AWS Client VPN

Administrator Guide

AWS Client VPN: Administrator Guide

Table of Contents

What Is AWS Client VPN?

AWS Client VPN is a managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network. With Client VPN, you can access your resources from any location using an OpenVPN-based VPN client.

Contents

Features of Client VPN

Client VPN offers the following features:

- **Secure** — It provides a secure TLS connection from any location using the OpenVPN client.
- **Managed service** — It is an AWS managed service, so it removes the operational burden of deploying and managing a third-party remote access VPN solution.
- **Highly available and elastic** — It automatically scales to the number of users connecting to your AWS resources and on-premises resources.
- **Authentication** — It supports client authentication using Active Directory and certificate-based authentication.
- **Granular control** — It enables you to implement custom security controls by defining network-based access rules. These rules can be configured at the granularity of Active Directory groups. You can also implement access control using security groups.
- **Ease of use** — It enables you to access your AWS resources and on-premises resources using a single VPN tunnel.
- **Manageability** — It enables you to view connection logs, which provide details on client connection attempts. You can also manage active client connections, with the ability to terminate active client connections.
- **Deep integration** — It integrates with existing AWS services, including AWS Directory Service and Amazon VPC.

Components of Client VPN

The following are the key concepts for Client VPN:

Client VPN endpoint

The Client VPN endpoint is the resource that you create and configure to enable and manage client VPN sessions. It is the resource where all client VPN sessions are terminated.

Target network

A target network is the network that you associate with a Client VPN endpoint. A subnet from a VPC is a target network. Associating a subnet with a Client VPN endpoint enables you to establish VPN

sessions. You can associate multiple subnets with a Client VPN endpoint for high availability. All subnets must be from the same VPC. Each subnet must belong to a different Availability Zone.

Route

Each Client VPN endpoint has a route table that describes the available destination network routes. Each route in the route table specifies the path for traffic to specific resources or networks.

Authorization rules

An authorization rule restricts the users who can access a network. For a specified network, you configure the Active Directory group that is allowed access. Only users belonging to this Active Directory group can access the specified network. By default, there are no authorization rules and you must configure authorization rules to enable users to access resources and networks.

Client

The end user connecting to the Client VPN endpoint to establish a VPN session. End users need to download an OpenVPN client and use the Client VPN configuration file that you created to establish a VPN session.

Client VPN Ports

AWS Client VPN only supports port 443 for both TCP and UDP.

Accessing Client VPN

You can work with Client VPN in any of the following ways:

Amazon VPC console

The Amazon VPC console provides a web-based user interface for Client VPN. If you've signed up for an AWS account, you can sign into the Amazon VPC console and select Client VPN in the navigation pane.

AWS Command Line Interface (CLI)

The AWS CLI provides direct access to the Client VPN public APIs. It is supported on Windows, macOS, and Linux. For more information about getting started with the AWS CLI, see the AWS Command Line Interface User Guide. For more information about the commands for Client VPN, see the AWS CLI Command Reference.

AWS Tools for Windows PowerShell

AWS provides commands for a broad set of AWS offerings for those who script in the PowerShell environment. For more information about getting started with the AWS Tools for Windows PowerShell, see the AWS Tools for Windows PowerShell User Guide. For more information about the cmdlets for Client VPN, see the AWS Tools for Windows PowerShell Cmdlet Reference.

Query API

The Client VPN HTTPS Query API gives you programmatic access to Client VPN and AWS. The HTTPS Query API lets you issue HTTPS requests directly to the service. When you use the HTTPS API, you must include code to digitally sign requests using your credentials. For more information, see the Client VPN API Reference.

Limitations of Client VPN

Client VPN has the following limitations:

- Client CIDR ranges cannot overlap with the local CIDR of the VPC in which the associated subnet is located, or any routes manually added to the Client VPN endpoint's route table.
- The Client VPN endpoint and the VPC in which the associated subnet is located must belong to the same account.
- The subnets associated with a Client VPN endpoint must be in the same VPC.
- You cannot associate multiple subnets from the same Availability Zone with a Client VPN endpoint.
- Client VPN supports IPv4 traffic only.
- Client VPN is not Health Insurance Portability and Accountability Act (HIPAA) or Federal Information Processing Standards (FIPS) compliant.
- If multi-factor authentication (MFA) is disabled for your Active Directory, a user password cannot be in the following format.

```
SCRV1:<base64_encoded_string>:<base64_encoded_string>
```

Pricing of Client VPN

You are billed per active association per Client VPN endpoint on an hourly basis. Billing is pro-rated for the hour.

You are billed for each client VPN connection per hour. Billing is pro-rated for the hour.

For more information, see AWS Client VPN Pricing.

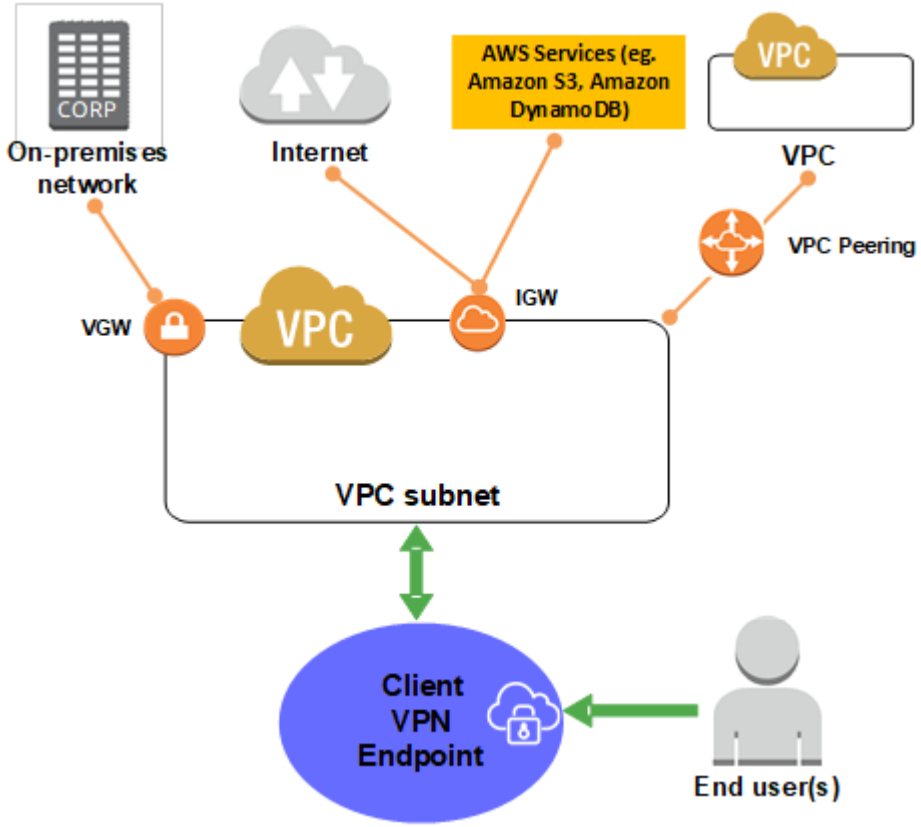
How AWS Client VPN Works

With AWS Client VPN, there are two types of user personas that interact with the Client VPN endpoint: administrators and clients.

The *administrator* is responsible for setting up and configuring the service. This involves creating the Client VPN endpoint, associating the target network, and configuring the authorization rules, and setting up additional routes (if required). After the Client VPN endpoint is set up and configured, the administrator downloads the Client VPN endpoint configuration file and distributes it to the clients who need access. The Client VPN endpoint configuration file includes the DNS name of the Client VPN endpoint and certificate information required to establish a VPN session. For more information about setting up the service, see Getting Started with Client VPN (p. 14).

The *client* is the end user. This is the person who connects to the Client VPN endpoint to establish a VPN session. The client establishes the VPN session from their local computer or mobile device using an OpenVPN-based VPN client application. After they have established the VPN session, they can securely access the resources in the VPC in which the associated subnet is located. They can also access other resources in AWS or an on-premises network if the required route and authorization rules have been configured. For more information about connecting to a Client VPN endpoint to establish a VPN session, see Getting Started in the *AWS Client VPN User Guide*.

The following graphic illustrates the basic Client VPN architecture.



Client Authentication and Authorization

Client VPN provides authentication and authorization capabilities.

Contents

Authentication

Authentication is implemented at the first point of entry into the AWS Cloud. It is used to determine whether clients are allowed to connect to the Client VPN endpoint. If authentication succeeds, clients connect to the Client VPN endpoint and establish a VPN session. If authentication fails, the connection is denied and the client is prevented from establishing a VPN session.

Client VPN offers two types of client authentication: Active Directory authentication and mutual authentication. You can choose to use either one or both authentication methods.

Active Directory Authentication

Client VPN provides Active Directory support by integrating with AWS Directory Service. With Active Directory authentication, clients are authenticated against existing Active Directory groups. Using AWS Directory Service, Client VPN can connect to existing Active Directories provisioned in AWS or in your on-premises network. This allows you to use your existing client authentication infrastructure. If you are using an on-premises Active Directory, you must configure an Active Directory Connector (AD Connector). You can use one Active Directory server to authenticate the users. For more information about Active Directory integration, see the AWS Directory Service Administration Guide.

Client VPN supports multi-factor authentication (MFA) when it's enabled for AWS Managed Microsoft AD or AD Connector. If MFA is enabled, clients must enter a user name, password, and MFA code when they connect to a Client VPN endpoint. For more information about enabling MFA, see Enable Multi-Factor Authentication for AWS Managed Microsoft AD and Enable Multi-Factor Authentication for AD Connector in the *AWS Directory Service Administration Guide*.

Mutual Authentication

With mutual authentication, Client VPN uses certificates to perform authentication between the client and the server. Certificates are a digital form of identification issued by a certificate authority (CA). The server uses client certificates to authenticate clients when they attempt to connect to the Client VPN endpoint. The server and client certificates must be uploaded to AWS Certificate Manager (ACM). For more information about provisioning and uploading certificates in ACM, see the AWS Certificate Manager User Guide.

You only need to upload the client certificate to ACM when the Certificate Authority (Issuer) of the client certificate is different from the Certificate Authority (Issuer) of the server certificate.

You can create a separate client certificate and key for each client that will connect to the Client VPN endpoint. This enables you to revoke a specific client certificate if a user leaves your organization.

A Client VPN endpoint supports 1024-bit and 2048-bit RSA key sizes only.

The following procedure uses OpenVPN easy-rsa to generate the server and client certificates and keys, and then uploads the server certificate and key to ACM. For more information, see the Easy-RSA 3 Quickstart README.

To generate the server and client certificates and keys and upload them to ACM

1. Clone the OpenVPN easy-rsa repo to your local computer.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

2. Navigate into the `easy-rsa/easyrsa3` folder in your local repo.

```
$ cd easy-rsa/easyrsa3
```

3. Initialize a new PKI environment.

```
$ ./easyrsa init-pki
```

4. Build a new certificate authority (CA).

```
$ ./easyrsa build-ca nopass
```

Follow the prompts to build the CA.

5. Generate the server certificate and key.

```
$ ./easyrsa build-server-full server nopass
```

6. Generate the client certificate and key.

Make sure to save the client certificate and the client private key because you will need them when you configure the client.

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

You can optionally repeat this step for each client (end user) that requires a client certificate and key.

7. Copy the server certificate and key and the client certificate and key to a custom folder and then navigate into the custom folder.

Before you copy the certificates and keys, create the custom folder by using the `mkdir` command. The following example creates a custom folder in your home directory.

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

8. Upload the server certificate and key to ACM.

```
$ aws acm import-certificate --certificate file://server.crt --private-key file://
server.key --certificate-chain file://ca.crt --region region
```

Note
Be sure to upload the certificate and key in the same Region in which you intend to create the Client VPN endpoint.

9. Upload the client certificate and key to ACM.

```
$ aws acm import-certificate --certificate file://client1.domain.tld.crt --private-key
 file://client1.domain.tld.key --certificate-chain file://ca.crt --region region
```

Note
Be sure to upload the certificate and key in the same Region in which you intend to create the Client VPN endpoint.

Authorization

Client VPN supports two types of authorization: security groups and network-based authorization (using authorization rules).

Security Groups

Client VPN automatically integrates with security groups. When you associate a subnet with a Client VPN endpoint, we automatically apply the VPC's default security group. You can change the security group after you associate the first target network. You can enable Client VPN users to access your applications in a VPC, by adding a rule to allow traffic from the security group that was applied to the association. Conversely, you can restrict access for Client VPN users, by not specifying the security group that was applied to the association. For more information, see Apply a Security Group to a Target Network (p. 24). The security group rules you require might also depend on the kind of VPN access you want to configure. For more information, see Scenarios and Examples (p. 10).

Network-based Authorization

Network-based authorization is implemented using authorization rules. For each network that you want to enable access, you must configure authorization rules that limits the users who have access. For a specified network, you configure the Active Directory group that is allowed access. Only users who belong to the specified Active Directory group can access the specified network. If you are not using Active Directory, or you want to open access to all users, you can specify a rule that grants access to all clients. For more information, see Authorization Rules (p. 25).

Split-Tunnel on AWS Client VPN Endpoints

By default, when you have an AWS Client VPN endpoint, all client traffic is routed over the AWS Client VPN tunnel. When you enable split-tunnel on the AWS Client VPN endpoint, we will push the routes on the AWS Client VPN endpoint route table to the device which is connected to the AWS Client VPN. This ensures that only traffic with a destination to the network matching a route from the AWS Client VPN endpoint route table is routed via the Client VPN tunnel.

You can use a split-tunnel AWS Client VPN endpoint when you do not want all user traffic to route through the AWS Client VPN endpoint.

Split-Tunnel on AWS Client VPN Endpoints Benefits

Split-tunnel on AWS Client VPN endpoints offers the following benefits:

- With split-tunnel, customers can optimize the routing of traffic from the client, by having only the AWS destined traffic traverse the VPN tunnel.
- By optimizing the traffic, customers also reduce the volume of outgoing traffic from AWS, therefore reducing the data transfer cost.

Split-Tunnel AWS Client VPN Endpoint Routing Considerations

When you enable split-tunnel on an AWS Client VPN endpoint, all of the routes that are in the AWS Client VPN route tables are added to the client route table when the VPN is established. This operation

is different from the default AWS Client VPN endpoint operation, which overwrites the client route table with the entry 0.0.0.0/0 to route all traffic over the VPN.

Using Service-Linked Roles for Client VPN

AWS Client VPN uses a service-linked role for the permissions that it requires to call other AWS services on your behalf. For more information, see Using Service-Linked Roles in the *IAM User Guide*.

Service-Linked Role Permissions for Client VPN

AWS Client VPN uses the service-linked role named **AWSServiceRoleForClientVPN** to call the following actions on your behalf when you work with Client VPN endpoints:

- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeInternetGateways`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ds:AuthorizeApplication`
- `ds:DescribeDirectories`
- `ds:GetDirectoryLimits`
- `ds:ListAuthorizedApplications`
- `ds:UnauthorizeApplication`
- `logs:DescribeLogStreams`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogGroups`
- `acm:GetCertificate`
- `acm:DescribeCertificate`

The **AWSServiceRoleForClientVPN** service-linked role trusts the clientvpn.amazonaws.com principal to assume the role.

Creating a Service-Linked Role for Client VPN

You don't need to manually create the **AWSServiceRoleForClientVPN** role. Client VPN creates this role for you when you create the first Client VPN endpoint in your account.

For Client VPN to create the service-linked role on your behalf, you must have the required permissions. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Editing a Service-Linked Role for Client VPN

Client VPN does not allow you to edit the **AWSServiceRoleForClientVPN** service-linked role.

Deleting a Service-Linked Role for Client VPN

If you no longer need to use Client VPN, we recommend that you delete the **AWSServiceRoleForClientVPN** service-linked role.

You can delete the **AWSServiceRoleForClientVPN** service-linked role only after first deleting the related Client VPN resources. This ensures that you do not inadvertently remove permission to access the resources.

Use the IAM console, the IAM CLI, or the IAM API to delete the **AWSServiceRoleForClientVPN** service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Scenarios and Examples

This section provides examples for creating and configuring VPN access for your clients.

Contents

Access to a VPC

The configuration for this scenario includes a single target VPC. We recommend this configuration if you need to give clients access to the resources inside a single VPC only.

To implement this configuration

1. Ensure that you have a VPC with at least one subnet. Identify the subnet in the VPC that you want to associate with the Client VPN endpoint and note its IPv4 CIDR ranges. For more information, see VPCs and Subnets in the *Amazon VPC User Guide*.
2. Ensure that the VPC's default security group allows inbound and outbound traffic to and from the elastic network interface IP address, or the VPC CIDR range (this option allows you to scale when you add additional elastic network interfaces). . For more information, see Security Groups for Your VPC in the *Amazon VPC User Guide*.

   Ensure the subnet you choose does not overlap with the resources that you want to access via the Client VPN endpoint, because the endpoint uses the source NAT (SNAT) to connect to resources in the associated VPCs.
3. Create a Client VPN endpoint in the same region as the VPC. To do this, perform the steps described in Create a Client VPN Endpoint (p. 20).
4. Associate the subnet with the Client VPN endpoint. To do this, perform the steps described in Associate a Target Network with a Client VPN Endpoint (p. 23) and select the subnet and the VPC you identified earlier.
5. Add an authorization rule to give clients access to the VPC. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25), and for **Destination network to enable** , enter the IPv4 CIDR range of the VPC.

Access to a Peered VPC

The configuration for this scenario includes a single VPC and an additional VPC that is peered with the target VPC. We recommend this configuration if you need to give clients access to the resources inside a target VPC and other VPCs that are peered with it.

To implement this configuration

1. Ensure that you have a VPC with at least one subnet. Identify the subnet in the VPC that you want to associate with the Client VPN endpoint and note its IPv4 CIDR ranges. For more information, see VPCs and Subnets in the *Amazon VPC User Guide*.

2. Ensure that the VPC's default security group allows inbound and outbound traffic to and from your clients. For more information, see Security Groups for Your VPC in the *Amazon VPC User Guide*.
3. Establish the VPC peering connection between the VPCs. Follow the steps at Creating and Accepting a VPC Peering Connection in the *Amazon VPC User Guide*.
4. Test the VPC peering connection. Confirm that instances in either VPC can communicate with each other as if they are within the same network. If the peering connection works as expected, continue to the next step.
5. Create a Client VPN endpoint in the same region as the VPC identified in **Step 1**. Perform the steps described in Create a Client VPN Endpoint (p. 20).
6. Associate the subnet you identified earlier with the Client VPN endpoint that you created. To do this, perform the steps described in Associate a Target Network with a Client VPN Endpoint (p. 23) and select the subnet and the VPC.
7. Add an authorization rule to give clients access to the VPC. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25), and for **Destination network to enable** , enter the IPv4 CIDR range of the VPC.
8. Add a route to direct traffic to the peered VPC. To do this, perform the steps described in Create an Endpoint Route (p. 27); for **Route destination**, enter IPv4 CIDR range of the peered VPC, and for **Target VPC Subnet ID**, select the subnet you associated with the Client VPN endpoint.
9. Add an authorization rule to give clients access to peered VPC. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25); for **Destination network**, enter IPv4 CIDR range of the peered VPC, and for **Grant access to**, select **Allow access to all users**.

Access to an On-Premises Network

The configuration for this scenario includes access to an on-premises network only. We recommend this configuration if you need to give clients access to the resources inside an on-premises network only.

To implement this configuration

1. Ensure that you have a VPC with at least one subnet. Identify the subnet in the VPC that you want to associate with the Client VPN endpoint and note its IPv4 CIDR ranges. For more information, see VPCs and Subnets in the *Amazon VPC User Guide*.
2. Ensure that the VPC's default security group allows inbound and outbound traffic to and from your clients. For more information, see Security Groups for Your VPC in the *Amazon VPC User Guide*.
3. Enable communication between the VPC and your own on-premises network over an AWS Site-to-Site VPN connection. To do this, perform the steps described in Setting Up an AWS VPN Connection in the *Amazon VPC User Guide*.
4. Test the AWS Site-to-Site VPN you created in the previous step. To do this, perform the steps described in Testing the VPN Connection in the *Amazon VPC User Guide*. If the AWS Site-to-Site VPN is functioning as expected, continue to the next step.
5. Create a Client VPN endpoint in the same region as the VPC. To do this, perform the steps described in Create a Client VPN Endpoint (p. 20).
6. Associate the subnet that you identified earlier with the Client VPN endpoint. To do this, perform the steps described in Associate a Target Network with a Client VPN Endpoint (p. 23) and select the VPC and the subnet.
7. Add a route that allows access to the AWS Site-to-Site VPN connection. To do this, perform the steps described in Create an Endpoint Route (p. 27); for **Route destination**, enter the Ipv4 CIDR range of the AWS Site-to-Site VPN connection, and for **Target VPC Subnet ID**, select the subnet you associated with the Client VPN endpoint.

8. Add an authorization rule to give clients access to the AWS Site-to-Site VPN connection. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25); for **Destination network to enable**, enter the AWS Site-to-Site VPN connection Ipv4 CIDR range, and for **Grant access to**, select **Allow access to all users**.

Access to the Internet

The configuration for this scenario includes a single target VPC and access to the internet. We recommend this configuration if you need to give clients access to the resources inside a single target VPC and allow access to the internet.

If you completed the Getting Started with Client VPN (p. 14) tutorial, then you've already implemented this scenario.

To implement this configuration

1. Ensure that you have a VPC with at least one subnet. Identify the subnet in the VPC that you want to associate with the Client VPN endpoint and note its IPv4 CIDR ranges. For more information, see VPCs and Subnets in the *Amazon VPC User Guide*.
2. Ensure that the VPC's default security group allows inbound and outbound traffic to and from your clients. For more information, see Security Groups for Your VPC in the *Amazon VPC User Guide*.
3. Ensure that the VPC's default security group allows inbound and outbound traffic to and from the internet. To do this, add inbound and outbound rules that allow traffic to and from 0.0.0.0/0.
4. Create an internet gateway and attach it to your VPC. For more information, see Creating and Attaching an Internet Gateway in the *Amazon VPC User Guide*.
5. Make your subnet public by adding a route to the internet gateway to its route table. In the VPC console, choose **Subnets**, select the subnet you intend to associate with the Client VPN endpoint, choose **Route Table**, and then choose the route table ID. Choose **Actions**, choose **Edit routes**, and choose **Add route**. For **Destination**, enter `0.0.0.0/0`, and for **Target**, choose the internet gateway from the previous step.
6. Create a Client VPN endpoint in the same region as the VPC. To do this, perform the steps described in Create a Client VPN Endpoint (p. 20).
7. Associate the subnet that you identified earlier with the Client VPN endpoint. To do this, perform the steps described in Associate a Target Network with a Client VPN Endpoint (p. 23) and select the VPC and the subnet.
8. Add an authorization rule to give clients access to the VPC. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25); and for **Destination network to enable** , enter the IPv4 CIDR range of the VPC.
9. Add a route that enables traffic to the Internet. To do this, perform the steps described in Create an Endpoint Route (p. 27); for **Route destination**, enter `0.0.0.0/0`, and for **Target VPC Subnet ID**, select the subnet you associated with the Client VPN endpoint.
10. Add an authorization rule to give clients access Internet. To do this, perform the steps described in Add an Authorization Rule to a Client VPN Endpoint (p. 25); for **Destination network to enable**, enter `0.0.0.0/0`, and for **Grant access to**, select **Allow access to all users**.

Restrict Access to Specific Resources in your VPC

You can grant or deny access to specific resources in your VPC.

This configuration expands on the scenario described in Access to a VPC (p. 10). This configuration is applied in addition to the authorization rule configured in that scenario.

Grant access to Client VPN clients only

This configuration grants only Client VPN clients access to a specific resource in a VPC.

On the instance on which your resource is running, create a security group rule that allows only traffic from the security group that was applied to the target network association.

Deny Client VPN clients access

This configuration prevents Client VPN clients from accessing a specific resource in a VPC.

On the instance on which your resource is running, the security group must not allow traffic from the security group that was applied to the target network association.

Getting Started with Client VPN

The following tasks help you become familiar with Client VPN. In this tutorial, you will create a Client VPN endpoint that does the following:

- Provides access to a single VPC.
- Provides access to the internet.
- Uses mutual authentication. For more information, see Mutual Authentication (p. 5).

Steps

Prerequisites

To complete this getting started tutorial, you need the following:

- The permissions required to work with Client VPN endpoints.
- A VPC with at least one subnet, an internet gateway, and a route to the internet gateway.

Step 1: Generate Server and Client Certificates and Keys

This tutorial uses mutual authentication. With mutual authorization, Client VPN uses certificates to perform authentication between the client and the server.

For detailed steps to generate the server and client certificates and keys, see Mutual Authentication (p. 5).

Step 2: Create a Client VPN Endpoint

When you create a Client VPN endpoint, you create the VPN construct to which clients can connect to establish a VPN connection.

After you create the Client VPN endpoint, take note of the following:

- The initial state of the Client VPN endpoint is `pending-associate`. Clients can only establish a VPN connection after you associate at least one target network.
- You receive a Client VPN endpoint DNS name. This is the DNS name that clients use to establish a VPN connection.
- You can download the Client VPN endpoint configuration file. You can provide this file to your clients who want to connect to the VPN.

To create a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints** and choose **Create Client VPN Endpoint.**
3. (Optional) For **Description**, enter a brief description for the Client VPN endpoint.
4. For **Client IPv4 CIDR**, specify an IP address range, in CIDR notation, from which to assign client IP addresses.

   Note
   The IP address range cannot overlap with the target network or any of the routes that will be associated with the Client VPN endpoint. The client CIDR range must have a block size that is between /16 and /22 and not overlap with VPC CIDR or any other route in the route table.

   Important
   The IP address range cannot be changed after the Client VPN endpoint has been created.
5. For **Server certificate ARN**, specify the ARN for the TLS certificate to be used by the server. Clients use the server certificate to authenticate the Client VPN endpoint to which they are connecting.

   Note
   The server certificate must be provisioned in AWS Certificate Manager (ACM).
6. Specify the authentication method to be used to authenticate clients when they establish a VPN connection. To use mutual certificate authentication, select **Use mutual authentication**, and then for **Client certificate ARN**, specify the ARN of the client certificate generated in Step 1.
7. Specify whether to log data about client connections using Amazon CloudWatch Logs. For **Do you want to log the details on client connections?**, do one of the following:

   - To enable client connection logging, choose **Yes**. For **CloudWatch Logs log group name**, enter the name of the log group to use, and for **CloudWatch Logs log stream name**, enter the name of the log stream to use.
   - To disable client connection logging, choose **No**.
8. (Optional) Specify which DNS servers to use for DNS resolution. To use custom DNS servers, for **DNS Server 1 IP address** and **DNS Server 2 IP address**, specify the IP addresses of the DNS servers to use. To use a VPC DNS server, for either **DNS Server 1 IP address** or **DNS Server 2 IP address**, specify the IP addresses, and add the VPC DNS server IP address.

   Note
   Ensure that the DNS servers can be reached by clients.
9. (Optional) To enable split-tunnel on a VPN endpoint, select **Enable split-tunnel**.

   By default, split-tunnel on a VPN endpoint is disabled.
10. (Optional) By default, the Client VPN server uses the `UDP` transport protocol. To use the `TCP` transport protocol instead, for **Transport Protocol**, select **TCP**.

    Note
    UDP typically offers better performance than TCP.
11. Choose **Create Client VPN Endpoint**.

Step 3: Enable VPN Connectivity for Clients

To enable clients to establish a VPN session, you must associate a target network with the Client VPN endpoint. A target network is a subnet in a VPC.

When you associate the first subnet with the Client VPN endpoint, the following happens:

- The state of the Client VPN endpoint changes to `available`. Clients can now establish a VPN connection, but they cannot access any resources in the VPC until you add the authorization rules.
- The local route of the VPC is automatically added to the Client VPN endpoint route table.
- The VPC's default security group is automatically applied for the subnet association. You can modify the security group after associating the subnet.

To associate a subnet with the Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint with which to associate the subnet and choose **Associations**, **Associate**.
4. For **VPC**, choose the VPC in which the subnet is provisioned.

   Note
   For the first subnet you associate, you can choose any subnet in any VPC that exists in the same account as the Client VPN endpoint. After you associate the first subnet with the Client VPN endpoint, all further subnet associations must be from the same VPC, but they must belong to different Availability Zones.
5. For **Subnet to associate**, choose the subnet to associate with the Client VPN endpoint.
6. Choose **Associate**.

   Note
   One subnet association is enough for clients to access a VPC's entire network if authorization rules allow it. You can associate additional subnets to provide high availability in case one of the zones goes down.

Step 4: Authorize Clients to Access a Network

To authorize clients to access the VPC in which the associated subnet is located, you must create an authorization rule. The authorization rule specifies which clients have access to the VPC. In this tutorial, we grant access to all users.

To add an authorization rule to the target network

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which to add the authorization rule, choose **Authorization**, and then choose **Authorize ingress**.
4. For **Destination network**, enter the IP address, in CIDR notation, of the network for which you want to allow access.
5. Specify which clients are allowed to access the specified network. To grant access to all users, for **For grant access to**, choose **Allow access to all users**.
6. For **Description**, enter a brief description of the authorization rule.

7. Choose **Add authorization rule**.

Step 5: (Optional) Enable Access to Additional Networks

You can enable access to additional networks connected to the VPC, such as AWS services, peered VPCs, and on-premises networks. For each additional network, you must add a route to the network and configure an authorization rule to give clients access.

In this tutorial, we add a route to the internet (`0.0.0.0/0`) and add an authorization rule that grants access to all users.

To enable access to additional networks (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which to add the route, choose **Route Table**, and then choose **Create Route**.
4. For **Route destination**, enter `0.0.0.0/0`.
5. For **Target VPC Subnet ID**, specify the ID of the subnet through which to route traffic.
6. For **Description**, enter a brief description for the route.
7. Choose **Create Route**.
8. Add an authorization rule for the network to specify which clients have access. Perform the steps at Step 4: Authorize Clients to Access a Network (p. 16), for **Step 4** enter `0.0.0.0/0`, and for **Step 5** choose **Allow access to all users**.
9. Ensure that the security group that's associated with subnet you are routing traffic through allows inbound and outbound traffic to and from the internet. To do this, add inbound and outbound rules that allow internet traffic to and from 0.0.0.0/0.

Step 6: Download the Client VPN Endpoint Configuration File

The final step is to download and prepare the Client VPN endpoint configuration file. The configuration file includes the Client VPN endpoint and certificate information required to establish a VPN connection. You must provide this file to the clients who need to connect to the Client VPN endpoint to establish a VPN connection. The client uploads this file into their VPN client application. For more information about using a client application to connect to the Client VPN endpoint, see the AWS Client VPN User Guide.

After you create the Client VPN endpoint in Step 2, the console displays the DNS name, for example, `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`. To specify the DNS name, you must specify a random string in front of the displayed name so that the format is *`random_string.displayed_DNS_name`*, for example, `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`.

To download and prepare the Client VPN endpoint configuration file (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint for which to download the Client VPN configuration file and choose **Download Client Configuration**.
4. Copy the client certificate and key, which were generated in **Step 1**, to the same folder as the downloaded Client VPN endpoint configuration file. The client certificate and key can be found in the following locations in the cloned OpenVPN easy-rsa repo:

   - Client certificate — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Client key — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Open the Client VPN endpoint configuration file using your preferred text editor and add the following to the end of the file. Replace *`/path/`* with the location of the client certificate and key (the location is relative to the client that's connecting to the endpoint).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

6. Prepend a random string to the Client VPN endpoint DNS name. Locate the line that specifies the Client VPN endpoint DNS name, and prepend a random string to it so that the format is *`random_string.displayed_DNS_name`*. For example:

   - Original DNS name: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
   - Modified DNS name: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
7. Save and close the Client VPN endpoint configuration file.
8. Distribute the Client VPN endpoint configuration file and the client certificate and key to your clients.

To download and prepare the Client VPN endpoint configuration file (AWS CLI)

1. Download the Client VPN endpoint configuration file.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>client-config.ovpn
```

2. Copy the client certificate and key, which were generated in **Step 1**, to the same folder as the downloaded Client VPN endpoint configuration file. The client certificate and key can be found in the following locations in the cloned OpenVPN easy-rsa repo:

   - Client certificate — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Client key — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
3. Open the Client VPN endpoint configuration file using your preferred text editor (such as **vim** or **nano**) or use the **cat >> client-config.ovpn** command and add the following to the end of the file. Replace *`/path/`* with the location of the client certificate and key (the location is relative to the client that's connecting to the endpoint).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

4. Prepend a random string to the Client VPN endpoint DNS name. Locate the line that specifies the Client VPN endpoint DNS name, and prepend a random string to it so that the format is *`random_string.displayed_DNS_name`*. For example:

   - Original DNS name: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`

- Modified DNS name: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`

5. Distribute the Client VPN endpoint configuration file and the client certificate and key to your clients.

Working with Client VPN

You can work with Client VPN using the Amazon VPC console or the AWS CLI.

Contents

Client VPN Endpoints

All client VPN sessions terminate at the Client VPN endpoint. You configure the Client VPN endpoint to manage and control all client VPN sessions.

Contents

Create a Client VPN Endpoint

You must create a Client VPN endpoint to enable your clients to establish a VPN session. After you create a new Client VPN endpoint, its status is `pending-associate`. Clients can only connect to the Client VPN endpoint after you associate the first target network.

The Client VPN must be created in the same AWS account in which the intended target network is provisioned.

Make sure that you have the client certificate and the client private key before you add a Client VPN endpoint.

You can create a Client VPN endpoint by using the console or the AWS CLI.

To create a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints** and choose **Create Client VPN Endpoint.**
3. (Optional) For **Description**, enter a brief description for the Client VPN endpoint.
4. For **Client IPv4 CIDR**, specify an IP address range, in CIDR notation, from which to assign client IP addresses.

   Note
   The IP address range cannot overlap with the target network or with any of the routes that will be associated with the Client VPN endpoint. The client CIDR range must have a block size of at least /22, and it must not be greater than /16.

Important
The IP address range cannot be changed after the Client VPN endpoint has been created.

5. For **Server certificate ARN**, specify the ARN for the TLS certificate to be used by the server. Clients use the server certificate to authenticate the Client VPN endpoint to which they are connecting.

   Note
   The server certificate must be provisioned in AWS Certificate Manager (ACM).

6. Specify the authentication method to be used to authenticate clients when they establish a VPN connection. You must select at least one authentication method.

   - To use Active Directory authentication, select **Use Active Directory authentication**, and then for **Directory ID**, specify the ID of the Active Directory to use.
   - To use mutual certificate authentication, select **Use mutual authentication**, and then for **Client certificate ARN**, specify the ARN of the client certificate.

     Note
     If the client certificate has been issued by the same Certificate Authority (Issuer) as the server certificate, then you can continue to use the server certificate ARN for the client certificate ARN. The client certificate must be provisioned in AWS Certificate Manager (ACM).

7. Specify whether to log data about client connections using Amazon CloudWatch Logs. For **Do you want to log the details on clients connections?**, do one of the following:

   - To enable client connection logging, choose **Yes**, for **CloudWatch Logs log group name** enter the name of the log group to use, and for **CloudWatch Logs log stream name**, enter the name of the log stream to use.
   - To disable client connection logging, choose **No**.

8. Specify which DNS servers to use for DNS resolution. To use custom DNS servers, for **DNS Server 1 IP address** and **DNS Server 2 IP address**, specify the IP addresses of the DNS servers to use. To use VPC DNS server, for either **DNS Server 1 IP address** or **DNS Server 2 IP address**, specify the IP addresses, and add the VPC DNS server IP address.

   Note
   Ensure that the DNS servers can be reached by clients.

9. (Optional) To have the endpoint be a split-tunnel VPN endpoint, select **Enable split-tunnel**.

   By default, split-tunnel on a VPN endpoint is disabled.

10. (Optional) By default, the Client VPN server uses the `UDP` transport protocol. To use the `TCP` transport protocol instead, for **Transport Protocol**, select **TCP**.

    Note
    UDP typically offers better performance than TCP.

11. Choose **Create Client VPN Endpoint**.

To create a Client VPN endpoint (AWS CLI)

Use the create-client-vpn-endpoint command.

Modify a Client VPN Endpoint

You can modify the server certificate, client connection logging options, DNS servers, and the description after the Client VPN endpoint has been created. You cannot modify the client IPv4 CIDR range, authentication options, or transport protocol after the Client VPN endpoint has been created.

You can modify a Client VPN endpoint by using the console or the AWS CLI.

To modify a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to modify, choose **Actions**, and then choose **Modify Client VPN Endpoint**.
4. Make the required changes and choose **Modify Client VPN Endpoint**.

To modify a Client VPN endpoint (AWS CLI)

Use the modify-client-vpn-endpoint command.

Export Client Configuration

The Client VPN endpoint configuration file is the file clients use to establish a VPN connection with the Client VPN endpoint. You must download this file and distribute it to all clients who need access to the VPN.

If your Client VPN endpoint uses Mutual Authentication, then you need to add the client certificate and the client private key (by using the <cert></cert> tag and the <key></key tag)) to the .ovpn configuration file that you downloaded. After you add the information, you can import the .ovpn file into the OpenVPN client software.

By default, the "--remote-random-hostname" option in the OpenVPN client configuration enables wild card DNS. Because wild card DNS is enabled, the client does not cache the IP address of the endpoint and you will not be able to ping the DNS name of the endpoint.

If your Client VPN endpoint uses Active Directory authentication and if you enable multi-factor authentication (MFA) on your directory after you distribute the client configuration file, you must download a new file and redistribute it to your clients. Clients cannot use the previous configuration file to connect to the Client VPN endpoint.

You can export the client configuration by using the console or the AWS CLI.

To export client configuration (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint for which to download the client configuration and choose **Download Client Configuration**.

To export client configuration (AWS CLI)

Use the export-client-vpn-client-configuration command and specify the output file name.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id --
output text>config_filename.ovpn
```

View Client VPN Endpoints

You can view information about Client VPN endpoints by using the console or the AWS CLI.

To view Client VPN endpoints using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to view.
4. Use tabs to view the associated target networks, authorization rules, routes, and client connections.

To view Client VPN endpoints using the AWS CLI

Use the describe-client-vpn-endpoints command.

Delete a Client VPN Endpoint

When you delete a Client VPN endpoint, its state is changed to `deleting` and clients can no longer connect to it. You must disassociate all associated target networks before you can delete a Client VPN endpoint.

You can delete a Client VPN endpoint by using the console or the AWS CLI.

To delete a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to delete, choose **Actions**, choose **Delete Client VPN Endpoint**, and then **Yes, Delete**.

To delete a Client VPN endpoint (AWS CLI)

Use the delete-client-vpn-endpoint command.

Target Networks

A target network is a subnet in a VPC. Associating a subnet with a Client VPN endpoint enables clients to establish a VPN session. You can associate multiple subnets with a Client VPN endpoint. All subnets must be from the same VPC. Each subnet must be in a different Availability Zone. We recommend that you associate at least two subnets in different Availability Zones to provide Availability Zone redundancy.

A Client VPN endpoint must have at least one target network to enable clients to connect to it and establish a VPN connection.

Contents

Associate a Target Network with a Client VPN Endpoint

After you associate the first target network with the Client VPN endpoint, the Client VPN endpoint's status changes from `pending-associate` to `available` and clients are able to establish a VPN connection.

To associate a subnet with a Client VPN endpoint, the subnet must have a CIDR block with at least a /27 bitmask, for example 10.0.0.0/27, and it must have at least 8 available IP addresses.

When you associate a subnet with a Client VPN endpoint, we automatically add the local route of the VPC in which the associated subnet is provisioned to the Client VPN endpoint's route table.

To associate a target network with a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint with which to associate the target network, choose **Associations**, and choose **Associate**.
4. For **VPC**, choose the VPC in which the subnet is provisioned.

   Note
   For the first subnet you associate, you can choose any subnet in any VPC that exists in the same account as the Client VPN endpoint. After you associate the first subnet with the Client VPN endpoint, all further subnet associations must be from the same VPC, but they must belong to different Availability Zones.
5. For **Subnet to associate**, choose the subnet to associate with the Client VPN endpoint.
6. Choose **Associate**.

To associate a target network with a Client VPN endpoint (AWS CLI)

Use the associate-client-vpn-target-network command.

Apply a Security Group to a Target Network

When you associate the first target network with a Client VPN endpoint, we automatically apply the default security group of the VPC in which the associated subnet is located. For more information, see Security Groups (p. 7).

You can change the security groups applied to the Client VPN endpoint after you associate the first target network. The security group rules you require depend on the kind of VPN access you want to configure. For more information, see Scenarios and Examples (p. 10).

To apply a security group to a target network (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which to apply the security groups.
4. Choose **Security Groups**, select the current security group, and choose **Apply Security Groups**.
5. Select the new security groups in the list and choose **Apply Security Groups**.

To apply a security group to a target network (AWS CLI)

Use the apply-security-groups-to-client-vpn-target-network command.

Disassociate a Target Network from a Client VPN Endpoint

If you disassociate all target networks from a Client VPN endpoint, clients can no longer establish a VPN connection. When you disassociate a subnet, we remove the route that was automatically created when the association was made.

To disassociate a target network from a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint with which the target network is associated and choose **Associations**.
4. Select the target network to disassociate, choose **Disassociate**, and then choose **Yes, Disassociate**.

To disassociate a target network from a Client VPN endpoint (AWS CLI)

Use the disassociate-client-vpn-target-network command.

View Target Networks

You can view the targets associated with a Client VPN endpoint using the console or the AWS CLI.

To view target networks (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint and choose **Associations**.

To view target networks using the AWS CLI

Use the describe-client-vpn-target-networks command.

Authorization Rules

Authorization rules act as firewall rules that grant access to networks. You should have an authorization rule for each network for which you want to grant access.

Contents

Add an Authorization Rule to a Client VPN Endpoint

By adding authorization rules, you grant the specific clients access to the specified network.

You can add authorization rules to a Client VPN endpoint using the console and the AWS CLI.

To add an authorization rule to a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which to add the authorization rule, choose **Authorization**, and choose **Authorize ingress**.
4. For **Destination network**, enter the IP address, in CIDR notation, of the network for which you want to allow access.

5. Specify which clients are allowed to access the specified network. For **For grant access to**, do one of the following:

   - To grant access to all clients, choose **Allow access to all users**.
   - To restrict access to specific clients, choose **Allow access to users in a specific Active Directory group**, and then for **Active Directory group name**, enter the security identifier (SID) of the Active Directory group to grant access.

   You can use the Microsoft Powershell Get-ADGroup cmdlet to get the SID. For more information about Get-ADGroup, see the Get-ADGroup command page in the *Microsoft Windows 10 and Windows Server 2016 PowerShell Module Reference*.

   Example

   ```
   Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
   ```

6. For **Description**, enter a brief description of the authorization rule.
7. Choose **Add authorization rule**.

To add an authorization rule to a Client VPN endpoint (AWS CLI)

Use the authorize-client-vpn-ingress command.

Remove an Authorization Rule from a Client VPN Endpoint

By deleting an authorization rule, you remove access to the specified network.

You can remove authorization rules from a Client VPN endpoint using the console and the AWS CLI.

To remove an authorization rule from a Client VPN endpoint (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which the authorization rule is added and choose **Authorization**.
4. Select the authorization rule to delete, choose **Revoke ingress**, and choose **Revoke ingress**.

To remove an authorization rule from a Client VPN endpoint (AWS CLI)

Use the revoke-client-vpn-ingress command.

View Authorization Rules

You can view authorization rules for a specific Client VPN endpoint using the console and the AWS CLI.

To view authorization rules (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint for which to view authorization rules and choose **Authorization**.

To view authorization rules (AWS CLI)

Use the describe-client-vpn-authorization-rules command.

Routes

Each Client VPN endpoint has a route table that describes the available destination network routes. Each route in the route table determines where the network traffic is directed. You must configure authorization rules for each Client VPN endpoint route to specify which clients have access to the destination network.

When you associate a subnet from a VPC with a Client VPN endpoint, a route for the VPC is automatically added to the Client VPN endpoint's route table. To enable access for additional networks, such as peered VPCs, on-premises networks, and the internet, you must manually add a route to the Client VPN endpoint's route table.

Split-Tunnel on AWS Client VPN Endpoint Considerations

When you use split-tunnel on an AWS Client VPN endpoint, all of the routes that are in the AWS Client VPN route tables are added to the client route table when the VPN is established. If you add a route after the VPN is established, you must reset the connection so that the new route is sent to the client.

We recommend that you account for the number of routes that the client device can handle before you modify the Client VPN endpoint route table.

Contents

Create an Endpoint Route

When you create a route, you specify how traffic for the destination network should be directed.

To allow clients to access the internet, add a destination `0.0.0.0/0` route.

You can add routes to a Client VPN endpoint by using the console and the AWS CLI.

To create a Client VPN endpoint route (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which to add the route, choose **Route Table**, and choose **Create Route**.
4. For **Route destination**, specify the IPv4 CIDR range for the destination network. For example:
   - To add a route for internet access, enter `0.0.0.0/0`.
   - To add a route for a peered VPC, enter the peered VPC's IPv4 CIDR range.
   - To add a route for an on-premises network, enter the AWS Site-to-Site VPN connection's IPv4 CIDR range.
5. For **Target VPC Subnet ID**, select the subnet that is associated with the Client VPN endpoint.
6. For **Description**, enter a brief description for the route.

7. Choose **Create Route**.

To create a Client VPN endpoint route (AWS CLI)

Use the create-client-vpn-route command.

View Endpoint Routes

You can view the routes for a specific Client VPN endpoint by using the console or the AWS CLI.

To view Client VPN endpoint routes (console)

1. In the navigation pane, choose **Client VPN Endpoints**.
2. Select the Client VPN endpoint for which to view routes and choose **Route Table**.

To view Client VPN endpoint routes (AWS CLI)

Use the describe-client-vpn-routes command.

Delete an Endpoint Route

You can only delete routes that you added manually. You can't delete routes that were automatically added when you associated a subnet with the Client VPN endpoint. To delete routes that were automatically added, you must disassociate the subnet that initiated its creation from the Client VPN endpoint.

You can delete a route from a Client VPN endpoint by using the console or the AWS CLI.

To delete a Client VPN endpoint route (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint from which to delete the route and choose **Route Table**.
4. Select the route to delete, choose **Delete Route**, and choose **Delete Route**.

To delete a Client VPN endpoint route (AWS CLI)

Use the delete-client-vpn-route command.

Client Certificate Revocation Lists

You can use client certificate revocation lists to blacklist specific client certificates. Blacklisting clients revokes their access to a Client VPN endpoint.

> **Note**
> For more information about generating the server and client certificates and keys, see Mutual Authentication (p. 5)

Contents

Generate a Client Certificate Revocation List

You must generate a client certificate revocation list using the OpenVPN easy-rsa command line utility.

To generate a client certificate revocation list using OpenVPN easy-rsa

1. Clone the OpenVPN easy-rsa repo to your local computer.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

2. Navigate into the `easy-rsa/easyrsa3` folder in your local repo.

```
$ cd easy-rsa/easyrsa3
```

3. Revoke the client certificate and generate the client revocation list.

```
$ ./easyrsa revoke client_certificate_name
$ ./easyrsa gen-crl
```

   Type `yes` when prompted.

Import a Client Certificate Revocation List

You must have a client certificate revocation list file to import. For more information about generating a client certificate revocation list, see Generate a Client Certificate Revocation List (p. 29).

You can import a client certificate revocation list using the console and the AWS CLI.

To import a client certificate revocation list (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint for which to import the client certificate revocation list.
4. Choose **Actions**, and choose **Import Client Certificate CRL**.
5. For **Certificate Revocation List**, enter the contents of the client certificate revocation list file, and choose **Import CRL**.

To import a client certificate revocation list (AWS CLI)

Use the import-client-vpn-client-certificate-revocation-list command.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-revocation-
list file:path_to_CRL_file --client-vpn-endpoint-id endpoint_id --region region
```

Export a Client Certificate Revocation List

You can export client certificate revocation lists using the console and the AWS CLI.

To export a client certificate revocation list (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.

3. Select the Client VPN endpoint for which to export the client certificate revocation list.
4. Choose **Actions**, choose **Export Client Certificate CRL**, and choose **Yes, Export**.

To export a client certificate revocation (AWS CLI)

Use the export-client-vpn-client-certificate-revocation-list command.

Client Connections

Connections are VPN sessions that have been established by clients. A connection is established when a client successfully connects to a Client VPN endpoint.

Contents

View Client Connections

You can view client connections using the console and the AWS CLI.

To view client connections (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint for which to view client connections.
4. Choose the **Connections** tab. The **Connections** tab lists all active and terminated client connections.

To view client connections (AWS CLI)

Use the describe-client-vpn-connections command.

Terminate a Client Connection

When you terminate a client connection, the VPN session ends.

You can terminate client connections using the console and the AWS CLI.

To terminate a client connection (console)

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Client VPN Endpoints**.
3. Select the Client VPN endpoint to which the client is connected and choose **Connections**.
4. Select the connection to terminate, choose **Terminate Connection**, and choose **Terminate Connection**.

To terminate a client connection (AWS CLI)

Use the terminate-client-vpn-connections command.

Identity and Access Management for Client VPN

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way, without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources, such as a Client VPN endpoint, and perform tasks, you must create an IAM policy. This policy must grant the IAM user permission to use the specific resources and API actions they need. Then, attach the policy to the IAM user or the group to which the IAM user belongs. When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

For example, the following policy enables read-only access. Users can view Client VPN endpoints and their components, but they cannot create, modify, or delete them.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeClientVpnEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

You can also use resource-level permissions to restrict what resources users can use when they invoke Client VPN actions. For example, the following policy allows users to work with Client VPN endpoints, but only if the Client VPN endpoint has the tag `purpose=test`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteClientVpnEndpoint",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:CreateClientVpnRoute",
                "ec2:DeleteClientVpnRoute",
                "ec2:RevokeClientVpnIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
                }
            }
        }
    ]
}
```

For more information about IAM, see the IAM User Guide. For a list of Amazon EC2 actions, including Client VPN actions, see Actions, Resources, and Condition Keys for Amazon EC2 in the *IAM User Guide*.

For more information about authentication and authorization for connecting to a Client VPN endpoint, see Client Authentication and Authorization (p. 4).

Monitoring Client VPN

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Client VPN and your other AWS solutions. You can use the following features to monitor your Client VPN endpoints, analyze traffic patterns, and troubleshoot issues with your Client VPN endpoints.

Amazon CloudWatch

Monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.

AWS CloudTrail

Captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Amazon CloudWatch Logs

Enables you to monitor connection attempts made to your AWS Client VPN endpoint. You can view the connection attempts and connection resets for the Client VPN connections. For the connection attempts, you can see both the successful and failed connection attempts. You can specify the CloudWatch Logs log stream to log the connection details. For more information, see the Amazon CloudWatch Logs User Guide.

Amazon CloudWatch

AWS Client VPN publishes the following metrics to Amazon CloudWatch for your Client VPN endpoints. Metrics are published to Amazon CloudWatch every five minutes.

Metric	Description
ActiveConnectionsCount	The number of active connections to the Client VPN endpoint. Units: Count
AuthenticationFailures	The number of authentication failures for the Client VPN endpoint. Units: Count
EgressBytes	The number of bytes sent from the Client VPN endpoint. Units: Bytes
EgressPackets	The number of packets sent from the Client VPN endpoint. Units: Count

Metric	Description
IngressBytes	The number of bytes received by the Client VPN endpoint. Units: Bytes
IngressPackets	The number of packets received by the Client VPN endpoint. Units: Count

You can filter the metrics for your Client VPN endpoint by endpoint.

CloudWatch enables you to retrieve statistics about those data points as an ordered set of time series data, known as metrics. Think of a metric as a variable to monitor, and the data points as the values of that variable over time. Each data point has an associated timestamp and an optional unit of measurement.

You can use metrics to verify that your system is performing as expected. For example, you can create a CloudWatch alarm to monitor a specified metric and initiate an action (such as sending a notification to an email address) if the metric goes outside what you consider an acceptable range.

For more information, see the Amazon CloudWatch User Guide.

AWS CloudTrail

AWS Client VPN is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Client VPN. CloudTrail captures all API calls for Client VPN as events. The calls captured include calls from the Client VPN console and code calls to the Client VPN API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Client VPN. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Use the information collected by CloudTrail to determine the request that was made to Client VPN, the requesting IP address, the requester, when it was made, and additional details.

For more information about CloudTrail, see the AWS CloudTrail User Guide.

Client VPN Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Client VPN, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Client VPN, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail

- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Client VPN actions are logged by CloudTrail and are documented in the Amazon EC2 API Reference. For example, calls to the `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork`, and `AuthorizeClientVpnIngress` actions generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding Client VPN Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

AWS Client VPN Quotas

Your AWS account has the following quotas related to Client VPN endpoints. You can request an increase for some of these quotas.

- Number of Client VPN endpoints per account: 5
- Number of authorization rules per Client VPN endpoint: 50
- Number of routes per Client VPN endpoint: 10
- Number of concurrent client connections per Client VPN endpoint: 2000
- Number of concurrent operations per Client VPN endpoint: 10

  Operations include:
  - Associating or disassociating subnets
  - Creating or deleting routes
  - Creating or deleting inbound and outbound rules
  - Creating or deleting security groups

Take the following into consideration when you use Client VPN endpoints.

- The Client VPN endpoint must belong to the same account as the VPC that contains the subnet that you want to associate with the Client VPN endpoint.
- If you use Active Directory to authenticate the user, the Client VPN endpoint must belong to the same account as the AWS Directory Service resource used for Active Directory authentication.

Troubleshooting Client VPN

The following topic can help you troubleshoot problems that you might have with a Client VPN endpoint.

For more information about troubleshooting OpenVPN-based software that clients use to connect to a Client VPN, see Troubleshooting Your Client VPN Connection in the *AWS Client VPN User Guide*.

Common problems

Unable to Resolve Client VPN Endpoint DNS Name

Problem

I am unable to resolve the Client VPN endpoint's DNS name.

Cause

The Client VPN endpoint configuration file includes a parameter called `remote-random-hostname`. This parameter forces the client to prepend a random string to the DNS name to prevent DNS caching. Some clients do not recognize this parameter and therefore, they do not prepend the required random string to the DNS name.

Solution

Open the Client VPN endpoint configuration file using your preferred text editor. Locate the line that specifies the Client VPN endpoint DNS name, and prepend a random string to it so that the format is *`random_string.displayed_DNS_name`*. For example:

- Original DNS name: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Modified DNS name: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Traffic Is Not Being Split between Subnets

Problem

I am trying to split network traffic between two subnets. Private traffic should be routed through a private subnet, while internet traffic should be routed through a public subnet. However, only one route is being used even though I have added both routes to the Client VPN endpoint route table.

Cause

You can associate multiple subnets with a Client VPN endpoint, but you can associate only one subnet per Availability Zone. The purpose of multiple subnet association is to provide high availability and Availability Zone redundancy for clients. However, Client VPN does not enable you to selectively split traffic between the subnets that are associated with the Client VPN endpoint.

Clients connect to a Client VPN endpoint based on the DNS round-robin algorithm. This means that their traffic can be routed through any of the associated subnets when they establish a connection. Therefore, they might experience connectivity issues if they land on an associated subnet that does not have the required route entries.

For example, say that you configure the following subnet associations and routes:

- Subnet associations
  - Association 1: Subnet-A (us-east-1a)
  - Association 2: Subnet-B (us-east-1b)
- Routes
  - Route 1: 10.0.0.0/16 routed to Subnet-A
  - Route 2: 172.31.0.0/16 routed to Subnet-B

In this example, clients that land on Subnet-A when they connect cannot access Route 2, while clients that land on Subnet-B when they connect cannot access Route 1.

Solution

Verify that the Client VPN endpoint has the same route entries with targets for each associated network. This ensures that clients have access to all routes regardless of the subnet through which their traffic is routed.

Authorization Rules for Active Directory Groups Not Working as Expected

Problem

I have configured authorization rules for my Active Directory groups, but they are not working as I expected. I have added an authorization rule for `0.0.0.0/0` to authorize traffic for all networks, but traffic still fails for specific destination CIDRs.

Cause

Authorization rules are indexed on network CIDRs. Authorization rules must grant Active Directory groups access to specific network CIDRs. Authorization rules for `0.0.0.0/0` are handled as a special case, and are therefore evaluated last, regardless of the order in which the authorization rules are created.

For example, say that you create three authorization rules in the following order:

- Rule 1: Group 1 access to `10.1.0.0/16`

- Rule 2: Group 1, Group 2, and Group 3 access to `0.0.0.0/0`
- Rule 3: Group 2 access to `172.131.0.0/16`

In this example, Rule 2 is evaluated last. Group 1 has access to `10.1.0.0/16` only, and Group 2 has access to `172.131.0.0/16` only. Group 3 does not have access to `10.1.0.0/16` or `172.131.0.0/16`, but it has access to all other networks. If you remove Rules 1 and 3, all three groups have access to all networks.

In addition, Client VPN uses longest prefix matching when evaluating authorization rules.

Solution

Verify that you create authorization rules that explicitly grant Active Directory groups access to specific network CIDRs. If you add an authorization rule for `0.0.0.0/0`, keep in mind that it will be evaluated last, and that previous authorization rules may limit the networks to which it grants access.

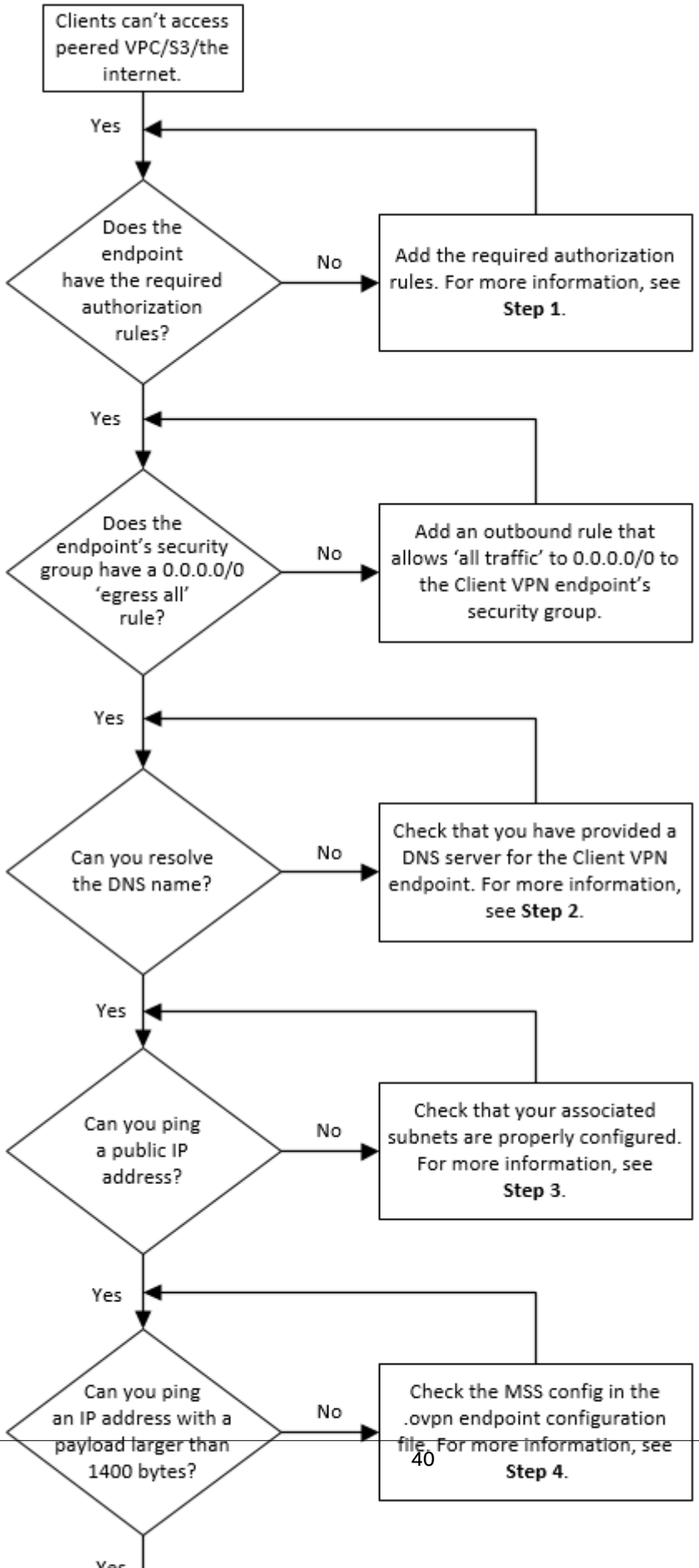
Clients Can't Access a Peered VPC, Amazon S3, or the Internet

Problem

I have properly configured my Client VPN endpoint routes, but my clients can't access a peered VPC, Amazon S3, or the internet.

Solution

The following flow chart contains the steps to diagnose internet, peered VPC, and Amazon S3 connectivity issues.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. For access to the internet, add an authorization rule for `0.0.0.0/0`.

   For access to a peered VPC, add an authorization rule for the IPv4 CIDR range of the VPC.

   For access to S3, specify the IP address of the Amazon S3 endpoint.
2. Check whether you are able to resolve the DNS name.

   If you are unable to resolve the DNS name, verify that you have specified the DNS servers for the Client VPN endpoint. If you manage your own DNS server, specify its IP address. Verify that the DNS server is accessible from the VPC.

   If you're unsure about which IP address to use, use *VPC DNS resolver .2 IP*.
3. Check whether you are able to ping an IP address. If you do not get a response, make sure that the route table for the associated subnets has a default route that targets either an internet gateway or a NAT gateway. If the default route is in place, verify that the associated subnet does not have network access control list rules that block inbound and outbound traffic.

   If you are unable to reach a peered VPC, verify that the associated subnet's route table has a route entry for the peered VPC.

   If you are unable to reach Amazon S3, verify that the associated subnet's route table has a route entry for the gateway VPC endpoint.
4. Check whether you can ping a public IP address with a payload larger than 1400 bytes. Use one of the following commands:

   - Windows

   ```
   C:\> ping  8.8.8.8 -l 1480 -f
   ```

   - Linux

   ```
   $ ping -s 1480 8.8.8.8 -M do
   ```

   If you cannot ping an IP address with a payload larger than 1400 bytes, open the Client VPN endpoint `.ovpn` configuration file using your preferred text editor, and add the following.

   ```
   mssfix 1328
   ```

Access to a Peered VPC, Amazon S3, or the Internet Is Intermittent

Problem

I have intermittent connectivity issues when connecting to a peered VPC, Amazon S3, or the internet, but access to associated subnets is unaffected. I need to disconnect and reconnect in order to resolve the connectivity issues.

Cause

Clients connect to a Client VPN endpoint based on the DNS round-robin algorithm. This means that their traffic can be routed through any of the associated subnets when they establish a connection. Therefore, they might experience connectivity issues if they land on an associated subnet that does not have the required route entries.

Solution

Verify that the Client VPN endpoint has the same route entries with targets for each associated network. This ensures that clients have access to all routes regardless of the associated subnet through which their traffic is routed.

For example, say that your Client VPN endpoint has three associated subnets (Subnet A, B, and C), and you want to enable internet access for your clients. To do this, you must add three `0.0.0.0/0` routes - one that targets each associated subnet:

- Route 1: `0.0.0.0/0` for Subnet A
- Route 2: `0.0.0.0/0` for Subnet B
- Route 3: `0.0.0.0/0` for Subnet C

Client Software Returns TLS Error

Problem

I used to be able to connect my clients to the Client VPN successfully, but now the OpenVPN-based client returns the following error when it tries to connect:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

Possible Causes

If you use mutual authentication and you imported a client certificate revocation list, the client certificate revocation list might have expired. During the authentication phase, the Client VPN endpoint checks the client certificate against the client certificate revocation list that you imported. If the client certificate revocation list has expired, you cannot connect to the Client VPN endpoint.

Alternatively, there might be an issue with the OpenVPN-based software that the client is using to connect to the Client VPN.

Solution

Check the expiry date of your client certificate revocation list by using the OpenSSL tool.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

The output displays the expiry date and time. If the client certificate revocation list has expired, you must create a new one and import it to the Client VPN endpoint. For more information, see Client Certificate Revocation Lists (p. 28).

For more information about troubleshooting OpenVPN-based software, see Troubleshooting Your Client VPN Connection in the *AWS Client VPN User Guide*.

Client Software Returns User Name and Password Errors

Problem

I use Active Directory authentication for my Client VPN endpoint and I used to be able to connect my clients to the Client VPN successfully. But now, clients are getting invalid user name and password errors.

Possible Causes

If you use Active Directory authentication and if you enabled multi-factor authentication (MFA) after you distributed the client configuration file, the file does not contain the necessary information to prompt users to enter their MFA code. Users are prompted to enter their user name and password only, and authentication fails.

Solution

Download a new client configuration file and distribute it to your clients. Verify that the new file contains the following line.

```
static-challenge "Enter MFA code " 1
```

For more information, see Export Client Configuration (p. 22). Test the MFA configuration for your Active Directory without using the Client VPN endpoint to verify that MFA is working as expected.

Document History

The following table describes the AWS Client VPN Administrator Guide updates.

Change	Description	Date
Support for multi-factor authentication (MFA)	Your AWS Client VPN endpoint supports MFA if it's enabled for your Active Directory (p. 5).	September 30, 2019
Support for split-tunnel	You can enable split-tunnel (p. 7) on your AWS Client VPN endpoint.	July 24, 2019
Initial release	This release introduces AWS Client VPN.	December 18, 2018