ZSCALER AND AWS TRAFFIC FORWARDING DEPLOYMENT GUIDE

MAY 2024, VERSION 2.2

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines the acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SA	Security Association
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VPC	Virtual Private Cloud
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

This document describes how to configure traffic forwarding for Zscaler and Amazon Web Services (AWS) deployment.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Flagship offerings Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

AWS Overview

AWS (NASDAQ: AMZN) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster. To learn more, refer to the AWS website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Zscaler Resources
- AWS Resources
- Appendix D: Requesting Zscaler Support

Software Versions

This document was authored using the latest Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and AWS Introduction

The following sections detail the Zscaler and partner products and services described in this guide.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet onramp—all you do is make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZIA Test Page	Provides information on your Zscaler cloud.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Amazon WorkSpaces Overview

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows and Linux that enables you to access resources from any supported device. With Amazon WorkSpaces, you can:

- **Onboard contingent workers**. Easily assign and remove desktops for contractors while keeping your sensitive data secure in the cloud.
- **Facilitate remote work**. Enable work-from-home and remote workers to access fully functional Windows and Linux desktops from any location.
- **Run powerful desktops**. Provide high-performance desktops for developers and engineers to store and access proprietary models, designs, and code.
- **Let contact center agents work from anywhere**. Enable contact center agents to work from anywhere with a secure, easy-to-use agent experience.

AWS Resources

The following table contains links to AWS support resources.

Name	Definition
Amazon WorkSpaces	Help documentation for Amazon WorkSpaces.
Amazon WorkSpaces Clients	Help documentation for Amazon WorkSpaces clients.
Amazon WorkSpaces Administration Guide	WorkSpaces administration guide.
WorkSpaces Bring Your Own License	Help documentation for using third-party licenses in WorkSpaces.
AWS Site-to-Site VPN Connection	Help documentation for Amazon site-to-site VPN connections.
AWS Transit Gateway	Help documentation for Amazon transit gateway connections.
AWS Customer Gateway	Help documentation for Amazon customer gateway connections.
AWS Command Line Interface	Help documentation for Amazon CLI.

Amazon WorkSpaces and Forwarding Traffic to ZIA

Amazon WorkSpaces provides a cloud-based desktop environment using either Microsoft Windows 10 (Server 2016 or Server 2019) or Amazon Linux. Amazon supports WorkSpaces clients for several different platforms. For information on setting up Amazon WorkSpaces, refer to the Amazon documentation.

Each WorkSpaces OS has the Firefox browser installed, while Windows Server 2016 and Server 2019 also has Internet Explorer (IE) installed, for accessing the web. Zscaler supports several traffic forwarding options (government agencies, see several traffic forwarding options) for forwarding traffic to the ZIA service—including Zscaler Client Connector, PAC Files, and IPSec tunnels. The following sections describe how those options apply to WorkSpaces.

Zscaler Client Connector

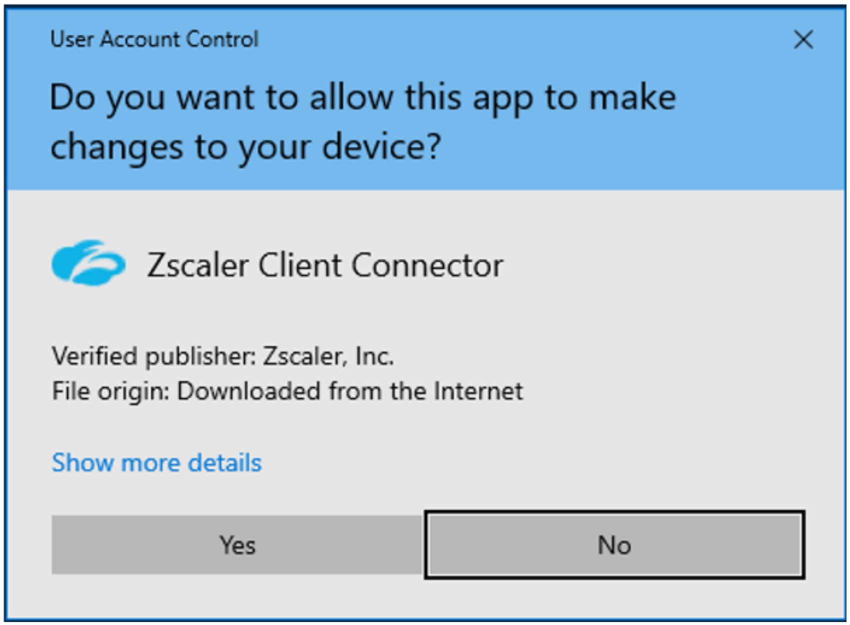
Zscaler Client Connector includes Amazon's support of Microsoft Windows 10 Desktop in WorkSpaces using Bring Your Own Windows Desktop Licenses, and Zscaler Client Connector version 3.9 supports both Windows Server 2016 and Windows Server 2019 bundles in WorkSpaces.

Because authenticating to an identity provider (IdP) makes use of embedded IE within Zscaler Client Connector, disable the IE Enhanced Security feature to use ZIA instead (for web security for authentication). For information on disabling IE Enhanced Security, see Appendix B: Disabling IE Enhanced Security.

You must get the Zscaler Client Connector installation file for Windows from your administrator (there are no publicly-accessible download links). This guide uses the 64-bit EXE version of the latest 3.9 or later release.

To install the file:

1. Double-click the **Zscaler Client Connector installation file** to start the installation. Click **Yes** when asked if you want to allow this app to make changes to your drive.



User Account Control

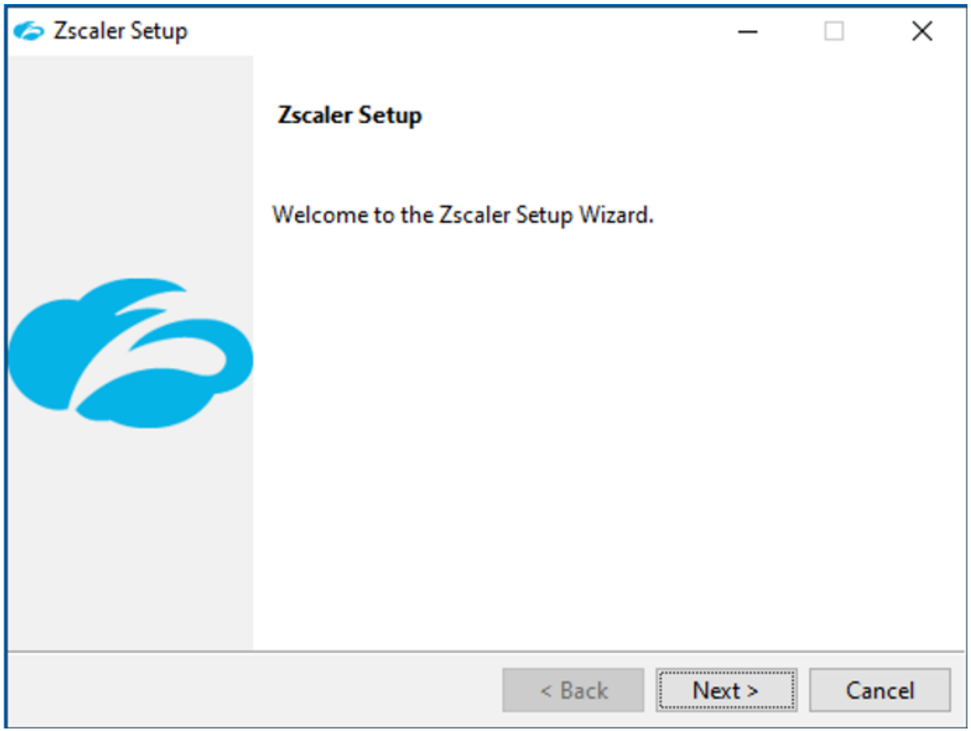
Do you want to allow this app to make changes to your device?

Zscaler Client Connector

Verified publisher: Zscaler, Inc.
File origin: Downloaded from the Internet

Figure 1. Allow device changes

2. Click **Next** to start the **Zscaler Setup Wizard**.

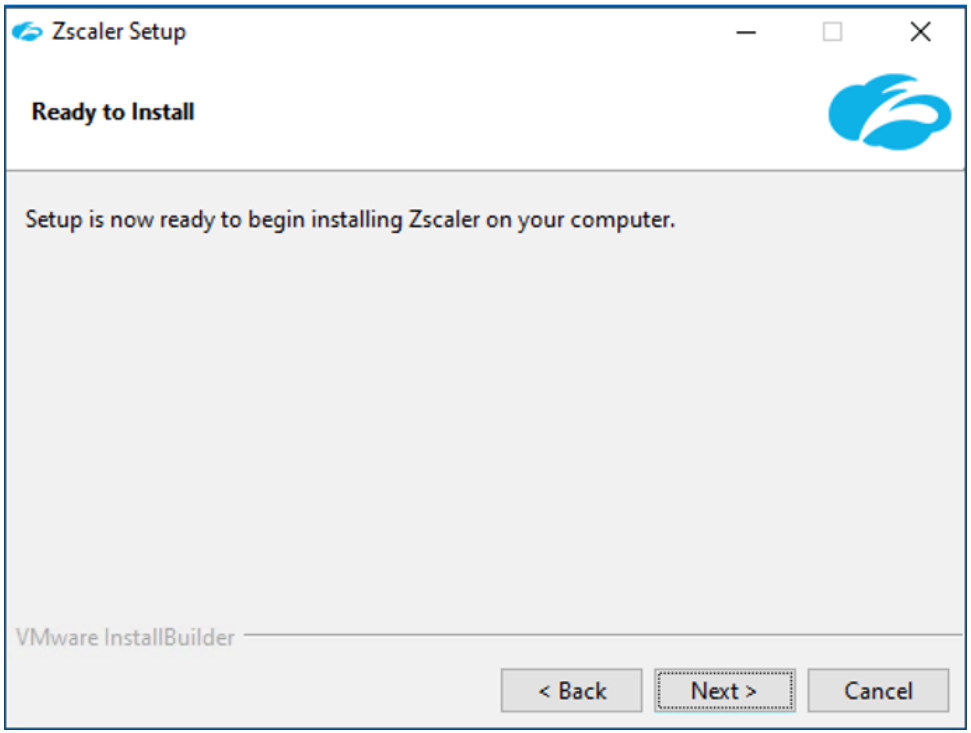


Zscaler Setup

Welcome to the Zscaler Setup Wizard.

Figure 2. Zscaler Setup Wizard

3. Click **Next** to begin the installation.

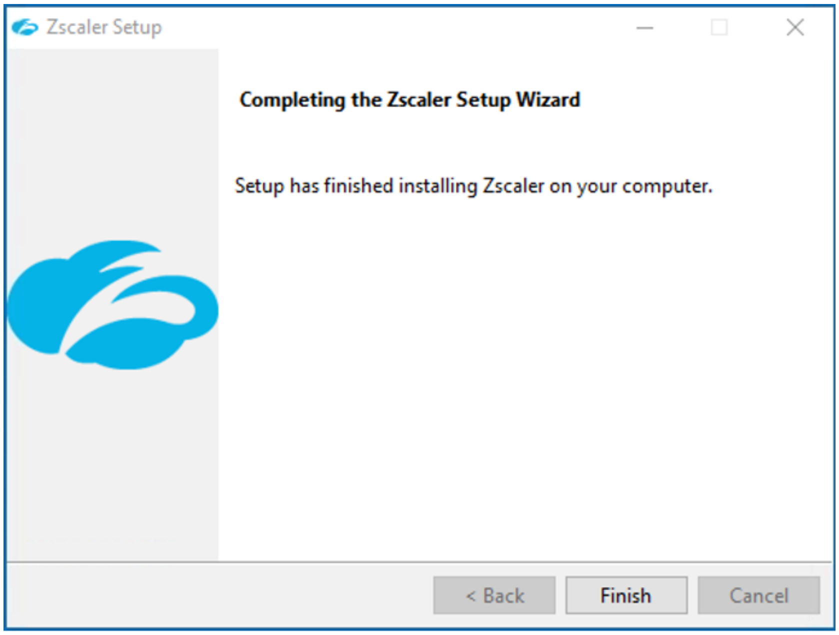


Ready to Install

Setup is now ready to begin installing Zscaler on your computer.

Figure 3. Install file

4. Click **Finish** when the installation is completed.



Zscaler Setup

Completing the Zscaler Setup Wizard

Setup has finished installing Zscaler on your computer.

Figure 4. Installation completed

5. In the Zscaler Client Connector window, enter your username. After entering your username, you are redirected to your Identity Provider (IdP) to complete authentication. When authentication is successful, the Zscaler Client Connector window closes.

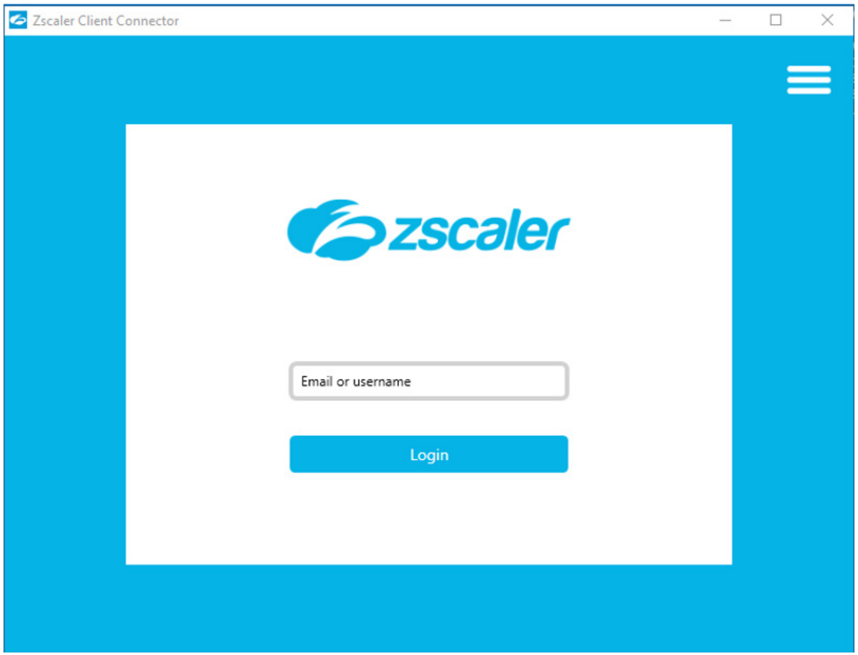


Figure 5. Zscaler Client Connector window

For detailed instructions on installing Zscaler Client Connector, see Zscaler Client Connector (government agencies, see Zscaler Client Connector).

6. Zscaler Client Connector was tested on WorkSpaces with Tunnel (both Z-Tunnel 1.0 and Z-Tunnel 2.0) and Tunnel with Local Proxy forwarding. To learn more, see Configuring Forwarding Profiles for Zscaler Client Connector (government agencies, see Configuring Forwarding Profiles for Zscaler Client Connector).
7. You must bypass the WorkSpaces management addresses for Z-Tunnel 2.0. In addition to the already-included RFC-1918 address space:
   a. Go to **App Profiles** > **Edit Window**.
   b. In the **Destination Exclusions for IPv4** configuration, copy and paste the following list to quickly add the needed addresses into the **Destinations Exclusions** dialog box:

```
10.0.0.0/8,   100.64.0.0/10,   172.16.0.0/12,   192.168.0.0/16, 198.18.0.0/15,
198.19.0.0/16,   172.31.0.0/16,   54.239.224.0/20,   54.239.236.220/32,
127.0.0.2/32,   127.0.0.1/32,   169.254.169.123/32,   169.254.169.249/32,
169.254.169.250/32,   169.254.169.251/32,   169.254.169.253/32,
169.254.169.254/32:
```

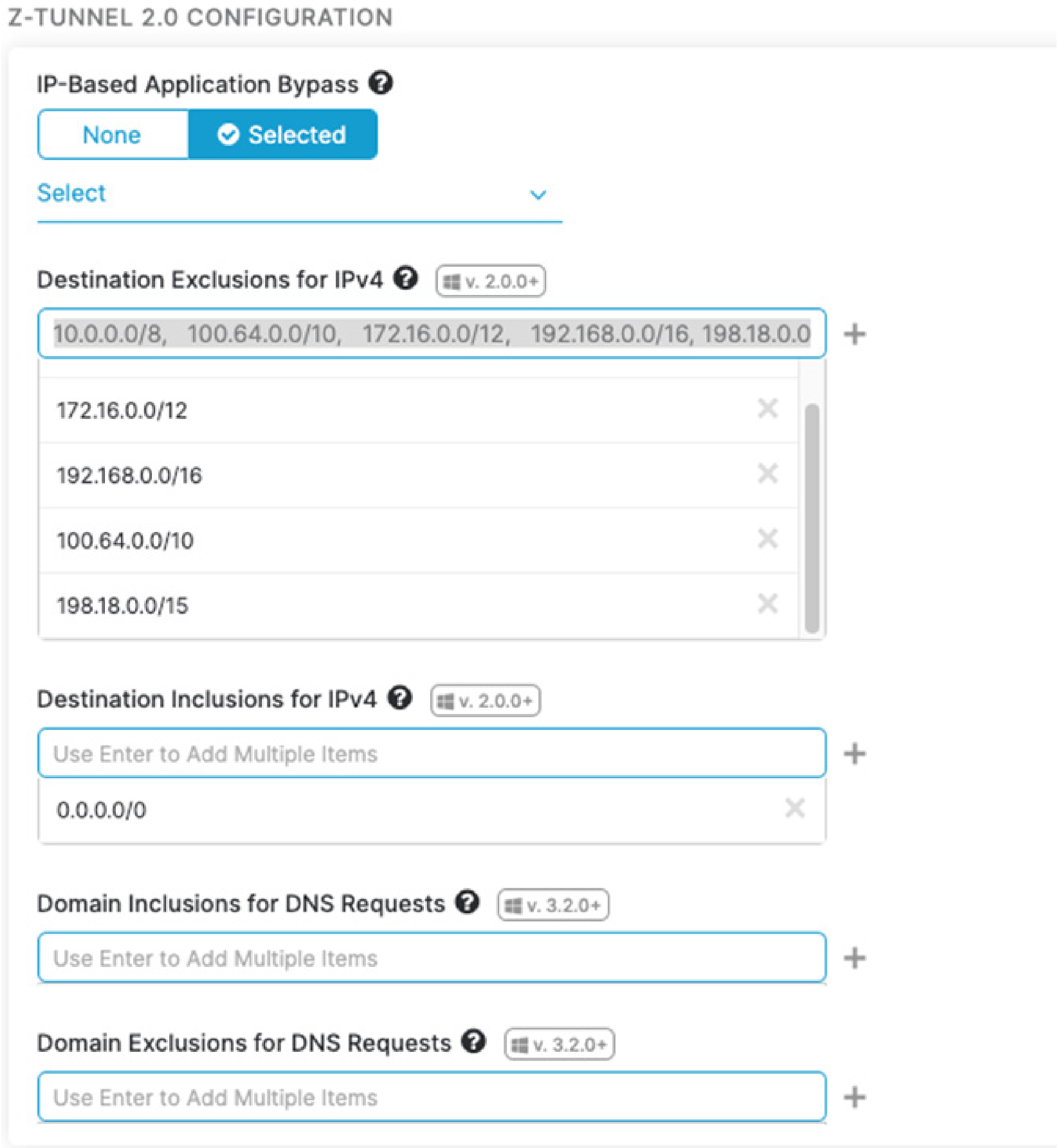
If you enter duplicate IP addresses, Zscaler Client Connect sends an error. Double check that the IP addresses you want to add aren't already listed in **Destination Exclusions for IPv4**.

Zscaler changes the Windows firewall profile (aka network category) for the first network interface (eth0) to a domain network that can cause connection failures to the WorkSpace, or the WorkSpace to report as unhealthy.

To prevent this, either explicitly add a new inbound rule to allow TCP port 8200-8250.

Example using PowerShell:

```
New-NetFirewallRule -DisplayName "Allow TCP Port 8200-8250" -Direction Inbound
-LocalPort 8200-8250 -Protocol TCP -Action Allow
```



Z-TUNNEL 2.0 CONFIGURATION

IP-Based Application Bypass

None | Selected

Select

Destination Exclusions for IPv4 v. 2.0.0+

10.0.0.0/8, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16, 198.18.0.0

172.16.0.0/12

192.168.0.0/16

100.64.0.0/10

198.18.0.0/15

Destination Inclusions for IPv4 v. 2.0.0+

Use Enter to Add Multiple Items

0.0.0.0/0

Domain Inclusions for DNS Requests v. 3.2.0+

Use Enter to Add Multiple Items

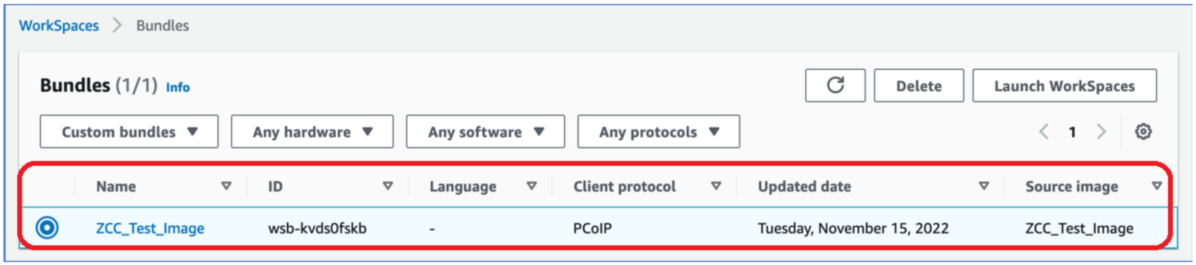
Domain Exclusions for DNS Requests v. 3.2.0+

Use Enter to Add Multiple Items

Figure 6. Edit Windows Policy

For detailed information on WorkSpaces IP/port requirements, refer to the Amazon documentation.

8. For deploying at scale, use a Windows image with IE Enhanced Security already disabled and Zscaler Client Connector installed (but no one logged in) to create an Image/Bundle for deploying WorkSpaces.

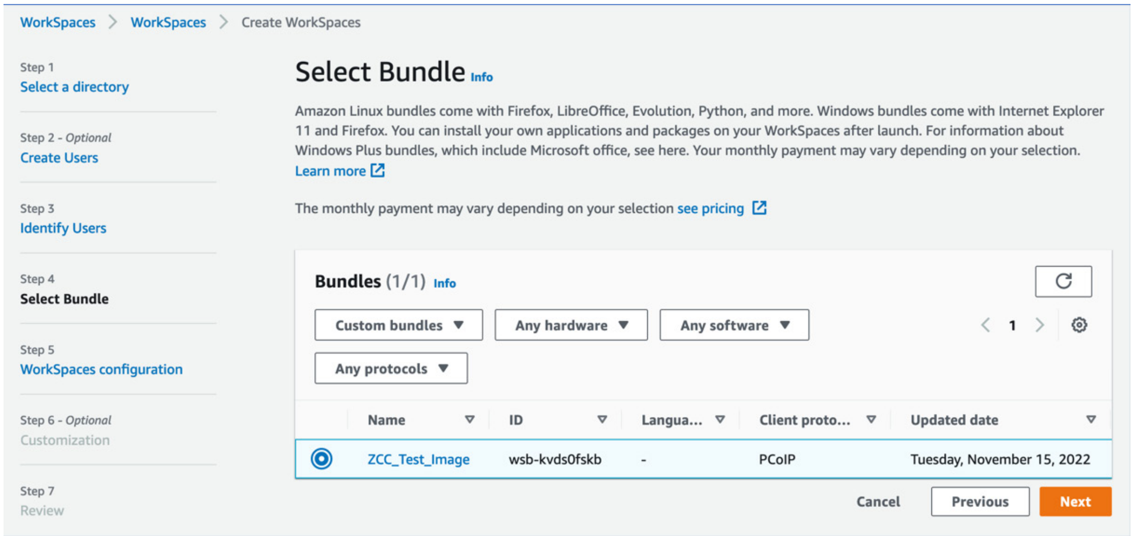


	Name	ID	Language	Client protocol	Updated date	Source image
●	ZCC_Test_Image	wsb-kvds0fskb	-	PCoIP	Tuesday, November 15, 2022	ZCC_Test_Image

Figure 7. Bundles

9. When creating a new workspace, select the custom bundle just created from the **Custom bundles** drop-down menu.

10. Select **Next**.



Amazon Linux bundles come with Firefox, LibreOffice, Evolution, Python, and more. Windows bundles come with Internet Explorer 11 and Firefox. You can install your own applications and packages on your WorkSpaces after launch. For information about Windows Plus bundles, which include Microsoft office, see here. Your monthly payment may vary depending on your selection. Learn more

The monthly payment may vary depending on your selection see pricing

	Name	ID	Langua...	Client proto...	Updated date
●	ZCC_Test_Image	wsb-kvds0fskb	-	PCoIP	Tuesday, November 15, 2022

Figure 8. Select Bundle

11. Upon logging into the new workspace, log in to Zscaler Client Connector.

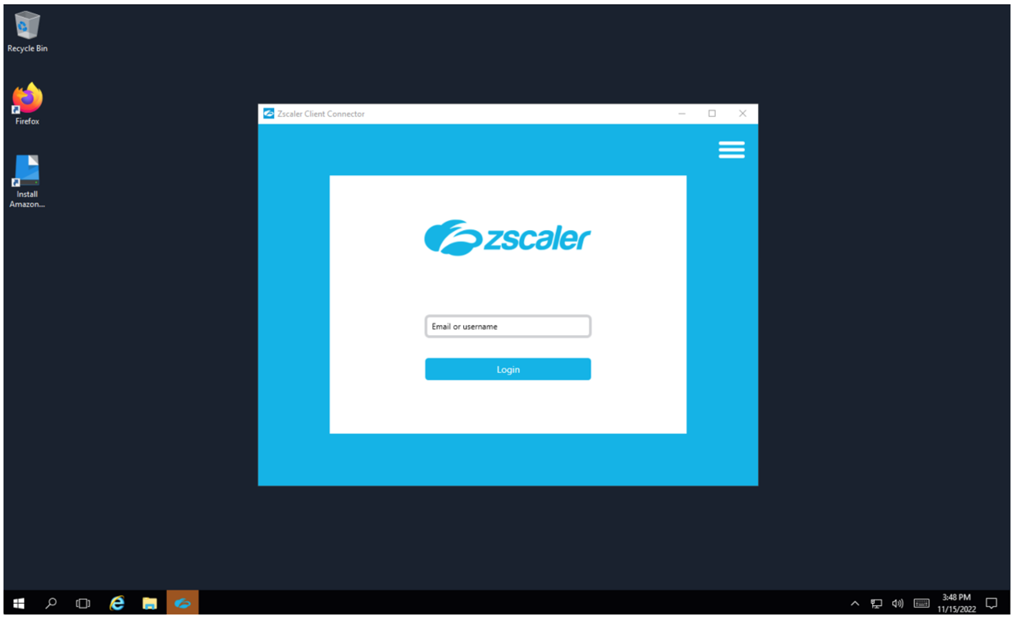


Figure 9. Zscaler Client Connector

PAC Files

You can configure any current browser to use a PAC file (government agencies, see PAC file) to forward traffic through a proxy such as ZIA. To uniquely identify WorkSpaces traffic for more granular policy control in ZIA, Zscaler recommends that you either use a custom PAC file (government agencies, see custom PAC file) with a Dedicated Proxy Port (government agencies, see Dedicated Proxy Port) and corresponding Location (government agencies, see Location), or define a location using the Elastic IP associated with WorkSpaces. You can then use this location as part of the criteria to make policy decisions for WorkSpaces web traffic.

You can find Information on configuring a browser to use a PAC File on the Zscaler Help Portal, including both default browsers Internet Explorer (government agencies, see Internet Explorer) and Firefox (government agencies, see Firefox) By default, Firefox on WorkSpaces is configured to use the same system proxy settings as IE. However, the two browsers handle installing a Certificate for SSL inspection differently: IE uses the system default certificate store, and Firefox uses its own certificate store (government agencies, see Firefox uses its own certificate store).

SSL inspection is an option, using the Zscaler Intermediate Certificate or a Custom Intermediate Root Certificate (government agencies, see Zscaler Intermediate Certificate or a Custom Intermediate Root Certificate). For information on installing the Zscaler certificate for IE, see Appendix A: Installing Zscaler Certificate on Windows. For information on disabling Internet Explorer Enhanced Security (to allow Zscaler to provide security), see Appendix B: Disabling IE Enhanced Security.

AWS Site-to-Site VPN

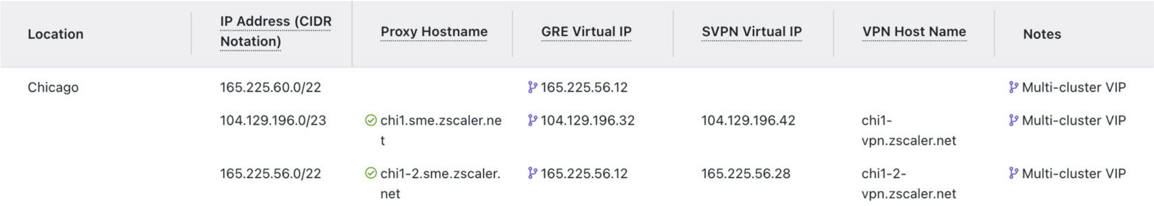
AWS can send traffic from a virtual private cloud (VPC) to a remote gateway via a Site-to-Site VPN Connection using IPSec tunnels. This feature routes all traffic from a VPC, such as a WorkSpaces VPC, to a ZIA Public Service Edge with the following caveats:

- An AWS Site-to-Site VPN provides redundant tunnels to the same destination. Zscaler recommends that redundant tunnels use two geographically disparate data centers for failover.
- An AWS Site-to-Site VPN does not support NULL encryption for Phase 2, which requires the Zscaler Encrypted VPN subscription option to allow encrypted IPSec tunnels.
- An AWS Site-to-Site VPN does not support the Zscaler recommended (government agencies, see Zscaler recommended) IPSec SA lifetime values.

An AWS site-to-site VPN Connection can use either a Virtual Private Gateway or a Transit Gateway. This document uses a Transit Gateway design, but the configuration for the Site-to-Site VPN Connection is the same. Refer to Appendix C: AWS Transit Gateway Lab Environment for a lab environment to use for testing.

Identifying the Zscaler VPN Endpoint

First, determine the VPN endpoint to be used in the Zscaler cloud by going to the Cloud Enforcement Node Ranges website (government agencies, see Cloud Enforcement Node Ranges website) and selecting your cloud at the top (e.g., zscaler.net). In the Current Data Centers list, locate the data center location closest to your AWS region and resolve the VPN Host Name to obtain the IP address to use when configuring the AWS VPN Customer Gateway.



Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	SVPN Virtual IP	VPN Host Name	Notes
Chicago	165.225.60.0/22		165.225.56.12			Multi-cluster VIP
	104.129.196.0/23	✓ chi1.sme.zscaler.net	104.129.196.32	104.129.196.42	chi1-vpn.zscaler.net	Multi-cluster VIP
	165.225.56.0/22	✓ chi1-2.sme.zscaler.net	165.225.56.12	165.225.56.28	chi1-2-vpn.zscaler.net	Multi-cluster VIP

Figure 10. Cloud Enforcement Node Ranges list

To resolve the hostname, use "nslookup" from the command line:

```
nslookup chi1-2-vpn.zscaler.net

Non-authoritative answer:

Name:    chi1-2-vpn.zscaler.net

Address: 165.225.56.14
```

Alternatively, you can use Method 2 as described on the SD-WAN Integrations Using API (government agencies, see SD-WAN Integrations Using API). Using your Elastic IP address, you can get an automated determination of the closest Zscaler Data Center location to the AWS region. Using the following URL (with your Zscaler cloud and AWS Elastic IP substituted for <Zscaler Cloud> and <Elastic IP>), the **primaryIP** value returned is the Zscaler VPN endpoint you are to use.

```
https://pac.<Zscaler Cloud>.net/getVpnEndpoints?srcIp=<Elastic IP>
```

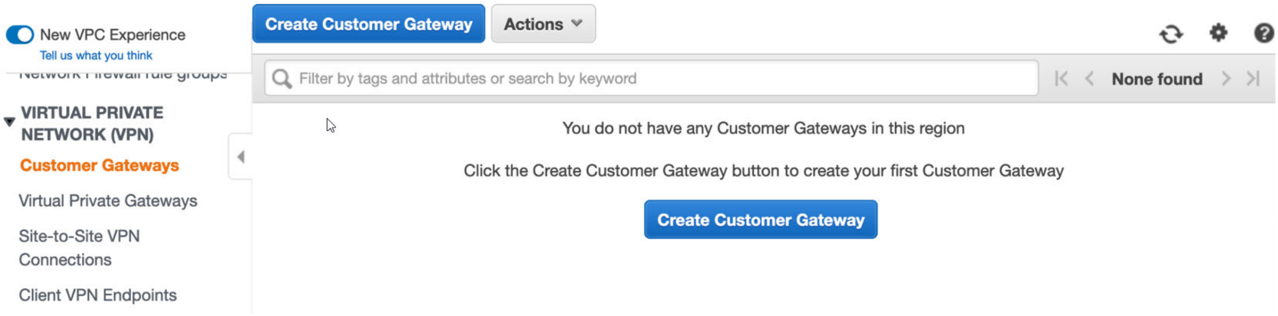
To fetch the endpoints, use `curl` from the command line:

```
curl https://pac.zscaler.net/getVpnEndpoints?srcIp=3.20.82.111
{
    "primaryIp": "165.225.56.14",
    "primaryMeta": {
          "region": "NorthAmerica",
          "country": "United States",
          "city": "Chicago",
          "dcName": "CHI1",
          "latitude": 41.000000,
          "longitude": -87.000000
    },
    "secondaryIp": "104.129.194.33",
    "secondaryMeta": {
          "region": "NorthAmerica",
          "country": "United States",
          "city": "Washington, DC",
          "dcName": "WAS1",
          "latitude": 39.000000,
          "longitude": -77.000000
    },
    "tertiaryIp": "165.225.208.18",
    "tertiaryMeta": {
          "region": "NorthAmerica",
          "country": "Canada",
          "city": "Toronto",
          "dcName": "YTO3",
          "latitude": 44.000000,
          "longitude": -79.000000
    }
}
```

Create a Customer Gateway

After logging into your AWS Management Console:

1. Select **VPC Service**.
2. On the **AWS portal VPC Service page**, select **Customer Gateways** under the **Virtual Private Network (VPN)** section.
3. Click **Create Customer Gateway**.

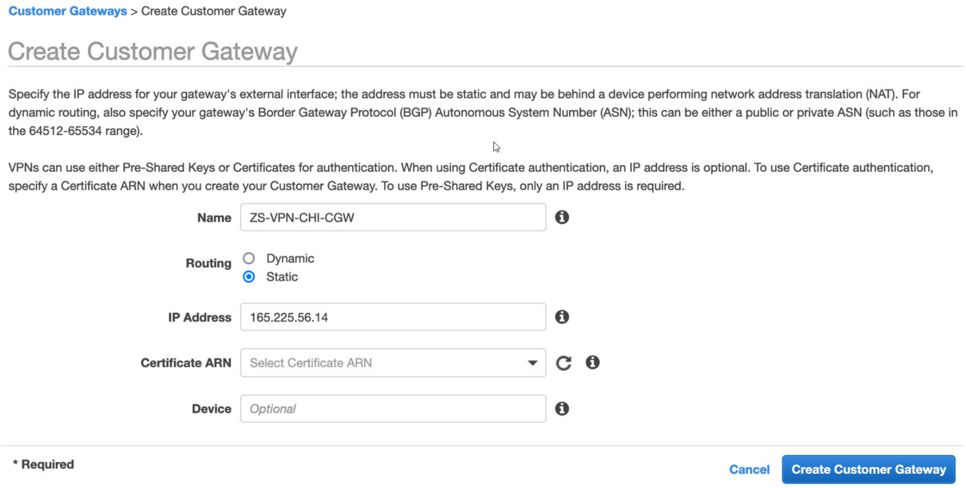


You do not have any Customer Gateways in this region

Click the Create Customer Gateway button to create your first Customer Gateway

Figure 11. AWS Create Customer Gateway

4. On the **Create Customer Gateway** window:
   a. Enter a name for your **Customer Gateway**.
   b. Select **Static** for **Routing**.
   c. Enter the **IP Address** for your closest Zscaler VPN endpoint (determined previously).
   d. Click **Create Customer Gateway**.



Create Customer Gateway

Specify the IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name	ZS-VPN-CHI-CGW
Routing	○ Dynamic ● Static
IP Address	165.225.56.14
Certificate ARN	Select Certificate ARN
Device	Optional

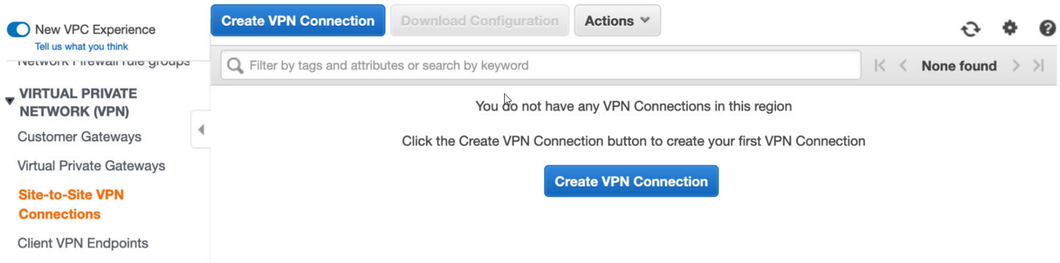
* Required

Figure 12. AWS Create Customer Gateway configuration

Create a Site-to-Site VPN Connection

On the VPC Service page:

1. Select **Site-to-Site VPN Connections** under the **Virtual Private Network (VPN)** section.
2. Click **Create VPN Connection**.

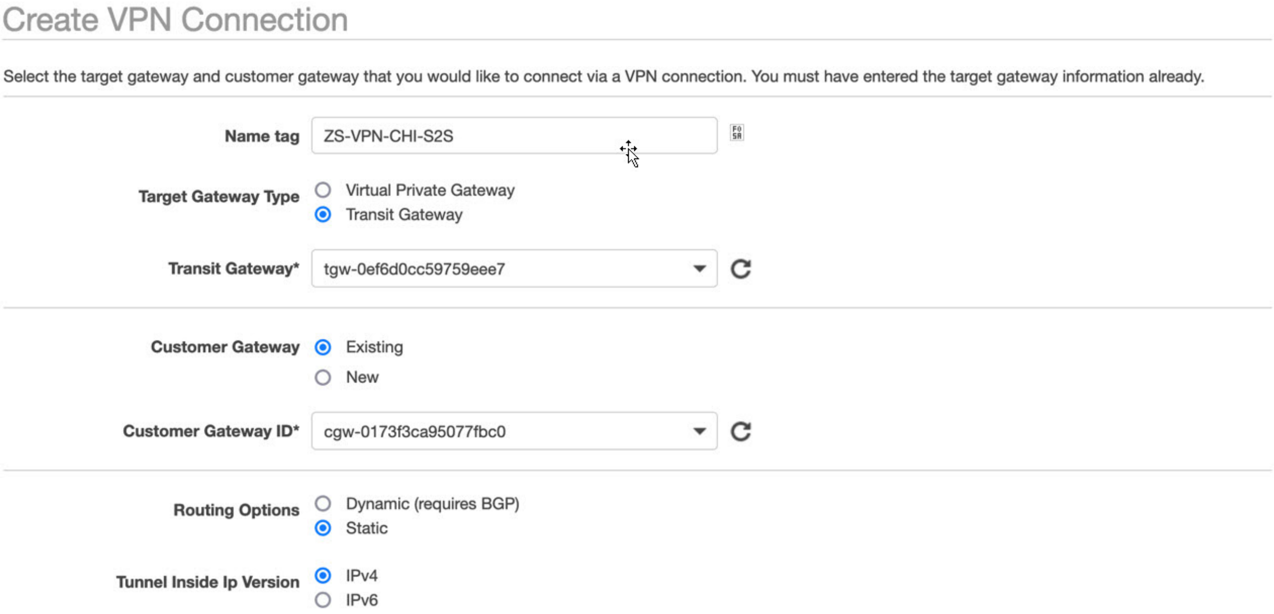


You do not have any VPN Connections in this region

Click the Create VPN Connection button to create your first VPN Connection

Figure 13. AWS Site-to-Site VPN Connections

3. On the **Create VPN Connection** window:
   a. Enter a **Name** tag for your VPN Connection.
   b. Select **Transit Gateway** for the **Target Gateway Type**.
   c. Select your **Transit Gateway** from the drop-down menu.
   d. Select the **Customer Gateway** you just created under **Customer Gateway ID**.
   e. Select **Static** for **Routing Options**.
   f. Select **IPv4** for the **Tunnel Inside Ip Version**.



Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the target gateway information already.

Name tag ZS-VPN-CHI-S2S

Target Gateway Type ○ Virtual Private Gateway ● Transit Gateway

Transit Gateway* tgw-0ef6d0cc59759eee7

Customer Gateway ● Existing ○ New

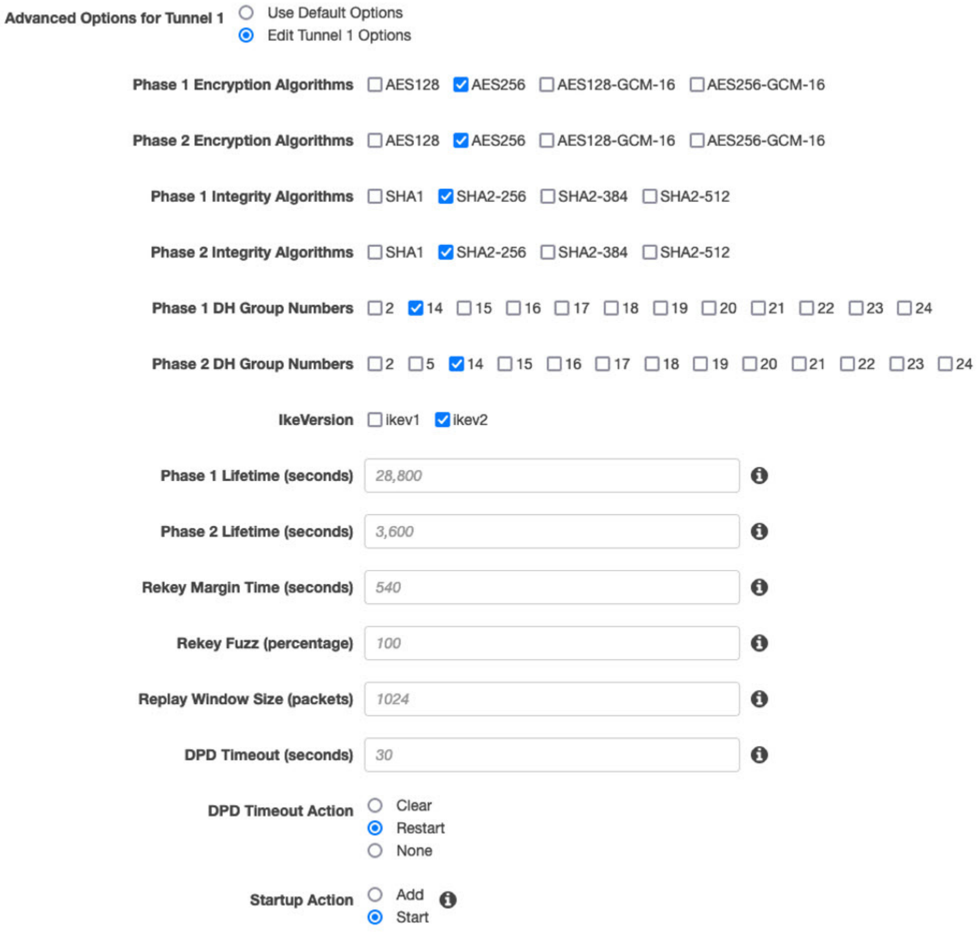
Customer Gateway ID* cgw-0173f3ca95077fbc0

Routing Options ○ Dynamic (requires BGP) ● Static

Tunnel Inside Ip Version ● IPv4 ○ IPv6

Figure 14. AWS Create VPN Connection configuration

4. Scroll to **Advanced Options for Tunnel 1**, select **Edit Tunnel 1 Options**, then set the following options to only these values:
   a. **Phase 1 Encryption Algorithms**: **AES256**
   b. **Phase 2 Encryption Algorithms**: **AES256**
   c. **Phase 1 Integrity Algorithms**: **SHA2-256**
   d. **Phase 2 Integrity Algorithms**: **SHA2-256**
   e. **Phase 1 DH Group Numbers**: **14**
   f. **Phase 2 DH Group Numbers**: **14**
   g. **IkeVersion**: **ikev2**
   h. **DPD Timeout Action**: **Restart**
   i. **Startup Action**: **Start**



Advanced Options for Tunnel 1 ○ Use Default Options ● Edit Tunnel 1 Options

Phase 1 Encryption Algorithms □ AES128 ☑ AES256 □ AES128-GCM-16 □ AES256-GCM-16

Phase 2 Encryption Algorithms □ AES128 ☑ AES256 □ AES128-GCM-16 □ AES256-GCM-16

Phase 1 Integrity Algorithms □ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 2 Integrity Algorithms □ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 1 DH Group Numbers □ 2 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

Phase 2 DH Group Numbers □ 2 □ 5 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

IkeVersion □ ikev1 ☑ ikev2

Phase 1 Lifetime (seconds) 28,800

Phase 2 Lifetime (seconds) 3,600

Rekey Margin Time (seconds) 540

Rekey Fuzz (percentage) 100

Replay Window Size (packets) 1024

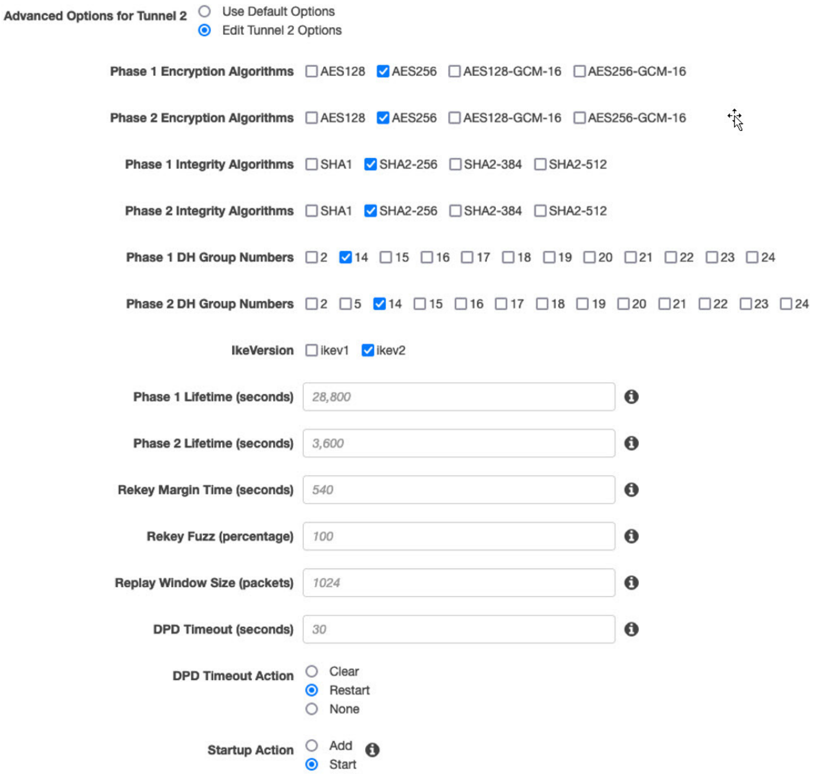
DPD Timeout (seconds) 30

DPD Timeout Action ○ Clear ● Restart ○ None

Startup Action ○ Add ● Start

Figure 15. AWS advanced tunnel options (Tunnel 1)

5. Scroll to **Advanced Options for Tunnel 2** and select **Edit Tunnel 2 Options**. Select the same options and values as Tunnel 1.



Advanced Options for Tunnel 2 ○ Use Default Options ● Edit Tunnel 2 Options

Phase 1 Encryption Algorithms □ AES128 ☑ AES256 □ AES128-GCM-16 □ AES256-GCM-16

Phase 2 Encryption Algorithms □ AES128 ☑ AES256 □ AES128-GCM-16 □ AES256-GCM-16

Phase 1 Integrity Algorithms □ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 2 Integrity Algorithms □ SHA1 ☑ SHA2-256 □ SHA2-384 □ SHA2-512

Phase 1 DH Group Numbers □ 2 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

Phase 2 DH Group Numbers □ 2 □ 5 ☑ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24

IkeVersion □ ikev1 ☑ ikev2

Phase 1 Lifetime (seconds) 28,800

Phase 2 Lifetime (seconds) 3,600

Rekey Margin Time (seconds) 540

Rekey Fuzz (percentage) 100

Replay Window Size (packets) 1024

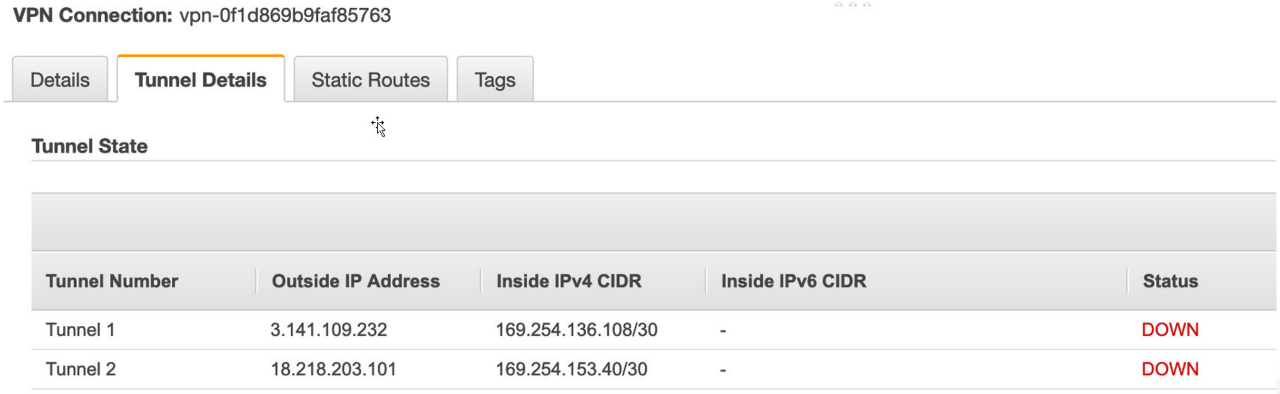
DPD Timeout (seconds) 30

DPD Timeout Action ○ Clear ● Restart ○ None

Startup Action ○ Add ● Start

Figure 16. AWS advanced tunnel options (Tunnel 2)

6. Click **Create VPN Connection**. This automatically creates a Transit Gateway Attachment. The **Name** tag is empty, but **Resource** type is VPN.
7. Name the attachment (e.g., `VPN-Attachment`) for ease of identification later.
8. Select your newly created VPN Connection.
9. Click the **Tunnel Details** tab to see the Elastic IPs assigned to the tunnels in the **Outside IP Address** column. Notice that the **Status** is currently **DOWN** because you still need to configure the Zscaler side.



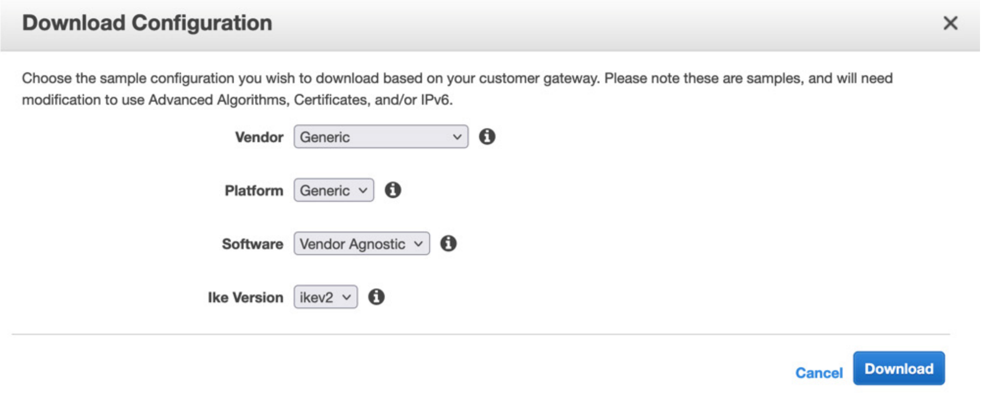
VPN Connection: vpn-0f1d869b9faf85763

Tunnel State

Tunnel Number	Outside IP Address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status
Tunnel 1	3.141.109.232	169.254.136.108/30	-	DOWN
Tunnel 2	18.218.203.101	169.254.153.40/30	-	DOWN

Figure 17. AWS Site-to-Site Connection Tunnel Details

10. Click **Download Configuration** at the top of the window.
11. Choose **Generic** for the **Vendor** and **ikev2** for the **Ike Version**.
12. Click **Download** to download the configuration.



Download Configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Generic

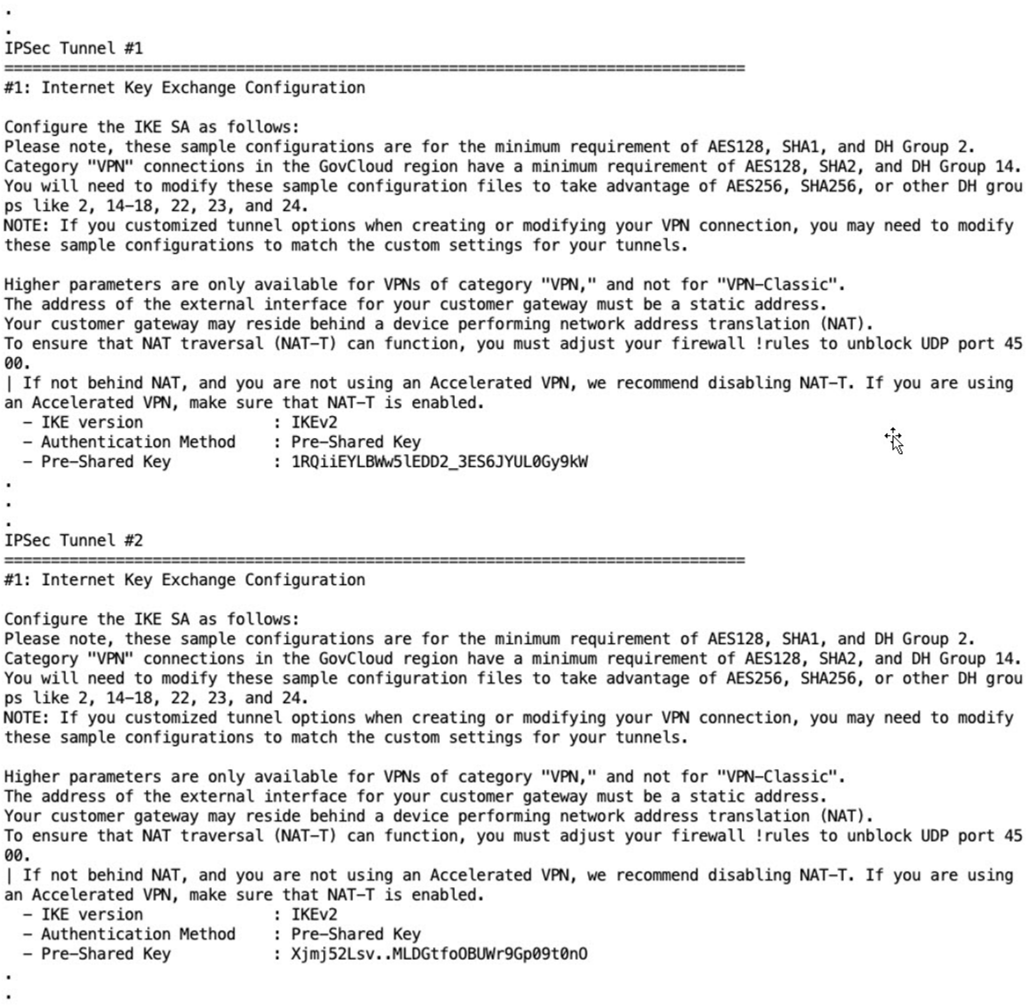
Platform: Generic

Software: Vendor Agnostic

Ike Version: ikev2

Figure 18. Downloaded configuration

13. Locate the **Pre-Shared Keys** for Tunnel 1 and Tunnel 2 in the downloaded file. The Elastic IPs for the tunnels and their corresponding Pre-Shared Keys are needed in the next section.



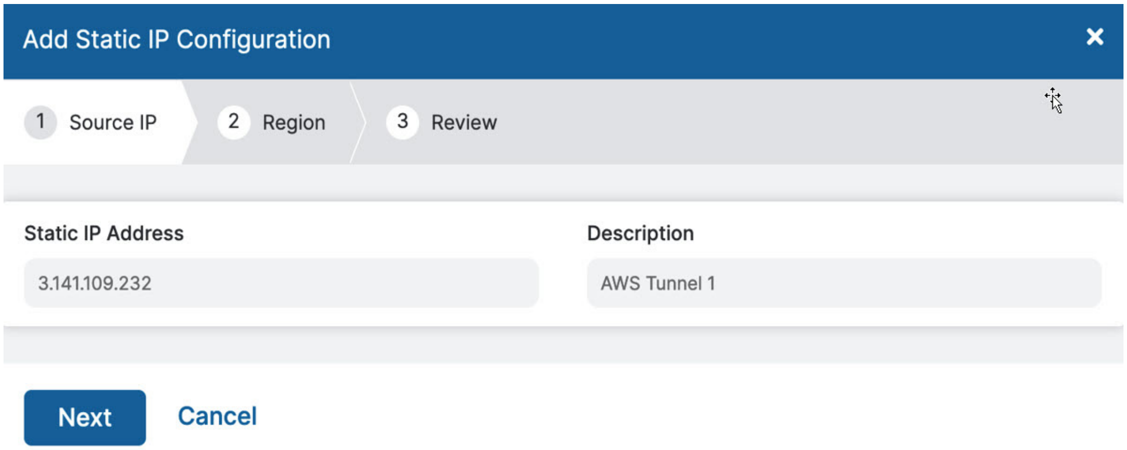
```
.
.
IPSec Tunnel #1
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH grou
ps like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify
these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 45
00.
| If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using
an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version              : IKEv2
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : 1RQiiEYLBWw5lEDD2_3ES6JYUL0Gy9kW
.
.
.
IPSec Tunnel #2
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH grou
ps like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify
these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 45
00.
| If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using
an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version              : IKEv2
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : Xjmj52Lsv..MLDGtfoOBUWr9Gp09t0nO
.
.
```

Figure 19. Downloaded tunnel configuration

Configure ZIA

In the ZIA Admin Portal:

1. Go to **Administration** > **Static IPs & GRE Tunnels**.
2. Select **Add Static IP**.
3. For **Static IP Address**, enter the **Outside IP Address** for Tunnel 1.
4. Provide a description.
5. Click **Next**.

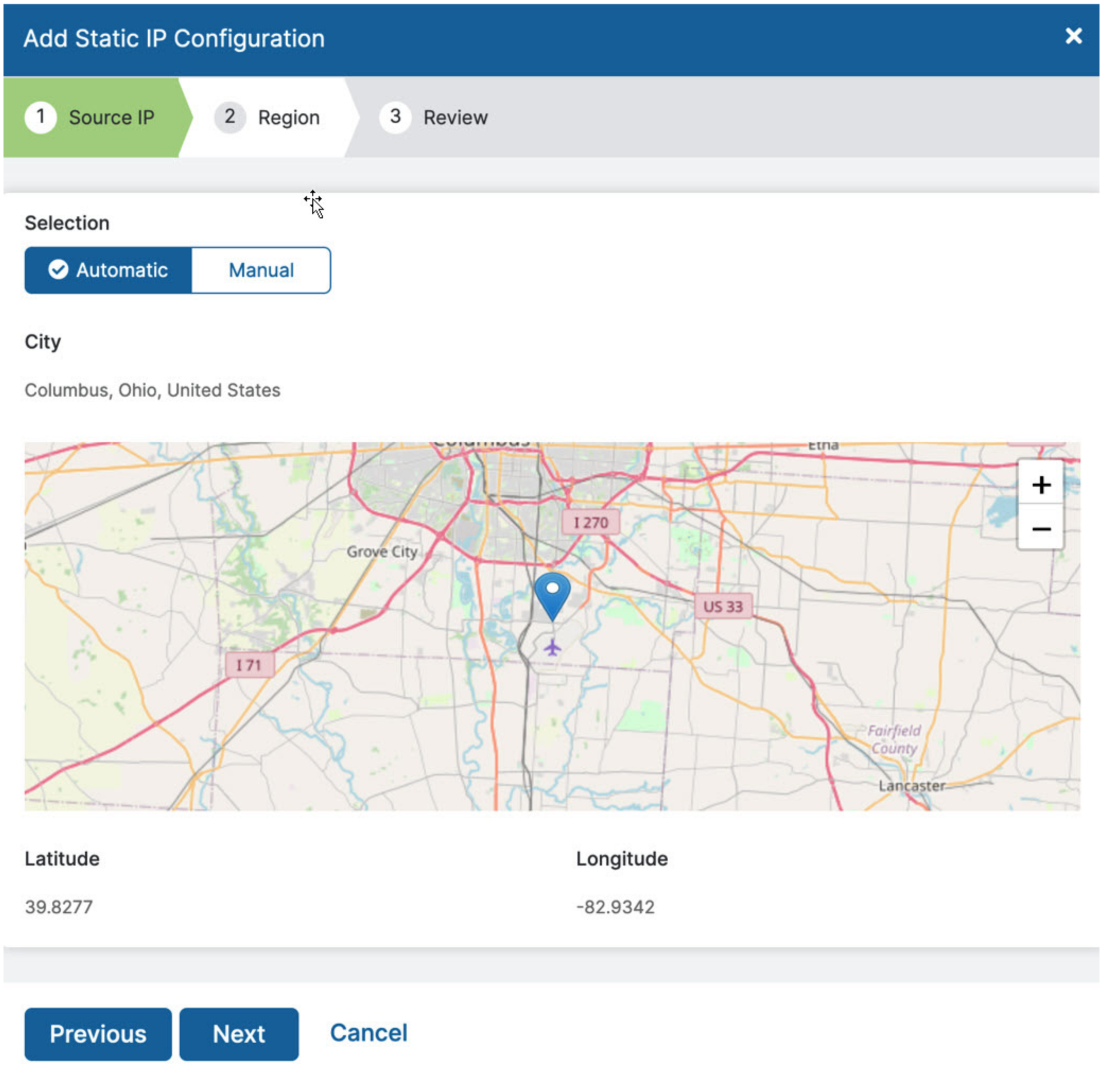


Static IP Address: 3.141.109.232

Description: AWS Tunnel 1

Figure 20. Add Static IP Configuration page

6. Verify that the geographic location makes sense based on your AWS region.
7. Click **Next** and then **Save**. If the geographic location is not accurate, you can manually set it by **City** or **Latitude and Longitude**.
8. Repeat these configuration steps for the Tunnel 2 IP.



Add Static IP Configuration

Selection

City

Columbus, Ohio, United States

Latitude

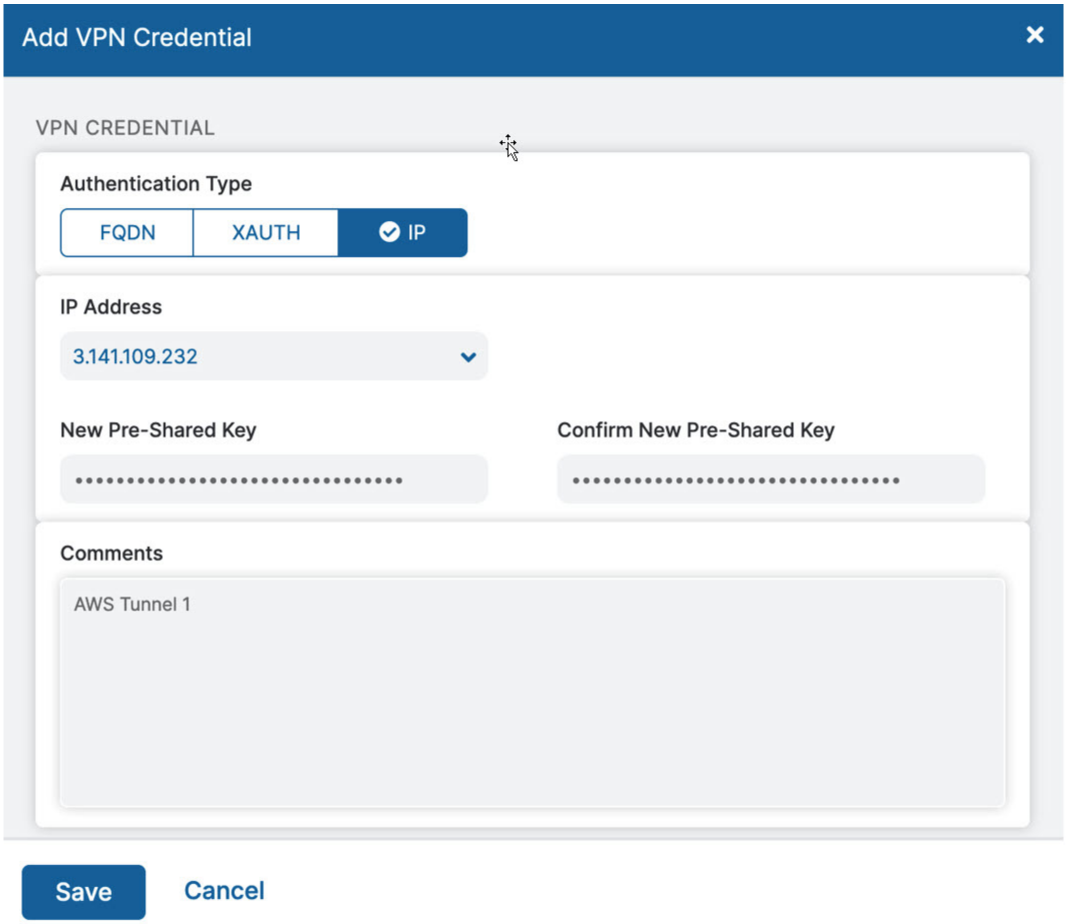
39.8277

Longitude

-82.9342

Figure 21. Static IP location

9. Go to **Administration** > **VPN Credentials** > **Add VPN Credentials**.
10. For **Authentication Type**, select **IP**.
11. Select your AWS Tunnel 1 IP address from the drop-down menu. Paste the associated Pre-Shared Key in the **New Pre-Shared Key** and **Confirm New Pre-Shared Key** fields.
12. Add a comment, then click **Save**.
13. Repeat these steps for Tunnel 2 IP and associated Pre-Shared Key.



Authentication Type: ✓ IP

IP Address: 3.141.109.232

New Pre-Shared Key: ••••••••••••••••••••••••••••••••

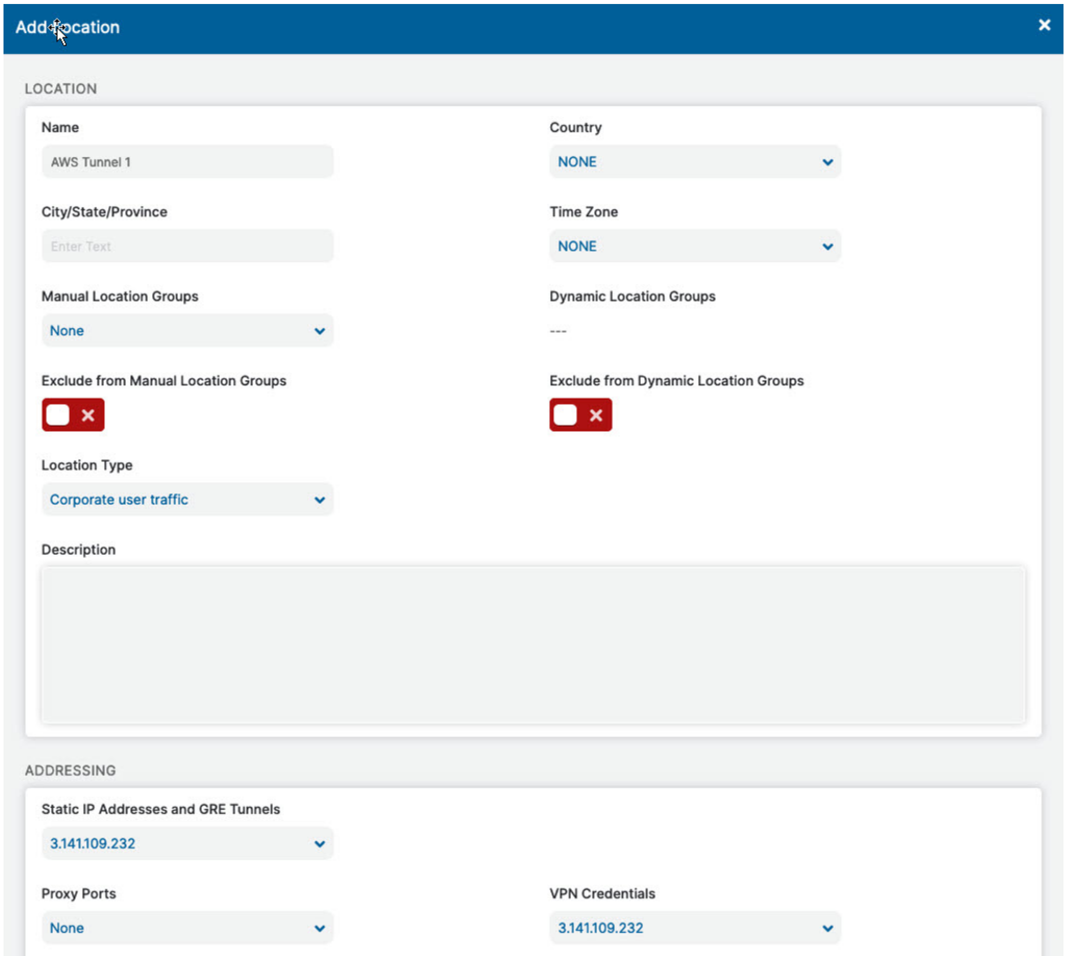
Confirm New Pre-Shared Key: ••••••••••••••••••••••••••••••••

Comments: AWS Tunnel 1

Figure 22. Add VPN Credentials

14. Go to **Administration** > **Location Management** > **Add Location**.
15. Enter a **Name** for the location.
16. Select a **Location Type** (required).
17. Select the Tunnel 1 IP address under both the **Static IP Addresses and GRE Tunnels** and the **VPN Credentials** drop-down menus.
18. Click **Save**.
19. Repeat these steps for the Tunnel 2 IP and then **Activate** the changes.

    Zscaler does not respond to tunnel initiation requests from AWS until the location configuration is activated.



Add Location

LOCATION

Name: AWS Tunnel 1

Country: NONE

City/State/Province: Enter Text

Time Zone: NONE

Manual Location Groups: None

Dynamic Location Groups: ---

Exclude from Manual Location Groups: ☒

Exclude from Dynamic Location Groups: ☒

Location Type: Corporate user traffic

Description

ADDRESSING

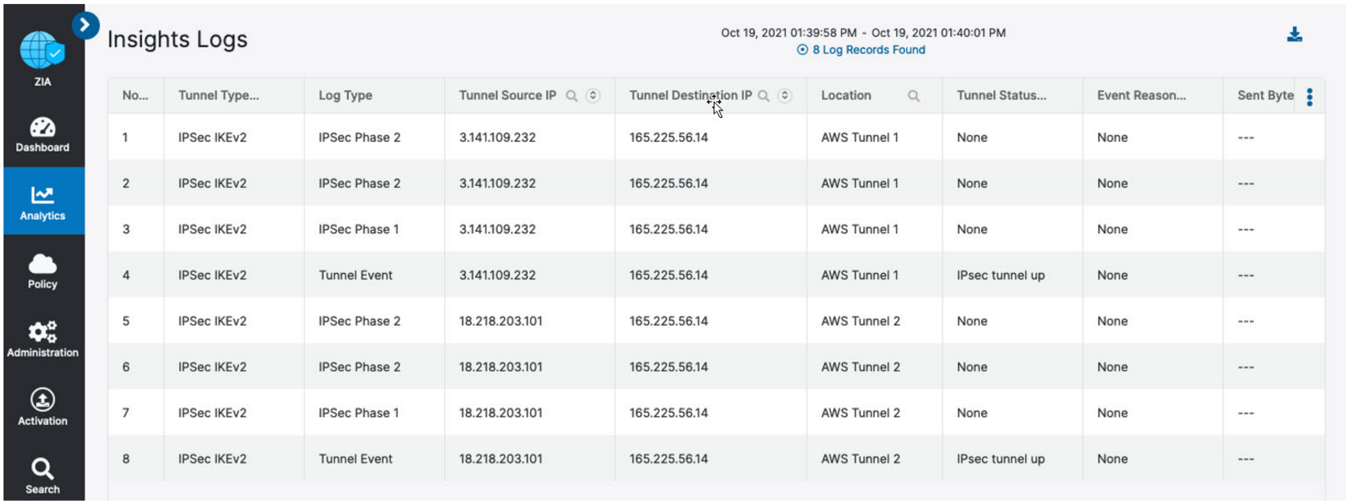
Static IP Addresses and GRE Tunnels: 3.141.109.232

Proxy Ports: None

VPN Credentials: 3.141.109.232

Figure 23. Add location configuration page

20. To verify that the tunnels are established, go to **Analytics** > **Tunnel Insights**.
21. Select **Logs**, and click **Apply Filters**. After a short time (you might need to refresh your view) both tunnels appear (**IPSec tunnel up**) in the **Tunnel Status** column.
22. If needed, add a filter for the AWS tunnel locations to limit the number of logs returned.



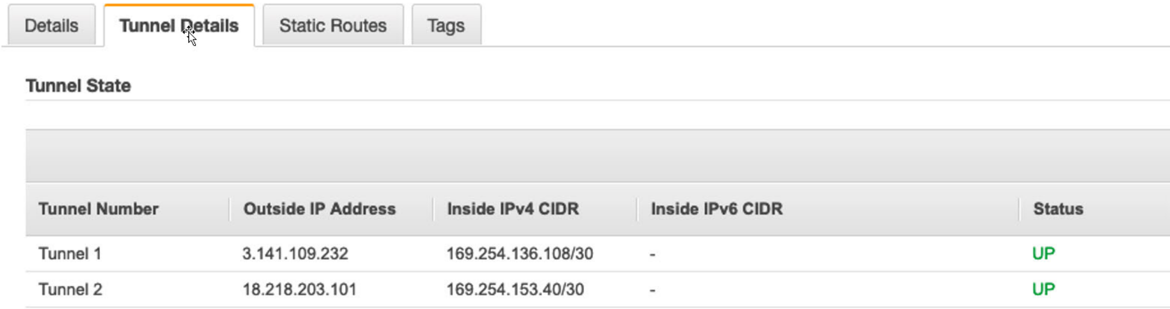
Insights Logs

Oct 19, 2021 01:39:58 PM - Oct 19, 2021 01:40:01 PM
8 Log Records Found

No...	Tunnel Type...	Log Type	Tunnel Source IP	Tunnel Destination IP	Location	Tunnel Status...	Event Reason...	Sent Byte
1	IPSec IKEv2	IPSec Phase 2	3.141.109.232	165.225.56.14	AWS Tunnel 1	None	None	---
2	IPSec IKEv2	IPSec Phase 2	3.141.109.232	165.225.56.14	AWS Tunnel 1	None	None	---
3	IPSec IKEv2	IPSec Phase 1	3.141.109.232	165.225.56.14	AWS Tunnel 1	None	None	---
4	IPSec IKEv2	Tunnel Event	3.141.109.232	165.225.56.14	AWS Tunnel 1	IPsec tunnel up	None	---
5	IPSec IKEv2	IPSec Phase 2	18.218.203.101	165.225.56.14	AWS Tunnel 2	None	None	---
6	IPSec IKEv2	IPSec Phase 2	18.218.203.101	165.225.56.14	AWS Tunnel 2	None	None	---
7	IPSec IKEv2	IPSec Phase 1	18.218.203.101	165.225.56.14	AWS Tunnel 2	None	None	---
8	IPSec IKEv2	Tunnel Event	18.218.203.101	165.225.56.14	AWS Tunnel 2	IPsec tunnel up	None	---

Figure 24. Tunnel Insights Logs page

23. In the AWS Management Console, in the **Site-to-Site VPN Connection** section and on the **Tunnel Details** tab for your VPN Connection, ensure that the **Status** is **UP**.



Tunnel State

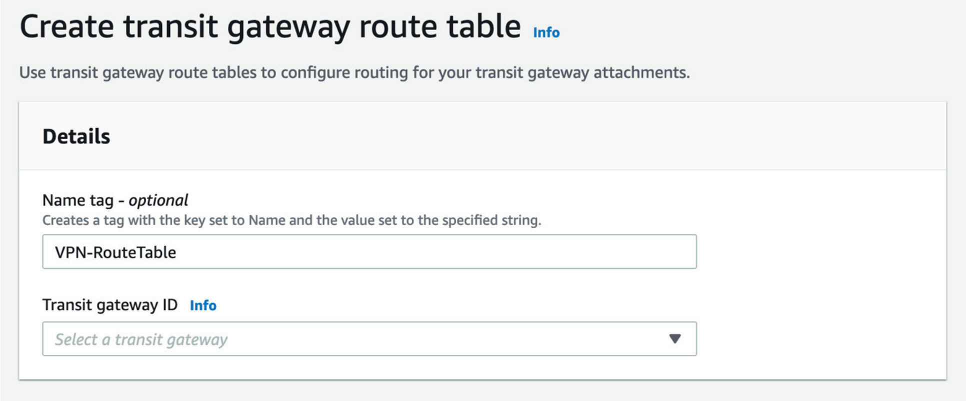
Tunnel Number	Outside IP Address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status
Tunnel 1	3.141.109.232	169.254.136.108/30	-	UP
Tunnel 2	18.218.203.101	169.254.153.40/30	-	UP

Figure 25. AWS Site-to-Site Connection Tunnels Details

Configure Routing for Site-to-Site VPN Connection

You now must route traffic to and from the active tunnels for your VPCs before traffic is sent to ZIA.

1. In the AWS Management Console **VPC Service** page under **Transit Gateway Route Tables**, click **Create transit gateway route table**.
2. Create a Transit Gateway route table for the VPN connection with an appropriate **Name**.
3. Select the **Transit gateway ID** from the drop-down menu, and click **Create transit gateway route table**.



Create transit gateway route table

Use transit gateway route tables to configure routing for your transit gateway attachments.

Details

Name tag - *optional*

Creates a tag with the key set to Name and the value set to the specified string.

VPN-RouteTable

Transit gateway ID

Select a transit gateway

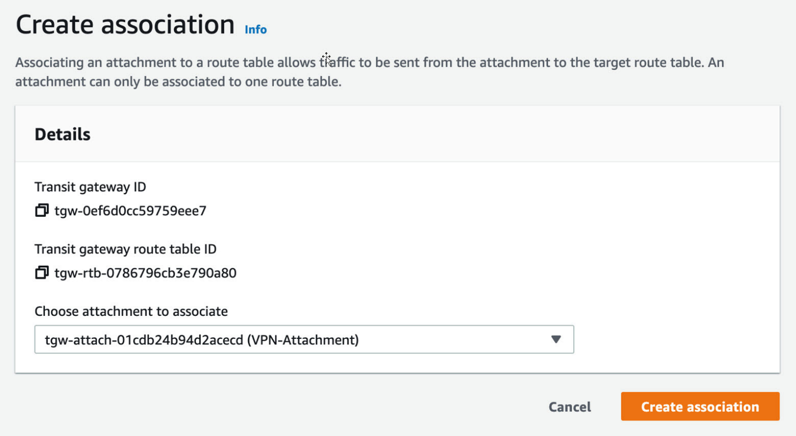
Figure 26. AWS Create transit gateway route table

The Transit gateway ID drop-down menu might be broken. In that case, you can use the AWS CLI to create a Transit Gateway Route Table for the Transit Gateway ID:

```
aws ec2 create-transit-gateway-route-table --region us-east-2 --transit-gateway-
id <Your Transit gateway ID> --tag-specifications "ResourceType=transit-gateway-
route-table,Tags=[{Key=Name,Value=VPN-RouteTable}]"
```

4. When the state of the newly-created VPN Transit Gateway Route Table is **Available**, select the table and select the **Associations** tab.
5. Click **Create association**.
6. Select your VPN attachment from the drop-down menu under **Choose attachment to associate**.
7. Click **Create association**.

If you named the attachment earlier, look for that name.



Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Details

Transit gateway ID

tgw-0ef6d0cc59759eee7

Transit gateway route table ID

tgw-rtb-0786796cb3e790a80

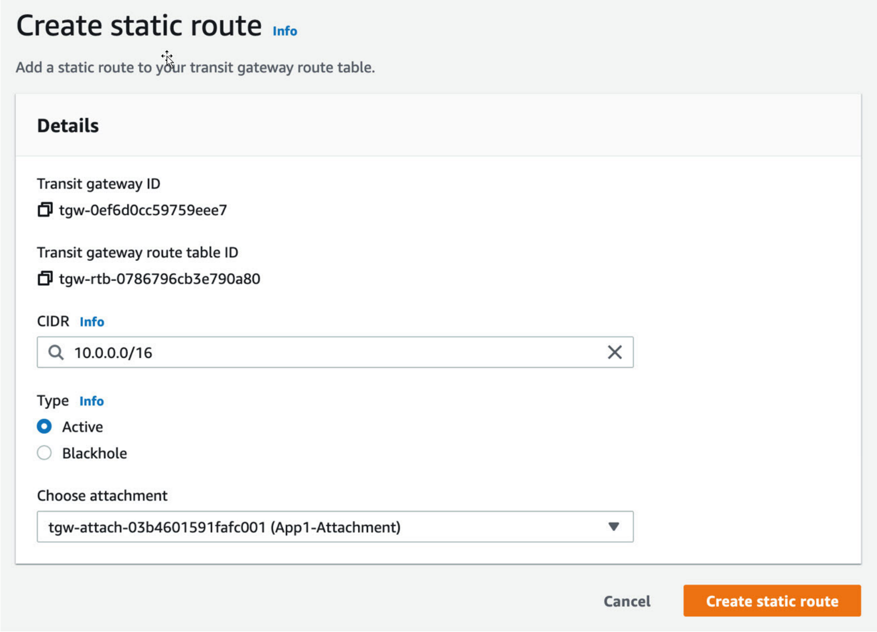
Choose attachment to associate

tgw-attach-01cdb24b94d2acecd (VPN-Attachment)

Figure 27. AWS Create association page

8. Click the **Routes** tab.
9. Add a static route for the VPC subnet Classless Inter-Domain Routing (CIDR) range you want to send through the VPN tunnels to ZIA. Choose the appropriate Transit Gateway attachment for that VPC subnet from the **Choose attachment** drop-down menu.
10. Click **Create static route**.
11. Repeat these steps for any other VPCs that send their traffic through the VPN tunnels to ZIA. The association allows the traffic returning from the VPN tunnels to flow back to the subnet that initiated the traffic via the associated attachment.

    As an example, if you are using the lab environment from Appendix C: AWS Transit Gateway Lab Environment, add the following routes for the App1 and App2 VPCs.



Create static route Info

Add a static route to your transit gateway route table.

Details

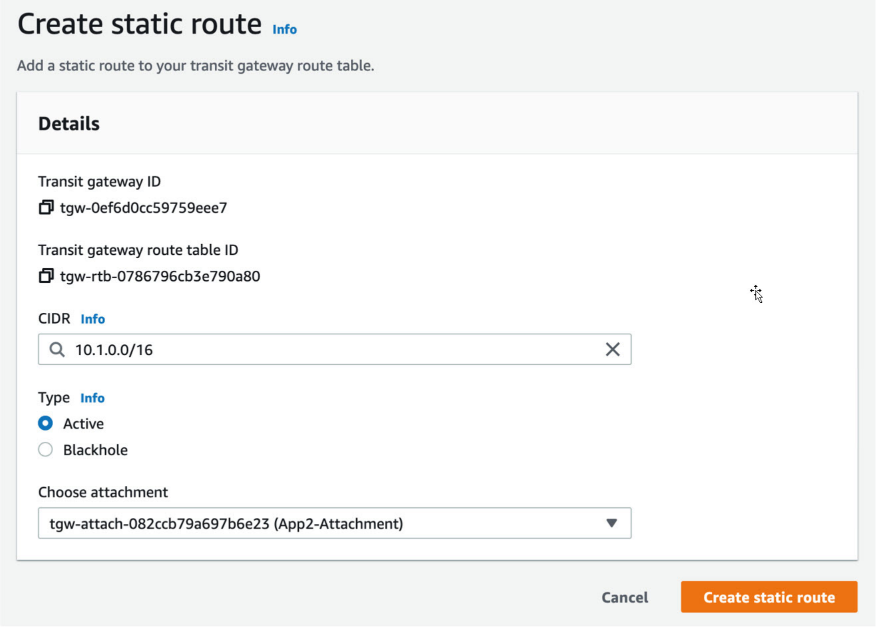
Transit gateway ID
tgw-0ef6d0cc59759eee7

Transit gateway route table ID
tgw-rtb-0786796cb3e790a80

CIDR Info
10.0.0.0/16

Type Info
● Active
○ Blackhole

Choose attachment
tgw-attach-03b4601591fafc001 (App1-Attachment)



Create static route Info

Add a static route to your transit gateway route table.

Details

Transit gateway ID
tgw-0ef6d0cc59759eee7

Transit gateway route table ID
tgw-rtb-0786796cb3e790a80

CIDR Info
10.1.0.0/16

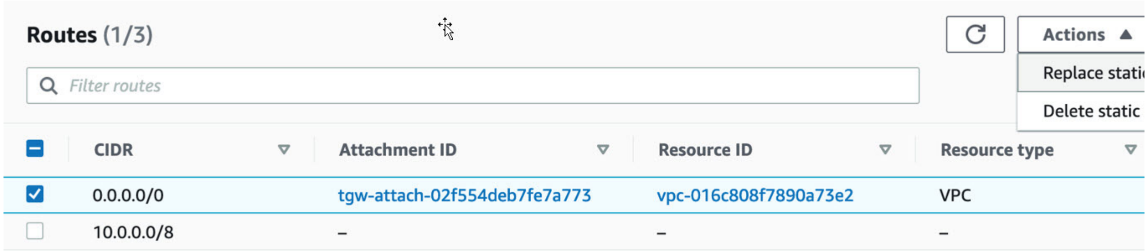
Type Info
● Active
○ Blackhole

Choose attachment
tgw-attach-082ccb79a697b6e23 (App2-Attachment)

Figure 28. AWS Create static route details

12. Change your App VPC route table's default route to point to the VPN Attachment instead of the Egress VPC.

    As an example, if you are using the lab environment from Appendix C: AWS Transit Gateway Lab Environment, replace the following default route attachment to point to the VPN attachment.

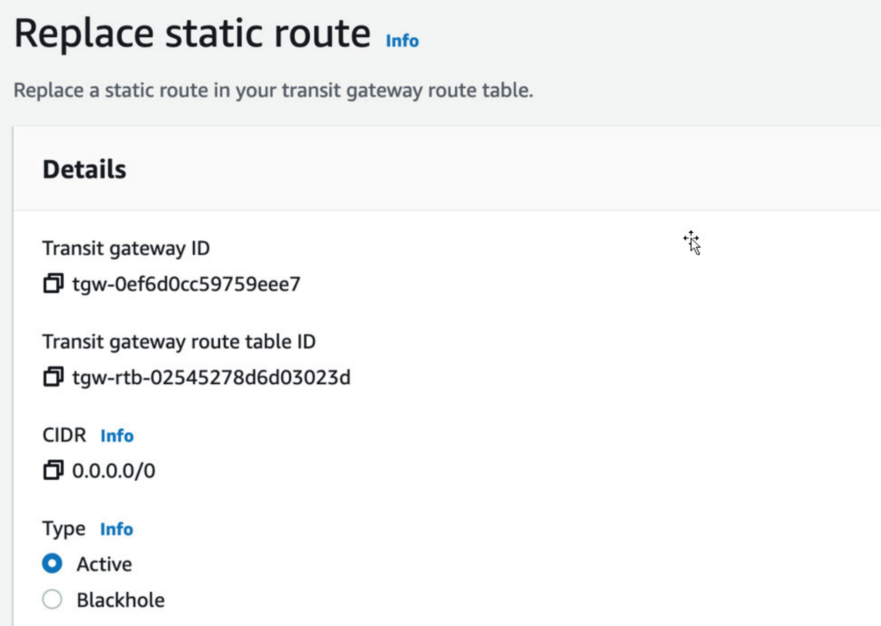


Routes (1/3)

▬	CIDR	Attachment ID	Resource ID	Resource type
☑	0.0.0.0/0	tgw-attach-02f554deb7fe7a773	vpc-016c808f7890a73e2	VPC
□	10.0.0.0/8	–	–	–

Figure 29. Static routes

The following image shows the static route replacement.



Replace static route Info

Replace a static route in your transit gateway route table.

Details

Transit gateway ID
tgw-0ef6d0cc59759eee7

Transit gateway route table ID
tgw-rtb-02545278d6d03023d

CIDR Info
0.0.0.0/0

Type Info
● Active
○ Blackhole

Figure 30. AWS Replace static route details

13. Test the route from an EC2 instance in the App VPC, through the Site-to-Site VPN Connection, to ZIA.

If you are using the lab environment from Appendix B: Disabling IE Enhanced Security, you must add a route for 192.168.0.0/16 in your App VPC route table pointing to the Egress-Attachment. This route allows traffic back to the Bastion host before you can connect to the App EC2 instances from the Bastion host (otherwise, the default route sends it through the VPN tunnels).

Example testing

Use the following quick test to determine if the source IP can be done using `curl` and the JSON output from ip.zscaler.com.

The following example shows testing from EC2 instance in App VPC with the default route pointing to the Egress attachment. The `clientip` shown is egress Elastic IP:

```
curl http://ip.zscaler.com?json

{"srcip":"3.20.82.111","clientip":"3.20.82.111"}
```

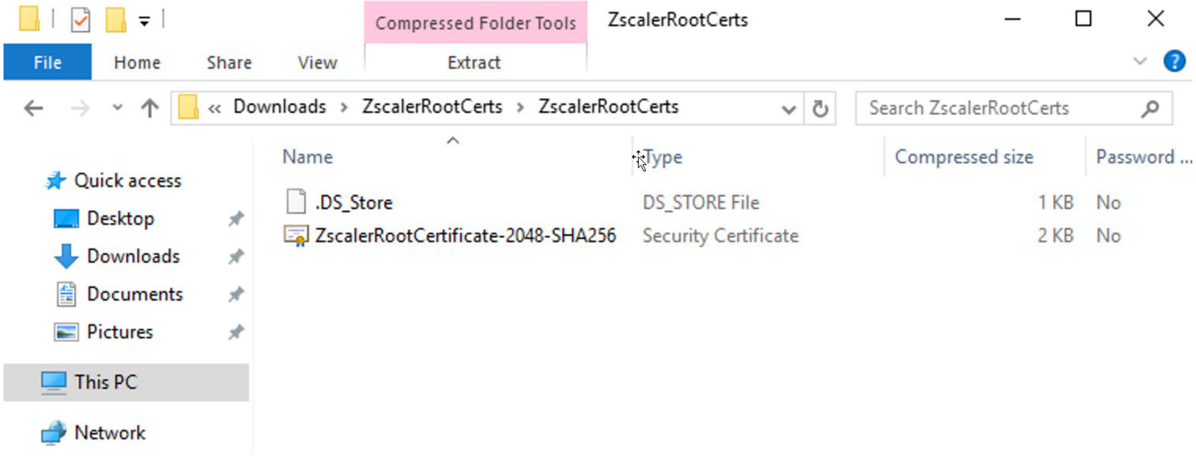
The following example shows testing from the EC2 instance in App VPC with the default route pointing to the VPN attachment. The `clientip` is Tunnel 1 Outside IP address:

```
curl http://ip.zscaler.com?json

{"srcip":"165.225.58.247","vip":"165.225.56.19",
"nodename":"zsn-chi1-4e1 sme","cloud":"zscaler.
net","datacenter":"Chicago","xff":"3.141.109.232","clientip":"3.141.109.232"}
```

Appendix A: Installing Zscaler Certificate on Windows

To install the Zscaler Certificate on Windows:

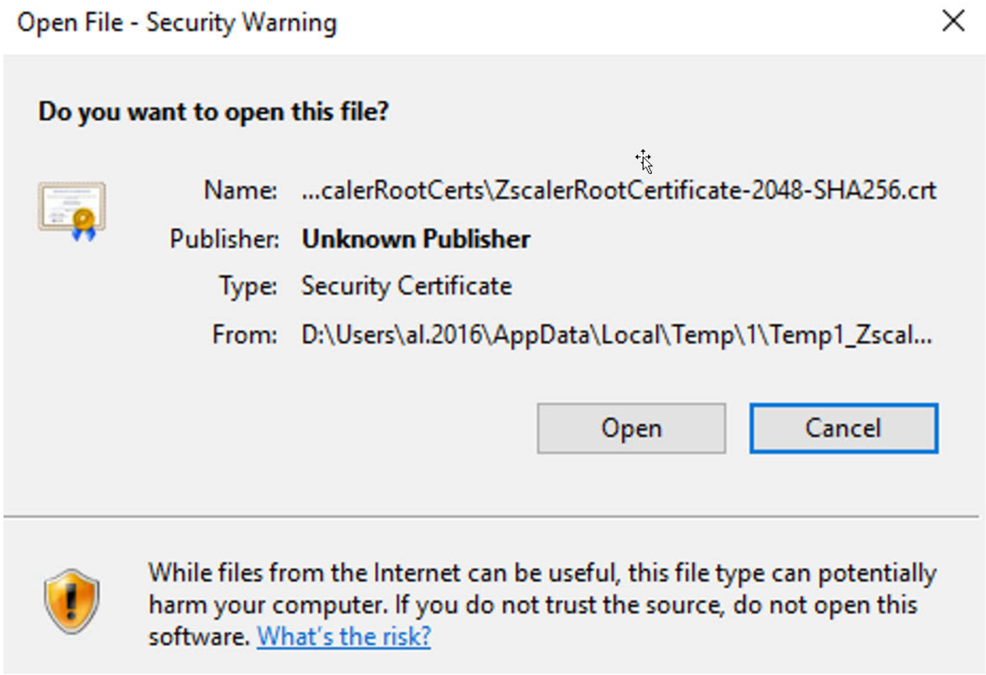
1. Download the Zscaler Intermediate Root Certificate (government agencies, see Zscaler Intermediate Root Certificate) to the Windows system. Use File Explorer to navigate to the certificate.



Name	Type	Compressed size	Password ...
.DS_Store	DS_STORE File	1 KB	No
ZscalerRootCertificate-2048-SHA256	Security Certificate	2 KB	No

Figure 31. Root Certificate in File Explorer

2. Double-click the certificate file.
3. Click **Open**.



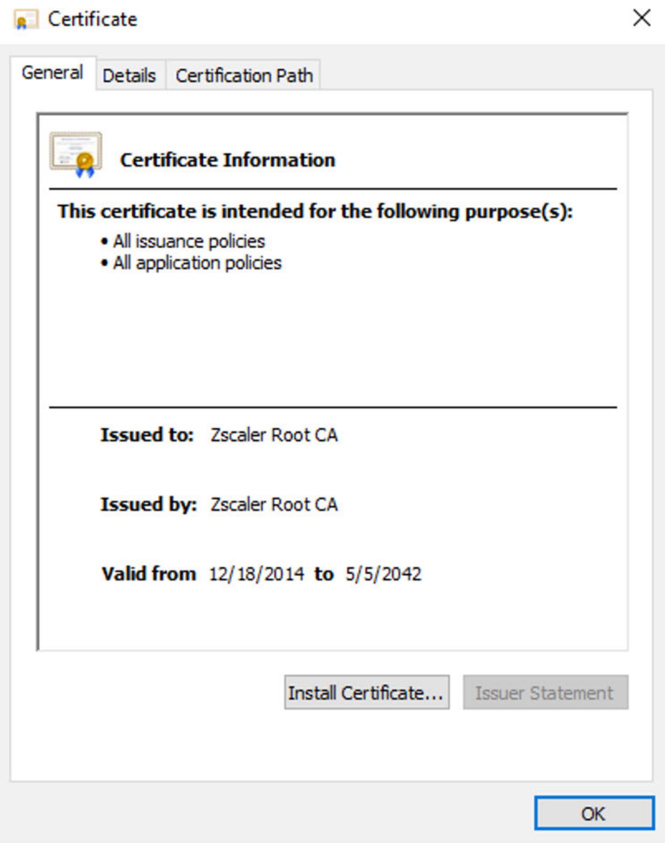
Do you want to open this file?

Name: ...calerRootCerts\ZscalerRootCertificate-2048-SHA256.crt
Publisher: **Unknown Publisher**
Type: Security Certificate
From: D:\Users\al.2016\AppData\Local\Temp\1\Temp1_Zscal...

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Figure 32. Windows File Warning

4. Click **Install Certificate** on the **Certificate** window.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

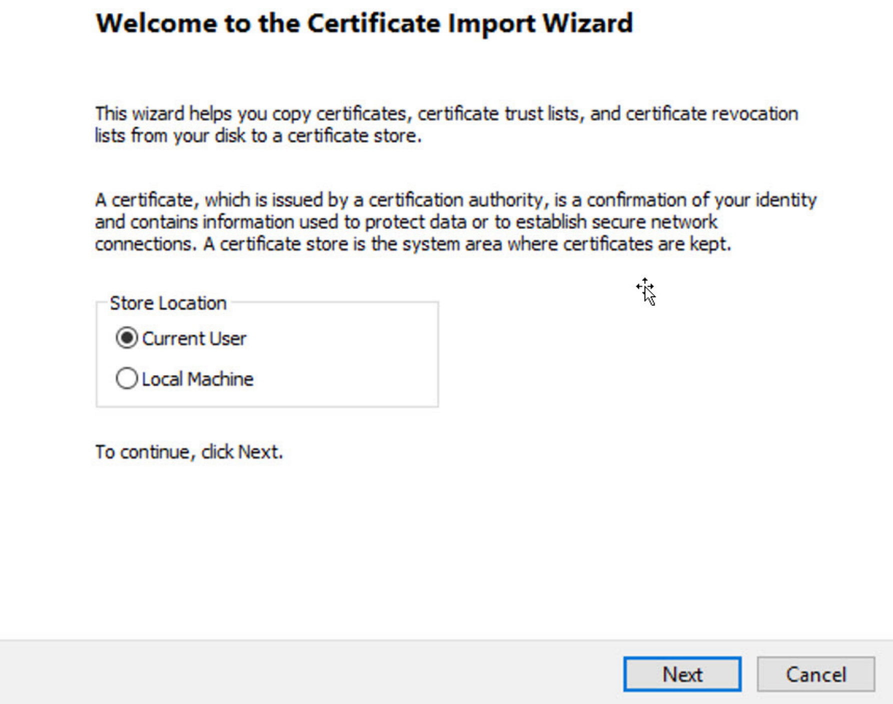
Issued to: Zscaler Root CA

Issued by: Zscaler Root CA

Valid from 12/18/2014 to 5/5/2042

Figure 33. Windows Certificate install dialog

5. Select **Current User** as the **Store Location** in the **Import Wizard**.
6. Click **Next**.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

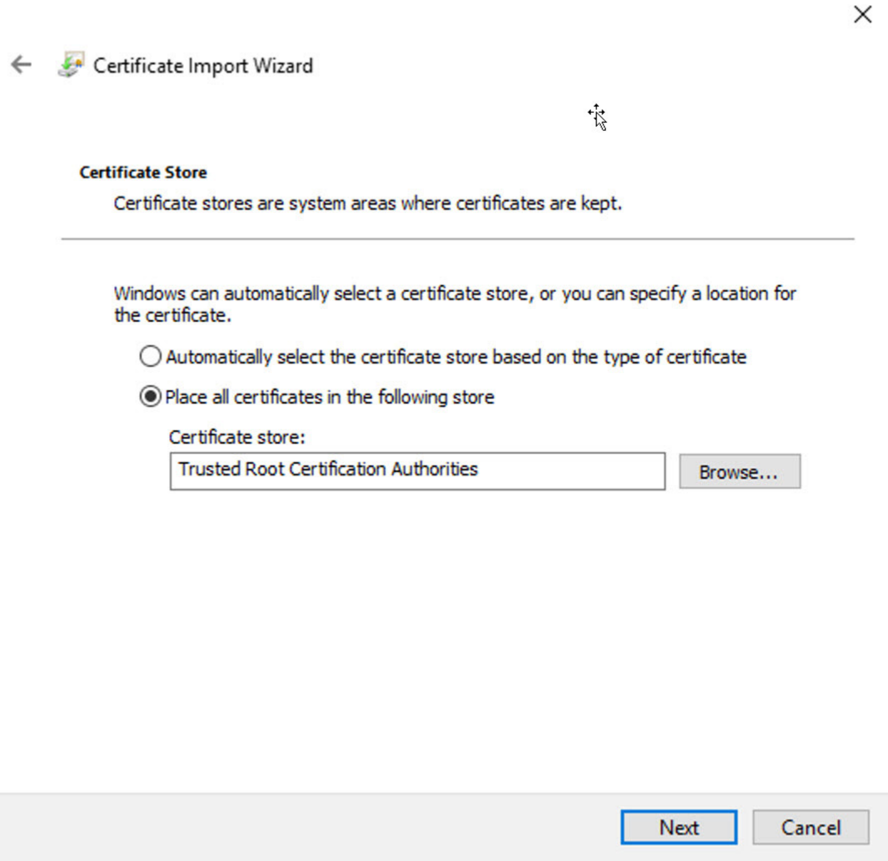
● Current User

○ Local Machine

To continue, click Next.

Figure 34. Windows certificate store location install dialog

7. Select **Place all certificates in the following store** and click **Browse**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

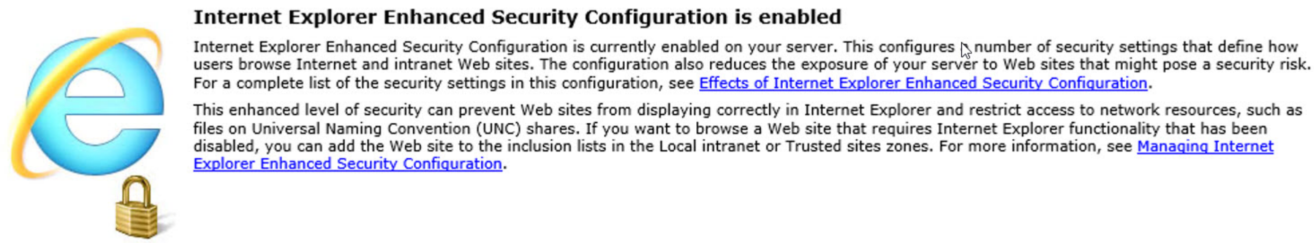
Trusted Root Certification Authorities

Figure 35. Windows certificate install finish

8. Select **Trusted Root Certification Authorities** for the **Certificate Store**.
9. Click **Next** and then click **Finish**.

Appendix B: Disabling IE Enhanced Security

By default, IE (in the WorkSpaces Windows Server OS) enables Enhanced Security Configuration, and the following message appears when IE is first started (or within Zscaler Client Connector during authentication).



Internet Explorer Enhanced Security Configuration is enabled

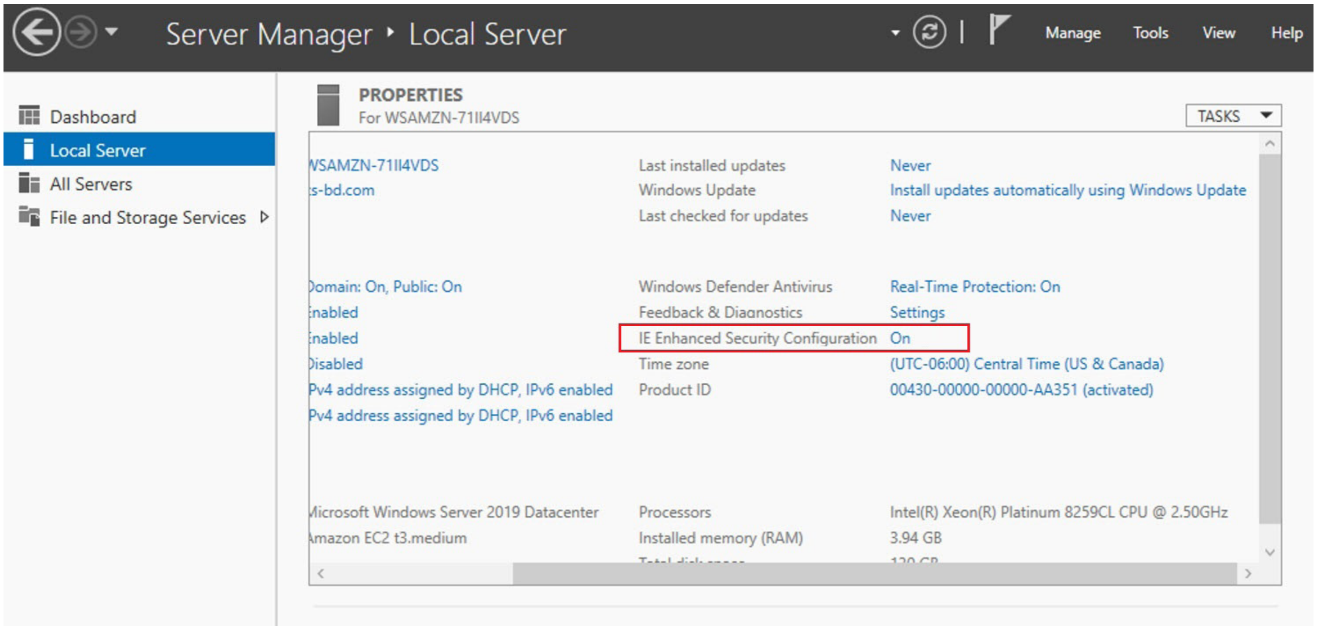
Internet Explorer Enhanced Security Configuration is currently enabled on your server. This configures number of security settings that define how users browse Internet and intranet Web sites. The configuration also reduces the exposure of your server to Web sites that might pose a security risk. For a complete list of the security settings in this configuration, see Effects of Internet Explorer Enhanced Security Configuration.

This enhanced level of security can prevent Web sites from displaying correctly in Internet Explorer and restrict access to network resources, such as files on Universal Naming Convention (UNC) shares. If you want to browse a Web site that requires Internet Explorer functionality that has been disabled, you can add the Web site to the inclusion lists in the Local intranet or Trusted sites zones. For more information, see Managing Internet Explorer Enhanced Security Configuration.

Figure 36. IE Enhanced Security Message

To disable the Enhanced Security Configuration and allow ZIA to provide protection instead:

1. Start **Server Manager** and select **Local Server**.
2. For the **IE Enhanced Security Configuration** option, click **On** to change the setting.

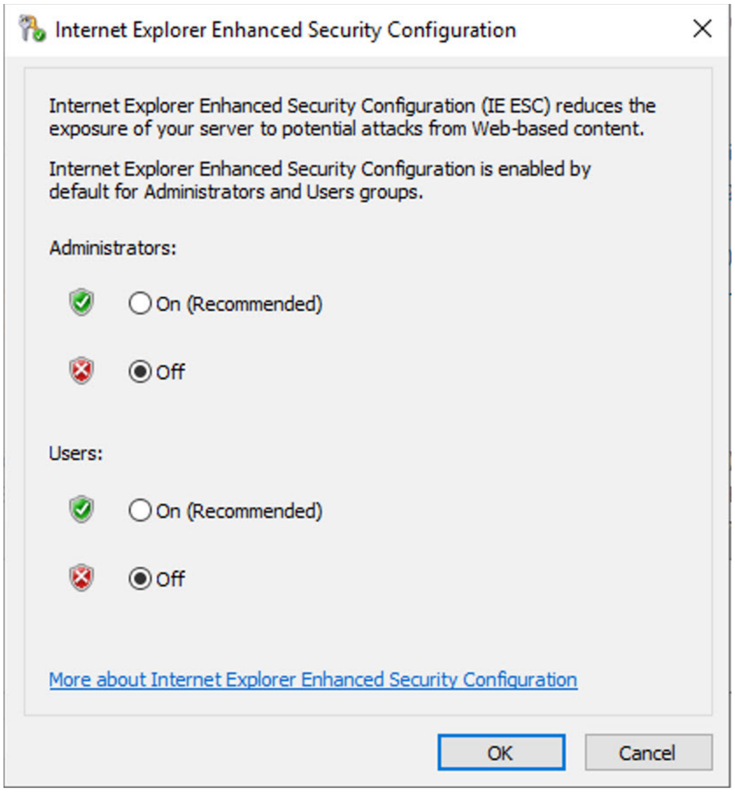


WSAMZN-71II4VDS
s-bd.com
Domain: On, Public: On
Enabled
Enabled
Disabled
Pv4 address assigned by DHCP, IPv6 enabled
Pv4 address assigned by DHCP, IPv6 enabled
Microsoft Windows Server 2019 Datacenter
Amazon EC2 t3.medium

Last installed updates	Never
Windows Update	Install updates automatically using Windows Update
Last checked for updates	Never
Windows Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC-06:00) Central Time (US & Canada)
Product ID	00430-00000-00000-AA351 (activated)
Processors	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz
Installed memory (RAM)	3.94 GB

Figure 37. Server Manager local server configuration, enhanced security On

3. Turn both settings **Off** and click **OK**.



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

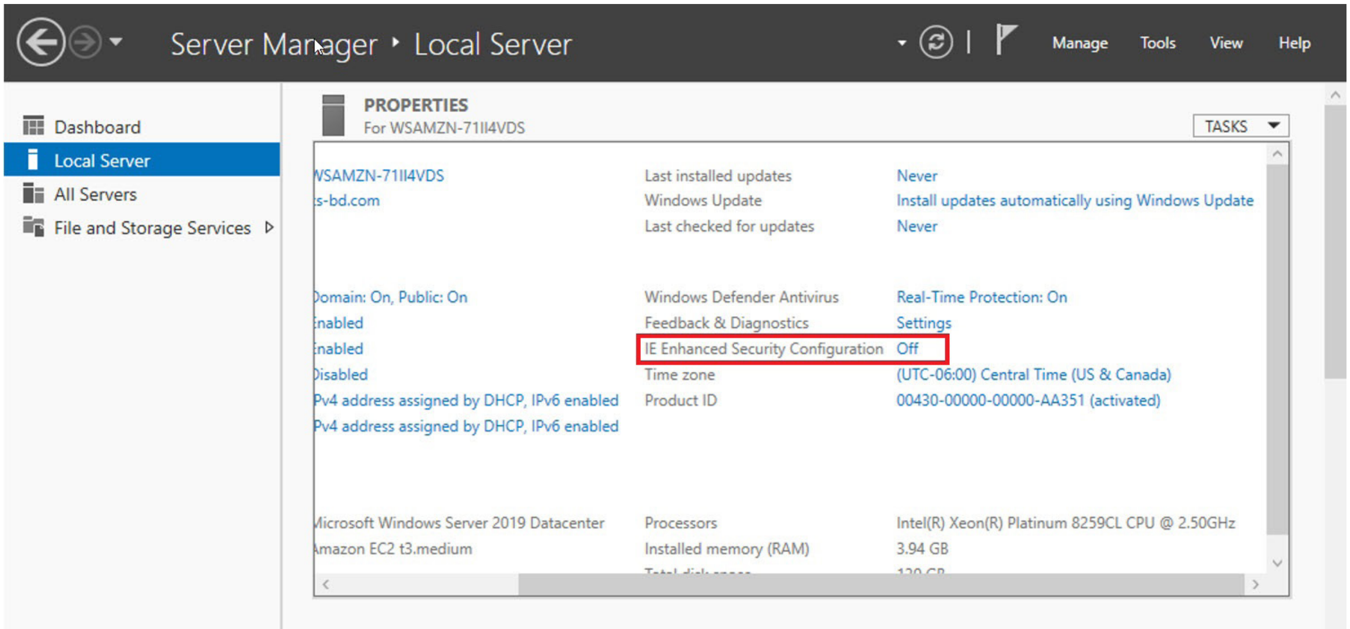
○ On (Recommended)

● Off

More about Internet Explorer Enhanced Security Configuration

Figure 38. IE Enhanced Security Configuration

The new setting for **IE Enhanced Security Configuration** option shows as **Off** (you might have to refresh the page).



PROPERTIES
For WSAMZN-71II4VDS

VSAMZN-71II4VDS	Last installed updates	Never
s-bd.com	Windows Update	Install updates automatically using Windows Update
	Last checked for updates	Never
Domain: On, Public: On	Windows Defender Antivirus	Real-Time Protection: On
nabled	Feedback & Diagnostics	Settings
nabled	IE Enhanced Security Configuration	Off
Disabled	Time zone	(UTC-06:00) Central Time (US & Canada)
Pv4 address assigned by DHCP, IPv6 enabled	Product ID	00430-00000-00000-AA351 (activated)
Pv4 address assigned by DHCP, IPv6 enabled		
Microsoft Windows Server 2019 Datacenter	Processors	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz
Amazon EC2 t3.medium	Installed memory (RAM)	3.94 GB

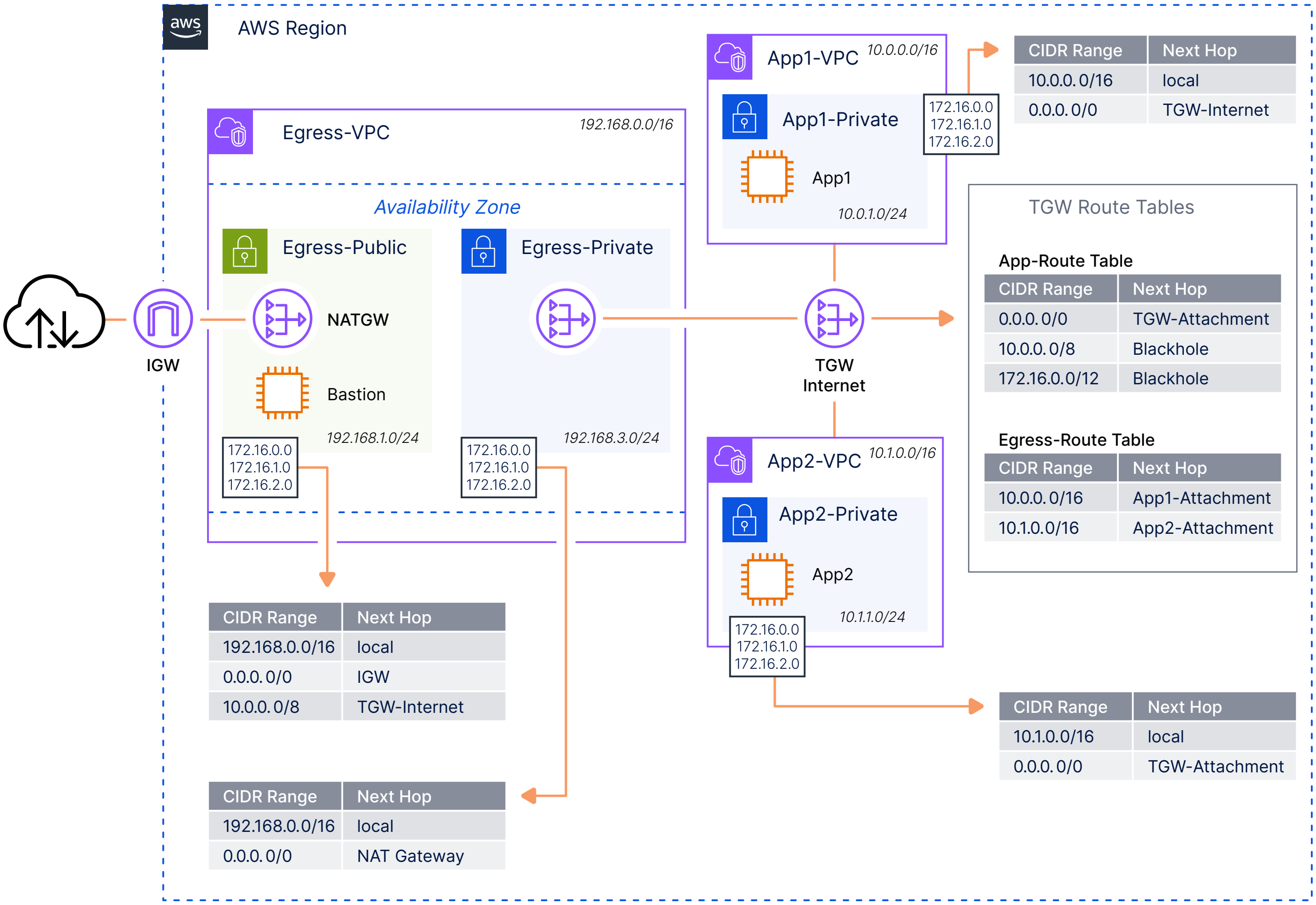
Figure 39. Server Manager local server configuration, enhanced security Off

Appendix C: AWS Transit Gateway Lab Environment

The following GitHub page shows a diagram of a Transit Gateway (TGW) lab from an example AWS blog post, which includes a Cloud formation template. You can refer to this page as you test your Site-to-Site VPN Connection. You can find instructions on testing on the AWS blog post.

Transit Gateway lab on GitHub

Transit Gateway lab environment diagram:



CIDR Range	Next Hop
10.0.0. 0/16	local
0.0.0. 0/0	TGW-Internet

TGW Route Tables

App-Route Table

CIDR Range	Next Hop
0.0.0. 0/0	TGW-Attachment
10.0.0. 0/8	Blackhole
172.16.0.0/12	Blackhole

Egress-Route Table

CIDR Range	Next Hop
10.0.0. 0/16	App1-Attachment
10.1.0.0/16	App2-Attachment

CIDR Range	Next Hop
192.168.0.0/16	local
0.0.0.0/0	IGW
10.0.0. 0/8	TGW-Internet

CIDR Range	Next Hop
10.1.0.0/16	local
0.0.0. 0/0	TGW-Attachment

CIDR Range	Next Hop
192.168.0.0/16	local
0.0.0.0/0	NAT Gateway

Figure 40. Example transit gateway lab environment diagram

Appendix D: Requesting Zscaler Support

If you need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues, Zscaler Support is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

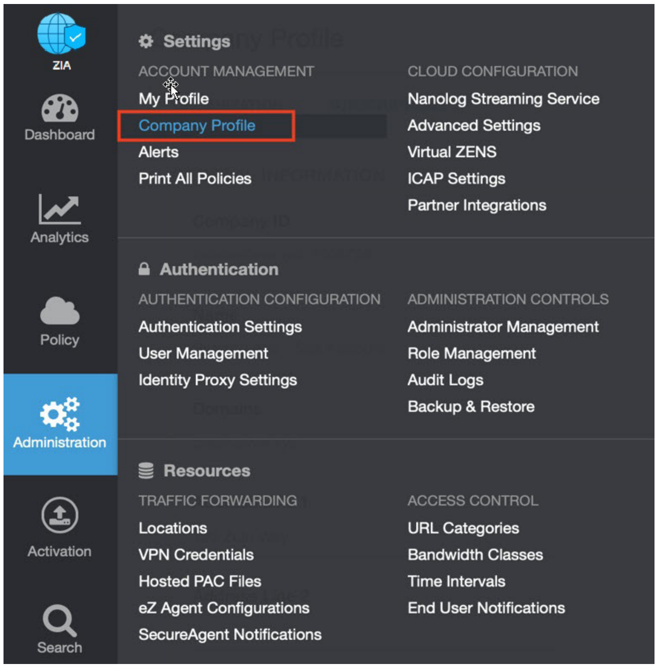
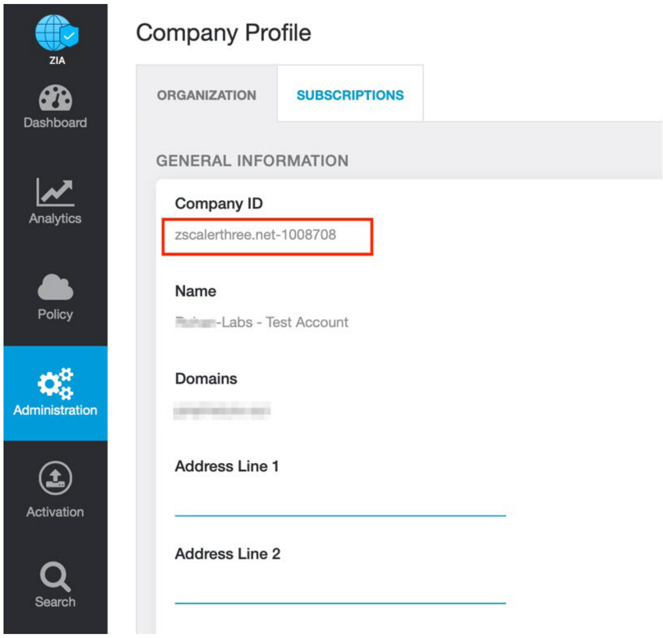


Figure 41. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 42. Company ID

3. Use the company ID to open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

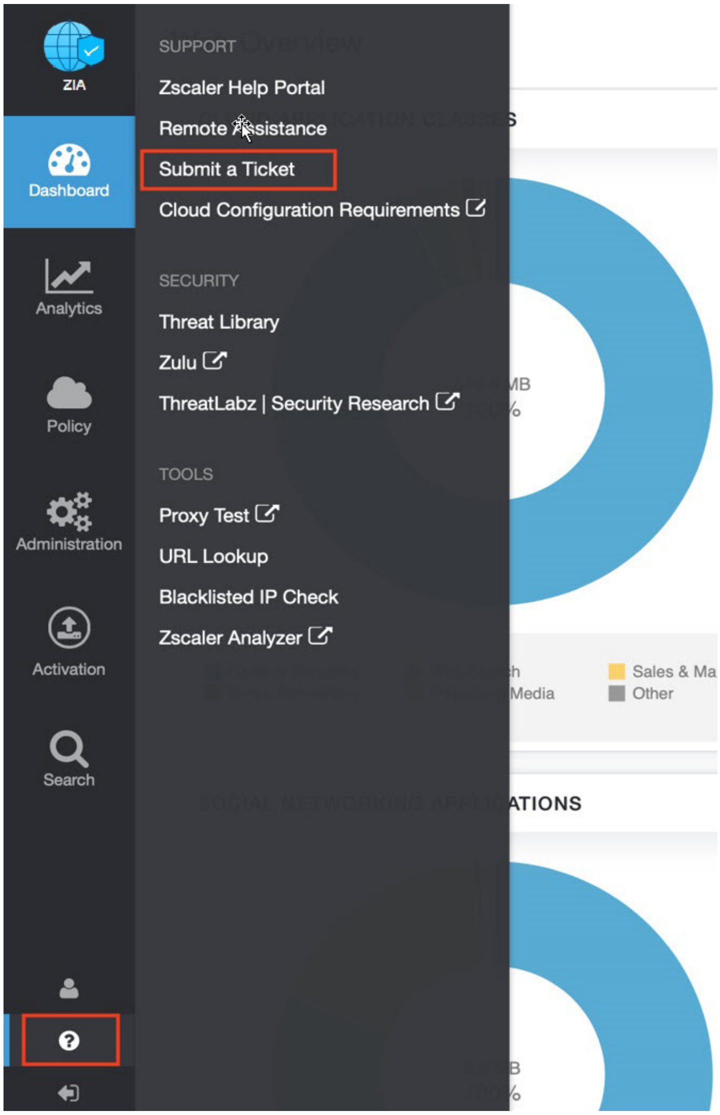


Figure 43. Submit a ticket