

Customer Responsibility for AWS VPN



Contents

Abstract.....	3
Introduction.....	3
VPN – AWS to Customer Network.....	4
VPC.....	5
VPN Setup – Who is the initiator.....	5
NAT on the Customer Gateway.....	5
Troubleshooting VPN Tunnel Issue.....	5
Configuring Customer Gateway.....	7
Conclusion.....	7
References.....	7
About the Author.....	8



Abstract

The aim of the whitepaper is to bring customer responsibilities in one space while creating the VPN connection between AWS and the Customer Network. This document discusses the initiator of the VPN establishment, followed by a few Troubleshooting checks during any failure.

Introduction

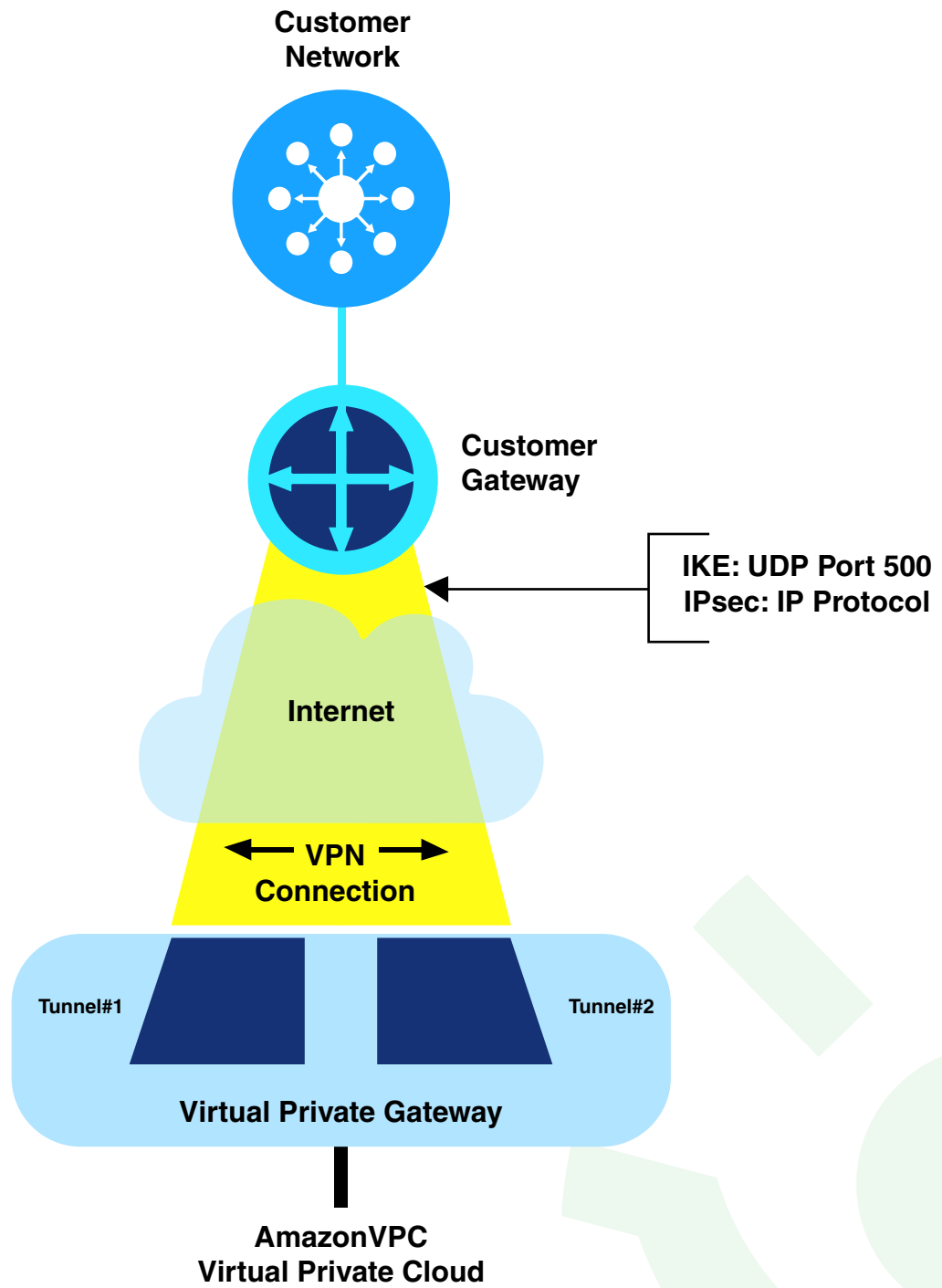
The wider penetration of Internet and the rapid need of securing the network has made the term VPN connection a very popular one. Amazon's VPC documentation describes VPN connection as the connection between your Virtual Private Cloud (VPC) and your own network. Amazon Web Service (AWS) supports Internet Protocol security (IPsec) VPN connections.

A VPN connection consists of the following elements:

- Virtual Private Gateway: a VPN concentrator on Amazon side of the VPN connection.
- Customer Gateway: a physical device or software application on your side of the VPN connection.

This document will primarily cover all the responsibility of the customer while configuring the customer gateway, once the VPN configuration is established at the AWS end. We will also discuss which port requires to be unblocked in case of NAT and the troubleshooting steps which can be handy if any VPN establishment fails.

Reference VPN network Diagram:



VPC

Amazon Virtual Private Cloud (Amazon VPC) enables us to provision a logically isolated section of the Amazon Web Services (AWS) Cloud where it can launch AWS resources in a private virtual network. It allows us to bear a complete mastery over the virtual networking environment. Can create multiple subnets in the VPC, covering multiple AWS availability zones.

Customer Gateway and Virtual Private Gateway

A customer gateway is the anchor on your side of the connection. It can be a physical or software appliance. The anchor on the AWS side of the VPN connection is called a virtual private gateway.

VPN Setup – Who is the initiator

Once the VPN setup is completed on the AWS environment, the initiation does not take place until the setup is done on the Customer's firewall or network as per the configuration provided by the AWS.

Even after the AWS VPN setup is completed on AWS, client will not see any logs from the AWS Tunnel IP knocking at the Customer Network because the initiator is always from the client firewall. Therefore, the VPN Tunnel shows up only when the traffic is generated from customer's firewall or network of the VPN connection.

Virtual Private Gateway is not the initiator, customer gateway must initiate the tunnel and is not similar to that of the traditional Datacenter VPN connection.

NAT on the Customer Gateway

If the external interface for your customer gateway is a static address. Your customer gateway might reside behind a device performing Network address Translation (NAT). To ensure that NAT traversal (NAT-T) functions properly, you must adjust your firewall rules to unblock UDP port 4500. You can create additional VPN connections to other VPCs using the same customer gateway device. You can reuse the same customer gateway IP address for each of those VPN connections.

Why Primary and Failover Tunnel needs to be configured on the Customer Firewall

On a regular basis, AWS performs routine maintenance on the virtual private gateway itself. This maintenance may disable one of the two tunnels of your VPN connection for a brief period of time. Your VPN connection automatically fails over to the second tunnel while this maintenance is performed. To ensure uninterrupted service, it's important that you configure both the tunnels.

Troubleshooting VPN Tunnel Issue

Below reference's details troubleshooting steps which needs to be followed if VPN connection fails to establish on IKE or IPSEC

- Can't establish VPN tunnel: Internet Key Exchange (IKE) is failing issue

You are setting up a virtual private network (VPN) in Amazon VPC, however, the Internet Key Exchange phase (phase 1) fails

Short Description

The purpose of phase 1 is to negotiate a secure channel, over which phase 2 passes its parameters. Phase 2 cannot be established without the successful establishment of phase 1. You can examine IKE debug logs to diagnose the exact cause of the phase 1 negotiation failure, but here are some common troubleshooting steps which you can follow.

Resolution:

Check the following:

- IKEv1 is being used instead of IKEv2; AWS supports only IKEv1.
- Diffie-Hellman Group 2 is being used.
- Phase 1 lifetime is set to 28800 seconds (480 minutes or 8 hours).
- Endpoints configured are matching. If the customer gateway endpoint is behind a NAT device, make sure that the customer gateway IP address is not translated and is exposed directly to the AWS peer. AWS currently does not support NAT-T (NAT traversal).
- UDP packets on port 500 are allowed to pass to and from your network to the AWS VPC.
- Phase 1 is using the SHA-1 hashing algorithm.
- Phase 1 is using AES-128 as the encryption algorithm.
- The pre-shared keys provided in the original AWS configuration match the running configuration you have created in your on-premises device.
- There is no firewall in place between your customer gateway and the virtual gateway of your virtual private cloud deployment that could be blocking the required traffic.

• Can't establish my VPN tunnel: IPsec is failing

Issue

Trying to set up a virtual private network (VPN) in Amazon VPC, but the Internet Protocol security (IPsec) phase (phase 2) fails.

Short Description

The purpose of IPsec (phase 2) is to negotiate and establish a secure tunnel for the transmission of the data between VPN peers. Without a successful phase 2 negotiation, you cannot send and receive traffic across the VPN tunnel. You can examine IPsec debug logs to understand the exact cause of the phase 2 failure, but here are some common troubleshooting steps you can take.

Resolution:

Check the following:

- Encapsulating Security Payload (ESP) protocol 50 is not blocked inbound or outbound.
- Security association lifetime is 3600 seconds (60 minutes).
- There are no firewall ACLs interfering with IPsec traffic.
- Phase 2 is using the SHA-1 hashing algorithm.
- Phase 2 is using AES-128 as the encryption algorithm.
- Perfect forward secrecy (PFS) is enabled and using Diffie-Hellman Group 2 for key generation.

Check the following:

- Encapsulating Security Payload (ESP) protocol 50 is not blocked inbound or outbound.
- Security association lifetime is 3600 seconds (60 minutes).
- There are no firewall ACLs interfering with IPsec traffic.
- Phase 2 is using the SHA-1 hashing algorithm.
- Phase 2 is using AES-128 as the encryption algorithm.
- Perfect forward secrecy (PFS) is enabled and using Diffie-Hellman Group 2 for key generation.

Configuring Customer Gateway

Once the AWS VPN Setup is completed. One task in the process is to configure the customer gateway. The following table summarizes what you need to do to configure the customer gateway.

Process for Configuring the Customer Gateway

Designate an appliance to act as your customer gateway (for more information, see [Customer Gateway Devices We've Tested and Requirements for Your Customer Gateway](#)).

Determine the following information about the customer gateway:

- The vendor (for example, Cisco Systems), the platform (for example, ISR Series Routers), and the software version (for example, IOS 12.4)
 - The Internet-routable IP address for the customer gateway device interface
 - We assume that the BGP ASN for the customer gateway is 65000.
- Give the preceding information to your integration team. The integration team creates your VPN connection and gets the information that you need to configure the customer gateway.
 - Get the configuration information from the integration team.
 - Configure your customer gateway using the configuration information that you received from the integration team.
 - Notify your integration team when you're done configuring the customer gateway.

Conclusion:

This blog details the customer responsibility for the VPN setup to AWS in one place. Once setup is completed on the customer end the VPN Tunnel Status changes to UP and the connection is confirmed to be established.

References:

<http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#Summary>

<https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-1-ike/>

<https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/>

About the Author



Avishek

Avishek has 9 Years of IT industry experience. Currently working as a Senior Technical Lead for Happiest Minds Technologies where he is responsible for providing Cloud Solutions to the customers.

Active member of Organization Cloud Practice and is engaged with clients for pre-sales and consulting stages, providing architectural solution and involved in implementing the environment for the client.

Working with client to understand their niche requirement on Cloud, Virtualization, Servers etc. and providing the best solution.

Specialties: Public Cloud - AWS and Azure, Virtualization (VMware, Hyper V), Citrix Xenapp, Citrix XenDesktop, Windows Servers

He also enjoys travelling and spending time with his lovely pets.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: **Big Data Analytics**, AI & Cognitive Computing, **Internet of Things**, Cloud, Security, **SDN-NFV**, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and **security services**. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Happiest Minds. All Rights Reserved.

Business Contact: Business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on

