	Advantages	Limitations
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 • Fully customer-managed solution	• Customer is responsible for implementing HA solutions for all VPN endpoints (if required)
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 multi-data center redundancy and automated failover	• Customer is responsible for implementing HA solutions for the software appliance VPN endpoints (if required)
Hardware VPN	Customer managed VPC-to-VPC routing over hardware-based, IPsec VPN connections using customer 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 are dependent on the Internet conditions • Customer-managed endpoint is responsible for implementing redundancy and failover (if required)
AWS Direct Connect	Customer managed VPC-to-VPC routing using customer 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

Software VPN

Amazon VPC provides customers with 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, allowing instances in each VPC to seamlessly connect to each other using private IP addresses. This option is recommended for customers who want to manage both ends of the VPN connection using their preferred VPN software provider. This option uses the "Internet" Gateway[2] attached to two VPCs to facilitate communication between the software VPN appliances.

AWS customers may 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 Checkpoint, 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 the customer 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.

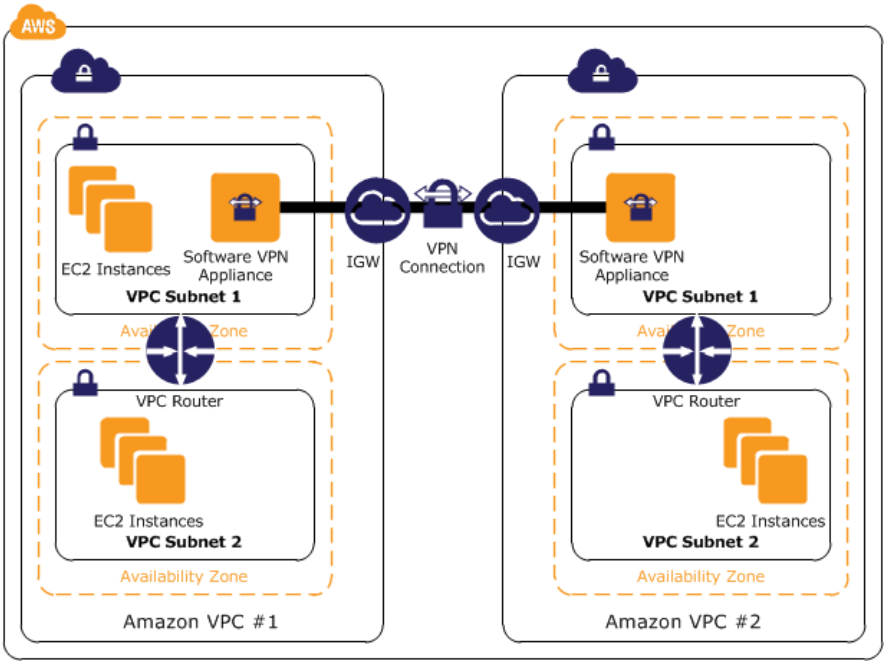

Figure 7 – Intra-Region VPC-to-VPC Routing

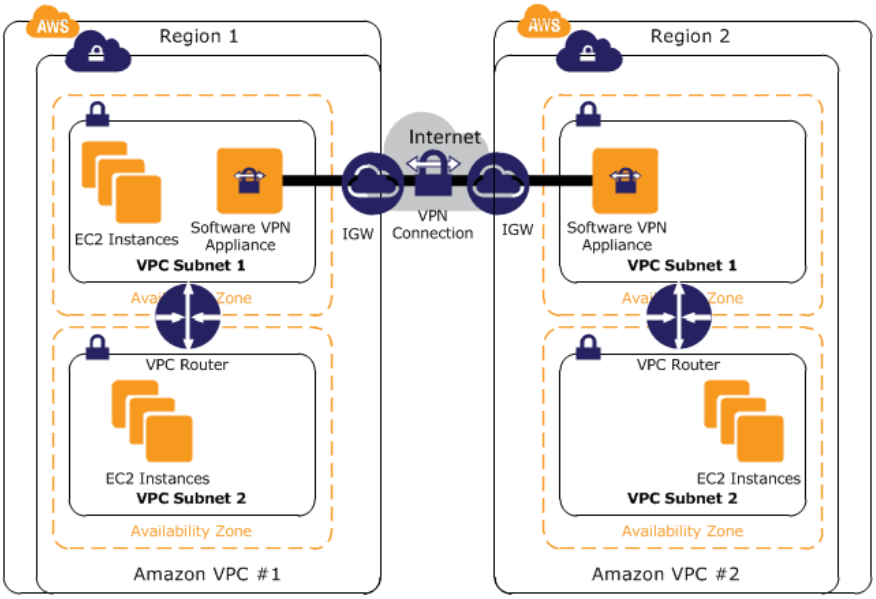

Figure 8 – Inter-Region VPC-to-VPC Routing

Additional Resources

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

[2] "Internet" is in quotes because an Internet Gateway will only route the VPN connections over the Internet when Amazon VPCs are located in separate regions (Figure 7). When communicating between VPCs in the same AWS Region, the IGW will route traffic directly between the VPCs using the AWS network (Figure 6).

Software-to-Hardware VPN

Amazon VPC provides customers with the flexibility to combine the hardware VPN and software VPN options to interconnect multiple VPCs. This design allows customers to 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 for customers who would like to take advantage of the AWS-managed hardware VPN endpoint including automated multi-data 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 the "Internet" Gateway[3] and software VPN appliance in another Amazon VPC as shown in Figure9.

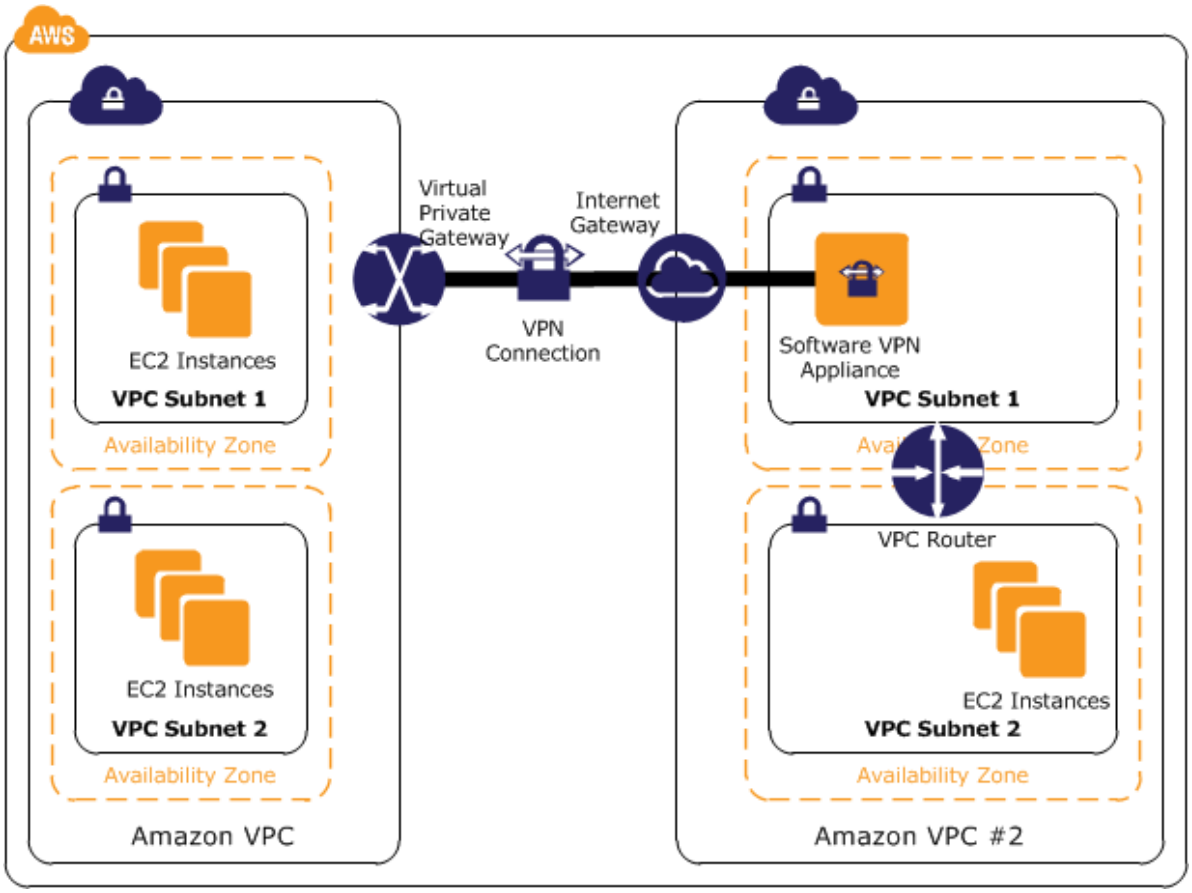

Figure 9 – Intra-Region VPC-to-VPC Routing

Please note that this design introduces a potential single point of failure into the network design as the ASG 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

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

[3] "Internet" is in quotes because an Internet Gateway will only route the VPN connections over the Internet when Amazon VPCs are located in separate regions. See the footnote in the previous section for additional information.

Hardware VPN

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

We recommend this approach for customers who would like to take advantage of AWS-managed VPN endpoints including automated multi-data 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 Connectivity Options" - Hardware VPN section and shown in Figure 2), allowing customers to implement redundancy and failover on their side of the VPN connection. This solution can also leverage BGP peering to exchange routing information between AWS and these remote endpoints. Customers may specify routing priorities, policies, and weights (metrics) in their BGP advertisements to influence the network path traffic will take to and from their network(s) and AWS.

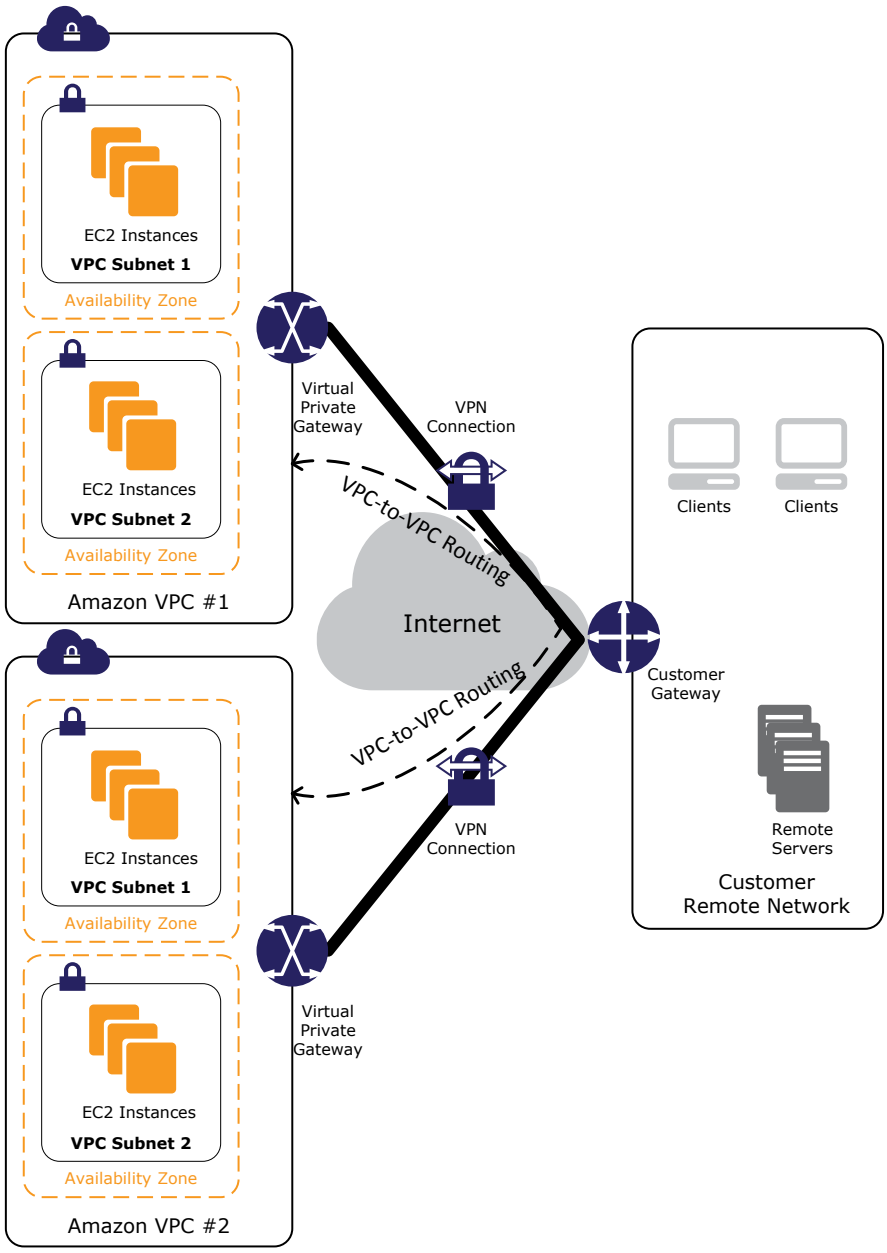

Figure 10 – Routing Traffic Between VPCs

This approach is suboptimal from a routing perspective since the traffic must traverse the Internet to get to and from the customer's network, but it provides the customer with a lot of flexibility for controlling and managing routing on their 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
- Article- Connecting a Single Router to Multiple VPCs

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated network connection from your premise to your Amazon VPC or between 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.

A physical AWS Direct Connect connection can be divided into multiple logical connections, one for each VPC. These logical connections can then be used for routing traffic between each VPC, as shown in Figure 11. In addition to intra-region routing, customers can connect AWS Direct Connect locations in other regions using their existing WAN providers and leverage AWS Direct Connect to route traffic between regions over their WAN backbone network.

We recommend this approach for existing AWS Direct Connect customers or customers who would like to take advantage of AWS Direct Connect's reduced network costs, increased bandwidth throughput, and more consistent network experience. It 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, it provides the customer with the most flexibility for controlling and managing routing on their local and remote networks, as well as the potential ability to reuse AWS Direct Connect connections.

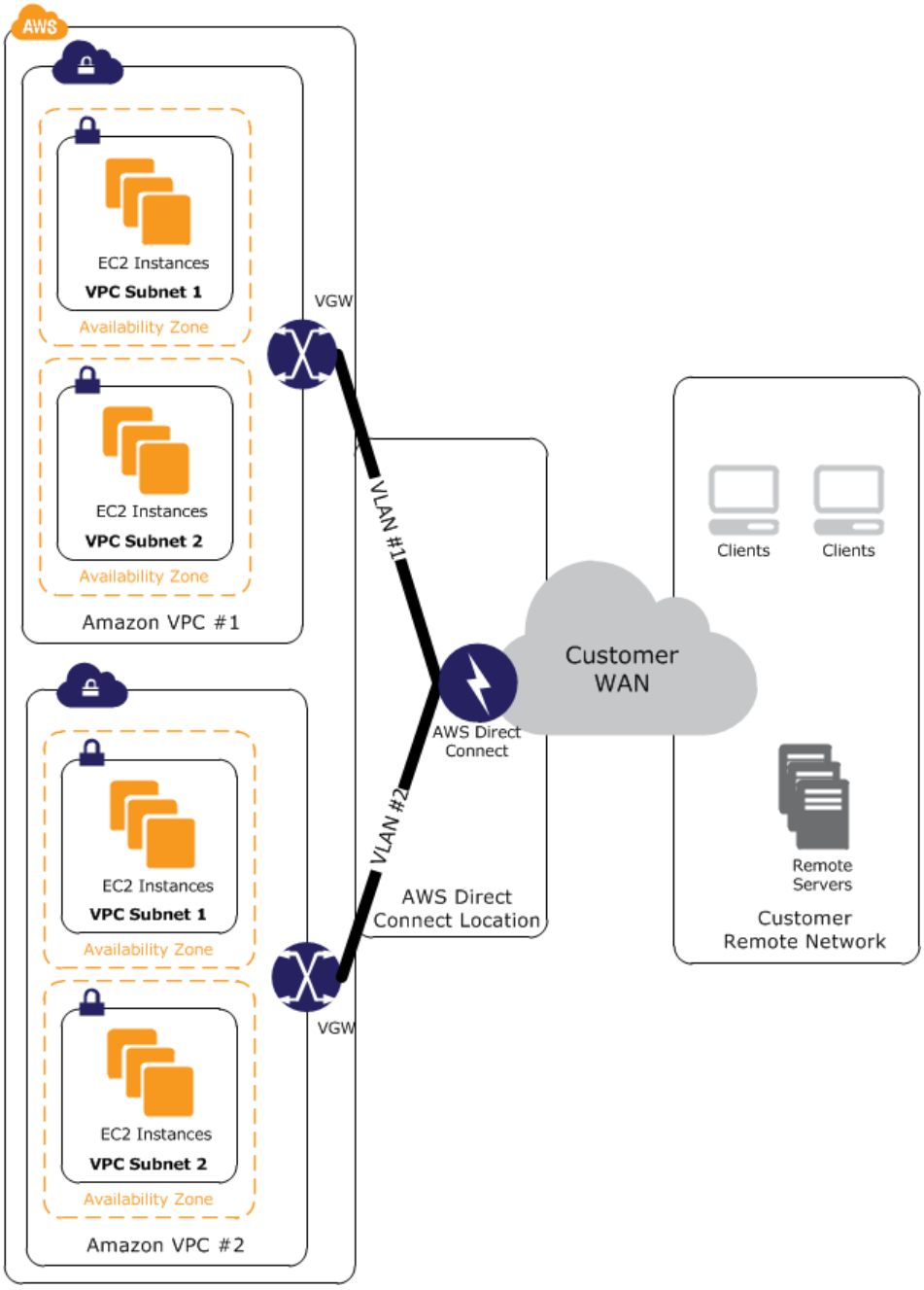

Figure 11 – Intra-Region VPC-to-VPC Routing with AWS Direct Connect

Additional Resources

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

Internal User–to–Amazon VPC Connectivity Options

Internal user access to Amazon VPC resources is typically accomplished either through Customer Network–to–Amazon VPC Connectivity Options or the use of software remote access VPNs to connect internal users to VPC resources. The former option allows customers to reuse their existing on-premise and remote access solutions for managing end-user access, while still providing a seamless experience connecting to AWS hosted resources. Describing on-premise internal and remote access solutions in any more detail than what has been described in the "Customer Network–to–Amazon VPC Connectivity Options" section is beyond the scope of this document.

The Software Remote Access VPN approach allows customers to 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. Additionally, software remote access VPNs can be combined with customer 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 associated with these options.

Option	Use Case	Advantages	Limitations
Customer Network–to–Amazon VPC Options	Virtual extension of a customer's 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

AWS customers may 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 Checkpoint, Sophos, OpenVPN Technologies and Microsoft. Figure 12 shows a simple remote access solution leveraging an internal remote user database.

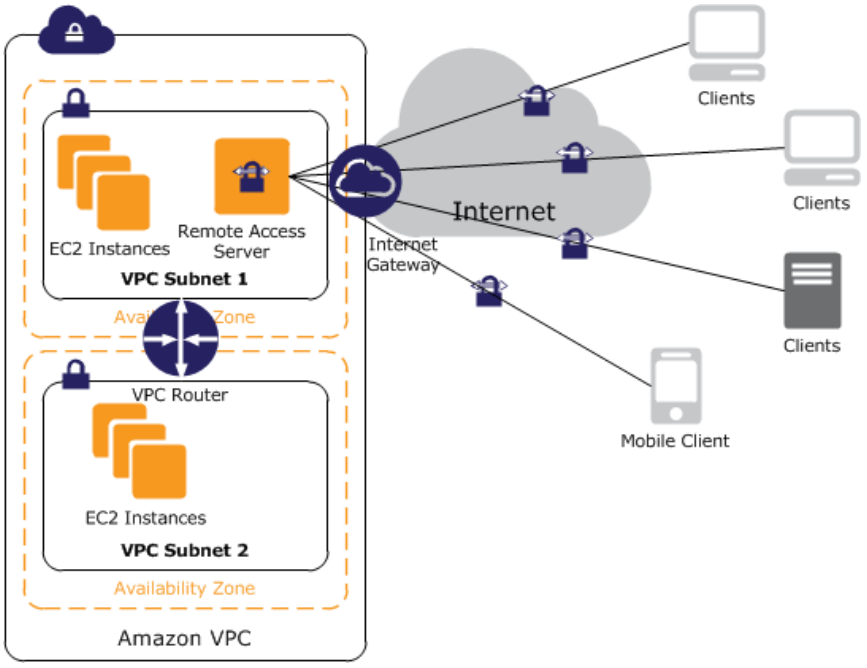

Figure 12 – Remote Access Solution

Remote access solutions range in complexity, support multiple client authentication options (including multi-factor authentication) and can be integrated with either Amazon VPC or remotely hosted identity and access management solutions (leveraging one of the Customer Network–to–Amazon VPC Connectivity Options) like Microsoft Active Directory or other LDAP/multi-factor authentication solutions. Figure 13 shows this combination, allowing the Remote Access Server to leverage internal access management solutions if desired.

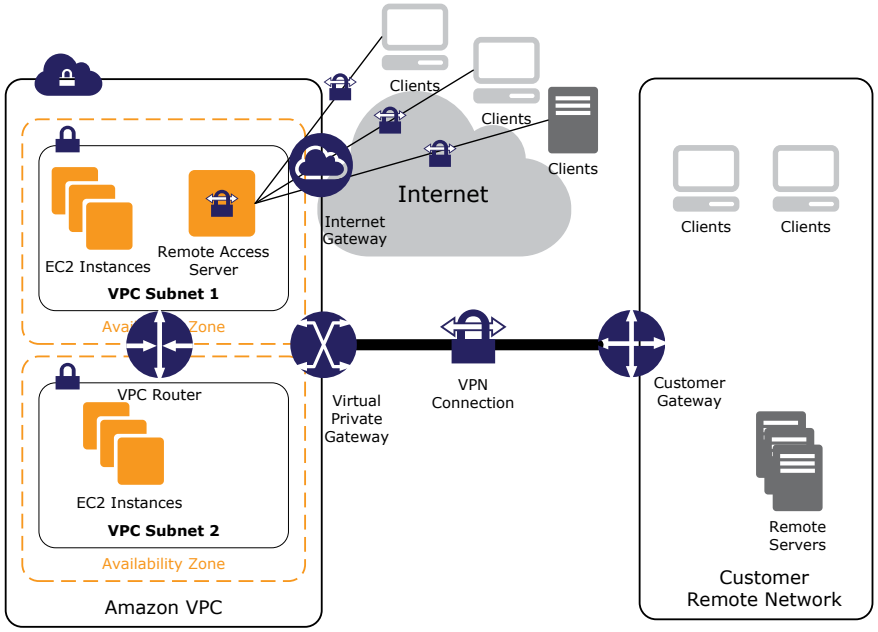

Figure 13 – Combination Remote Access Solution

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

Conclusion

AWS provides a number of efficient, secure connectivity options to help customers get the most out of AWS when integrating their remote networks with Amazon VPC. The options provided in this whitepaper highlight several of the connectivity options and patterns that our customers 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.

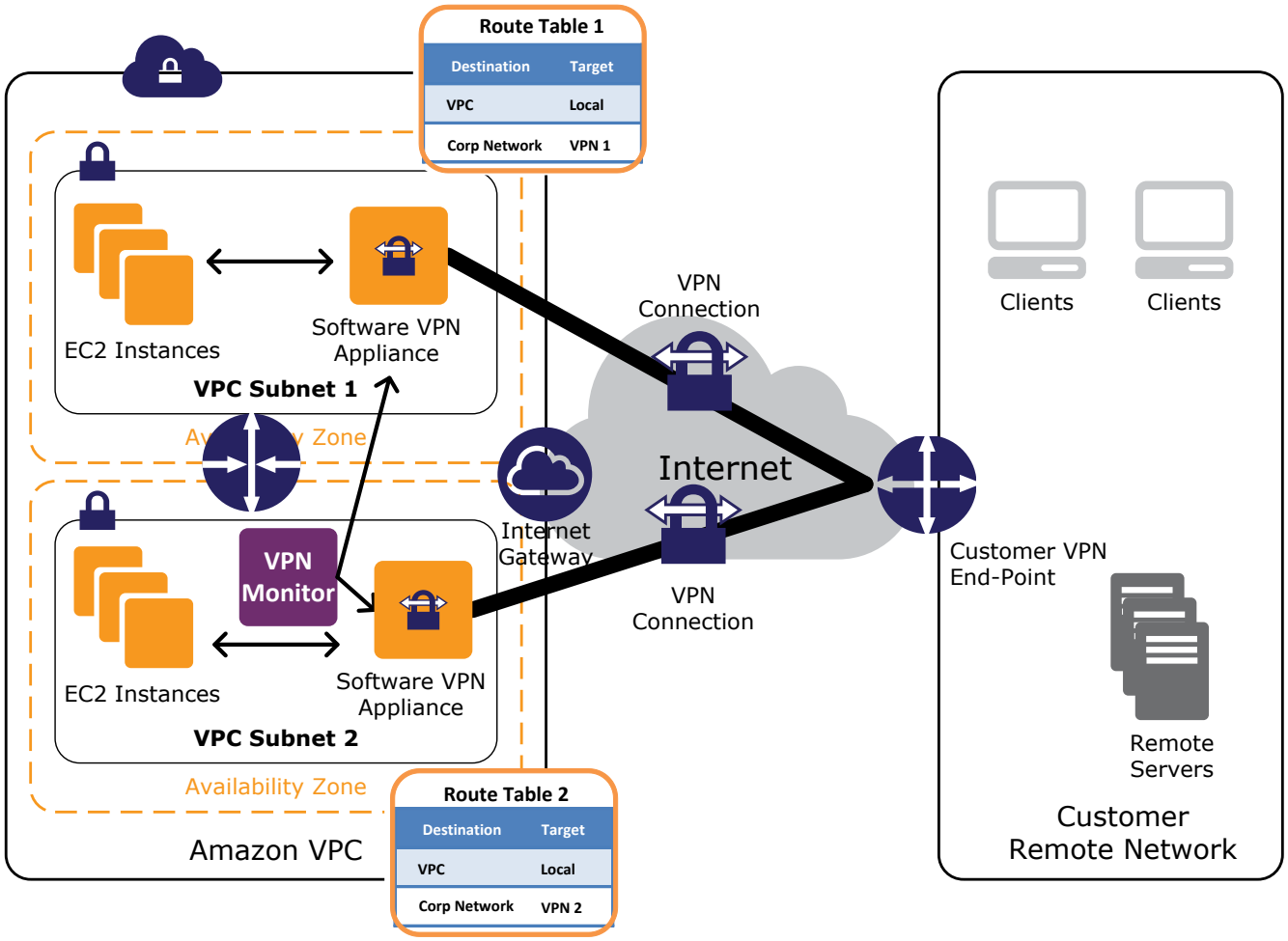

Figure 14 – High-Level HA Design

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 will need 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 any guidance or scripts to use to set up this monitoring instance. 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.