**AWS Managed VPN Connections**

By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

Although the term *VPN connection* is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network. AWS supports Internet Protocol security (IPsec) VPN connections.

Your AWS managed VPN connection is either an AWS Classic VPN or an AWS VPN. For more information, see [AWS Managed VPN Categories](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-categories).

**Important**

We currently do not support IPv6 traffic through a VPN connection.

For information about how you're charged for using a VPN connection with your VPC, see the [Amazon VPC product page](http://aws.amazon.com/vpc).

**Components of Your VPN**

A VPN connection consists of the following components. For more information about VPN limits, see [Amazon VPC Limits](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html).

**Virtual Private Gateway**

A *virtual private gateway* is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.

When you create a virtual private gateway, you can specify the private Autonomous System Number (ASN) for the Amazon side of the gateway. If you don't specify an ASN, the virtual private gateway is created with the default ASN (64512). You cannot change the ASN after you've created the virtual private gateway. To check the ASN for your virtual private gateway, view its details in the **Virtual Private Gateways** screen in the Amazon VPC console, or use the [describe-vpn-gateways](http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-vpn-gateways.html) AWS CLI command.

**Note**

If you create your virtual private gateway before 2018-06-30, the default ASN is 17493 in the Asia Pacific (Singapore) region, 10124 in the Asia Pacific (Tokyo) region, 9059 in the EU (Ireland) region, and 7224 in all other regions.

**Customer Gateway**

A *customer gateway* is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. The following table describes the information you'll need to create a customer gateway resource.

|  |  |
| --- | --- |
| **Item** | **Description** |
| Internet-routable IP address (static) of the customer gateway's external interface. | The public IP address value must be static. If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500. |
| The type of routing—static or dynamic. | For more information, see [VPN Routing Options](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPNRoutingTypes). |
| (Dynamic routing only) Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway. | You can use an existing ASN assigned to your network. If you don't have one, you can use a private ASN (in the 64512–65534 range).  If you use the VPC wizard in the console to set up your VPC, we automatically use 65000 as the ASN. |

To use Amazon VPC with a VPN connection, you or your network administrator must also configure the customer gateway device or application in your remote network. When you create the VPN connection, we provide you with the required configuration information and your network administrator typically performs this configuration. For information about the customer gateway requirements and configuration, see the [Your Customer Gateway](http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html) in the *Amazon VPC Network Administrator Guide*.

The VPN tunnel comes up when traffic is generated from your side of the VPN connection. The virtual private gateway is not the initiator; your customer gateway must initiate the tunnels. If your VPN connection experiences a period of idle time (usually 10 seconds, depending on your configuration), the tunnel may go down. To prevent this, you can use a network monitoring tool to generate keepalive pings; for example, by using IP SLA.

For a list of customer gateways that we have tested with Amazon VPC, see [Amazon Virtual Private Cloud FAQs](http://aws.amazon.com/vpc/faqs/#C9).

**AWS Managed VPN Categories**

Your AWS managed VPN connection is either an AWS Classic VPN connection or an AWS VPN connection. Any new VPN connection that you create is an AWS VPN connection. The following features are supported on AWS VPN connections only:

* NAT traversal
* 4-byte ASN (in addition to 2-byte ASN)
* CloudWatch metrics
* Reusable IP addresses for your customer gateways
* Additional encryption options; including AES 256-bit encryption, SHA-2 hashing, and additional Diffie-Hellman groups
* Configurable tunnel options
* Custom private ASN for the Amazon side of a BGP session

You can find out the category of your AWS managed VPN connection by using the Amazon VPC console or a command line tool.

**To identify the VPN category using the console**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **VPN Connections**.
3. Select the VPN connection, and check the value for **Category** in the details pane. A value of VPNindicates an AWS VPN connection. A value of VPN-Classic indicates an AWS Classic VPN connection.

**To identify the VPN category using a command line tool**

* You can use the [describe-vpn-connections](http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-vpn-connections.html) AWS CLI command. In the output that's returned, take note of the Category value. A value of VPN indicates an AWS VPN connection. A value of VPN-Classicindicates an AWS Classic VPN connection.

In the following example, the VPN connection is an AWS VPN connection.

aws ec2 describe-vpn-connections --vpn-connection-ids *vpn-1a2b3c4d*

{

"VpnConnections": [

{

"VpnConnectionId": "vpn-1a2b3c4d",

...

"State": "available",

"VpnGatewayId": "vgw-11aa22bb",

"CustomerGatewayId": "cgw-ab12cd34",

"Type": "ipsec.1",

"Category": "VPN"

}

]

}

Alternatively, use one of the following commands:

* [DescribeVpnConnections](http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeVpnConnections.html) (Amazon EC2 Query API)
* [Get-EC2VpnConnection](http://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2VpnConnection.html) (Tools for Windows PowerShell)

**Migrating to AWS VPN**

If your existing VPN connection is an AWS Classic VPN connection, you can migrate to an AWS VPN connection by creating a new virtual private gateway and VPN connection, detaching the old virtual private gateway from your VPC, and attaching the new virtual private gateway to your VPC.

If your existing virtual private gateway is associated with multiple VPN connections, you must recreate each VPN connection for the new virtual private gateway. If there are multiple AWS Direct Connect private virtual interfaces attached to your virtual private gateway, you must recreate each private virtual interface for the new virtual private gateway. For more information, see [Creating a Virtual Interface](http://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html) in the *AWS Direct Connect User Guide*.

If your existing AWS managed VPN connection is an AWS VPN connection, you cannot migrate to an AWS Classic VPN connection.

**Note**

During this procedure, connectivity over the current VPC connection is interrupted when you disable route propagation and detach the old virtual private gateway from your VPC. Connectivity is restored when the new virtual private gateway is attached to your VPC and the new VPN connection is active. Ensure that you plan for the expected downtime.

**To migrate to an AWS VPN connection**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Virtual Private Gateways**, **Create Virtual Private Gateway** and create a virtual private gateway.
3. In the navigation pane, choose **VPN Connections**, **Create VPN Connection**. Specify the following information, and choose **Yes, Create**.
   * **Virtual Private Gateway**: Select the virtual private gateway that you created in the previous step.
   * **Customer Gateway**: Choose **Existing**, and select the existing customer gateway for your current AWS Classic VPN connection.
   * Specify the routing options as required.
4. Select the new VPN connection and choose **Download Configuration**. Download the appropriate configuration file for your customer gateway device.
5. Use the configuration file to configure VPN tunnels on your customer gateway device. For examples, see the [*Amazon VPC Network Administrator Guide*](http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/). Do not enable the tunnels yet. Contact your vendor if you need guidance on keeping the newly configured tunnels disabled.
6. (Optional) Create test VPC and attach the virtual private gateway to the test VPC. Change the encryption domain/source destination addresses as required, and test connectivity from a host in your local network to a test instance in the test VPC.
7. If you are using route propagation for your route table, choose **Route Tables** in the navigation pane. Select the route table for your VPC, and choose **Route Propagation**, **Edit**. Clear the check box for the old virtual private gateway and choose **Save**.

**Note**

From this step onwards, connectivity is interrupted until the new virtual private gateway is attached and the new VPN connection is active.

1. In the navigation pane, choose **Virtual Private Gateways**. Select the old virtual private gateway and choose **Actions**, **Detach from VPC**, **Yes, Detach**. Select the new virtual private gateway, and choose **Actions**, **Attach to VPC**. Specify the VPC for your VPN connection, and choose **Yes, Attach**.
2. In the navigation pane, choose **Route Tables**. Select the route table for your VPC and do one of the following:
   * If you are using route propagation, choose **Route Propagation**, **Edit**. Select the new virtual private gateway that's attached to the VPC and choose **Save**.
   * If you are using static routes, choose **Routes**, **Edit**. Modify the route to point to the new virtual private gateway, and choose **Save**.
3. Enable the new tunnels on your customer gateway device and disable the old tunnels. To bring the tunnel up, you must initiate the connection from your local network.

If applicable, check your route table to ensure that the routes are being propagated. The routes propagate to the route table when the status of the VPN tunnel is UP.

**Note**

If you need to revert to your previous configuration, detach the new virtual private gateway and follow steps 8 and 9 to re-attach the old virtual private gateway and update your routes.

1. If you no longer need your AWS Classic VPN connection and do not want to continue incurring charges for it, remove the previous tunnel configurations from your customer gateway device, and delete the VPN connection. To do this, go to **VPN Connections**, select the VPN connection, and choose **Delete**.

**Important**

After you've deleted the AWS Classic VPN connection, you cannot revert or migrate your new AWS VPN connection back to an AWS Classic VPN connection.

**VPN Configuration Examples**

The following diagrams illustrate single and multiple VPN connections. The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.

When you create multiple VPN connections to a single VPC, you can configure a second customer gateway to create a redundant connection to the same external location. You can also use it to create VPN connections to multiple geographic locations.

**Single VPN Connection**


            VPN layout
          

**Multiple VPN connections**


            Multiple VPN layout
          

**VPN Routing Options**

When you create a VPN connection, you must do the following:

* Specify the type of routing that you plan to use (static or dynamic)
* Update the route table for your subnet

There are limits on the number of routes that you can add to a route table. For more information, see the Route Tables section in [Amazon VPC Limits](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html).

**Static and Dynamic Routing**

The type of routing that you select can depend on the make and model of your VPN devices. If your VPN device supports Border Gateway Protocol (BGP), specify dynamic routing when you configure your VPN connection. If your device does not support BGP, specify static routing. For a list of static and dynamic routing devices that have been tested with Amazon VPC, see the [Amazon Virtual Private Cloud FAQs](http://aws.amazon.com/vpc/faqs/#C9).

When you use a BGP device, you don't need to specify static routes to the VPN connection because the device uses BGP to advertise its routes to the virtual private gateway. If you use a device that doesn't support BGP, you must select static routing and enter the routes (IP prefixes) for your network that should be communicated to the virtual private gateway.

We recommend that you use BGP-capable devices, when available, because the BGP protocol offers robust liveness detection checks that can assist failover to the second VPN tunnel if the first tunnel goes down. Devices that don't support BGP may also perform health checks to assist failover to the second tunnel when needed.

**Route Tables and VPN Route Priority**

[Route tables](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html) determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that's destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you.

Only IP prefixes that are known to the virtual private gateway, whether through BGP advertisements or static route entry, can receive traffic from your VPC. The virtual private gateway does not route any other traffic destined outside of received BGP advertisements, static route entries, or its attached VPC CIDR.

When a virtual private gateway receives routing information, it uses path selection to determine how to route traffic to your remote network. Longest prefix match applies; otherwise, the following rules apply:

* If any propagated routes from a VPN connection or AWS Direct Connect connection overlap with the local route for your VPC, the local route is most preferred even if the propagated routes are more specific.
* If any propagated routes from a VPN connection or AWS Direct Connect connection have the same destination CIDR block as other existing static routes (longest prefix match cannot be applied), we prioritize the static routes whose targets are an Internet gateway, a virtual private gateway, a network interface, an instance ID, a VPC peering connection, a NAT gateway, or a VPC endpoint.

If you have overlapping routes within a VPN connection and longest prefix match cannot be applied, then we prioritize the routes as follows in the VPN connection, from most preferred to least preferred:

* BGP propagated routes from an AWS Direct Connect connection
* Manually added static routes for a VPN connection
* BGP propagated routes from a VPN connection

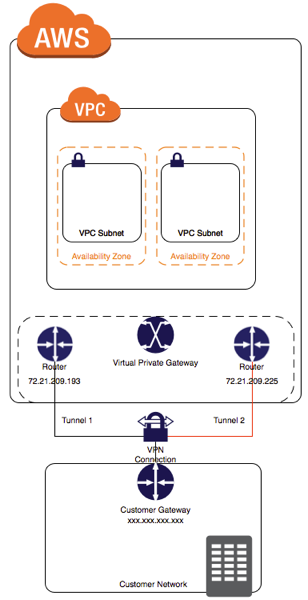
In this example, your route table has a static route to an internet gateway (that you added manually), and a propagated route to a virtual private gateway. Both routes have a destination of 172.31.0.0/24. In this case, all traffic destined for 172.31.0.0/24 is routed to the internet gateway — it is a static route and therefore takes priority over the propagated route.

|  |  |
| --- | --- |
| **Destination** | **Target** |
| 10.0.0.0/16 | Local |
| 172.31.0.0/24 | vgw-1a2b3c4d (propagated) |
| 172.31.0.0/24 | igw-11aa22bb |

**Configuring the VPN Tunnels for Your VPN Connection**

You use a VPN connection to connect your remote network to a VPC. Each VPN connection has two tunnels, with each tunnel using a unique virtual private gateway public IP address. It is important to configure both tunnels for redundancy. When one tunnel becomes unavailable (for example, down for maintenance), network traffic is automatically routed to the available tunnel for that specific VPN connection.

The following diagram shows the two tunnels of the VPN connection.



When you create a VPN connection, you download a configuration file specific to your customer gateway device that contains information for configuring the device, including information for configuring each tunnel. You can optionally specify some of the tunnel options yourself when you create the VPN connection. Otherwise, AWS provides default values.

The following table describes the tunnel options that you can configure.

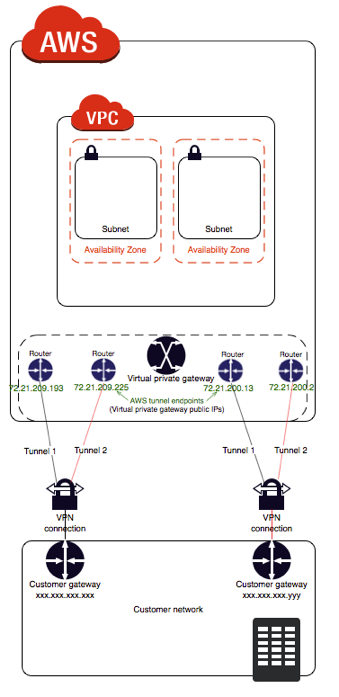
|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **AWS-provided default value** |
| Inside tunnel CIDR | The range of inside IP addresses for the VPN tunnel. You can specify a size /30 CIDR block from the 169.254.0.0/16 range. The CIDR block must be unique across all VPN connections that use the same virtual private gateway.  The following CIDR blocks are reserved and cannot be used:   * 169.254.0.0/30 * 169.254.1.0/30 * 169.254.2.0/30 * 169.254.3.0/30 * 169.254.4.0/30 * 169.254.5.0/30 * 169.254.169.252/30 | A size /30 CIDR block from the 169.254.0.0/16range. |
| Pre-shared key (PSK) | The pre-shared key (PSK) to establish the initial IKE Security Association between the virtual private gateway and customer gateway.  The PSK must be between 8 and 64 characters in length and cannot start with zero (0). Allowed characters are alphanumeric characters, periods (.), and underscores (\_). | A 32-character alphanumeric string. |

You cannot modify tunnel options after you create the VPN connection. To change the inside tunnel IP addresses or the PSKs for an existing connection, you must delete the VPN connection and create a new one. You cannot configure tunnel options for an AWS Classic VPN connection.

**Using Redundant VPN Connections to Provide Failover**

As described earlier, a VPN connection has two tunnels to help ensure connectivity in case one of the VPN connections becomes unavailable. To protect against a loss of connectivity in case your customer gateway becomes unavailable, you can set up a second VPN connection to your VPC and virtual private gateway by using a second customer gateway. By using redundant VPN connections and customer gateways, you can perform maintenance on one of your customer gateways while traffic continues to flow over the second customer gateway's VPN connection. To establish redundant VPN connections and customer gateways on your remote network, you need to set up a second VPN connection. The customer gateway IP address for the second VPN connection must be publicly accessible.

The following diagram shows the two tunnels of each VPN connection and two customer gateways.



Dynamically routed VPN connections use the Border Gateway Protocol (BGP) to exchange routing information between your customer gateways and the virtual private gateways. Statically routed VPN connections require you to enter static routes for the remote network on your side of the customer gateway. BGP-advertised and statically entered route information allow gateways on both sides to determine which tunnels are available and reroute traffic if a failure occurs. We recommend that you configure your network to use the routing information provided by BGP (if available) to select an available path. The exact configuration depends on the architecture of your network.