AWS Site-to-Site VPN

User Guide

AWS Site-to-Site VPN: User Guide

Table of Contents

What is AWS Site-to-Site VPN?

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 Site-to-Site VPN (Site-to-Site VPN) connection.

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

Your Site-to-Site VPN connection is either an AWS Classic VPN or an AWS VPN. For more information, see AWS Site-to-Site VPN Categories (p. 2).

> **Important**
> We currently do not support IPv6 traffic through a Site-to-Site VPN connection.

Contents

Components of Your Site-to-Site VPN

A Site-to-Site VPN connection consists of the following components. For more information about Site-to-Site VPN limits, see Amazon VPC Limits in the *Amazon VPC User Guide*.

Virtual Private Gateway

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

AWS Transit Gateway

You can modify the target gateway of AWS Site-to-Site VPN connection from a virtual private gateway to a transit gateway. A transit gateway is a transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks. For more information, see *Modifying a Site-to-Site VPN Connection's Target Gateway* (p. 19).

Customer Gateway

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

To create a Site-to-Site 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 Site-to-Site VPN Routing Options (p. 7).
(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 Site-to-Site VPN connection, you or your network administrator must also configure the customer gateway device or application in your remote network. When you create the Site-to-Site 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 in the *Amazon VPC Network Administrator Guide*.

The VPN tunnel comes up when traffic is generated from your side of the Site-to-Site VPN connection. The virtual private gateway is not the initiator; your customer gateway must initiate the tunnels. If your Site-to-Site 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.

AWS Site-to-Site VPN Categories

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

- Internet Key Exchange version 2 (IKEv2)
- 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 Site-to-Site VPN connection by using the Amazon VPC console or a command line tool.

To identify the Site-to-Site VPN category using the console

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

To identify the Site-to-Site VPN category using a command line tool

- You can use the describe-vpn-connections 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-Classic` indicates an AWS Classic VPN connection.

  In the following example, the Site-to-Site 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 (Amazon EC2 Query API)
- Get-EC2VpnConnection (Tools for Windows PowerShell)

Migrating from AWS Classic VPN to AWS VPN

If your existing Site-to-Site VPN connection is an AWS Classic VPN connection, you can migrate to an AWS VPN connection by creating a new virtual private gateway and Site-to-Site 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 Site-to-Site VPN connections, you must recreate each Site-to-Site 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 in the *AWS Direct Connect User Guide*.

If your existing Site-to-Site 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 Site-to-Site 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 **Site-to-Site 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 Site-to-Site 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*. 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 Site-to-Site VPN connection is active.
8. 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 Site-to-Site VPN connection, and choose **Yes, Attach**.
9. 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**.

10. 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.

11. 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 Site-to-Site VPN connection. To do this, go to **Site-to-Site VPN Connections**, select the Site-to-Site VPN connection, and choose **Delete**.

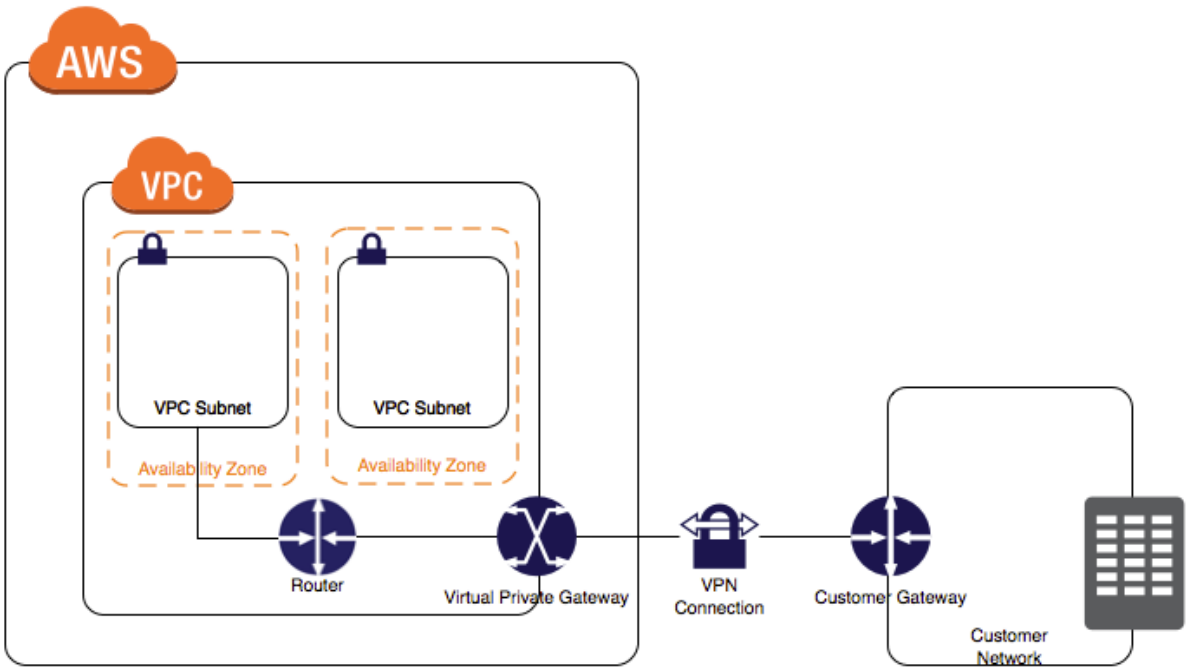
    Important
    After you've deleted the AWS Classic VPN connection, you cannot revert or migrate your new AWS VPN connection back to an AWS Classic VPN connection.

Site-to-Site VPN Configuration Examples

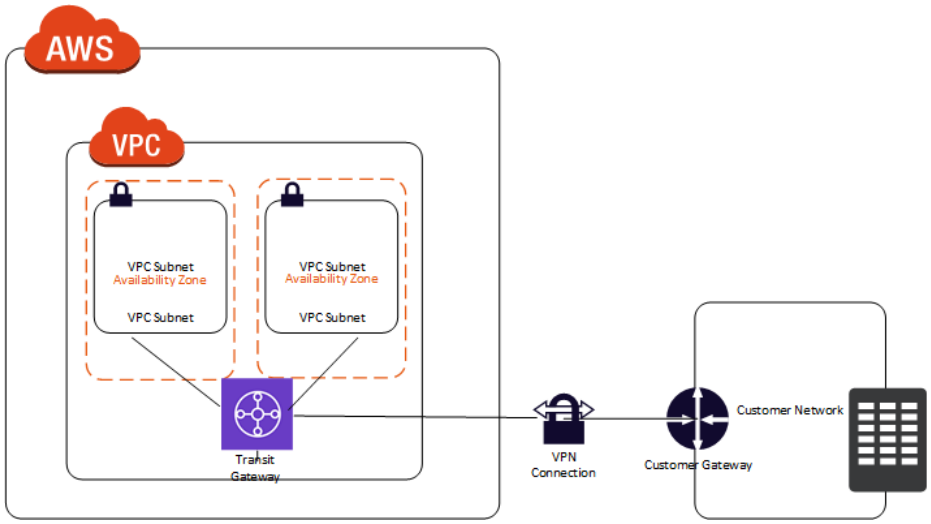
The following diagrams illustrate single and multiple Site-to-Site VPN connections. The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the Site-to-Site VPN connection. You set up the routing so that any traffic from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

When you create multiple Site-to-Site 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 Site-to-Site VPN connections to multiple geographic locations.

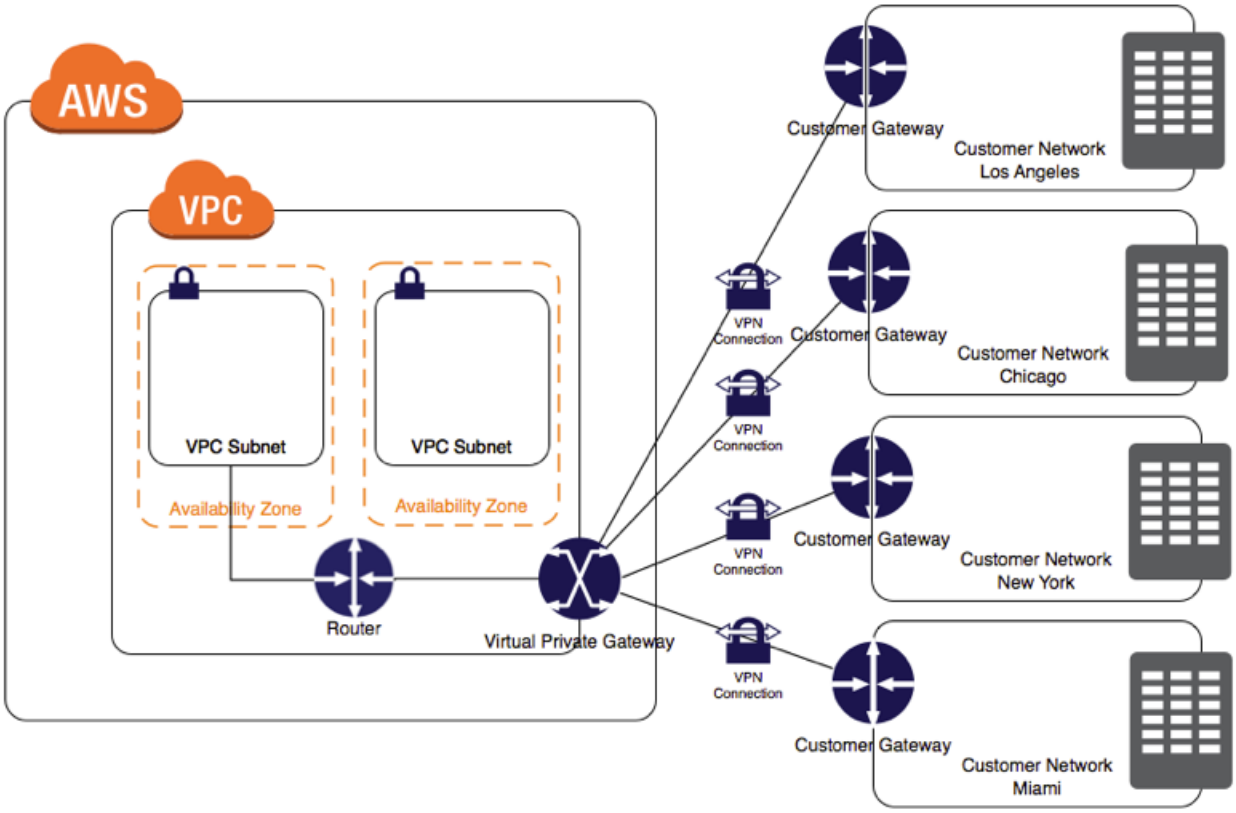
Single Site-to-Site VPN Connection



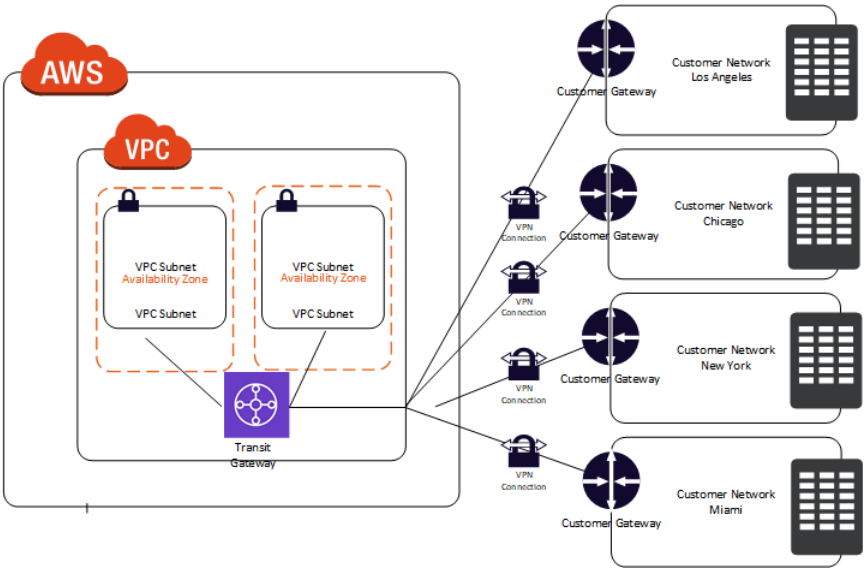
Single Site-to-Site VPN Connection with a Transit Gateway



Multiple Site-to-Site VPN Connections



Multiple Site-to-Site VPN Connections with a Transit Gateway



Site-to-Site VPN Routing Options

When you create a Site-to-Site 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 in the *Amazon VPC User Guide*.

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 Site-to-Site 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.

When you use a BGP device, you don't need to specify static routes to the Site-to-Site VPN connection because the device uses BGP to advertise its routes to the virtual private gateway. If you use a device that supports BGP advertising, then you cannot specify static routes, 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 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 Site-to-Site 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 Site-to-Site 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 Site-to-Site VPN connection and longest prefix match cannot be applied, then we prioritize the routes as follows in the Site-to-Site VPN connection, from most preferred to least preferred:

- BGP propagated routes from an AWS Direct Connect connection
- Manually added static routes for a Site-to-Site VPN connection
- BGP propagated routes from a Site-to-Site 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.

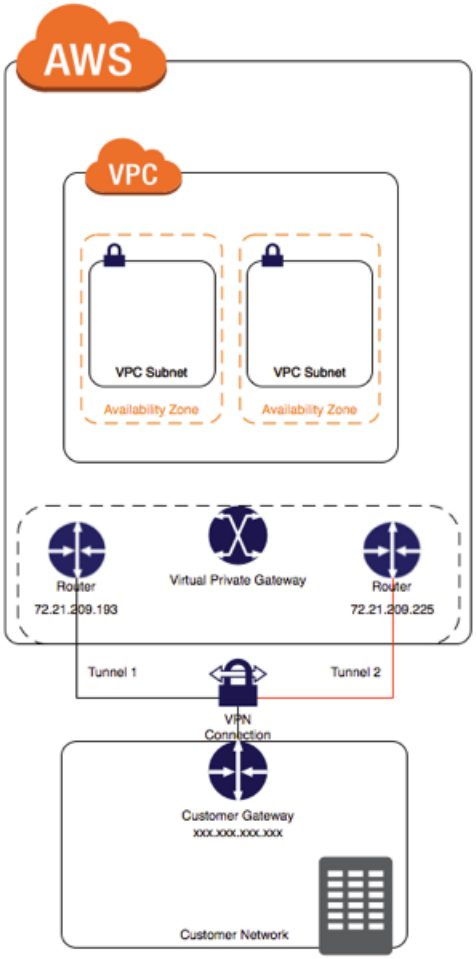
Destination	Target
10.0.0.0/16	Local
172.31.0.0/24	vgw-1a2b3c4d (propagated)
172.31.0.0/24	igw-11aa22bb

Configuring the VPN Tunnels for Your Site-to-Site VPN Connection

You use a Site-to-Site VPN connection to connect your remote network to a VPC. Each Site-to-Site 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 Site-to-Site VPN connection.

The following diagram shows the two tunnels of the Site-to-Site VPN connection.



When you create a Site-to-Site 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 Site-to-Site 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 Site-to-Site VPN connections that use the same virtual private gateway. The following CIDR blocks are reserved and cannot be used:	A size /30 CIDR block from the `169.254.0.0/16` range.

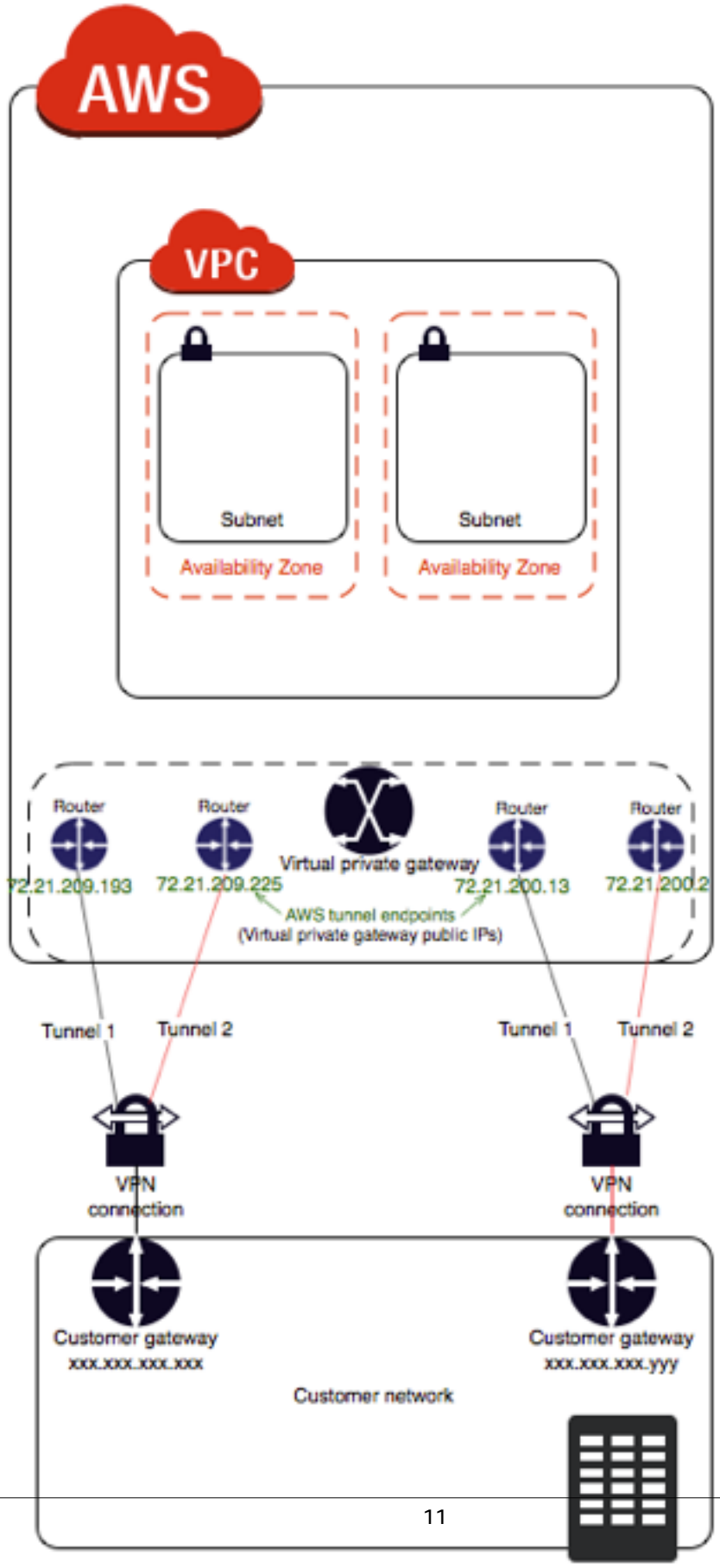
Item	Description	AWS-provided default value
	• 169.254.0.0/30 • 169.254.1.0/30 • 169.254.2.0/30 • 169.254.3.0/30 • 169.254.4.0/30 • 169.254.5.0/30 • 169.254.169.252/30	
Pre-shared key (PSK)	The pre-shared key (PSK) to establish the initial IKE Security Association between the virtual private gateway 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 Site-to-Site VPN connection. To change the inside tunnel IP addresses or the PSKs for an existing connection, you must delete the Site-to-Site VPN connection and create a new one. You cannot configure tunnel options for an AWS Classic VPN connection.

Using Redundant Site-to-Site VPN Connections to Provide Failover

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

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


AWS
VPC
Subnet
Availability Zone
Subnet
Availability Zone
Router
Router
Virtual private gateway
Router
Router
72.21.209.193
72.21.209.225
72.21.200.13
72.21.200.2
AWS tunnel endpoints
(Virtual private gateway public IPs)
Tunnel 1
Tunnel 2
Tunnel 1
Tunnel 2
VPN
connection
VPN
connection
Customer gateway
xxx.xxx.xxx.xxx
Customer gateway
xxx.xxx.xxx.yyy
Customer network

Dynamically routed Site-to-Site VPN connections use the Border Gateway Protocol (BGP) to exchange routing information between your customer gateways and the virtual private gateways. Statically routed Site-to-Site 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.

Getting Started

Use the following procedures to manually set up the AWS Site-to-Site VPN connection. Alternatively, you can let the VPC creation wizard take care of many of these steps for you. For more information about using the VPC creation wizard to set up the virtual private gateway, see Scenario 3: VPC with Public and Private Subnets and AWS Site-to-Site VPN Access or Scenario 4: VPC with a Private Subnet Only and AWS Site-to-Site VPN Access in the *Amazon VPC User Guide*.

To set up a Site-to-Site VPN connection, you need to complete the following steps:

- Step 1: Create a Customer Gateway (p. 13)
- Step 2: Create a Virtual Private Gateway (p. 13)
- Step 3: Enable Route Propagation in Your Route Table (p. 14)
- Step 4: Update Your Security Group (p. 15)
- Step 5: Create a Site-to-Site VPN Connection and Configure the Customer Gateway (p. 15)

These procedures assume that you have a VPC with one or more subnets.

Create a Customer Gateway

A customer gateway provides information to AWS about your customer gateway device or software application. For more information, see Customer Gateway (p. 2).

To create a customer gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Customer Gateways**, and then **Create Customer Gateway**.
3. Complete the following and then choose **Create Customer Gateway**:
   - (Optional) For **Name**, type a name for your customer gateway. Doing so creates a tag with a key of `Name` and the value that you specify.
   - For **Routing**, select the routing type.
   - For dynamic routing, for **BGP ASN**, type the Border Gateway Protocol (BGP) Autonomous System Number (ASN).
   - For **IP Address**, type the static, internet-routable IP address for your customer gateway device. If your customer gateway is behind a NAT device that's enabled for NAT-T, use the public IP address of the NAT device.

To create a customer gateway using the command line or API

- CreateCustomerGateway (Amazon EC2 Query API)
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Create a Virtual Private Gateway

When you create a virtual private gateway, you can optionally specify the private Autonomous System Number (ASN) for the Amazon side of the gateway. The ASN must be different from the BGP ASN specified for the customer gateway.

After you create a virtual private gateway, you must attach it to your VPC.

To create a virtual private gateway and attach it to your VPC

1. In the navigation pane, choose **Virtual Private Gateways**, **Create Virtual Private Gateway**.
2. (Optional) Type a name for your virtual private gateway. Doing so creates a tag with a key of `Name` and the value that you specify.
3. For **ASN**, leave the default selection to use the default Amazon ASN. Otherwise, choose **Custom ASN** and type a value. For a 16-bit ASN, the value must be in the 64512 to 65534 range. For a 32-bit ASN, the value must be in the 4200000000 to 4294967294 range.
4. Choose **Create Virtual Private Gateway**.
5. Select the virtual private gateway that you created, and then choose **Actions**, **Attach to VPC**.
6. Select your VPC from the list and choose **Yes, Attach**.

To create a virtual private gateway using the command line or API

- CreateVpnGateway (Amazon EC2 Query API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

To attach a virtual private gateway to a VPC using the command line or API

- AttachVpnGateway (Amazon EC2 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Enable Route Propagation in Your Route Table

To enable instances in your VPC to reach your customer gateway, you must configure your route table to include the routes used by your Site-to-Site VPN connection and point them to your virtual private gateway. You can enable route propagation for your route table to automatically propagate those routes to the table for you.

For static routing, the static IP prefixes that you specify for your VPN configuration are propagated to the route table when the status of the Site-to-Site VPN connection is `UP`. Similarly, for dynamic routing, the BGP-advertised routes from your customer gateway are propagated to the route table when the status of the Site-to-Site VPN connection is `UP`.

Note
If your connection is interrupted, any propagated routes in your route table are not automatically removed. You may have to disable route propagation to remove the propagated routes; for example, if you want traffic to fail over to a static route.

To enable route propagation using the console

1. In the navigation pane, choose **Route Tables**, and then select the route table that's associated with the subnet; by default, this is the main route table for the VPC.
2. On the **Route Propagation** tab in the details pane, choose **Edit**, select the virtual private gateway that you created in the previous procedure, and then choose **Save**.

Note
For static routing, if you do not enable route propagation, you must manually enter the static routes used by your Site-to-Site VPN connection. To do this, select your route table, choose

Routes, **Edit**. For **Destination**, add the static route used by your Site-to-Site VPN connection . For **Target**, select the virtual private gateway ID, and choose **Save**.

To disable route propagation using the console

1. In the navigation pane, choose **Route Tables**, and then select the route table that's associated with the subnet.
2. Choose **Route Propagation**, **Edit**. Clear the **Propagate** check box for the virtual private gateway, and choose **Save**.

To enable route propagation using the command line or API

- EnableVgwRoutePropagation (Amazon EC2 Query API)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

To disable route propagation using the command line or API

- DisableVgwRoutePropagation (Amazon EC2 Query API)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Update Your Security Group

To allow access to instances in your VPC from your network, you must update your security group rules to enable inbound SSH, RDP, and ICMP access.

To add rules to your security group to enable inbound SSH, RDP and ICMP access

1. In the navigation pane, choose **Security Groups**, and then select the default security group for the VPC.
2. On the **Inbound** tab in the details pane, add rules that allow inbound SSH, RDP, and ICMP access from your network, and then choose **Save**. For more information about adding inbound rules, see Adding, Removing, and Updating Rules in the *Amazon VPC User Guide*.

For more information about working with security groups using the AWS CLI, see Security Groups for Your VPC in the *Amazon VPC User Guide*.

Create a Site-to-Site VPN Connection and Configure the Customer Gateway

After you create the Site-to-Site VPN connection, download the configuration information and use it to configure the customer gateway device or software application.

To create a Site-to-Site VPN connection and configure the customer gateway

1. In the navigation pane, choose **Site-to-Site VPN Connections**, **Create VPN Connection**.
2. Complete the following information, and then choose **Create VPN Connection**:

- (Optional) For **Name tag**, type a name for your Site-to-Site VPN connection. Doing so creates a tag with a key of `Name` and the value that you specify.
- Select the virtual private gateway that you created earlier.
- Select the customer gateway that you created earlier.
- Select one of the routing options based on whether your VPN router supports Border Gateway Protocol (BGP):
  - If your VPN router supports BGP, choose **Dynamic (requires BGP)**.
  - If your VPN router does not support BGP, choose **Static**. For **Static IP Prefixes**, specify each IP prefix for the private network of your Site-to-Site VPN connection.
- Under **Tunnel Options**, you can optionally specify the following information for each tunnel:
  - A size /30 CIDR block from the `169.254.0.0/16` range for the inside tunnel IP addresses.
  - The IKE pre-shared key (PSK). The following versions are supported: IKEv1 or IKEv2.

  For more information about these options, see Configuring the VPN Tunnels for Your Site-to-Site VPN Connection (p. 8).

It may take a few minutes to create the Site-to-Site VPN connection. When it's ready, select the connection and choose **Download Configuration**.

3. In the **Download Configuration** dialog box, select the vendor, platform, and software that corresponds to your customer gateway device or software, and then choose **Yes, Download**.
4. Give the configuration file to your network administrator, along with this guide: Amazon VPC Network Administrator Guide. After the network administrator configures the customer gateway, the Site-to-Site VPN connection is operational.

To create a Site-to-Site VPN connection using the command line or API

- CreateVpnConnection (Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Editing Static Routes for a Site-to-Site VPN Connection

For static routing, you can add, modify, or remove the static routes for your VPN configuration.

To add, modify, or remove a static route

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Site-to-Site VPN Connections**.
3. Choose **Static Routes**, **Edit**.
4. Modify your existing static IP prefixes, or choose **Remove** to delete them. Choose **Add Another Rule** to add a new IP prefix to your configuration. When you are done, choose **Save**.

Note
If you have not enabled route propagation for your route table, you must manually update the routes in your route table to reflect the updated static IP prefixes in your Site-to-Site VPN connection. For more information, see Enable Route Propagation in Your Route Table (p. 14).

To add a static route using the command line or API

- CreateVpnConnectionRoute (Amazon EC2 Query API)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

To delete a static route using the command line or API

- DeleteVpnConnectionRoute (Amazon EC2 Query API)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Replacing Compromised Credentials

If you believe that the tunnel credentials for your Site-to-Site VPN connection have been compromised, you can change the IKE pre-shared key. To do so, delete the Site-to-Site VPN connection, create a new one using the same virtual private gateway, and configure the new keys on your customer gateway. You can specify your own pre-shared keys when you create the Site-to-Site VPN connection. You also need to confirm that the tunnel's inside and outside addresses match, because these might change when you recreate the Site-to-Site VPN connection. While you perform the procedure, communication with your instances in the VPC stops, but the instances continue to run uninterrupted. After the network administrator implements the new configuration information, your Site-to-Site VPN connection uses the new credentials, and the network connection to your instances in the VPC resumes.

Important
This procedure requires assistance from your network administrator group.

To change the IKE pre-shared key

1. Delete the Site-to-Site VPN connection. For more information, see Deleting a Site-to-Site VPN Connection (p. 22). You don't need to delete the VPC or the virtual private gateway.
2. Create a new Site-to-Site VPN connection and specify your own pre-shared keys for the tunnels or let AWS generate new pre-shared keys for you. For more information, see Create a Site-to-Site VPN Connection and Configure the Customer Gateway (p. 15).
3. Download the new configuration file.

Testing the Site-to-Site VPN Connection

After you create th AWS Site-to-Site VPN connection and configure the customer gateway, you can launch an instance and test the connection by pinging the instance. You need to use an AMI that responds to ping requests, and you need to ensure that your instance's security group is configured to enable inbound ICMP. We recommend you use one of the Amazon Linux AMIs. If you are using instances running Windows Server, you'll need to log in to the instance and enable inbound ICMPv4 on the Windows firewall in order to ping the instance.

Important
You must configure any security group or network ACL in your VPC that filters traffic to the instance to allow inbound and outbound ICMP traffic.

To test end-to-end connectivity

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. On the dashboard, choose **Launch Instance**.
3. On the **Choose an Amazon Machine Image (AMI)** page, choose an AMI, and then choose **Select**.
4. Choose an instance type, and then choose **Next: Configure Instance Details**.
5. On the **Configure Instance Details** page, for **Network**, select your VPC. For **Subnet**, select your subnet. Choose **Next** until you reach the **Configure Security Group** page.
6. Select the **Select an existing security group** option, and then select the default group that you modified earlier. Choose **Review and Launch**.
7. Review the settings that you've chosen. Make any changes that you need, and then choose **Launch** to select a key pair and launch the instance.
8. After the instance is running, get its private IP address (for example, `10.0.0.4`). The Amazon EC2 console displays the address as part of the instance's details.
9. From a computer in your network that is behind the customer gateway, use the `ping` command with the instance's private IP address. A successful response is similar to the following:

```
ping 10.0.0.4
```

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

You can now use SSH or RDP to connect to your instance in the VPC. For more information about how to connect to a Linux instance, see Connect to Your Linux Instance in the *Amazon EC2 User Guide for Linux Instances*. For more information about how to connect to a Windows instance, see Connect to Your Windows Instance in the *Amazon EC2 User Guide for Windows Instances*.

Modifying a Site-to-Site VPN Connection's Target Gateway

You can modify the target gateway of AWS Site-to-Site VPN connection. The following migration options are available:

- An existing virtual private gateway to a transit gateway
- An existing virtual private gateway to another virtual private gateway
- An existing transit gateway to another transit gateway
- An existing transit gateway to a virtual private gateway

The following tasks help you complete the migration to a new gateway.

Tasks

Step 1: Create the Transit Gateway

Before you perform the migration to the new gateway, you must configure the new gateway. For information about adding a virtual private gateway, see the section called “Create a Virtual Private Gateway” (p. 13). For more information about adding a transit gateway, see Create a Transit Gateway in *Amazon VPC Transit Gateways*.

If the new target gateway is a transit gateway, attach the VPCs to the transit gateway. For information about VPC attachments, see Transit Gateway Attachments to a VPC in *Amazon VPC Transit Gateways*.

Step 2: Delete Your Static Routes (Required for a Static VPN Connection Migrating to a Transit Gateway)

This step is required when you migrate from a virtual private gateway with static routes to a transit gateway.

You must delete the static routes before you migrate to the new gateway.

> **Tip**
> Keep a copy of the static route before you delete it. You will need to add back these routes to the transit gateway after the VPN connection migration is complete.

To delete a route from a route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Route Tables**, and then select the route table.
3. In the **Routes** tab, choose **Edit**, and then choose **Remove** for the static route to the virtual private gateway..
4. Choose **Save** when you are done.

Step 3: Migrate to a New Gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Site-to-Site VPN Connections**.
3. Select the Site-to-Site VPN connection and choose **Actions**, **Modify VPN Connection**.
4. Under **Change Target**, do the following:

   a. For **Target Type**, choose the gateway type.
   b. Configure the connection target:

      [Virtual private gateway] For **Target VPN Gateway ID**, choose the virtual private gateway ID.

      [Transit Gateway] For **Target transit gateway ID**, choose the transit gateway ID.
5. Choose **Save**.

To modify a Site-to-Site VPN connection using the command line or API

- ModifyVpnConnection (Amazon EC2 Query API)
- modify-vpn-connection (AWS CLI)

Step 4: Update VPC Route Tables

After you migrate to the new gateway, you might need to modify your VPC route table. The following table provides information about the actions you need to take. For information about updating VPC route tables, see Route Tables in the *Amazon VPC User Guide*.

VPN Gateway Target Modification Required VPC Route Table Updates

Existing gateway	New gateway	VPC route table change
Virtual private gateway with propagated routes	Transit gateway	Add a route that points to the transit gateway ID.
Virtual private gateway with propagated routes	Virtual private gateway with propagated routes	There is no action required.
Virtual gateway with propagated routes	Virtual private gateway with static route	Add an entry that contains the new virtual private gateway ID.
Virtual gateway with static routes	Transit gateway	Update the VPC route table and change the entry that contains to the virtual private gateway ID to the transit gateway ID.

Existing gateway	New gateway	VPC route table change
Virtual gateway with static routes	Virtual private gateway with static routes	Update the entry that points to the virtual private gateway ID to be the new virtual private gateway ID.
Virtual gateway with static routes	Virtual private gateway with propagated routes	Delete the entry that contains the virtual private gateway ID.
Transit Gateway	Virtual private gateway with static routes	Update the entry that contains the transit gateway to the virtual private gateway ID.
Transit Gateway	Virtual private gateway with propagated routes	Delete the entry that contains the transit gateway ID.
Transit Gateway	Transit Gateway	Update the entry that contains the transit gateway ID to the new transit gateway ID.

Step 5: Update the Transit Gateway Routing (Required When the New Gateway is a Transit Gateway)

When the new gateway is a transit gateway, modify the transit gateway route table to allow traffic between the VPC and the Site-to-Site VPN. For information about transit gateway routing, see Transit Gateway Route Tables in the *Amazon VPC Transit Gateways*.

Important
If you deleted VPN static routes, you must add the static routes to the transit gateway route table.

Deleting a Site-to-Site VPN Connection

If you no longer need a AWS Site-to-Site VPN connection, you can delete it.

> **Important**
> If you delete your Site-to-Site VPN connection and then create a new one, you have to download new configuration information and have your network administrator reconfigure the customer gateway.

To delete a Site-to-Site VPN connection using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Site-to-Site VPN Connections**.
3. Select the Site-to-Site VPN connection and choose **Actions**, **Delete**.
4. Choose **Delete**.

If you no longer require a customer gateway, you can delete it. You can't delete a customer gateway that's being used in a Site-to-Site VPN connection.

To delete a customer gateway using the console

1. In the navigation pane, choose **Customer Gateways**.
2. Select the customer gateway to delete and choose **Actions**, **Delete Customer Gateway**.
3. Choose **Yes, Delete**.

If you no longer require a virtual private gateway for your VPC, you can detach it.

To detach a virtual private gateway using the console

1. In the navigation pane, choose **Virtual Private Gateways**.
2. Select the virtual private gateway and choose **Actions**, **Detach from VPC**.
3. Choose **Yes, Detach**.

If you no longer require a detached virtual private gateway, you can delete it. You can't delete a virtual private gateway that's still attached to a VPC.

To delete a virtual private gateway using the console

1. In the navigation pane, choose **Virtual Private Gateways**.
2. Select the virtual private gateway to delete and choose **Actions**, **Delete Virtual Private Gateway**.
3. Choose **Yes, Delete**.

To delete a Site-to-Site VPN connection using the command line or API

- DeleteVpnConnection (Amazon EC2 Query API)
- delete-vpn-connection (AWS CLI)

- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

To delete a customer gateway using the command line or API

- DeleteCustomerGateway (Amazon EC2 Query API)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

To detach a virtual private gateway using the command line or API

- DetachVpnGateway (Amazon EC2 Query API)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

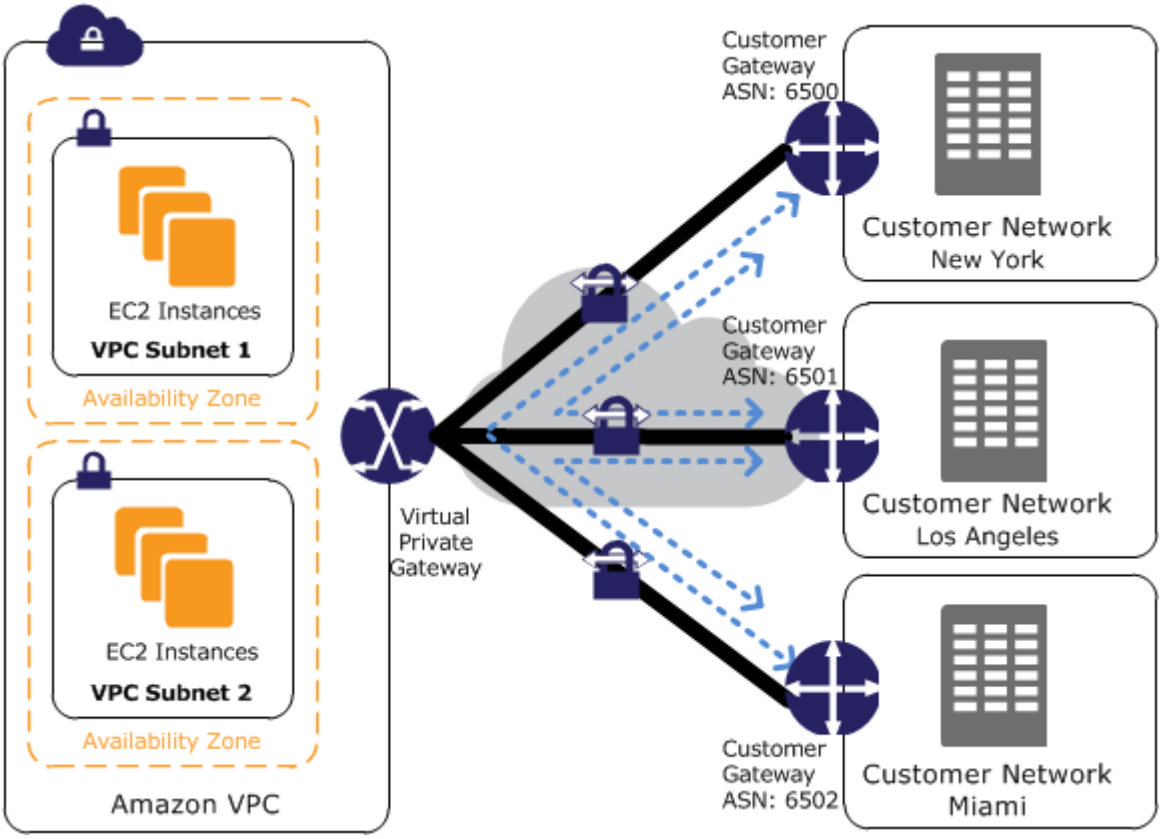
To delete a virtual private gateway using the command line or API

- DeleteVpnGateway (Amazon EC2 Query API)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Providing Secure Communication Between Sites Using VPN CloudHub

If you have multiple AWS Site-to-Site VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. 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'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

The following diagram shows the VPN CloudHub architecture, with blue dashed lines indicating network traffic between remote sites being routed over their Site-to-Site VPN connections.



To use the AWS VPN CloudHub, you must create a virtual private gateway with multiple customer gateways. You must use a unique Border Gateway Protocol (BGP) Autonomous System Number (ASN) for each customer gateway. Customer gateways advertise the appropriate routes (BGP prefixes) over their Site-to-Site VPN connections. These routing advertisements are received and re-advertised to each BGP peer, enabling each site to send data to and receive data from the other sites. 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 Site-to-Site VPN connection.

Sites that use AWS Direct Connect connections to the virtual private gateway can also be part of the AWS VPN CloudHub. For example, your corporate headquarters in New York can have an AWS Direct

Connect connection to the VPC and your branch offices can use Site-to-Site VPN connections to the VPC. The branch offices in Los Angeles and Miami can send and receive data with each other and with your corporate headquarters, all using the AWS VPN CloudHub.

To configure the AWS VPN CloudHub, you use the AWS Management Console to create multiple customer gateways, each with the public IP address of the gateway and the ASN. Next, you create a Site-to-Site VPN connection from each customer gateway to a common virtual private gateway. Each Site-to-Site VPN connection must advertise its specific BGP routes. This is done using the network statements in the VPN configuration files for the Site-to-Site VPN connection. The network statements differ slightly depending on the type of router you use.

When using an AWS VPN CloudHub, you pay typical Amazon VPC Site-to-Site VPN connection rates. You are billed the connection rate for each hour that each VPN is connected to the virtual private gateway. When you send data from one site to another using the AWS VPN CloudHub, there is no cost to send data from your site to the virtual private gateway. You only pay standard AWS data transfer rates for data that is relayed from the virtual private gateway to your endpoint. For example, if you have a site in Los Angeles and a second site in New York and both sites have a Site-to-Site VPN connection to the virtual private gateway, you pay $.05 per hour for each Site-to-Site VPN connection (for a total of $.10 per hour). You also pay the standard AWS data transfer rates for all data that you send from Los Angeles to New York (and vice versa) that traverses each Site-to-Site VPN connection; network traffic sent over the Site-to-Site VPN connection to the virtual private gateway is free but network traffic sent over the Site-to-Site VPN connection from the virtual private gateway to the endpoint is billed at the standard AWS data transfer rate. For more information, see Site-to-Site VPN Connection Pricing.

Monitoring Your Site-to-Site VPN Connection

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS Site-to-Site VPN connection. You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. Before you start monitoring your Site-to-Site VPN connection; however, you should create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What resources will you monitor?
- How often will you monitor these resources?
- What monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something goes wrong?

The next step is to establish a baseline for normal VPN performance in your environment, by measuring performance at various times and under different load conditions. As you monitor your VPN, store historical monitoring data so that you can compare it with current performance data, identify normal performance patterns and performance anomalies, and devise methods to address issues.

To establish a baseline, you should monitor the following items:

- The state of your VPN tunnels
- Data into the tunnel
- Data out of the tunnel

Contents

Monitoring Tools

AWS provides various tools that you can use to monitor a Site-to-Site VPN connection. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

Automated Monitoring Tools

You can use the following automated monitoring tools to watch a Site-to-Site VPN connection and report when something is wrong:

- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of

time periods. The action is a notification sent to an Amazon SNS topic. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see Monitoring VPN Tunnels Using Amazon CloudWatch (p. 27).

- **AWS CloudTrail Log Monitoring** – Share log files between accounts, monitor CloudTrail log files in real time by sending them to CloudWatch Logs, write log processing applications in Java, and validate that your log files have not changed after delivery by CloudTrail. For more information, see Logging API Calls Using AWS CloudTrail in the *Amazon EC2 API Reference* and Working with CloudTrail Log Files in the *AWS CloudTrail User Guide*

Manual Monitoring Tools

Another important part of monitoring a Site-to-Site VPN connection involves manually monitoring those items that the CloudWatch alarms don't cover. The Amazon VPC and CloudWatch console dashboards provide an at-a-glance view of the state of your AWS environment.

- The Amazon VPC dashboard shows:
  - Service health by region
  - Site-to-Site VPN connections
  - VPN tunnel status (In the navigation pane, choose **Site-to-Site VPN Connections**, select a Site-to-Site VPN connection, and then choose **Tunnel Details**)
- The CloudWatch home page shows:
  - Current alarms and status
  - Graphs of alarms and resources
  - Service health status

  In addition, you can use CloudWatch to do the following:
  - Create customized dashboards to monitor the services you care about
  - Graph metric data to troubleshoot issues and discover trends
  - Search and browse all your AWS resource metrics
  - Create and edit alarms to be notified of problems

Monitoring VPN Tunnels Using Amazon CloudWatch

You can monitor VPN tunnels using CloudWatch, which collects and processes raw data from the VPN service into readable, near real-time metrics. These statistics are recorded for a period of 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. VPN metric data is automatically sent to CloudWatch as it becomes available.

> **Important**
> CloudWatch metrics are not supported for AWS Classic VPN connections. For more information, see AWS Site-to-Site VPN Categories (p. 2).

For more information, see the Amazon CloudWatch User Guide.

VPN Tunnel Metrics and Dimensions

The following metrics are available for your VPN tunnels.

Metric	Description
`TunnelState`	The state of the tunnel. For static VPNs, 0 indicates DOWN and 1 indicates UP. For BGP VPNs, 1 indicates ESTABLISHED and 0 is used for all other states. Units: Boolean
`TunnelDataIn`	The bytes received through the VPN tunnel. Each metric data point represents the number of bytes received after the previous data point. Use the Sum statistic to show the total number of bytes received during the period. This metric counts the data after decryption. Units: Bytes
`TunnelDataOut`	The bytes sent through the VPN tunnel. Each metric data point represents the number of bytes sent after the previous data point. Use the Sum statistic to show the total number of bytes sent during the period. This metric counts the data before encryption. Units: Bytes

To filter the metric data, use the following dimensions.

Dimension	Description
`VpnId`	Filters the metric data by the Site-to-Site VPN connection ID.
`TunnelIpAddress`	Filters the metric data by the IP address of the tunnel for the virtual private gateway.

Viewing VPN Tunnel CloudWatch Metrics

When you create a new Site-to-Site VPN connection, the VPN service sends the following metrics about your VPN tunnels to CloudWatch as it becomes available. You can view the metrics for VPN tunnels as follows.

To view metrics using the CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Metrics**.
3. Under **All metrics**, choose the **VPN** metric namespace.
4. Select the metric dimension to view the metrics (for example, for the Site-to-Site VPN connection).

To view metrics using the AWS CLI

At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Creating CloudWatch Alarms to Monitor VPN Tunnels

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period you specify, and sends a notification to an Amazon SNS topic based on the value of the metric relative to a given threshold over a number of time periods.

For example, you can create an alarm that monitors the state of a VPN tunnel and sends a notification when the tunnel state is DOWN for 3 consecutive 5-minute periods.

To create an alarm for tunnel state

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Alarms**, **Create Alarm**.
3. Choose **VPN Tunnel Metrics**.
4. Choose the IP address of the VPN tunnel and the **TunnelState** metric. Choose **Next**.
5. Configure the alarm as follows, and choose **Create Alarm** when you are done:

   - Under **Alarm Threshold**, enter a name and description for your alarm. For **Whenever**, choose **<=** and enter `0`. Enter **3** for the consecutive periods.
   - Under **Actions**, select an existing notification list or choose **New list** to create a new one.
   - Under **Alarm Preview**, select a period of 5 minutes and specify a statistic of **Maximum**.

You can create an alarm that monitors the state of the Site-to-Site VPN connection. For example, the following alarm sends a notification when the status of both tunnels is DOWN for 1 consecutive 5-minute period.

To create an alarm for Site-to-Site VPN connection state

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Alarms**, **Create Alarm**.
3. Choose **VPN Connection Metrics**.
4. Select your Site-to-Site VPN connection and the **TunnelState** metric. Choose **Next**.
5. Configure the alarm as follows, and choose **Create Alarm** when you are done:

   - Under **Alarm Threshold**, enter a name and description for your alarm. For **Whenever**, choose **<=** and enter `0`. Enter **1** for the consecutive periods.
   - Under **Actions**, select an existing notification list or choose **New list** to create a new one.
   - Under **Alarm Preview**, select a period of 5 minutes and specify a statistic of **Maximum**.

     Alternatively, if you've configured your Site-to-Site VPN connection so that both tunnels are up, you can specify a statistic of **Minimum** to send a notification when at least one tunnel is down.

You can also create alarms that monitor the amount of traffic coming in or leaving the VPN tunnel. For example, the following alarm monitors the amount of traffic coming into the VPN tunnel from your network, and sends a notification when the number of bytes reaches a threshold of 5,000,000 during a 15 minute period.

To create an alarm for incoming network traffic

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.

2. In the navigation pane, choose **Alarms**, **Create Alarm**.
3. Choose **VPN Tunnel Metrics**.
4. Select the IP address of the VPN tunnel and the **TunnelDataIn** metric. Choose **Next**.
5. Configure the alarm as follows, and choose **Create Alarm** when you are done:

   - Under **Alarm Threshold**, enter a name and description for your alarm. For **Whenever**, choose **>=** and enter `5000000`. Enter **1** for the consecutive periods.
   - Under **Actions**, select an existing notification list or choose **New list** to create a new one.
   - Under **Alarm Preview**, select a period of 15 minutes and specify a statistic of **Sum**.

The following alarm monitors the amount of traffic leaving the VPN tunnel to your network, and sends a notification when the number of bytes is less than 1,000,000 during a 15 minute period.

To create an alarm for outgoing network traffic

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. In the navigation pane, choose **Alarms**, **Create Alarm**.
3. Choose **VPN Tunnel Metrics**.
4. Select the IP address of the VPN tunnel and the **TunnelDataOut** metric. Choose **Next**.
5. Configure the alarm as follows, and choose **Create Alarm** when you are done:

   - Under **Alarm Threshold**, enter a name and description for your alarm. For **Whenever**, choose **<=** and enter `1000000`. Enter **1** for the consecutive periods.
   - Under **Actions**, select an existing notification list or choose **New list** to create a new one.
   - Under **Alarm Preview**, select a period of 15 minutes and specify a statistic of **Sum**.

For more examples of creating alarms, see Creating Amazon CloudWatch Alarms in the *Amazon CloudWatch User Guide*.

Document History

The following table describes the AWS Site-to-Site VPN User Guide updates.

Change	Description	Date
You can modify the target gateway of AWS Site-to-Site VPN connection	You can modify the target gateway of AWS Site-to-Site VPN connection. For more information, see *Modifying a Site-to-Site VPN Connection's Target Gateway* (p. 19).	December 18, 2018
Initial release	This release separates the AWS Site-to-Site VPN (previously known as AWS Managed VPN) content from the *Amazon VPC User Guide*.	December 18, 2018