ZSCALER AND AZURE TRAFFIC FORWARDING DEPLOYMENT GUIDE

JANUARY 2022, VERSION 1.2

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms 4

About This Document 5

- Zscaler Overview 5
- Audience 5
- Software Revisions 5
- Request for Comments 5

Zscaler and Microsoft Introduction 6

- ZIA Overview 6
- ZPA Overview 6
- Zscaler Resources 6
- Microsoft Azure 7
  - Microsoft Resources 7

Understanding Zscaler and Azure WVD 8

- Product Overview 8
  - ZIA Overview 9
  - ZPA Overview 10
  - Azure WVD Overview 11

Azure WVD Installation 12

- Creating a WVD Host Pool 12
  - Installing WVD 13
  - Creating a Personal (Dedicated) Host Pool 14
  - Creating a Pooled (Shared) Host Pool 20

©2024 Zscaler, Inc. All rights reserved.

Zscaler Traffic Forwarding Options 21
Setting up Zscaler Client Connector 21
PAC Files 26
Site-to-Site VPN – IPSec Tunnels 28
Overview 28
Creating an Azure VPN Gateway 29
Configuring the Virtual Network Gateway Application 31
Gateway Deployment 32
Configuring Zscaler 39
Create a Redundant VPN Connection for Manual Fail-over 45
Create a Route Table 51
Appendix A: Troubleshooting 55
VPN Troubleshooting 55
Troubleshooting from the VNet 56
Verify Traffic is Going Through the Tunnel to Zscaler 57
Appendix B: PAC Examples 58
APP PAC Example: 58
Forward PAC: 61
Browser PAC: 64
Appendix C: Requesting Zscaler Support 68

©2024 Zscaler, Inc. All rights reserved.

Terms and Acronyms

The following terms and acronyms are used in this document. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
WVD	Windows Virtual Desktop
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
VPN	Virtual Private Network
PAC	Proxy Auto-Configuration
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
RDP	Remote Desktop Protocol
SSL	Secure Socket Layer (RFC6101)
VNet	Virtual Network (Azure)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZEN	Zscaler Enforcement Node (Zscaler)
ZPA	Zscaler Private Access (Zscaler)
ZCC	Zscaler Client Connector (Zscaler)

©2024 Zscaler, Inc. All rights reserved.

About This Document

This section describes the organizations and requirements referenced in this deployment guide.

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. 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.

Microsoft Overview

Microsoft (Nasdaq: MSFT), Microsoft develops and licenses consumer and enterprise software. It is known for its Windows operating systems and Office productivity suite. The company is organized into three equally sized broad segments: productivity and business processes (legacy Microsoft Office, cloud-based Office 365, Exchange, SharePoint, Skype, LinkedIn, Dynamics), intelligence cloud (infrastructure- and platform-as-a-service offerings Azure, Windows Server OS, SQL Server), and more personal computing (Windows Client, Xbox, Bing search, display advertising, and Surface laptops, tablets, and desktops). To learn more, refer to Microsoft's 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 About This Document.

Software Revisions

This document was authored using ZIA v6.0 and Zscaler Client Connector version 2.1.2.105 for the Windows 10 Dedicated Desktop, and PAC file Windows 10 Shared desktop.

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.

©2024 Zscaler, Inc. All rights reserved.

Zscaler and Microsoft Introduction

The following sections detail the Zscaler and Microsoft 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 ZIA as a secure internet onramp—just 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 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, data loss prevention (DLP), SaaS Security, and isolation, allowing you start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
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.

©2024 Zscaler, Inc. All rights reserved.

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
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.

Microsoft Azure

Microsoft Azure, part of the Microsoft suite of products, and commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

To learn more, go to Microsoft Azure's website.

Microsoft Resources

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

Name	Definition
Azure Trial License	Link to obtain Azure trial license.
Azure Documentation	Azure help documentation.
Windows Virtual Desktop Environment	Setup procedures for Windows Virtual Desktop Environment.
Azure Virtual Network	Help articles for Azure Virtual Network.
Microsoft Entra ID	Help articles for Microsoft Entra ID.
Azure Virtual Network Gateway	Tutorial: Create a Site-to-Site connection in the Azure portal.
Azure VPN High Availability	Highly Available cross-premises and VNet-to-VNet connectivity.
Azure Route Tables	Virtual network traffic routing.
Getting Started with WVD	Help article on getting started with Windows Virtual Desktop.

©2024 Zscaler, Inc. All rights reserved.

Understanding Zscaler and Azure WVD

The following sections detail how ZIA and ZPA operate and interact with Microsoft Azure WVD.

Product Overview

Figure 1 shows a high-level overview of ZIA and ZPA in a Microsoft WVD environment.

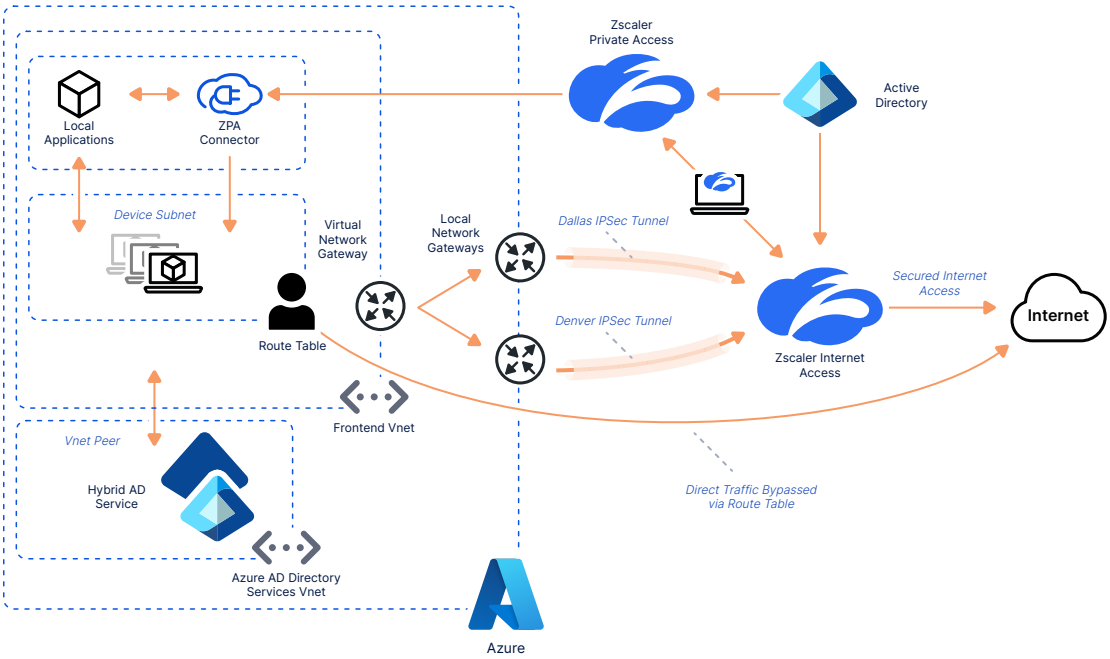

Figure 1. ZIA, ZPA in a Microsoft WVD environment

You can integrate Azure and Zscaler in multiple ways. You can forward internet traffic from Azure to ZIA by using the Zscaler Client Connector on a dedicated private WVD Instance, by using a browser PAC file, or by forwarding traffic over an IPSec tunnel. The IPSec tunnel can be created using various industry standard network and native Microsoft components.

You can connect customer traffic destined for internal private resources seamlessly and securely over ZPA by placing a ZPA Application Connector inside the Azure environment. ZPA initiated from inside Azure and destined to external private resources is currently limited to using the Zscaler Client Connector on a dedicated private WVD instance.

This deployment guide covers the available traffic forwarding methods. IPSec tunnels are created using the Azure Virtual Network Gateway, and the Zscaler Client Connector is deployed on a WVD private instance to both ZIA and ZPA.

©2024 Zscaler, Inc. All rights reserved.

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 through one of the following methods:

- Use a tunnel from a network device like an Azure Virtual Gateway or a Cisco CSR for general forwarding from Azure to ZIA.

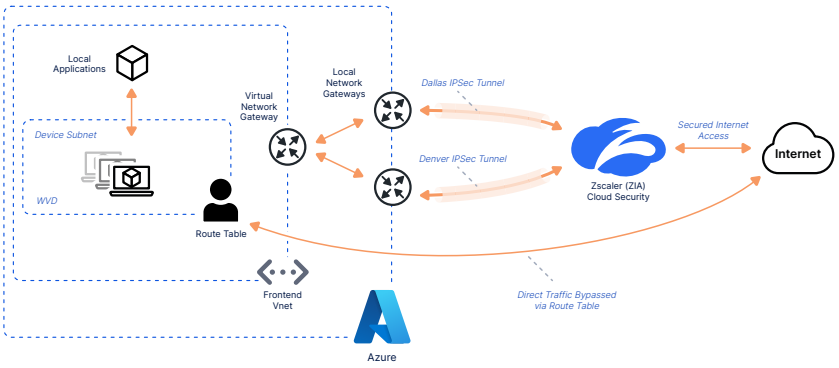

Figure 2. IPSec tunnel to ZIA

- Use Zscaler Client Connector, PAC file, or tunnel for Microsoft Azure WVD personal (dedicated workstation) instance.

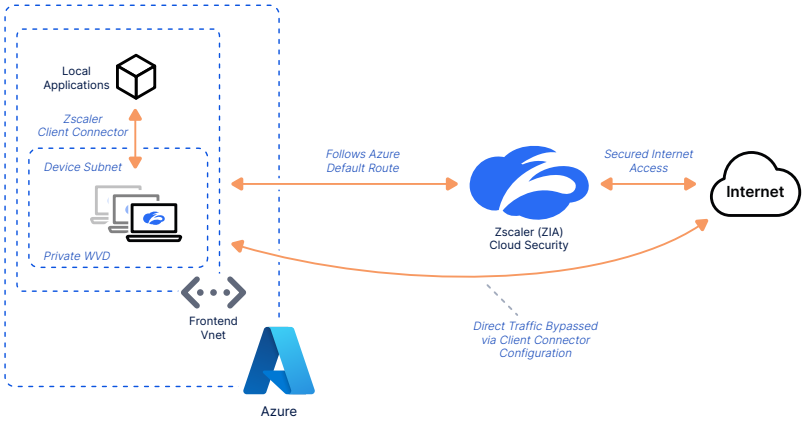

Figure 3. Zscaler Client Connector on a WVD private instance

- Use a PAC file or tunnel from a network device for Microsoft Azure WVD pooled (shared) instance.

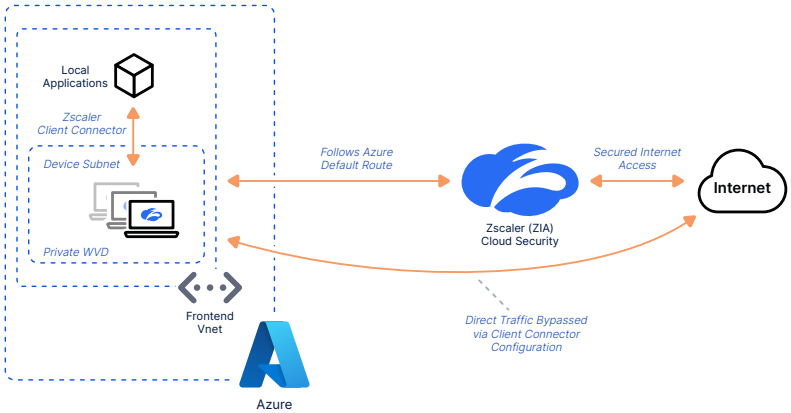

Figure 4. Browser PAC file

- Forward traffic via our lightweight Zscaler Client Connector or PAC file for mobile or remote employees.

©2024 Zscaler, Inc. All rights reserved.

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a WVD instance in Azure in South Korea—they get identical protection. ZIA sits between your users and the internet, inspecting every byte of traffic inline across multiple security techniques (even SSL-encrypted traffic).

You get full protection from web and internet threats. With a cloud platform that supports Standard and Advanced Cloud Firewall, IPS, Sandbox transactions, DLP, CASB, and Cloud Browser Isolation you can start with the services you need today and activate others as your needs grow. For more information, see the resources in Zscaler Resources.

ZPA Overview

The ZPA service enables organizations to provide access to internal applications and services while ensuring the security of their networks. ZPA is an easier to deploy, more cost-effective, and more secure alternative to VPNs. Unlike VPNs, which require users to connect to your network to access your enterprise applications, ZPA gives users policy-based secure access to only the internal apps they need to get their work done. With ZPA, application access does not require network access.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. The Zscaler Client Connector ensures the user's device posture, and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

ZPA is a separate cloud service from ZIA but is applicable for dedicated instance WVD environments for connectivity back to a client's internal applications. It is also applicable for external or remote clients, connecting into applications hosted in Azure and eliminating the need for a jump box. For this guide, ZPA access is used to RDP to the WVD instance for administrative purposes, and the internet-bound traffic is sent through an IPSec tunnel to ZIA providing a dark internet, zero-trust secured internet experience.

- To access Internal Azure Applications, install a ZPA Application Connector in your Azure environment. ZPA provides dark internet, zero-trust access using controlled Natural Access for the best possible user experience.

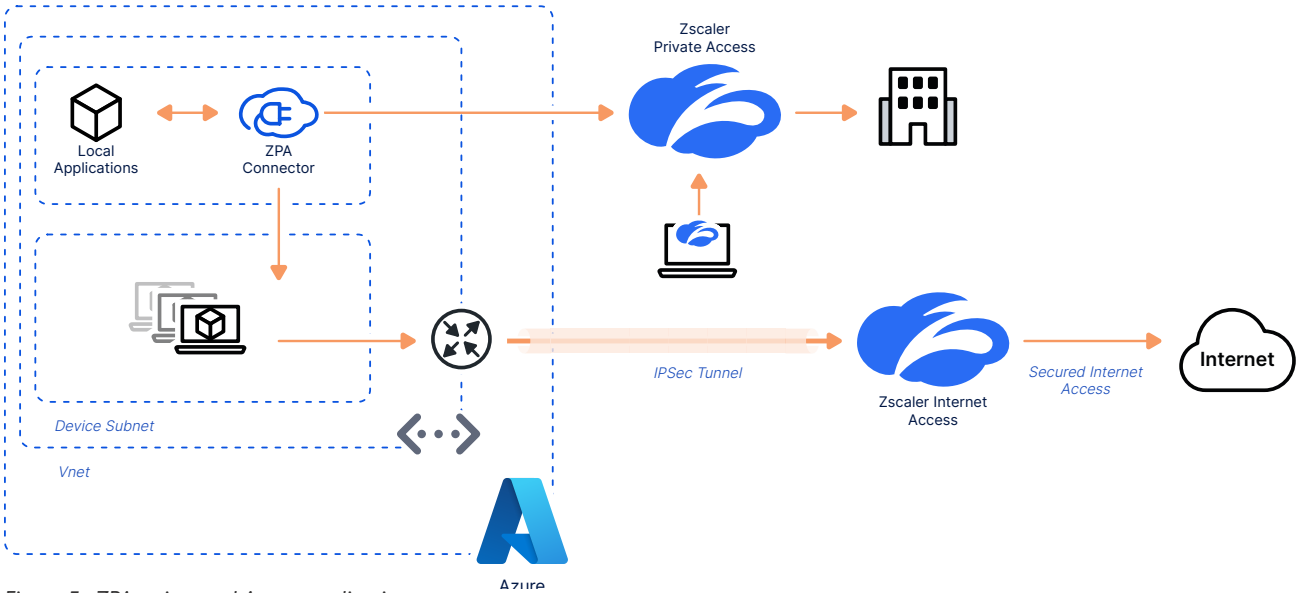

Figure 5. ZPA to internal Azure applications

©2024 Zscaler, Inc. All rights reserved.

- For access from the Azure WVD environment to the customers external private resources using ZPA, run the Zscaler Client Connector on a Private WVD instance.

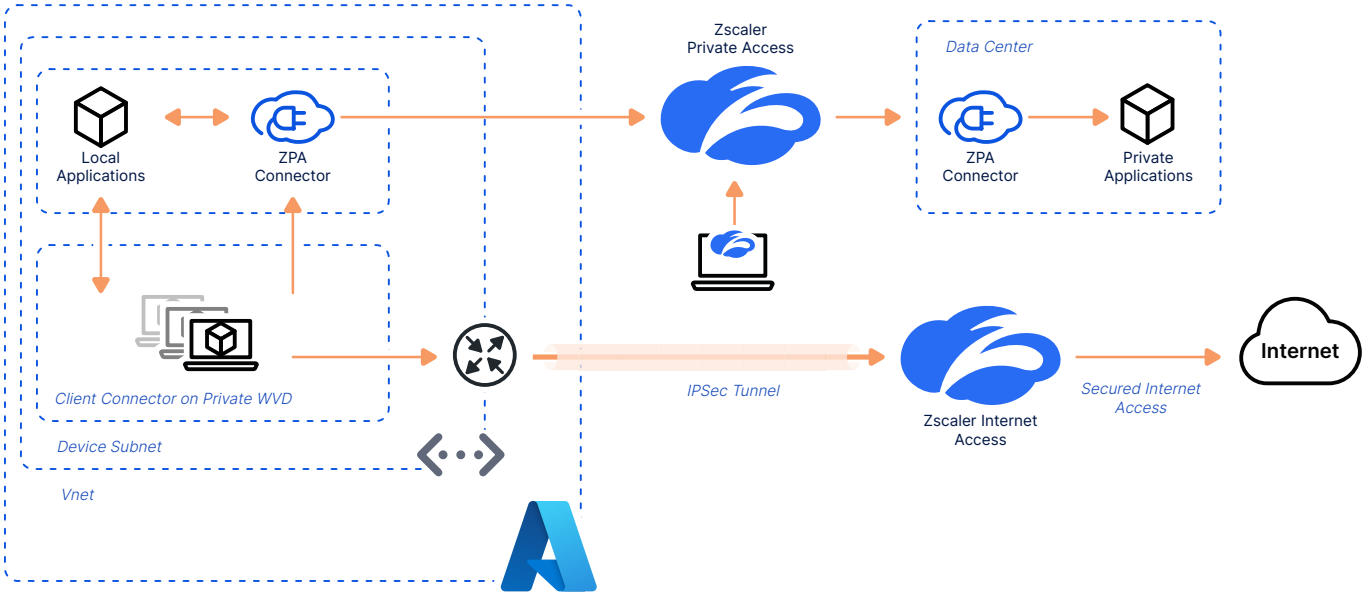

Figure 6. ZPA from a private WVD host running the Zscaler Client Connector

ZPA provides the clients with a zero trust environment and an always-on, VPN-like connectivity over a dark internet. Zero trust creates a user experience with secure, simple, low latency connectivity via the same ZIA client for secure internet browsing. For more information, see the resources in Zscaler Resources.

Azure WVD Overview

Microsoft WVD is a desktop and app virtualization service that runs on Azure. You can use Azure WVD to provision pools of resources on Windows 10 in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. You can pay either monthly or hourly, just for the WVD instances you launch, which helps you save money when compared to traditional desktops and on-premises VDI solutions. WVD helps you eliminate the complexity in managing hardware inventory, OS versions and patches, and Virtual Desktop Infrastructure (VDI), which helps simplify your desktop delivery strategy. With Microsoft WVD, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device. For more information, see the resources listed under Zscaler Resources.

©2024 Zscaler, Inc. All rights reserved.

Azure WVD Installation

This document provides Zscaler installation procedures for a WVD Personal or Pooled environment, and the options and requirements for each. The scope of this document does not include step-by-step procedures to install WVD in Azure.

Microsoft videos were followed to build and create the WVD pools for testing. The tested installation requires a working Hybrid Microsoft Entra ID instance to domain join the WVD VMs, a resource group, storage account, virtual network, network security group. The installation requires some basic PowerShell scripting to create the WVD tenant and bind the Azure subscription to the tenant. Creation of the tenant requires global admin privileges for Azure and local administrator privileges on the workstation used to create the WVD tenant.

Creating a WVD Host Pool

A WVD host pool in Azure is a resource pool of VM's that can be configured as personal stand-alone VM's with their own operating system that can be assigned to an individual user, or a pool of shared VM resources that share an operating system. The Zscaler Client Connector runs on a Personal Windows 10 Enterprise and on all Client Connectors that forward data using TSL or DTLS to ZIA, ZPA, and Zscaler Digital Experience (ZDX).

There are several technical and security benefits provided by using a Personal Windows-10 Workstation and the Zscaler Client Connector. The Zscaler Client Connector enables ZPA connectivity, which in turn allows access to all private applications. The Client Connector also enhances connectivity for ZIA, and provides all TCP and UDP ports to be forwarded to the ZEN which can provide traditional and Application Firewall protection using the Zscaler Cloud Firewall.

The addition of the ZDX on the Client Connector also gives you complete end-to-end traffic visibility, from the Zscaler client to any SaaS application in the cloud using application monitors sent by the Client Connector to your most critical applications.

After creating a Personal Pool, you need to define the criteria for the pool which includes the location where the VM's exist. Select a location that is a geographically central to your organization's population as possible for a single pool. If you create multiple pools, select a location as close as possible to your different locations. You also need to select Windows-10 Enterprise for Zscaler Client Connector support. Currently only single session is supported for the Zscaler Client Connector. Multisession is not supported.

The administrator account is a global administrator account or a service principle that joins the VM to the Azure domain. This is a requirement for reverse connect to work for the WVD environment.

Reverse connect is one of the core differences between a typical Remote Desktop Service and Microsoft WVD. It allows an Azure authenticated user to connect to an Azure domain joined VM through a Remote Desktop Gateway in Azure using a browser or the RD client which uses HTML5 over TCP port 443. For more information, see Getting Started with WVD.

The VM's were configured without a public IP address and you must use reverse connect to use the VM as a WVD resource. However, ZPA can be used to connect to internal Azure resources that do not have an external IP address, which eliminates the need to have a jump box for support or configuration. ZPA provides a zero-trust dark internet solution for administrators to attach to resources or applications.

©2024 Zscaler, Inc. All rights reserved.

Installing WVD

After the WVD tenant is created and assigned to the Azure license, create a host pool.

1. Enter `Windows Virtual Desktop` in the search field and select the service to install.
2. Select **Create a host pool** to start the installation wizard.

There are two types of host pools for a WVD environment: **Pooled** or **Personal**.

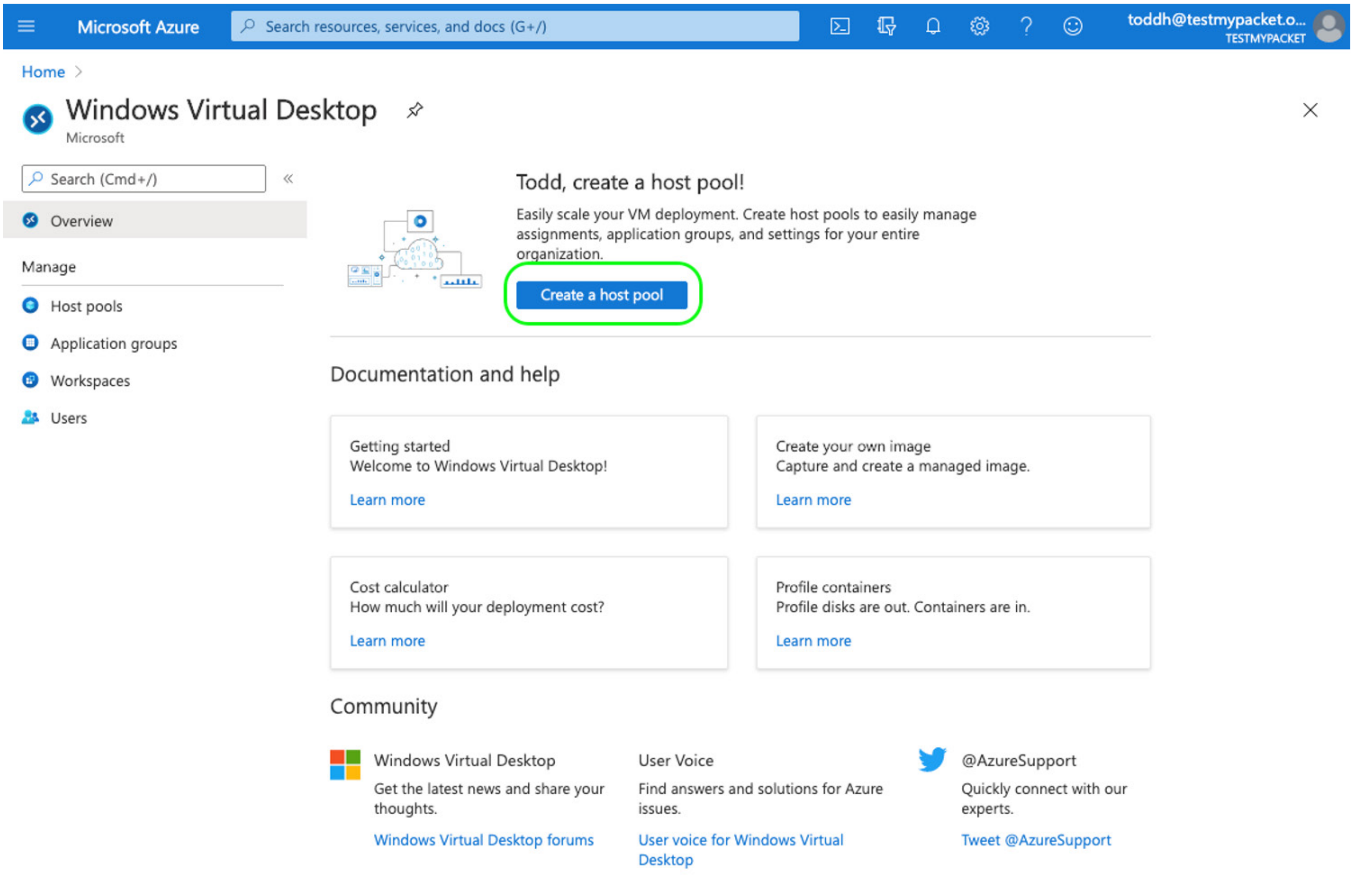

Figure 7. Create a WVD host pool

©2024 Zscaler, Inc. All rights reserved.

Creating a Personal (Dedicated) Host Pool

To select and create the pool type for the host pool, select either **Pooled** (which for Zscaler connectivity requires a PAC file for traffic forwarding, or **Personal** (which creates a stand-alone workstation that can load the Zscaler Client Connector).

The following example uses a Personal host pool. Use **Select a Host** type of **Personal**.

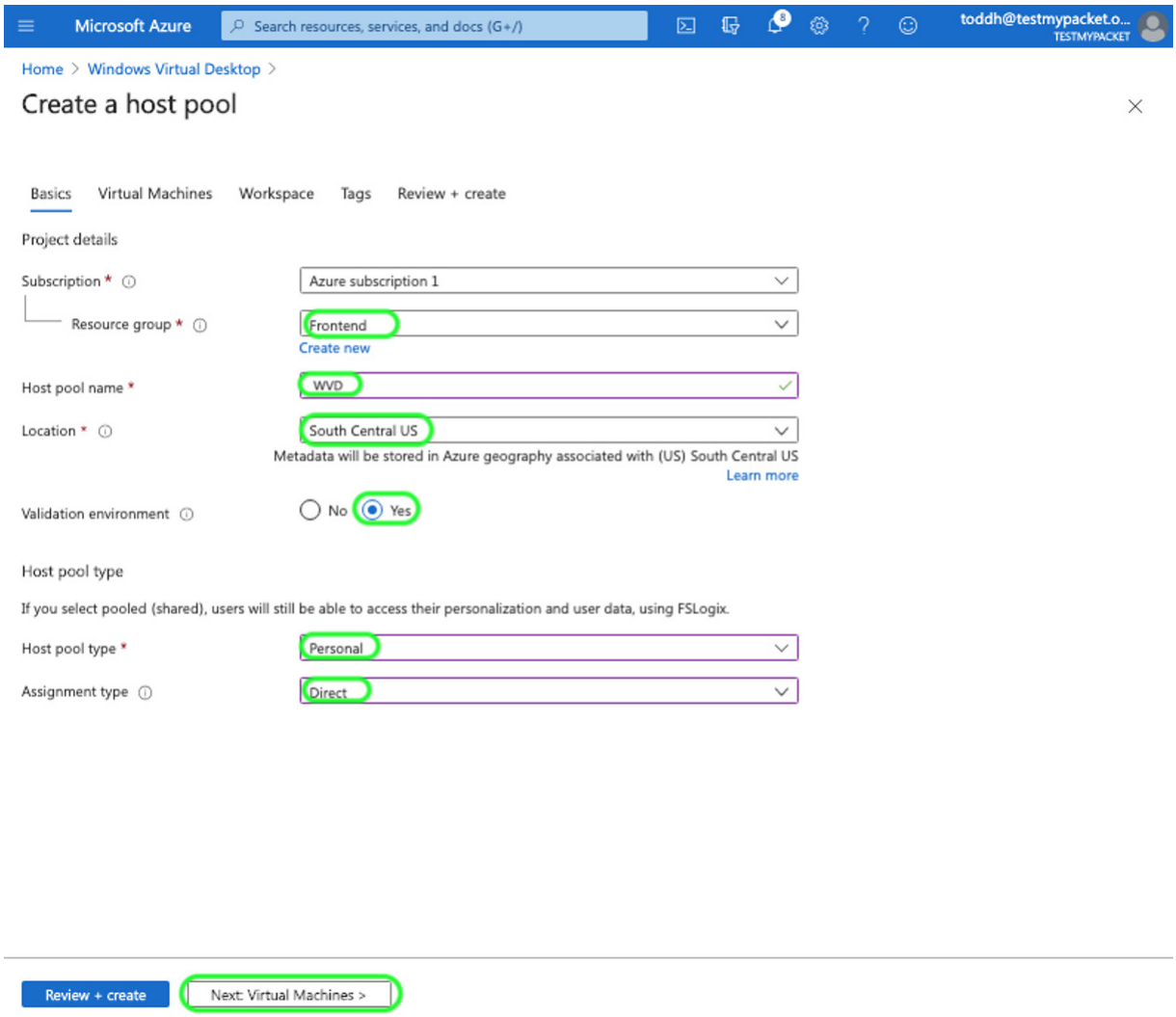

Figure 8. Select host pool type

Configure the VM:

1. Enter the **VM** and **Network** specifics for the **Pool**.
2. Enter the credentials of an Microsoft Entra IDministrator that can attach the VM to a domain.

The installation fails if the VM cannot attach to the domain.

3. Select **Next Virtual Machines** to continue.
4. Select **Yes** to register the **Desktop App Group** and create a new workspace name. This is the workspace the client sees when attaching from the RD client or a browser.

©2024 Zscaler, Inc. All rights reserved.

5. Select **Review + create** to create the host pool. The installation can take around 30 minutes.

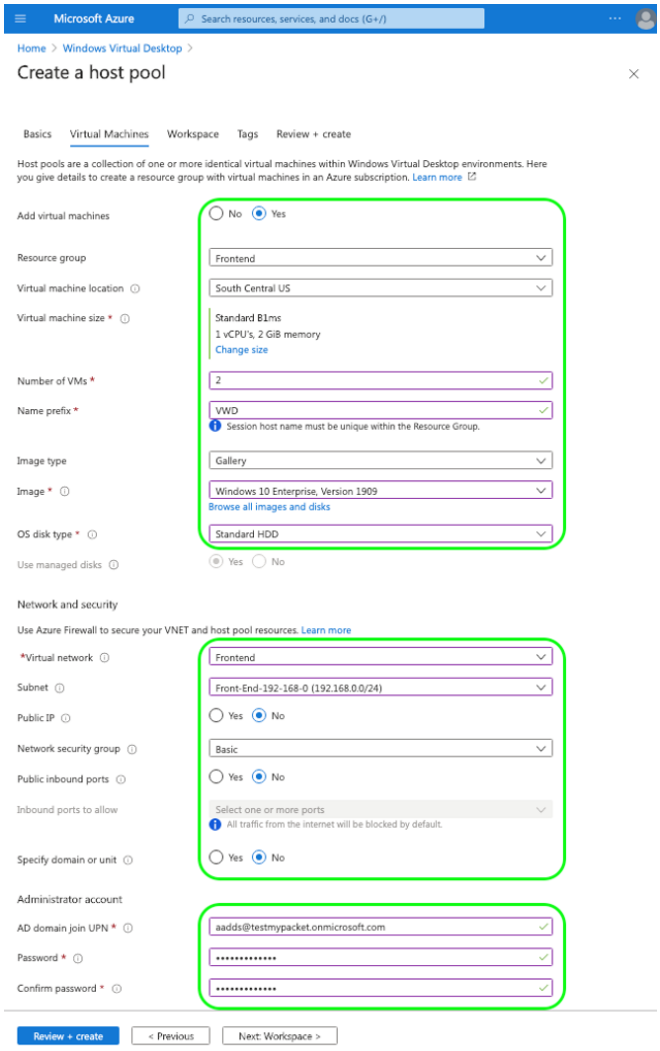

Figure 9. Configuration of the host pool (1 of 2)

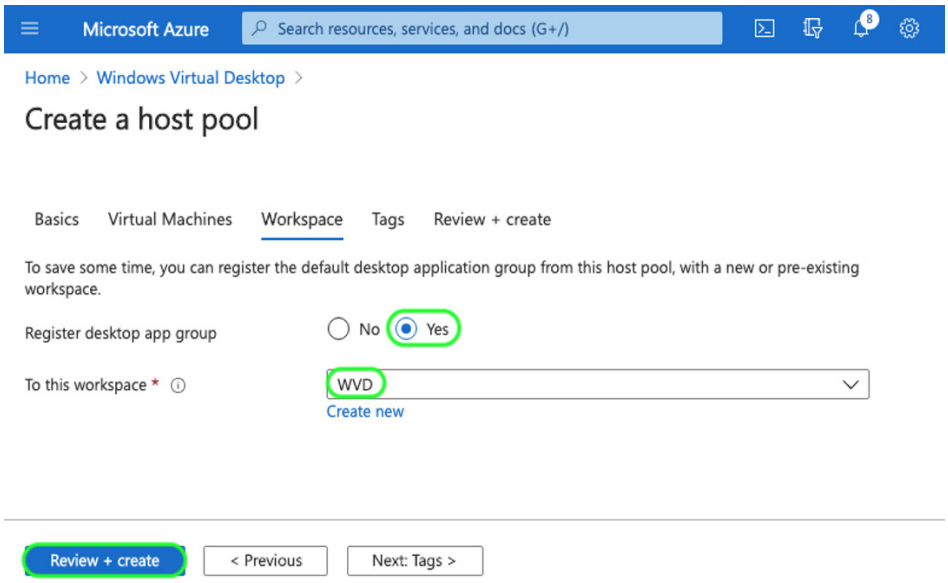

Figure 10. Configuration of the host pool (2 of 2)

©2024 Zscaler, Inc. All rights reserved.

The following image shows the configured host pool and the created resources from the installation processes. The highlighted devices are the **Host Pool**, the **Desktop Application Group (DAG)**, and the **Dedicated Personal Virtual Machines**. Assign the users to the VM by completing two steps:

1. Assign the user in the Desktop Application Group.
2. Assign the machine to the user is the Session Host Pool under the Host Pool.

Details about these two steps follow.

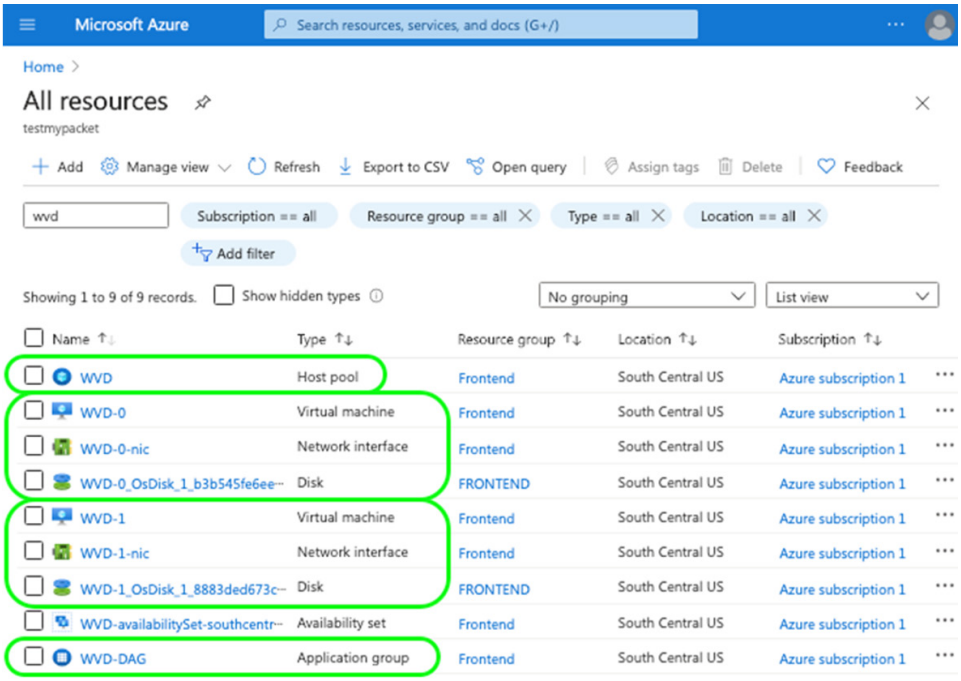

Figure 11. The created WVD host pool

©2024 Zscaler, Inc. All rights reserved.

Assigning the User in the Desktop Application Group

To start:

1. Select the **Application Group** to bring up the configuration parameters.
2. Select **Assignments** and then **Add** to bring up the Microsoft Entra ID User selection menu.
3. Select the users to assign to the dedicated VMs.
4. Click **Select** to give the user access to the WVD VM resources.

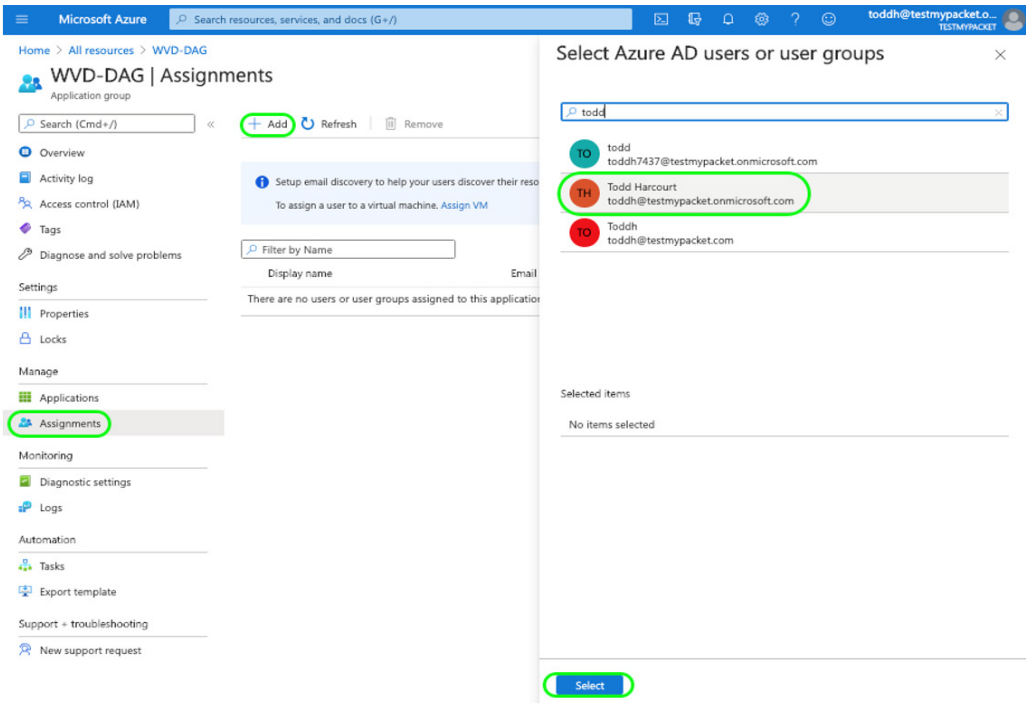

Figure 12. The created virtual machine (1 of 2)

©2024 Zscaler, Inc. All rights reserved.

Assigning the Machine to the User is the Session Host Pool Under the Host Pool

1. Select **All Resource**.
2. Select the **WVD Host Pool**, **Session hosts** and **Assign** to bring up the VMs.
3. Select **(Assign)**.
4. Select the user that is assigned to the VM.
5. Click **Select**.

Your users can now connect to the VM through the remote desktop application or a browser by using reverse connect.

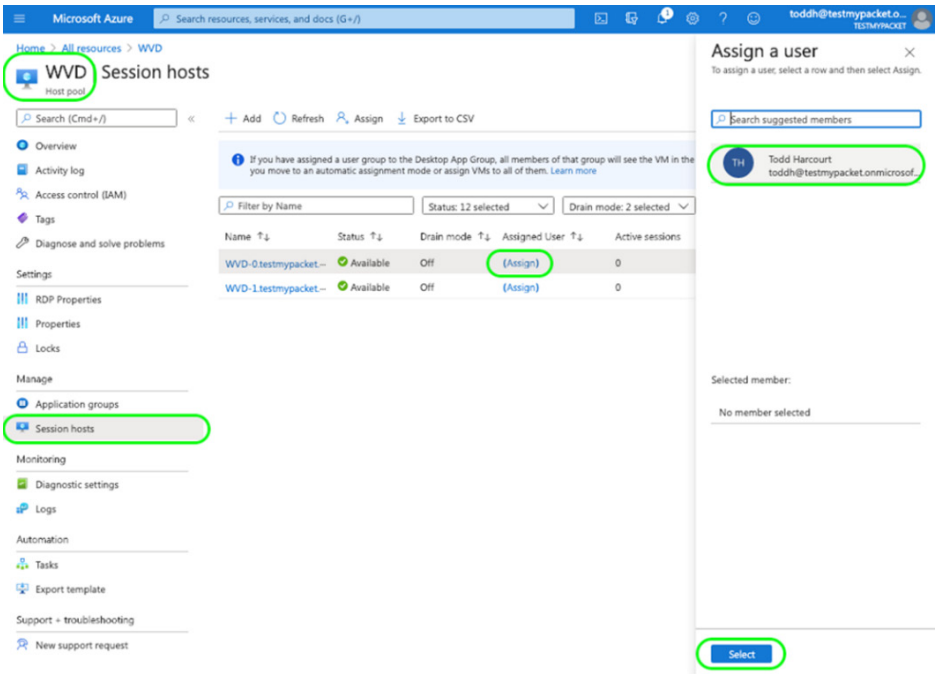

Figure 13. The created virtual machine (2 of 2)

Next, test the VM using reverse connect. Bring up a browser and go to the WVD webclient:

©2024 Zscaler, Inc. All rights reserved.

This brings up the workspace just created. Double-click on the **Default Desktop** icon and enter the Azure domain user credentials. This opens Windows-10 VM in the browser.

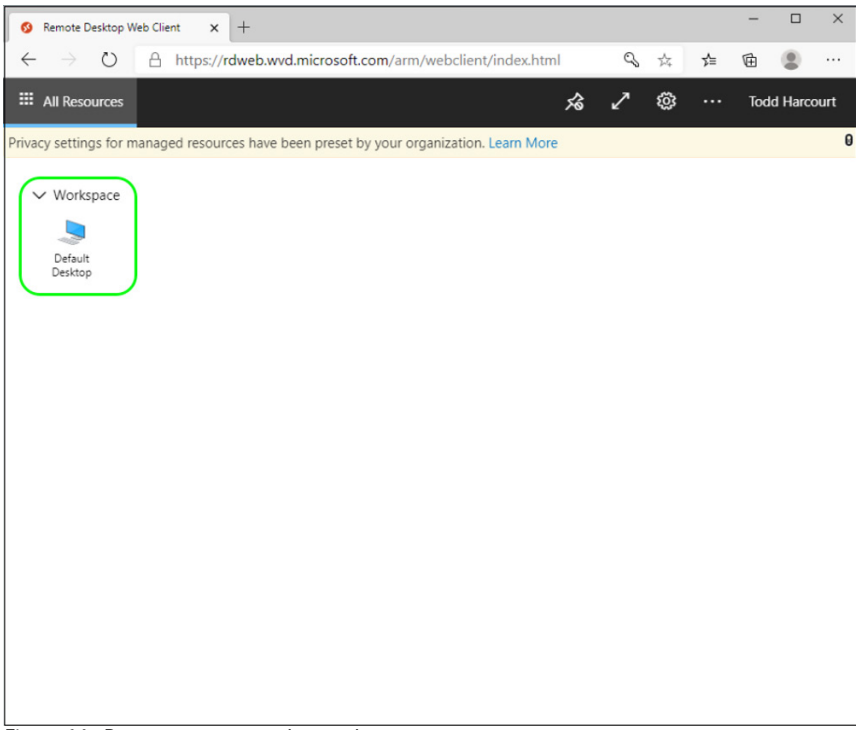

Figure 14. Browser access to the workspace

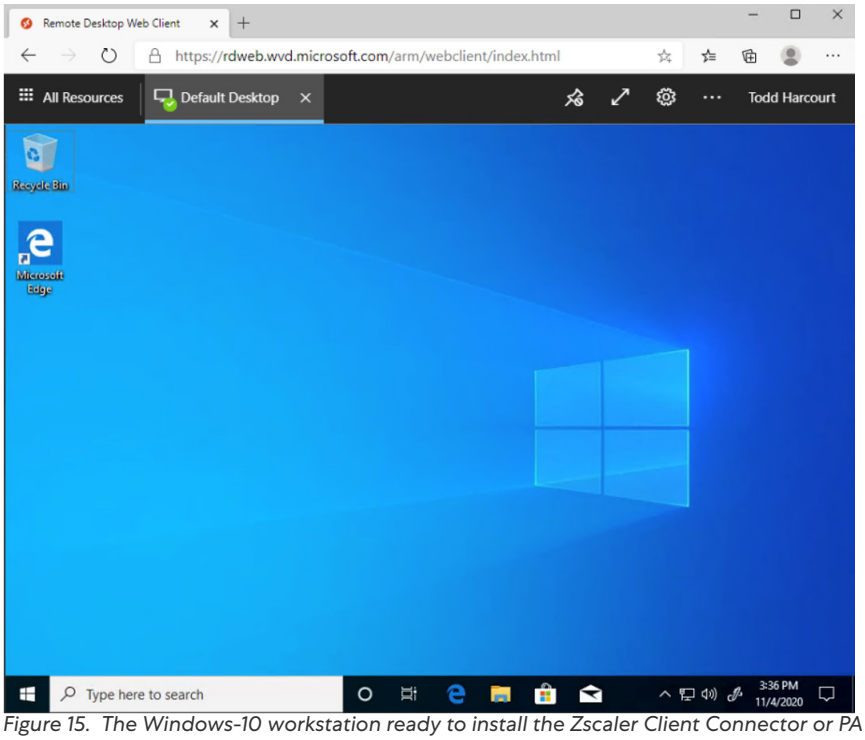

Figure 15. The Windows-10 workstation ready to install the Zscaler Client Connector or PA

©2024 Zscaler, Inc. All rights reserved.

The VM is ready to install traffic forwarding to Zscaler for network and end point security. Let's walk through the methods of configuring forwarding depending on the type of VM.

- If the VM is a pooled device using multi-threaded Windows-10 OS, install a PAC file using the example in Appendix B: PAC Examples with the appropriate bypasses.
- If the VM is a Private VM, use the Zscaler Client Connector—although a PAC file is an option for every browser if the Zscaler Client Connector is not an option for some reason.

You also configure a tunnel to ZIA for internet-bound traffic using a virtual network gateway.

Creating a Pooled (Shared) Host Pool

A pooled device is a shared virtual machine where each device has multiple users that use the same resources, but to the user it feels like a personal dedicated Windows workstation. This has financial advantages by pooling resources and provides some operational simplification of management.

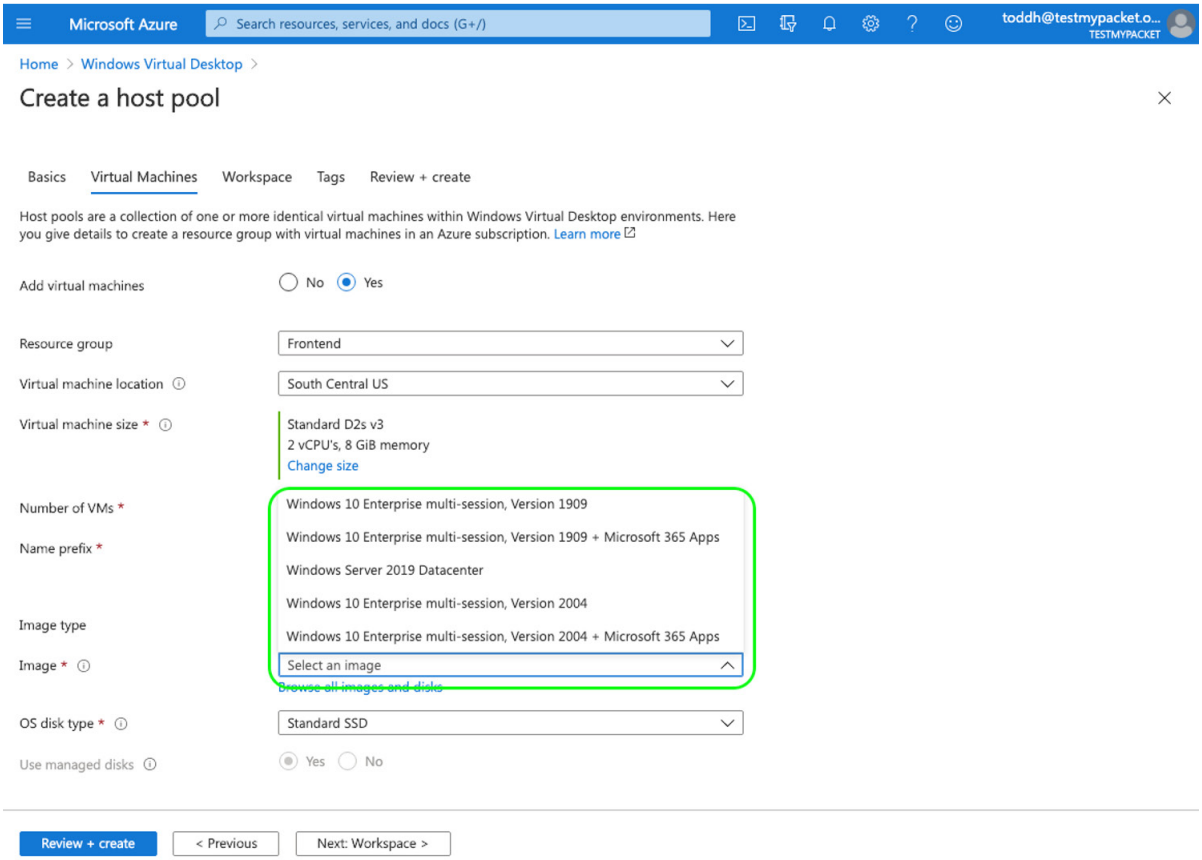

Figure 16. Selecting an image for pooled (shared) VM pool type

A pooled host environment also has ramifications for Zscaler. **The Zscaler Client Connector is not supported on pooled machines**. Connectivity to Zscaler is provided by other means, such as a PAC file for browsers on the pooled system, a Virtual Zscaler Cloud Connector, or a tunnel from a firewall or network device running in the Azure environment. VMs of this type run a Windows-10 Multi-Session OS, which is not currently supported by the Zscaler Client Connector.

©2024 Zscaler, Inc. All rights reserved.

Zscaler Traffic Forwarding Options

The following processes install the Zscaler Client Connector for the Private WVD VM, or a PAC file using a dedicated proxy port for the Pooled VM. For either the Zscaler Client Connector or a PAC file, you must add bypasses to keep traffic away from Zscaler, and keep control traffic local to the Azure environment. You can also include clients in their own internal domain.

Setting up Zscaler Client Connector

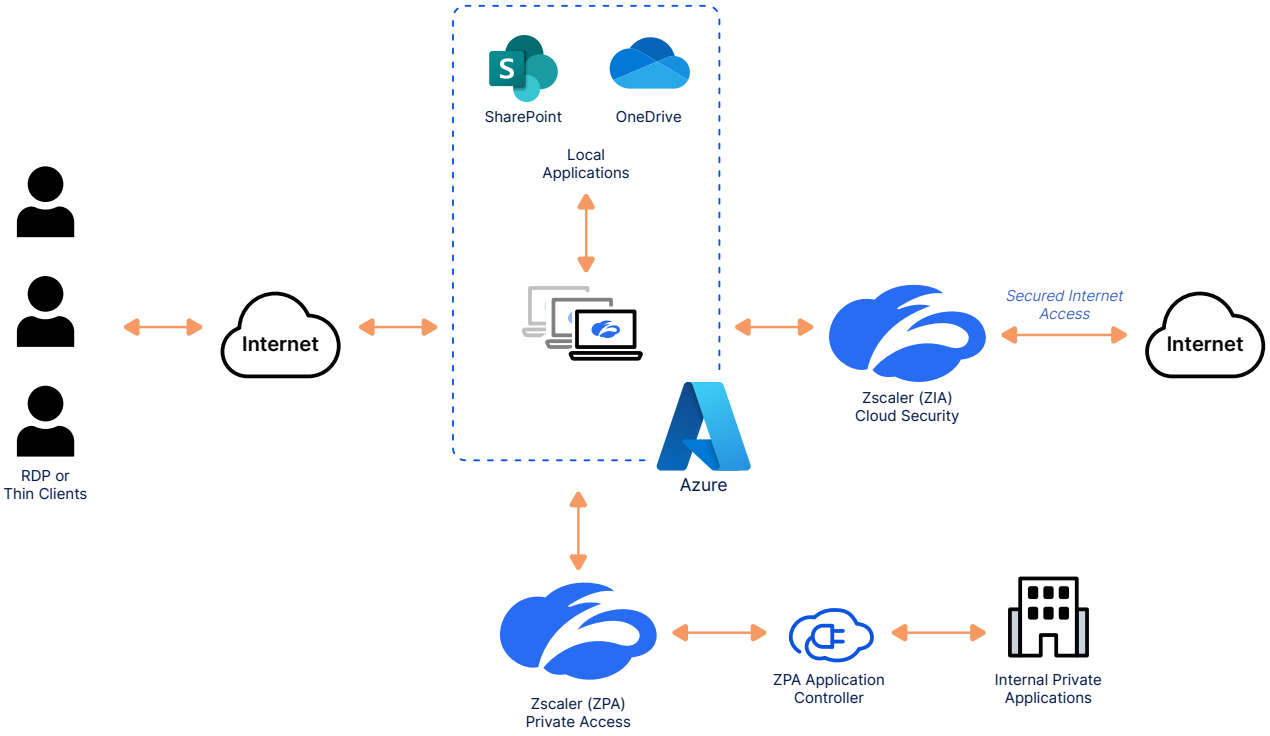

Figure 17. Traffic flow with Zscaler Client Connector using ZIA and ZPA

The Zscaler Client Connector is a common endpoint agent for both ZIA and ZPA services. Users can get all of the benefits of Zscaler internet security using ZIA, as well as granular, policy-based access to internal resources from a single end-point client using ZPA.

The Zscaler Client Connector has two different modes of operation for forwarding traffic to ZIA. These modes are referred to as Tunnel-1 and Tunnel-2. Tunnel-1 mode forwards only HTTP and HTTPS traffic to ZIA and all other traffic is sent direct to the destination. Whereas, Tunnel-2 mode forwards all TCP, UDP, and ICMP traffic. Using Tunnel-2 and Zscaler Cloud Firewall enables complete traffic coverage and security for Zscaler cloud services, but requires a bit more setup detail compared to Tunnel-1. Selection of Tunnel-1 or Tunnel-2 depends on where you enable Firewall services. If you have Zscaler Cloud Firewall, or want to use the Standard L4 Firewall, configure Tunnel-2 mode.

Zscaler Client Connector traffic forwarded to ZIA is evaluated and inspected according to your organization's security and access policies. By using the Client Connector and Tunnel-2 mode, all user traffic is secured and enforced from the Azure WVD instance out to internet destinations.

©2024 Zscaler, Inc. All rights reserved.

ZPA is a Zscaler cloud service that enables your users to securely access internal enterprise applications in traditional private data centers, or IaaS cloud providers. ZPA establishes a secure transport for accessing your enterprise apps by forwarding all TCP and UDP traffic destined for the application over a TLS connection regardless of the tunnel mode of ZIA. Using ZPA requires the Zscaler Client Connector. The Zscaler Client Connector offers advantages over using a private WVD instance. ZPA provides authenticated, zero trust access over internet connectivity that is invisible to discovery.

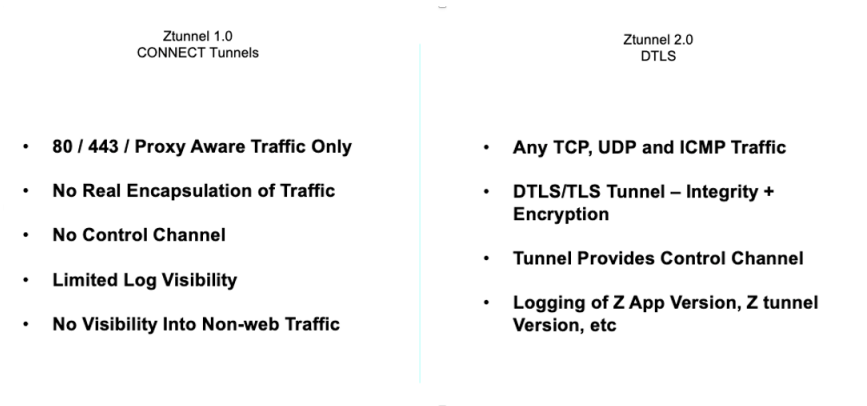

Figure 18. Comparison of Tunnel-1 and Tunnel-2 modes

After you've selected a tunnel mode, configure the Zscaler Client Connector to bypass specified local traffic using PAC files. For Tunnel-1 , add an App Profile PAC to bypass traffic. For Tunnel-2, configure and add a Forwarding Profile PAC. Configure the PAC files in the ZIA Admin Portal, under Hosted PAC Files using the examples in Appendix B: PAC Examples and then create forwarding profile for WVD.

Use the default forwarding profile for Tunnel-1. To create a Forwarding Profile for Tunnel-2 mode, open the Zscaler Client Connector and select **Administration > Forwarding Profile > Add Forwarding Profile**. This brings up the **Edit Forwarding Profile** window.

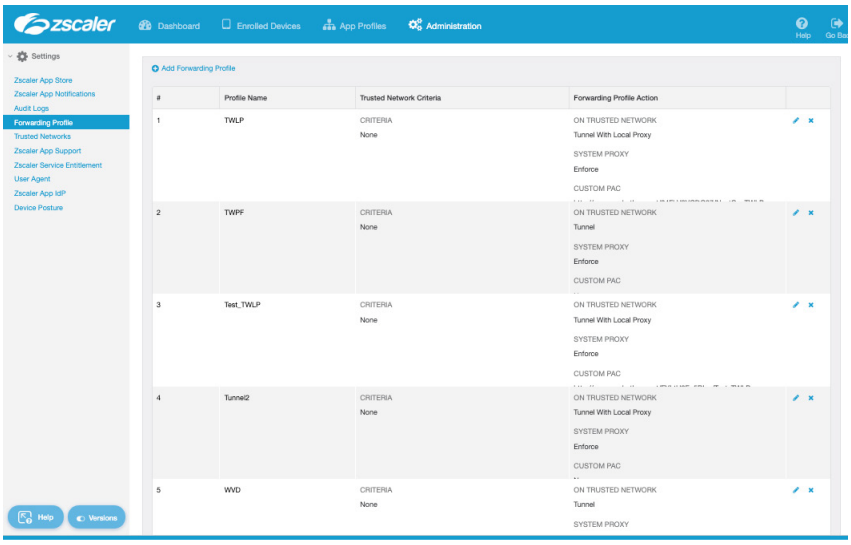

Figure 19. Create a forwarding profile

©2024 Zscaler, Inc. All rights reserved.

1. Enter the **Profile Name** and select the settings shown in the preceding image.
2. Under the **Z-Tunnel 2.0** > **Configure System Proxy Settings** > **Enforce** > **Use Automatic Configuration Script** add the location of the Forward Profile PAC file location just created on the ZIA Admin Portal.
3. Click **Save**.

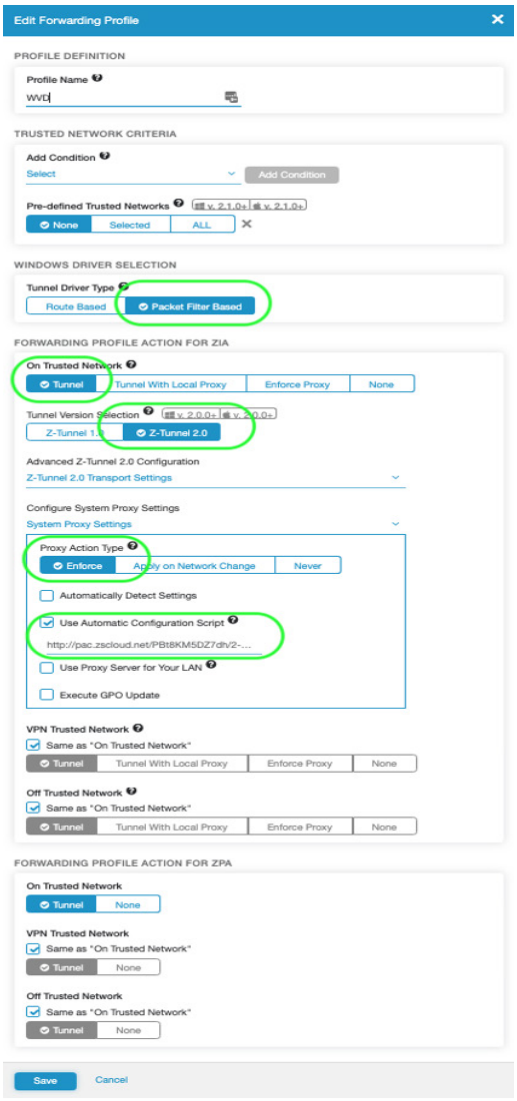

Figure 20. Create a forwarding profile for Tunnel 2.0

©2024 Zscaler, Inc. All rights reserved.

Next create the Application Profile for the Zscaler Client Connector to assign to the WVD devices. To add the Application profile, select **App Profile > Windows > Add Windows Policy**.

This brings up the **Windows Policy** screen.

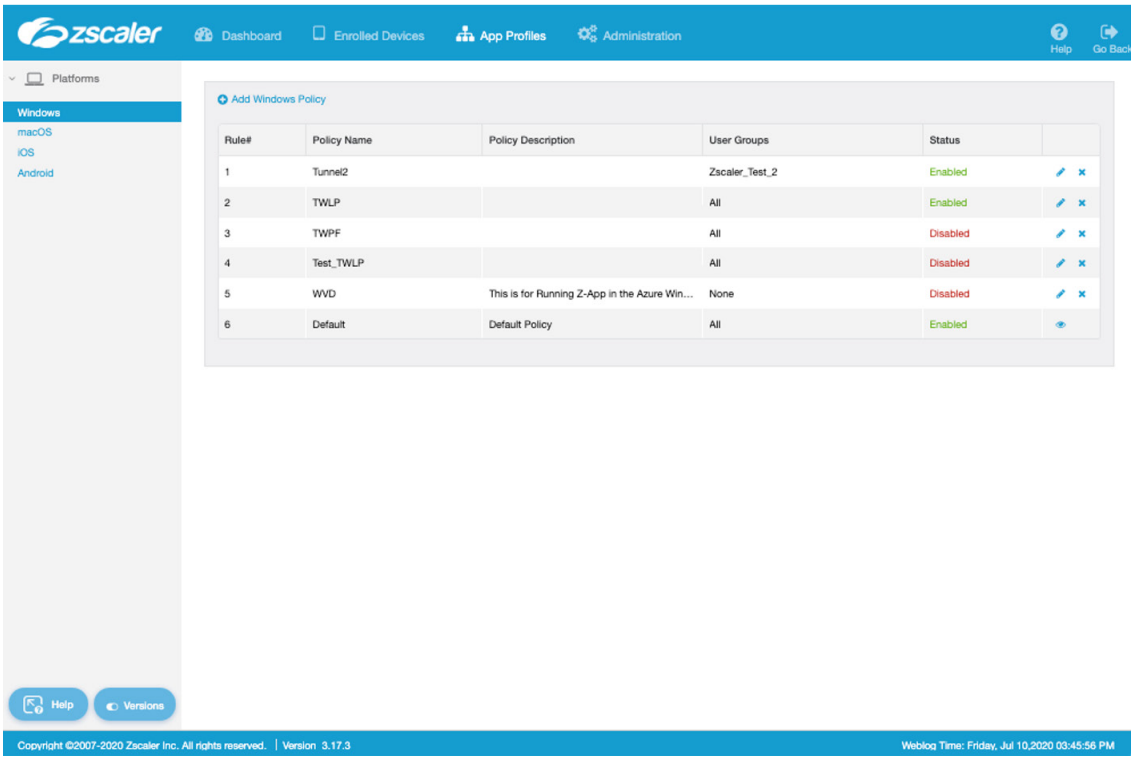

Figure 21. Create an application profile

To create the App Profile for a Tunnel-1 configuration:

1. **Name** the profile.
2. **Enable** the profile.
3. Select the **Groups** it applies to (typically an Microsoft Entra ID Group).
4. Enter the **Custom PAC URL** (this is the App PAC you created).
5. Enable **Install Zscaler SSL Certificate**.

The additional steps for Tunnel-2 are not required if you are deploying Zscaler Client Connector version 3.0 or later.

©2024 Zscaler, Inc. All rights reserved.

For Tunnel-2 complete two additional steps:

1. Select the **Forwarding Profile** you just created.
2. Under **Destination Exclusions** enter the public IP address of the Thin Client or remote device that connects to the VM.

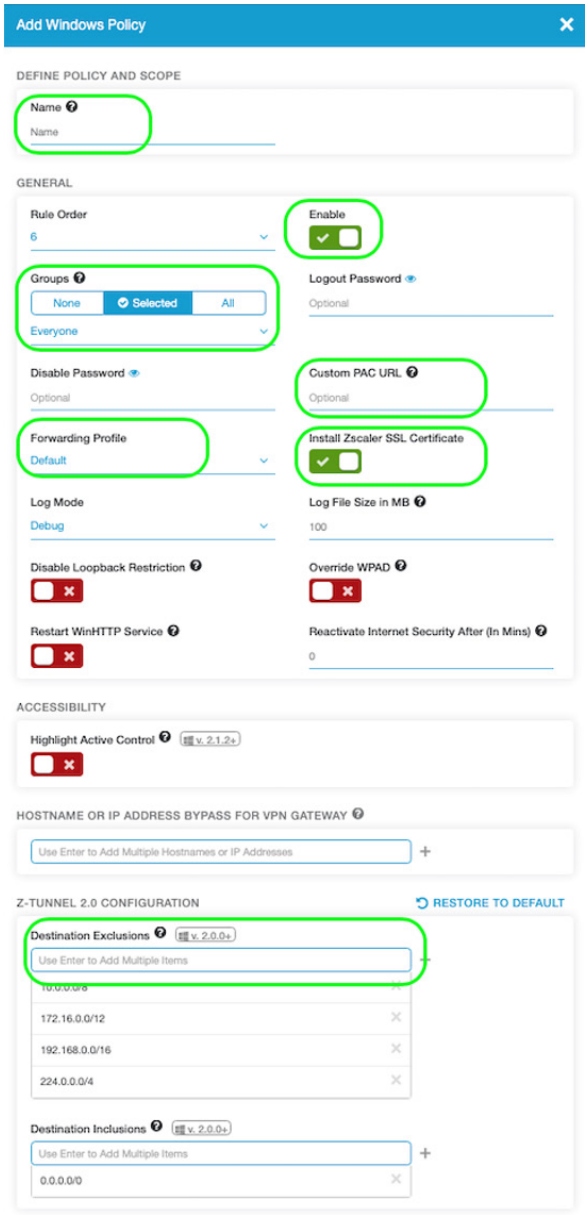

Figure 22. Create an application profile

Zscaler Client Connect on the VM is ready to launch after you deploy it with the appropriate switching: Zscaler Cloud, your customer domain, and any other preferred switches with the appropriate installation switching. See the Client Connector installation instructions link in Zscaler Resources.

©2024 Zscaler, Inc. All rights reserved.

PAC Files

PAC files are used to support explicit proxy deployments in which client browsers are explicitly configured to send traffic to Zscaler. PAC files can be used for HTTP and HTTP traffic.

A PAC file is a text file that instructs a browser to forward traffic to a proxy server, instead of directly to the destination server. It contains JavaScript that specifies the proxy server and, optionally, additional parameters that specify when and under what circumstances a browser forwards traffic to the proxy server.

For example, a PAC file can specify on what days of the week or what hours of the day that traffic is sent to a proxy, or for which domains and URLs that traffic is not sent to a proxy. Zscaler uses macros for proxy selection. The macros used in these examples are `PROXY ${COUNTRY_GATEWAY_FX}` in the APP and Browser PAC, and `PROXY ${ZAPP_TUNNEL2_BYPASS}";` for the forwarding PAC.

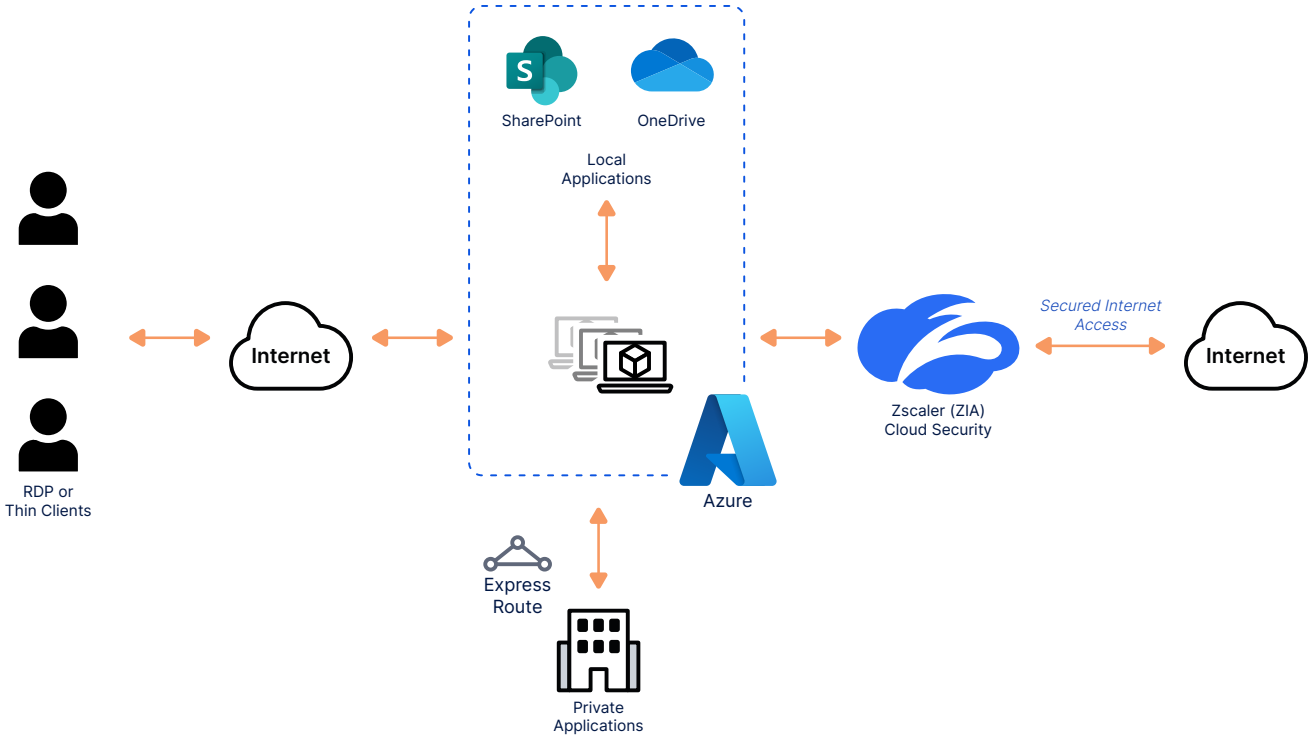

Figure 23. Traffic flow using Proxy Auto-Config (PAC) file

All major browsers support PAC files. Browsers require the address of the PAC file so they can fetch the file from the specified address and execute the JavaScript in the file. PAC files can be hosted on VDI, an internal web server, or a server outside the corporate network. For the Zscaler macros to work, the PAC must be hosted on Zscaler.

The Zscaler service hosts a default PAC file that uses geo-location technology to forward traffic to the nearest Zscaler cloud node. You can also upload custom PAC files to the Zscaler service.

In this document, three PAC files are used in various deployments, each differing in configuration. For the Zscaler Client Connector, think of the PAC file as a configuration file. It is not ever changing and unmanageable as is the reputation of normal browser PAC file use. The primary use case for using the PAC file is to define what IP addresses, URLs, and domains should bypass the Zscaler proxy. Bypasses allow for traffic to stay local or go direct to the defined resources. In the case of WVD, all control traffic and anything that is a local trusted resource stay local to Azure and are not forwarded to or returned from ZIA. However, any resource that is publicly resolvable can be forwarded to ZIA for security.

©2024 Zscaler, Inc. All rights reserved.

For the Pool or Shared VM, you should install a traditional browser PAC file in the browser settings. Depending on the Zscaler connectivity, you might need to use a dedicated proxy port provided by Zscaler and assigned to a specific domain. A dedicated proxy port allows Zscaler to identify any traffic that is received on that unique port and eliminates the initial authentication pop-up and along with integrated Windows authentication allows for transparent authentication and a better user experience. If traffic is received over a tunnel, a dedicated proxy port is not needed.

For Tunnel-1 mode on the Zscaler Client Connector, install an **Application PAC file** in the **App Profile** under the **Custom PAC URL**.

For Tunnel-2 mode on the Zscaler Client Connector, install the application PAC file in the **App Profile** under the **Custom PAC URL** and a **Forwarding Profile PAC** containing the same bypasses in the **APP PAC**. See the following example for the required syntax for each file.

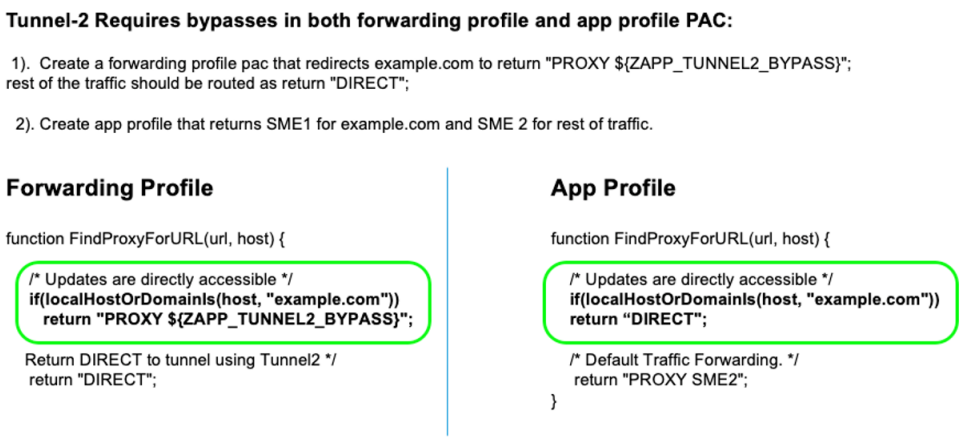

Figure 24. Tunnel-2 PAC file symbiosis

For more information and example PAC files including the Browser PAC, the App PAC, and the Forwarding PAC, see the resources in Zscaler Resources.

©2024 Zscaler, Inc. All rights reserved.

Site-to-Site VPN – IPSec Tunnels

You can use the Azure and the ZIA Admin Portals to create site-to-site VPN gateway connections from Azure to Zscaler. Use the connections to route and secure your internet.

Overview

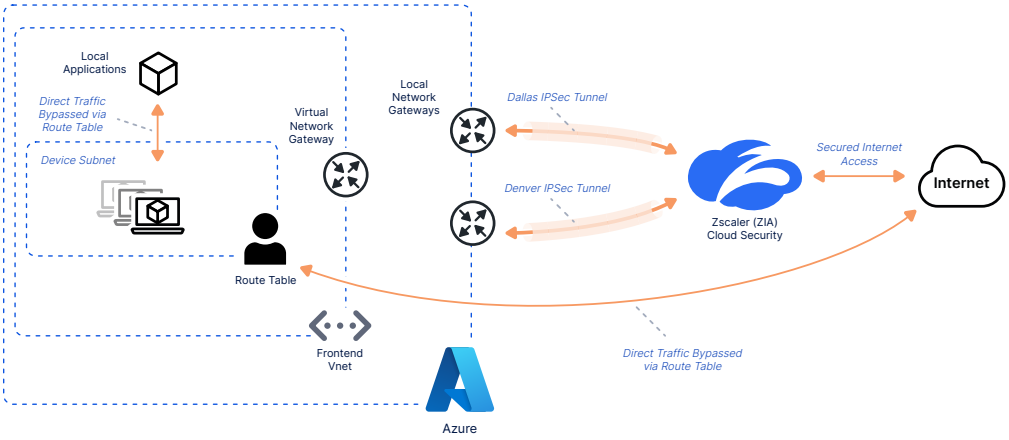

Figure 25. Active-Standby gateway redundancy active-active tunnels (1 of 2)

You can use a site-to-site VPN gateway to connect your Azure virtual network over an IPSec and IKEv2 VPN tunnel to the Zscaler cloud. All internet-bound traffic is then directed through the tunnel using a default route. This configuration uses the Microsoft virtual network gateway, a local network gateway and VPN connection per Zscaler location. A route table is used to direct traffic down the tunnel and to bypass local and unique traffic that must bypass the Zscaler cloud. The native Microsoft features also provide redundancy in case of a failure of one of the components.

©2024 Zscaler, Inc. All rights reserved.

Azure VPN Gateway Redundancy

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance takes over (failover) automatically and resumes the site-to-site VPN connections. The switch over causes a brief interruption. For planned maintenance, the connectivity should be restored within 10 to 15 seconds. For unplanned issues, the connection recovery can be longer, about one to one and a half minutes.

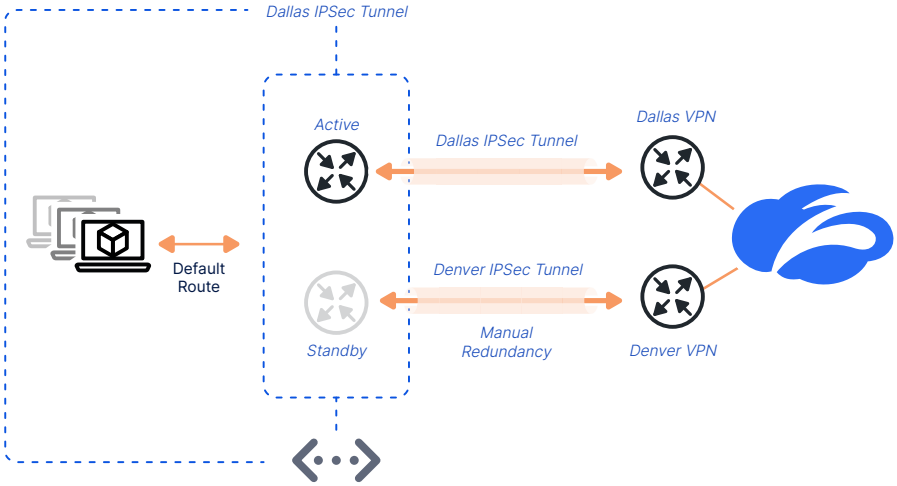

Figure 26. Active-Standby gateway redundancy active-active tunnels (2 of 2)

Both the Azure and Zscaler clouds are highly redundant, and the secondary tunnel is provided only as an example for manual redundancy in case of compliance requirements. The routes switch on the local gateways and use the secondary tunnel. Currently there is no state or health check to remove the primary failed routes in case of a tunnel failure event.

Creating an Azure VPN Gateway

You must add a resource to a VPN gateway in order to attach to Zscaler locations. Select all resources and then select **Add** to start the process of adding a new resource.

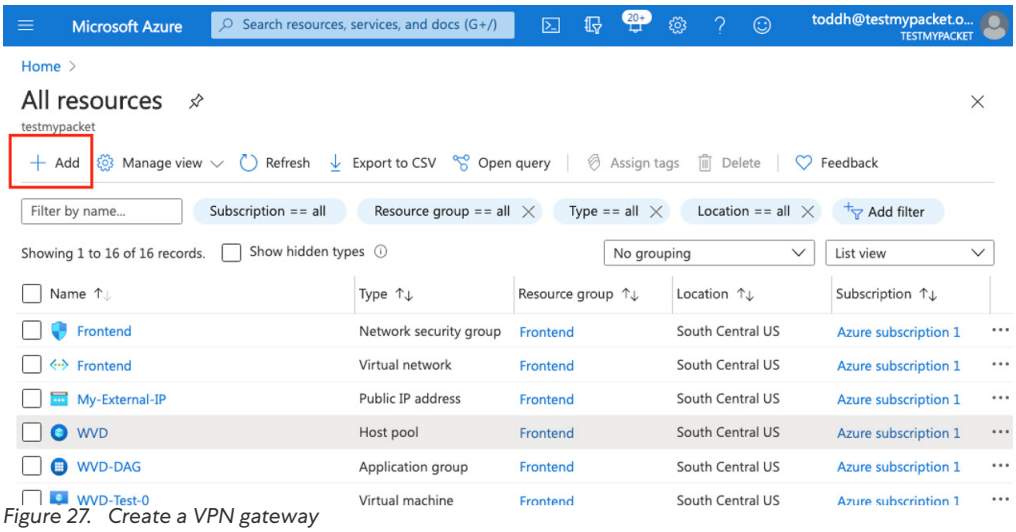

Figure 27. Create a VPN gateway

©2024 Zscaler, Inc. All rights reserved.

Installing the Virtual Network Gateway Application

After selecting **dd**, type `virtual network gateway` in the search field and press enter. This displays the VPN application.

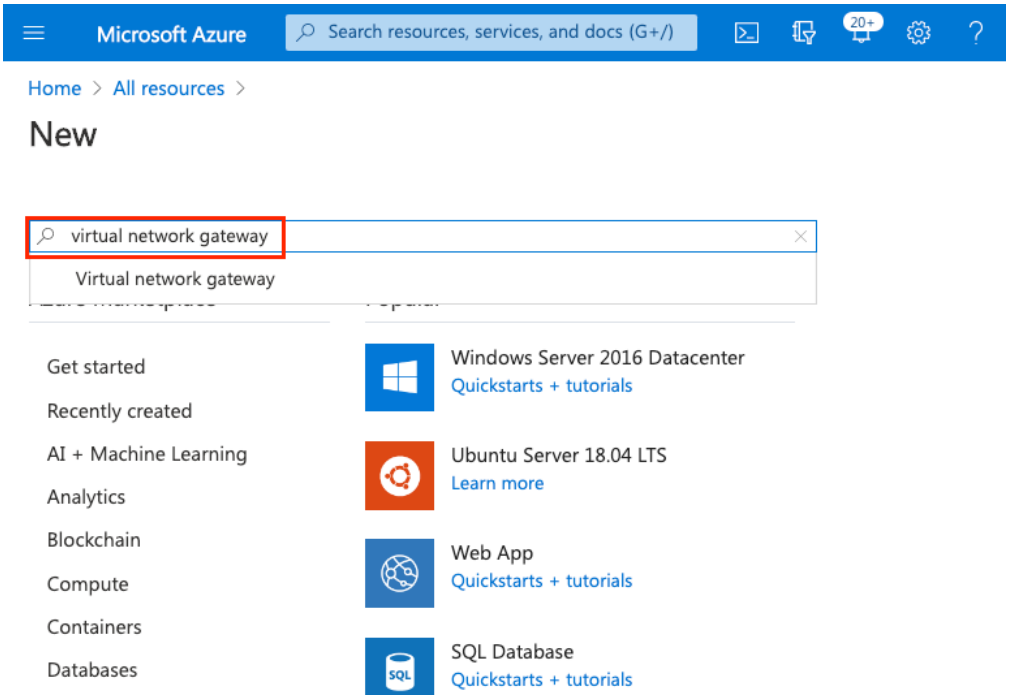

Figure 28. Search for the Resource

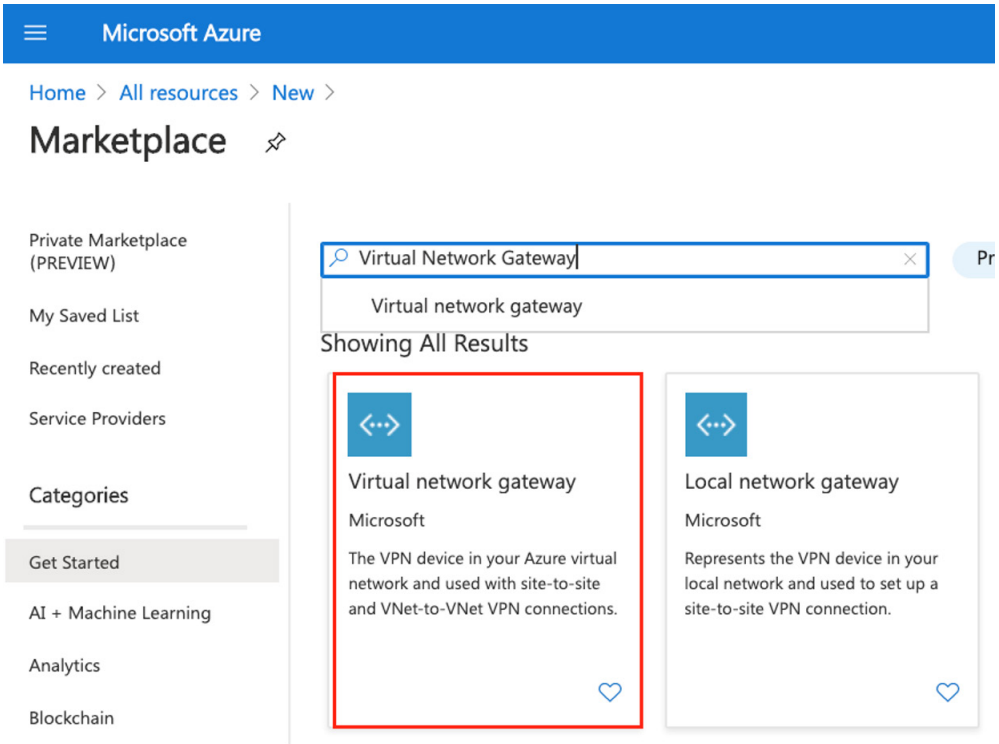

Figure 29. Virtual network gateway

©2024 Zscaler, Inc. All rights reserved.

Select the **Virtual network gateway** to get started with the configuration and then select **Create** to start the installation wizard for the gateway.

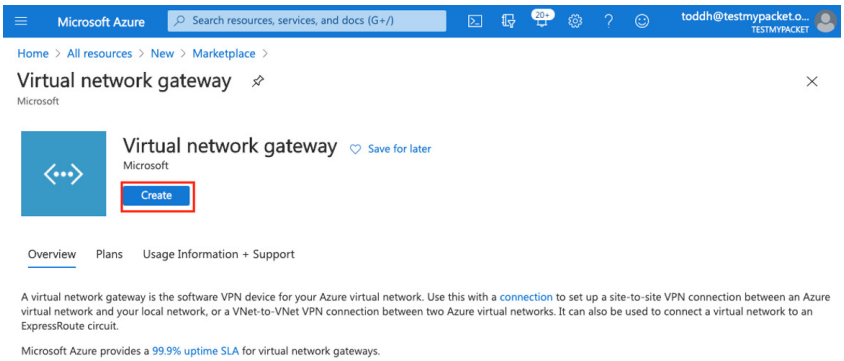

Figure 30. Create the virtual network gateway

Configuring the Virtual Network Gateway Application

To create the virtual network gateway, fill in the required information. Give the gateway a name that is easily identified as the VPN gateway. For this configuration, a Prefix of "A-" is used for all resources associated with this installation. That keeps everything together when you look at the resources created. Select the region for the gateway creation. The region selected is the location of the VNet. Select:

- A **Gateway type** of **VPN**
- A **VPN type** of **Route-based**
- The **Virtual Network** where the gateway is created, and traffic served
- Name the **External Public IP** associated with this gateway

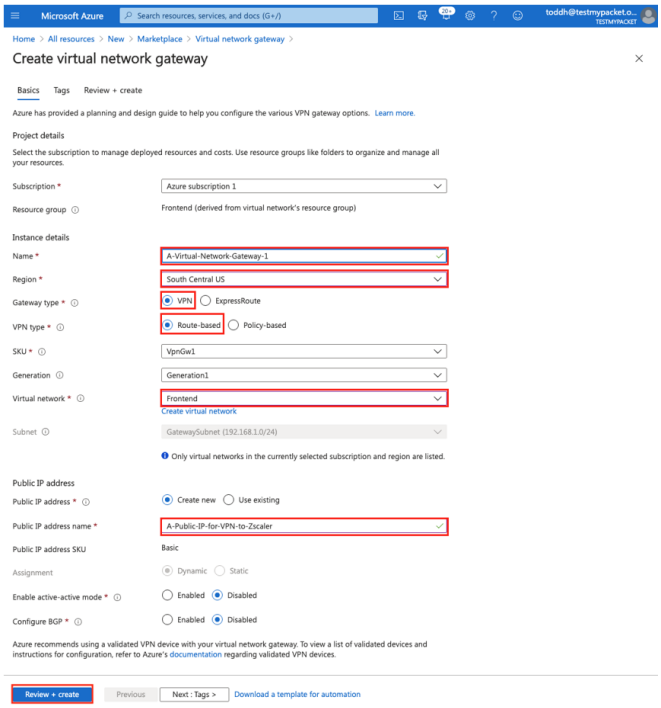

Figure 31. Create an application profile

This IP address is used as part of the VPN credentials and defined as a location in the ZIA Admin Portal. Click **Review and Create** the gateway.

©2024 Zscaler, Inc. All rights reserved.

Gateway Deployment

Deployment of the gateway can take up to 45 minutes to complete. When the gateway is created, a message saying the deployment is complete appears. You can then click **Go to resource** or select the gateway from the **All resources** page. The following procedures start from **All resources**.

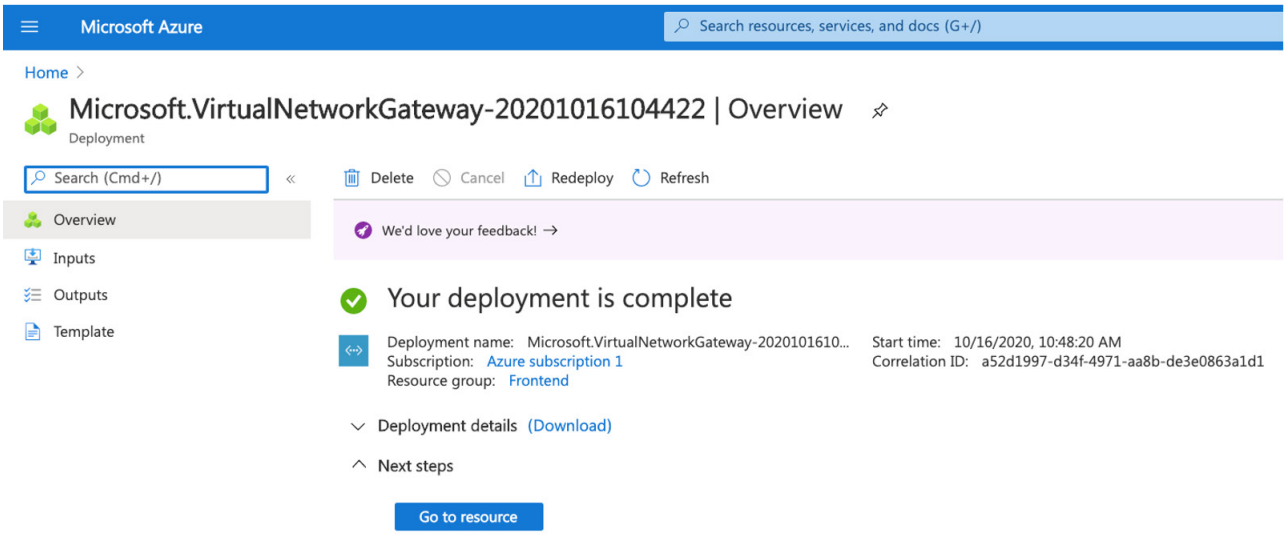

Figure 32. Deployment of the VPN gateway

Configuring the Virtual Network Gateway

From the **All resources** page, select the newly created **Virtual network gateway**. This brings up the gateway details and allows you to create the additional components.

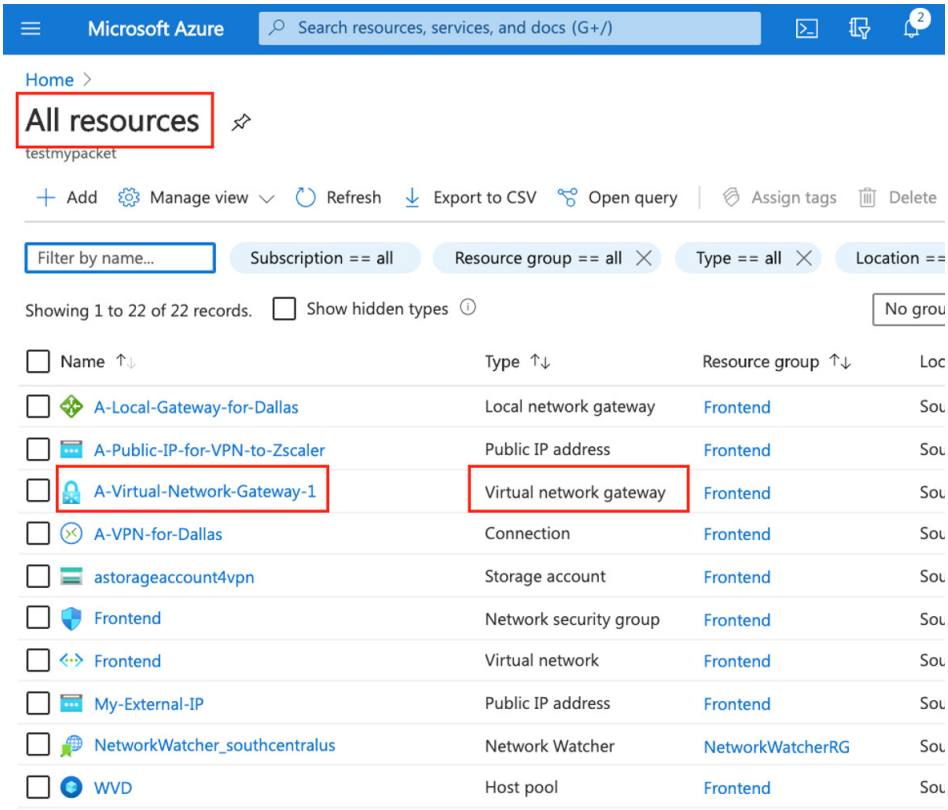

Figure 33. All resources

©2024 Zscaler, Inc. All rights reserved.

Adding Connections to the Gateway

To create a VPN connection to Zscaler, you need to create a VPN connection for each location you plan to connect to. The following example shows a connection to Dallas, and to Denver for redundancy.

Select **Connection** and then **Add**. This brings up the **Connection Wizard**.

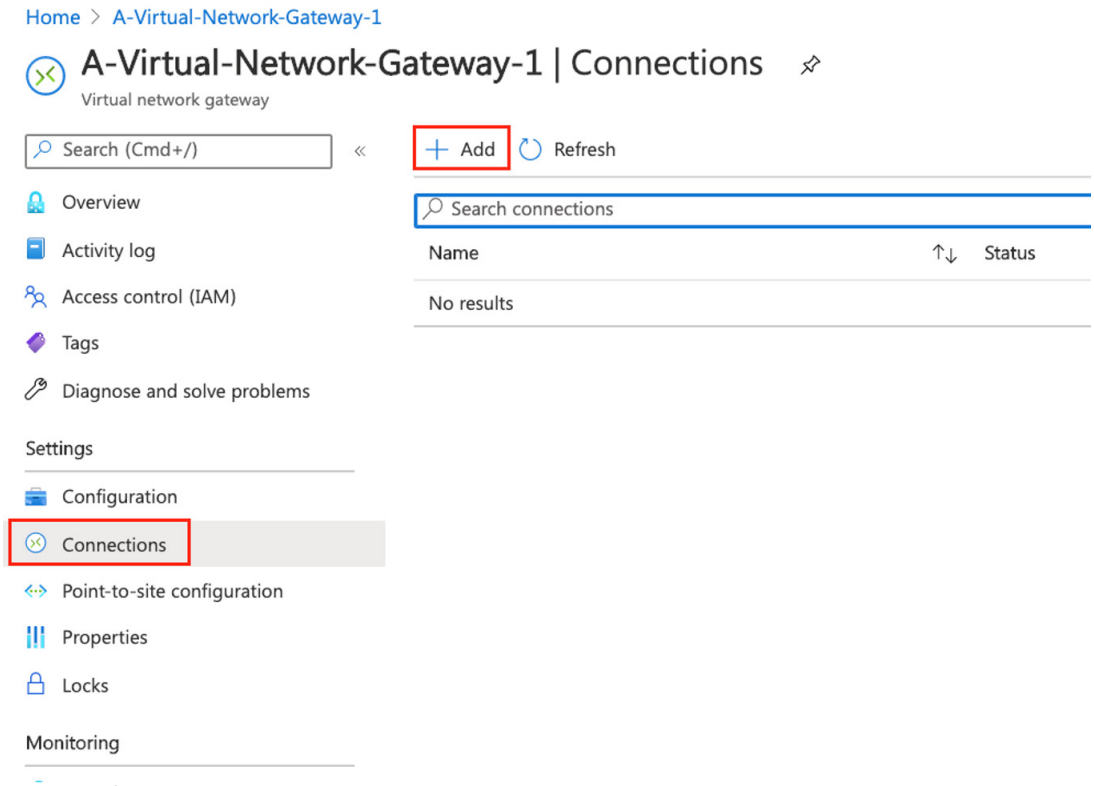

Figure 34. Creating connections

©2024 Zscaler, Inc. All rights reserved.

Configuring the Virtual Network Gateway

In the **Add Connection** wizard:

1. Enter a **Name** that identifies the connection.
2. Select a **Connection type** of Site-to-site (IPSec). The virtual network gateway should be pre-populated with the gateway you just created.
3. Enter the **Shared key (PSK)** that is used by the Zscaler setup as part of the VPN credentials.
4. Select **IKEv2**.
5. Select the arrow (**>**) next to the Local network gateway to start the wizard and create the local gateway that represents the Zscaler VPN.

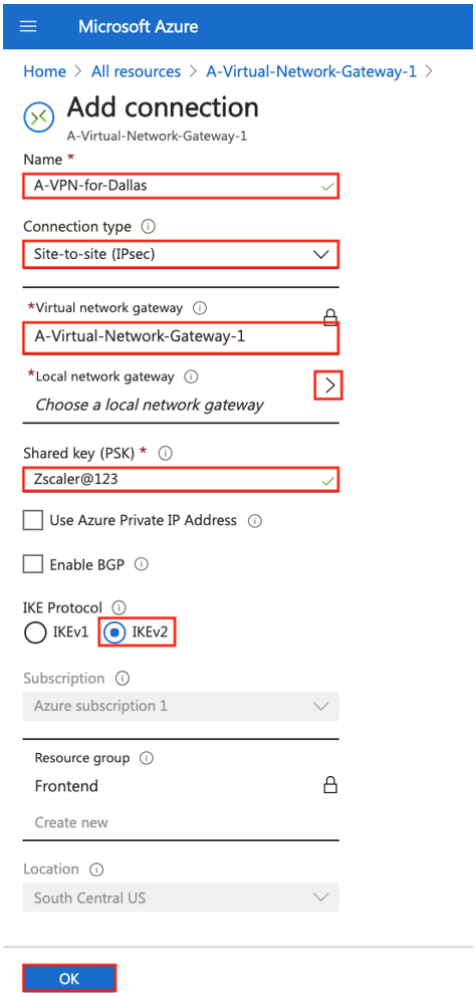

Figure 35. Create a VPN connection

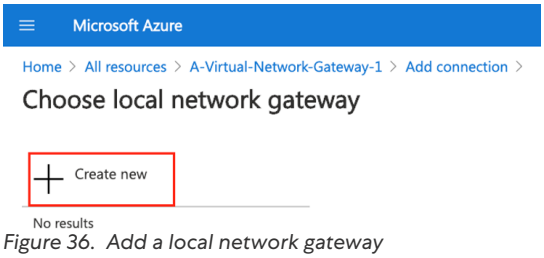

Figure 36. Add a local network gateway

©2024 Zscaler, Inc. All rights reserved.

After the wizard has launched:

1. Select **Create new** to create a new local gateway.
2. Give the gateway an intuitive **Name** that identifies it as a VPN to a Zscaler location.
3. Select an **Endpoint** of **FQDN**. The fully qualified domain name (FQDN) is selected from the Zscaler list of VPN hostnames for your cloud. (Zscaler Three Cloud is used for this example, but your cloud could be any of the Zscaler clouds.)

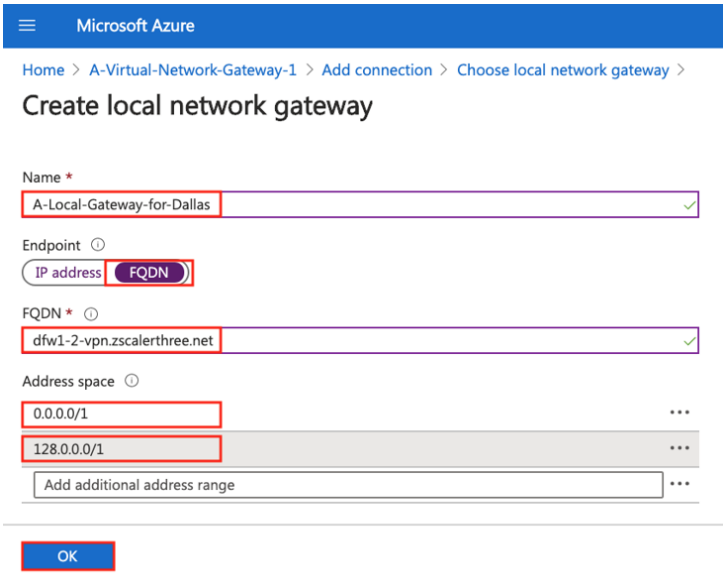

Figure 37. Create a local network gateway

The following sections describes how to identify your Zscaler cloud and the VPN Host as the FQDN.

Identify the FQDN for the VPN

To identify your Zscaler cloud, select **Administration**, and then **Company profile** from the Zscaler UI. Your cloud is identified as the prefix of your company ID.

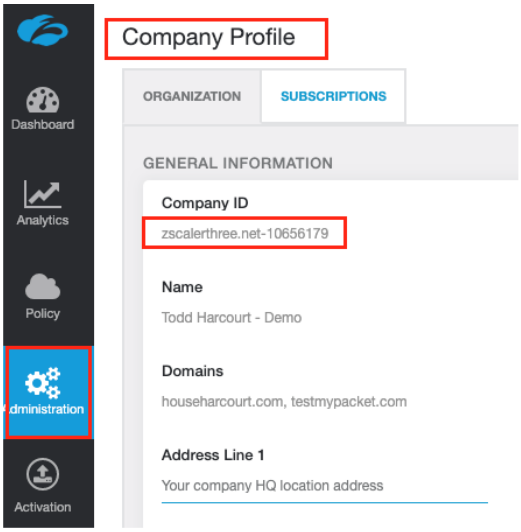

Figure 38. Your Zscaler cloud

©2024 Zscaler, Inc. All rights reserved.

Go to the URL for your Zscaler cloud service, e.g., `https://yourzscalercloudnamehere.net/cenr`. Select the VPN Host Name for the location that you want the VPN tunnel to terminate at. In the following example, `dfw1-2-vpn.zscalerthree.net` is the Zscaler Dallas location. Enter the name as the FQDN in the Azure gateway setup.

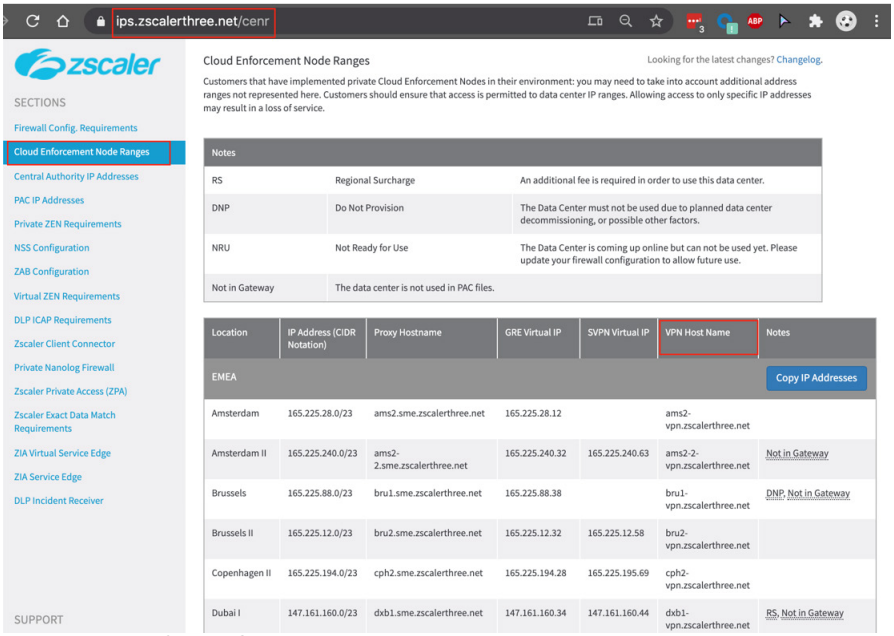

Figure 39. Identify the FQDN

Finish the Local Gateway Setup

After identifying the name of the VPN host, enter the name in the FQDN field. In **Address space**, enter the IP address or indicate which local gateway provides access. Address space entries are the destination IP addresses. In this case, it is the internet or all IP addresses in CIDR block format.

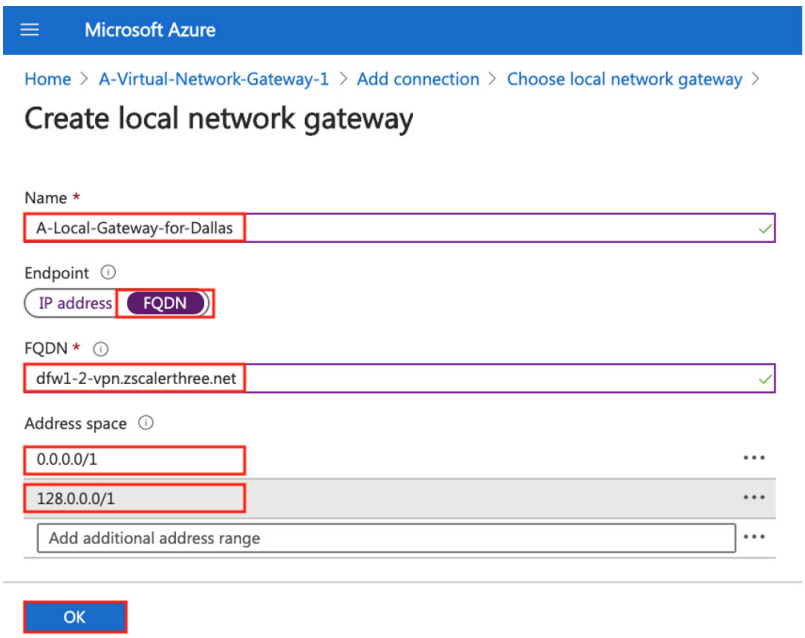

Figure 40. Create a local network gateway

You can't enter 0.0.0.0/0, but you can break up the address into two entries of **0.0.0.0/1 and 128.0.0.0/1** as the address space. Click **OK** to finish the local gateway configuration.

©2024 Zscaler, Inc. All rights reserved.

Finish the Virtual Network Gateway Setup

After the creation of the local gateway, you are returned to the **Virtual network gateway** wizard, which is now finished. Click **OK** to finish the configuration.

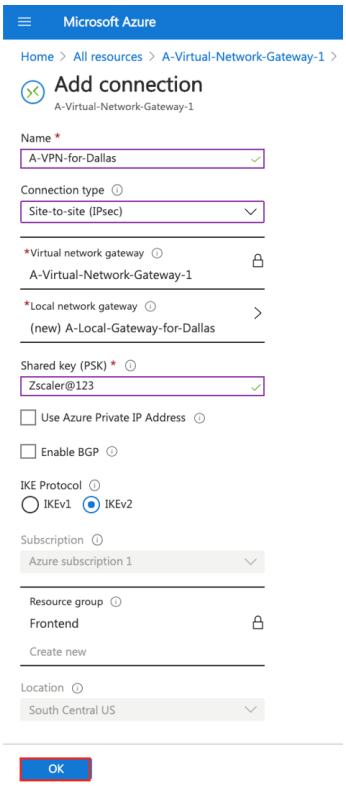

Figure 41. Create a connection

Configure the IPSec Parameters

Set the IPSec configuration parameters on the connection:

1. Select **All resources**.
2. Select the **Connection** that was just created.

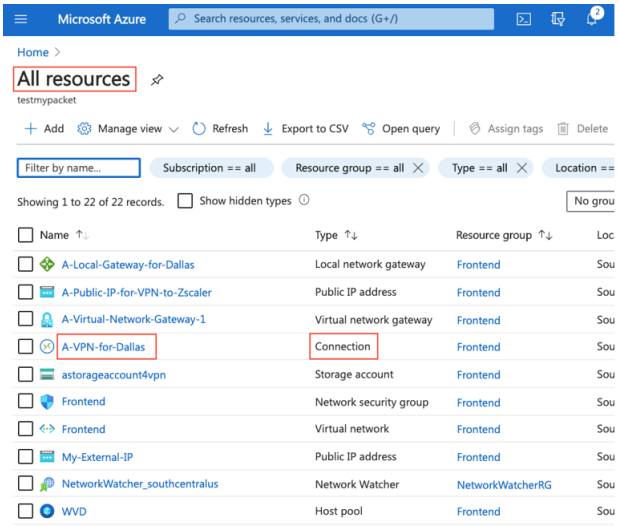

Figure 42. Select the connection

©2024 Zscaler, Inc. All rights reserved.

This opens the **Connection** screen. Select **Configuration** to bring up the configuration screen.

1. Under **IPsec / IKE policy**, select **Custom**. This opens the IPSec parameters. For **IKE Phase 1** set:
   - **Encryption** to **AES256**.
   - **Integrity** and **PRF** to **SHA256**.
   - **DH Group** to **DHGroup14**.
2. For **IKE Phase2 (IPsec)**, set:
   - **IPSec Encryption** to **none (Null Encryption)**.
   - **Integrity** to **SHA256**.
   - **PFS Group** to **none**.
3. Then select **Save**.

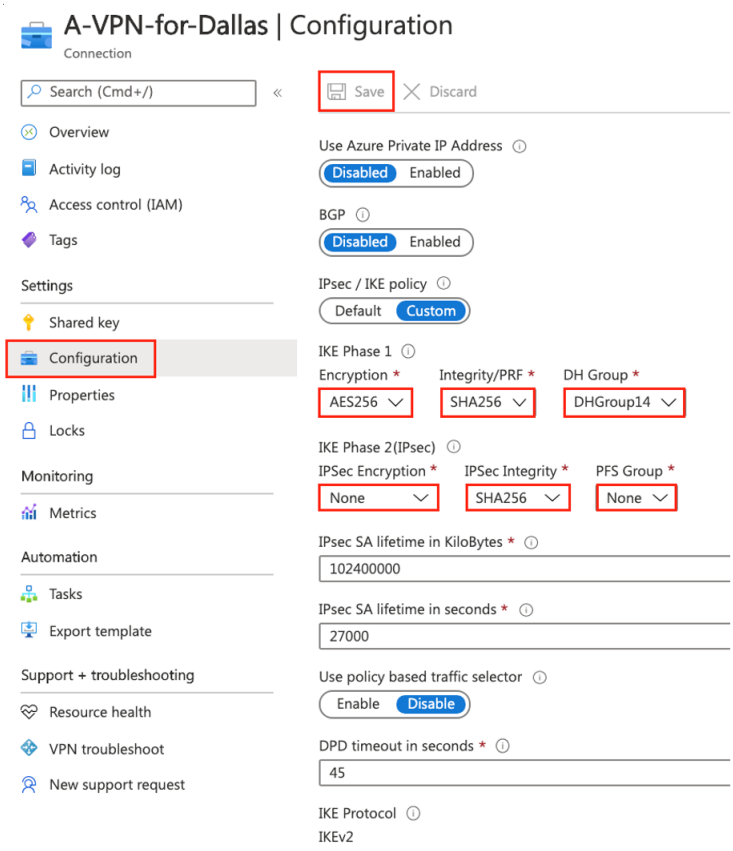

Figure 43. Customizing IPSec

©2024 Zscaler, Inc. All rights reserved.

Identify the Public IP Address

You must identify the public IP address used before you can connect to Zscaler in order to create the VPN credentials and specify the location that identifies the inbound traffic.

1. Select **All resources**.
2. Select the **Public IP Address** object created previously. The IP address is located on the right side of the parameter screen.
3. Copy the address and move to the next section to open a support ticket with Zscaler to have the address added as an identified IP address.

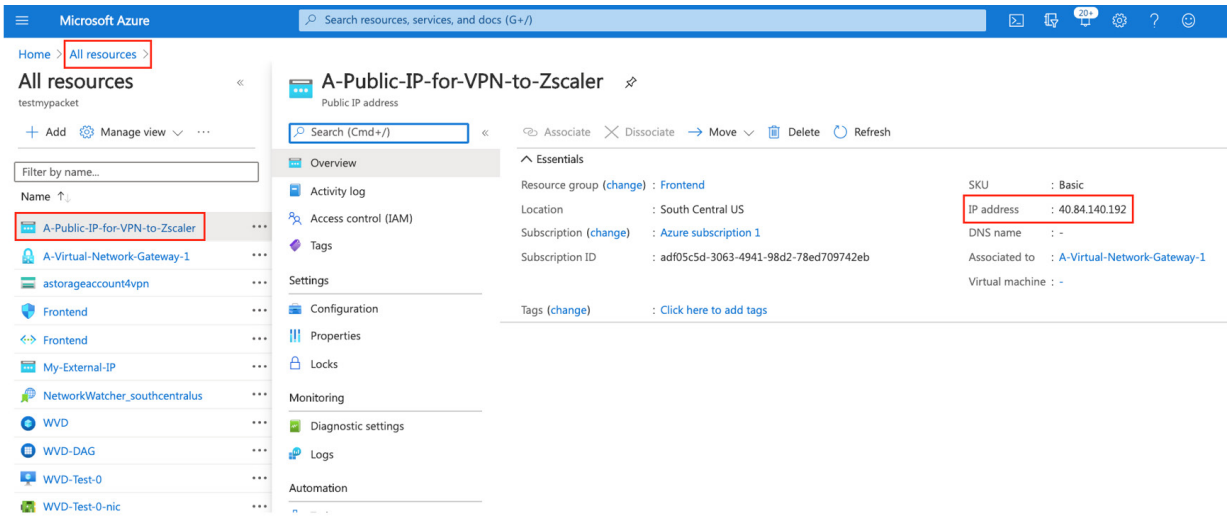

Figure 44. Identify the external IP address

Configuring Zscaler

Submit a Zscaler Ticket to Add the IP Address to your Zscaler Account

Zscaler support must provision the IP address saved from the previous step. From the ZIA Admin Portal, select the question mark (**?**) at the bottom left of the portal screen. Then select **Submit a Ticket**. This opens the **Submit a Case** page.

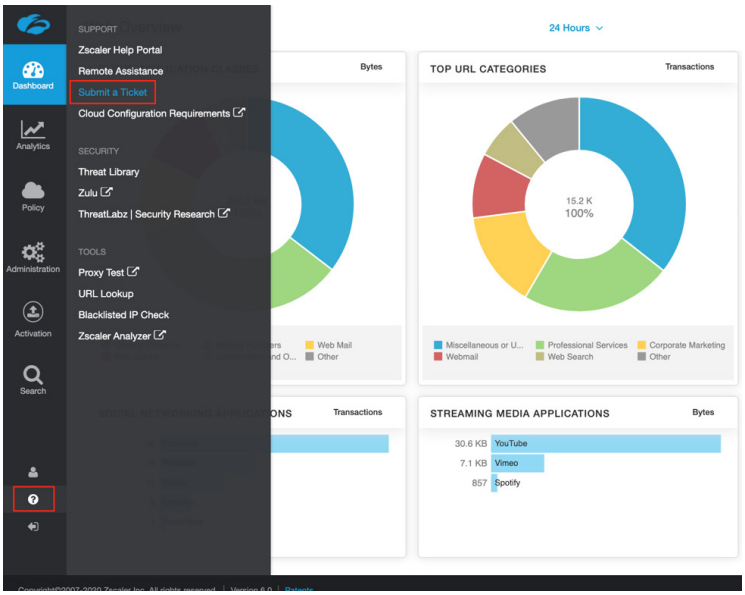

Figure 45. Submit a provisioning ticket

©2024 Zscaler, Inc. All rights reserved.

Fill in the fields to have the IP address added to the Zscaler tenant and select **Submit**.

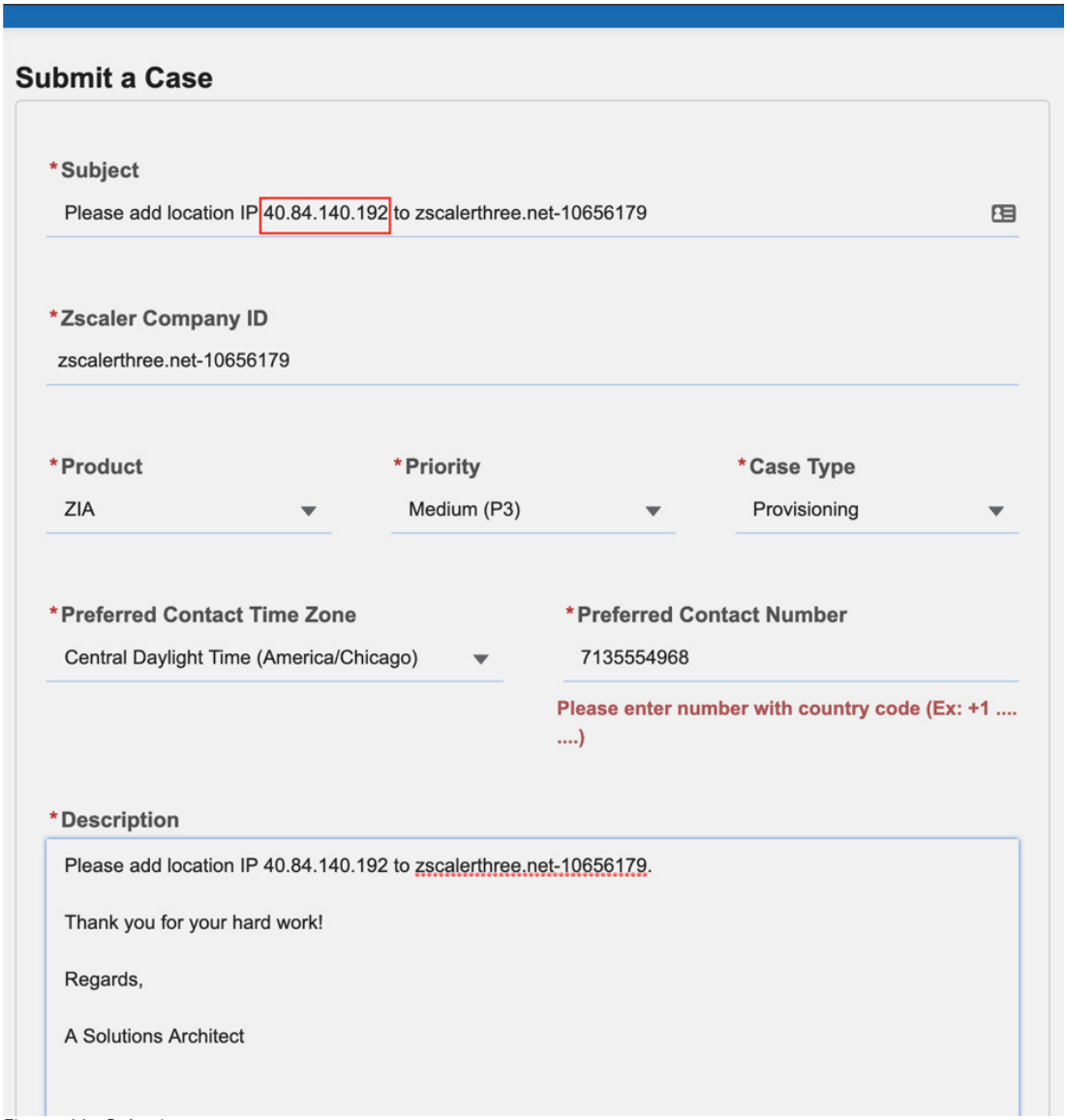

Figure 46. Submit a case

©2024 Zscaler, Inc. All rights reserved.

Create VPN Credentials

After you get confirmation that the IP has been added successfully, create the **VPN Credentials** and the **Location**.

1. Select **Administration** and then select **VPN Credentials**.

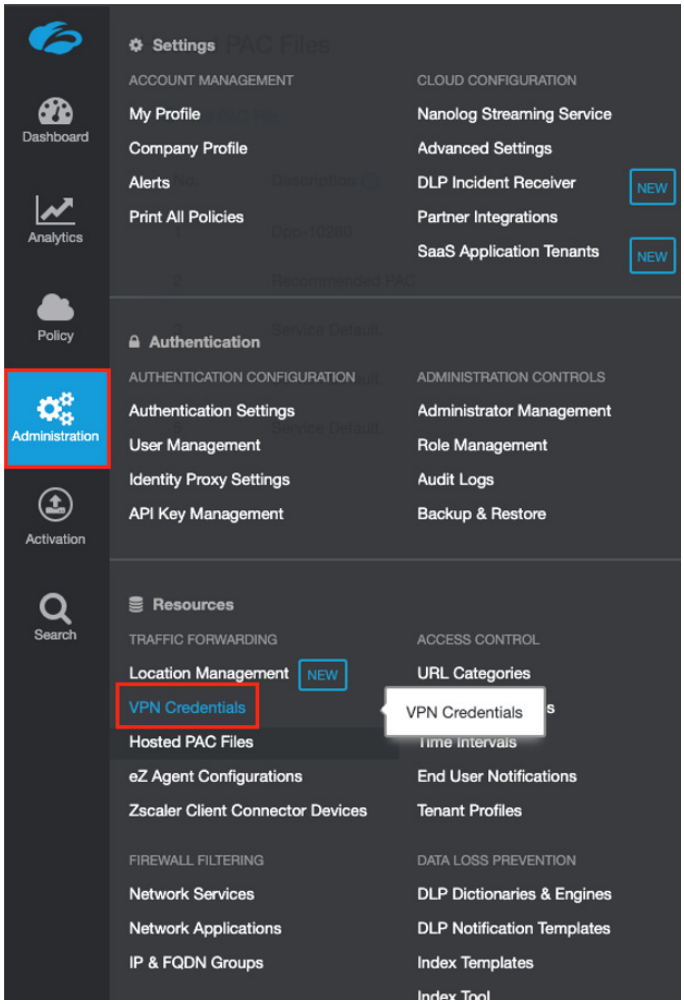

Figure 47. Create VPN credentials

2. Select **Administration** and **Add VPN Credentials**, which opens the **Add VPN Credential** screen.

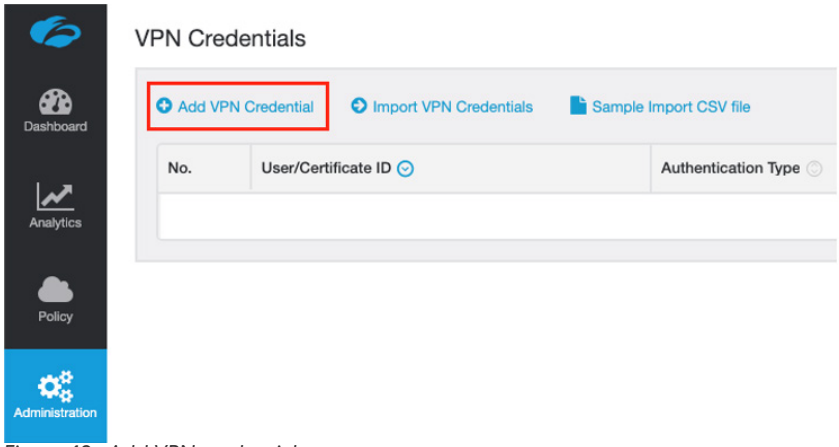

Figure 48. Add VPN credentials

©2024 Zscaler, Inc. All rights reserved.

3. Select **IP** and then select the **IP address** just added from the drop-down menu.
4. To complete the configuration, enter the **Shared Key (PSK)** created in Configuring the Virtual Network Gateway.
5. Click **Save**.

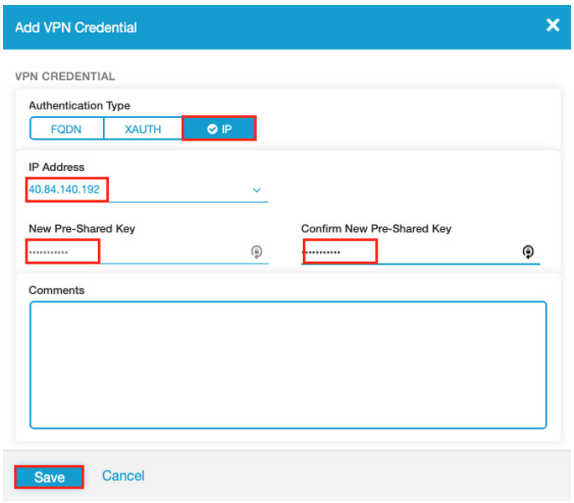

Figure 49. Create VPN credentials

Adding a Zscaler Location

You must create a location to terminate the IPSec VPN connection:

1. Select **Administration**.
2. Select **Location Management**.

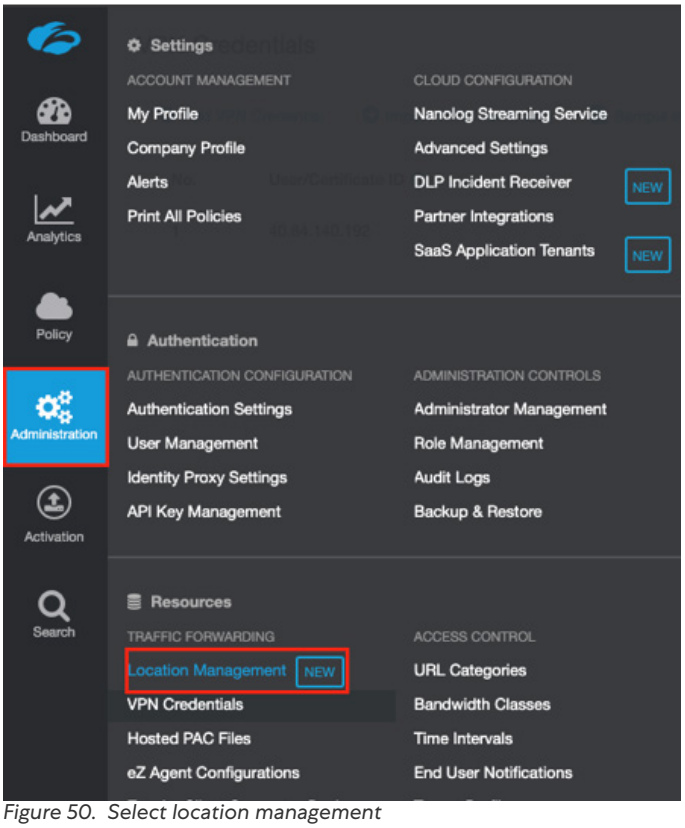

Figure 50. Select location management

©2024 Zscaler, Inc. All rights reserved.

3. Then select **Add Location**. This opens the **Add Location** screen.

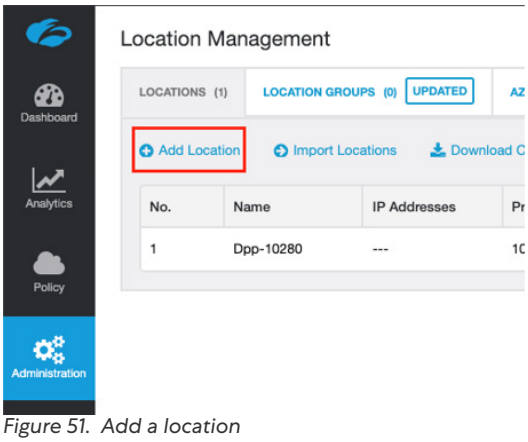

Figure 51. Add a location

Location Parameters

In the **Add Location** screen:

1. Enter an intuitive **Name** for the VPN tunnel.
2. Enter the **Country, City, State, Province**, and **Time-Zone information**.
3. Select the **Azure Public IP address** from the **Static IP Address** drop-down menu and the **VPN Credentials** created in the previous step.
4. Select the **Gateway Options** to enforce on the VPN connections.
5. Click **Save**.

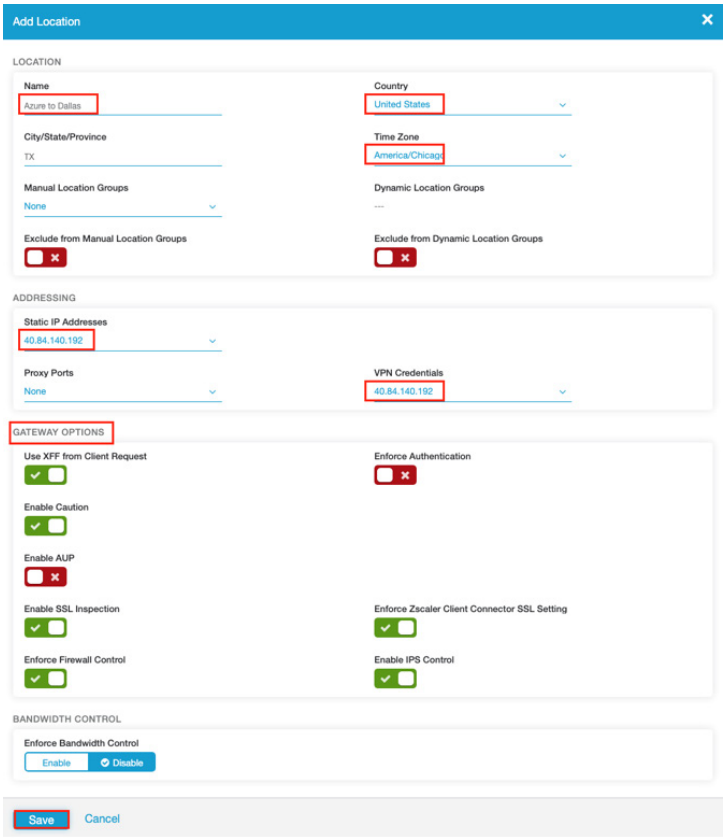

Figure 52. Create a location

©2024 Zscaler, Inc. All rights reserved.

Check the Status of the VPN Connection

To check the status of the VPN connection with tunnel insights select **Analytics** and **Tunnel Insights** from the ZIA Admin Portal. This brings up the Insights selection screen.

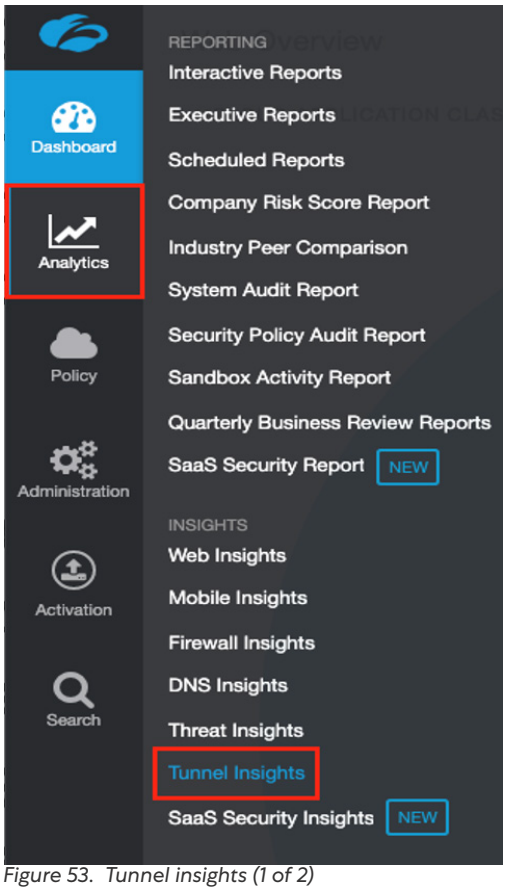

Figure 53. Tunnel insights (1 of 2)

Identify the Public IP Address

To check the VPN tunnel status, filter the logs to find the **Tunnel Status**. Depending on your installation you might need to provide additional filters to narrow down the logs.

In this example, this is the first tunnel. Select **Logs** at the top of the filter selections and then select a **Timeframe** to display. In the example, you can see the IPSec tunnel is now up. If no logs are displayed, or the logs show an error, revisit all of the configuration steps (or open a support ticket with Zscaler).

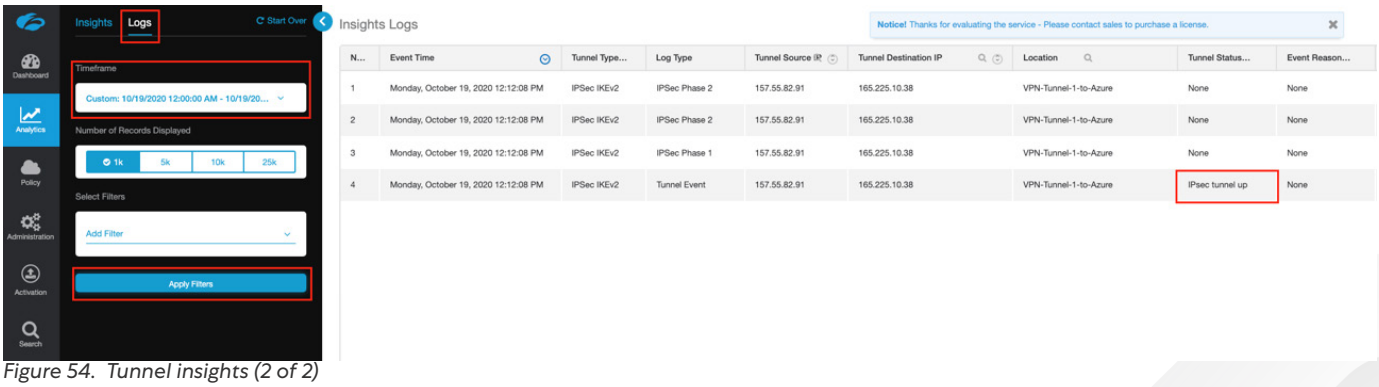

Figure 54. Tunnel insights (2 of 2)

©2024 Zscaler, Inc. All rights reserved.

Create a Redundant VPN Connection for Manual Fail-over

To create a redundant connection, repeat the steps that you followed to create a connection bound to the virtual network gateway. From **All resources**, select the **Virtual network gateway**.

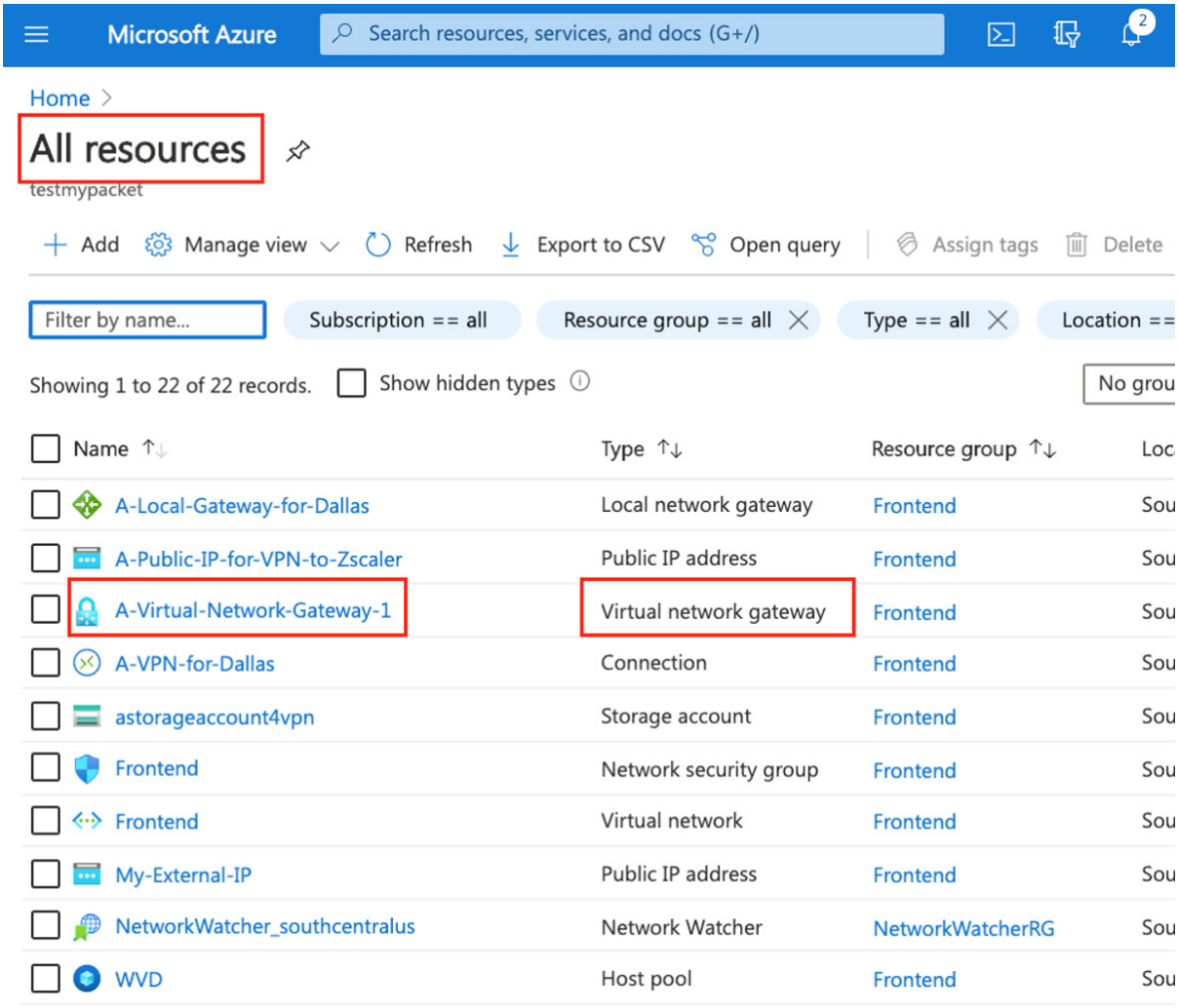

Figure 55. The virtual network gateway

©2024 Zscaler, Inc. All rights reserved.

Select **Connections** and then **Add**. This brings up the **Add Connection** screen.

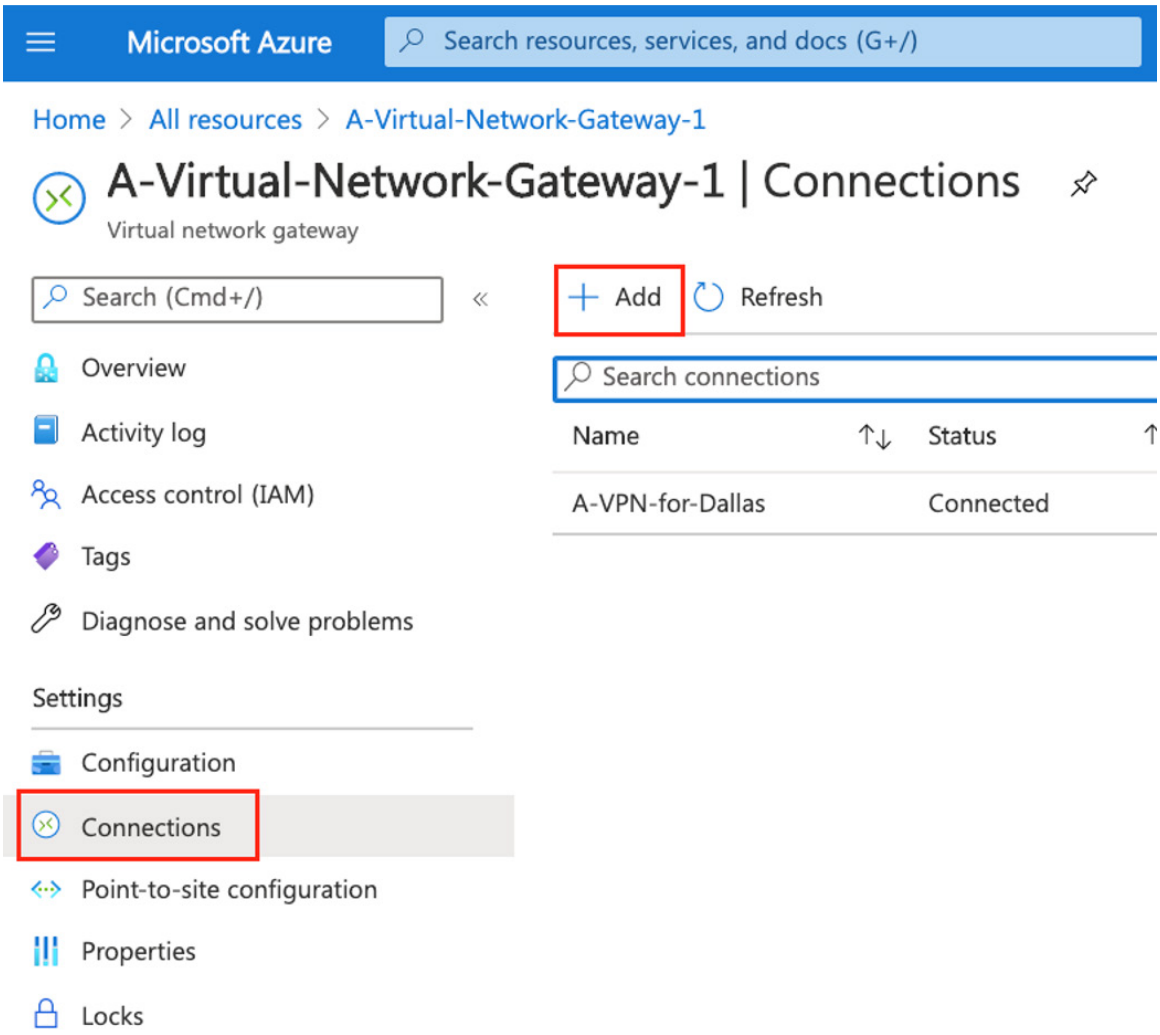

Figure 56. Add a connection

©2024 Zscaler, Inc. All rights reserved.

In the **Add Connection** wizard:

1. Give the connection a **Name** that identifies the connection.
2. Select a **Connection type** of **Site-to-site (IPsec)**. The virtual network gateway pre-populates with the gateway you just created.
3. Enter your **Shared key (PSK)** that is used as part of the VPN credentials configured on the Zscaler setup.
4. Select **IKEv2**.
5. Select the **arrow (>)** next to the **Local network gateway** to start the wizard to create the local gateway that represents the Zscaler VPN.

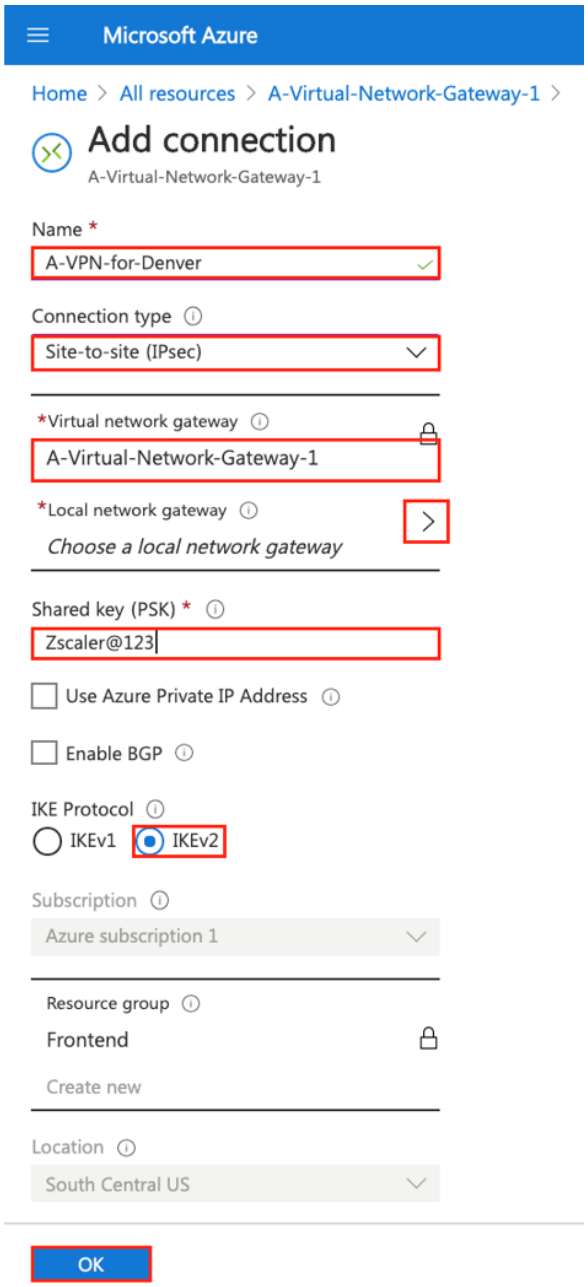

Figure 57. Configure the connection

©2024 Zscaler, Inc. All rights reserved.

In the wizard:

1. Select **Create new** to create a new local gateway.
2. Give the gateway an intuitive **Name** identifying it as a VPN to a Zscaler location.
3. Select an **Endpoint of FQDN**. The fully qualified domain name (FQDN) is selected from the Zscaler list of VPN hostnames for your cloud.
4. Repeat the steps you completed in Identify the FQDN for the VPN.

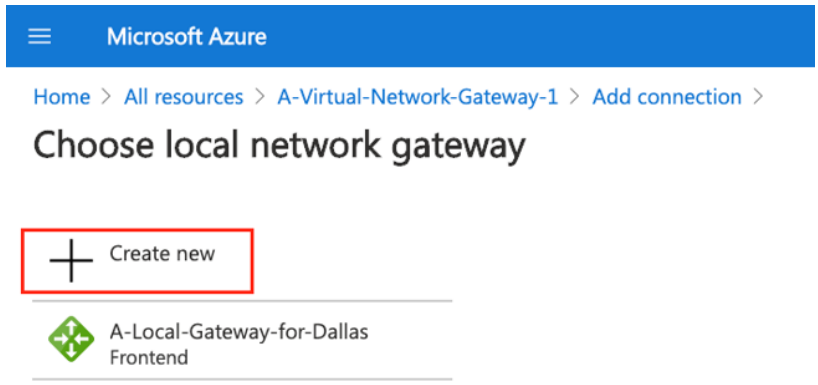

Figure 58. Create a local gateway

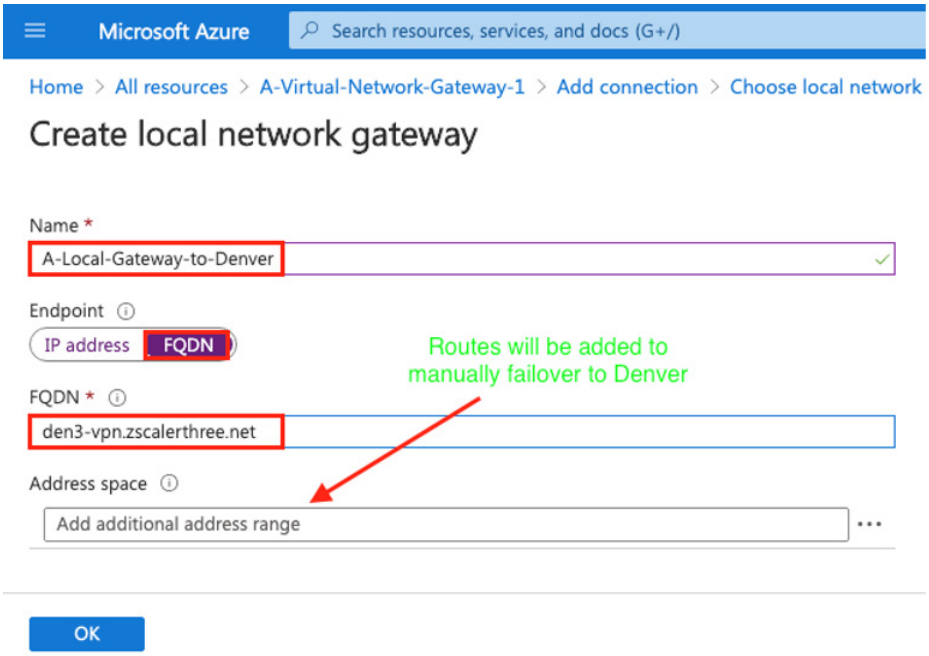

Figure 59. Configure the local gateway

In the **Virtual Network Gateway** wizard, select **OK** to finish the configuration.

You can manually add routes to the address space and remove routes from the other local network gateway to force redundancy in case of catastrophic failure.

©2024 Zscaler, Inc. All rights reserved.

Set the IPSec VPN Parameters

You need to set the IPSec configuration parameters on the connection:

1. Select **All resources** and then select the **Connection** that you just created. This opens the **Connection** screen.

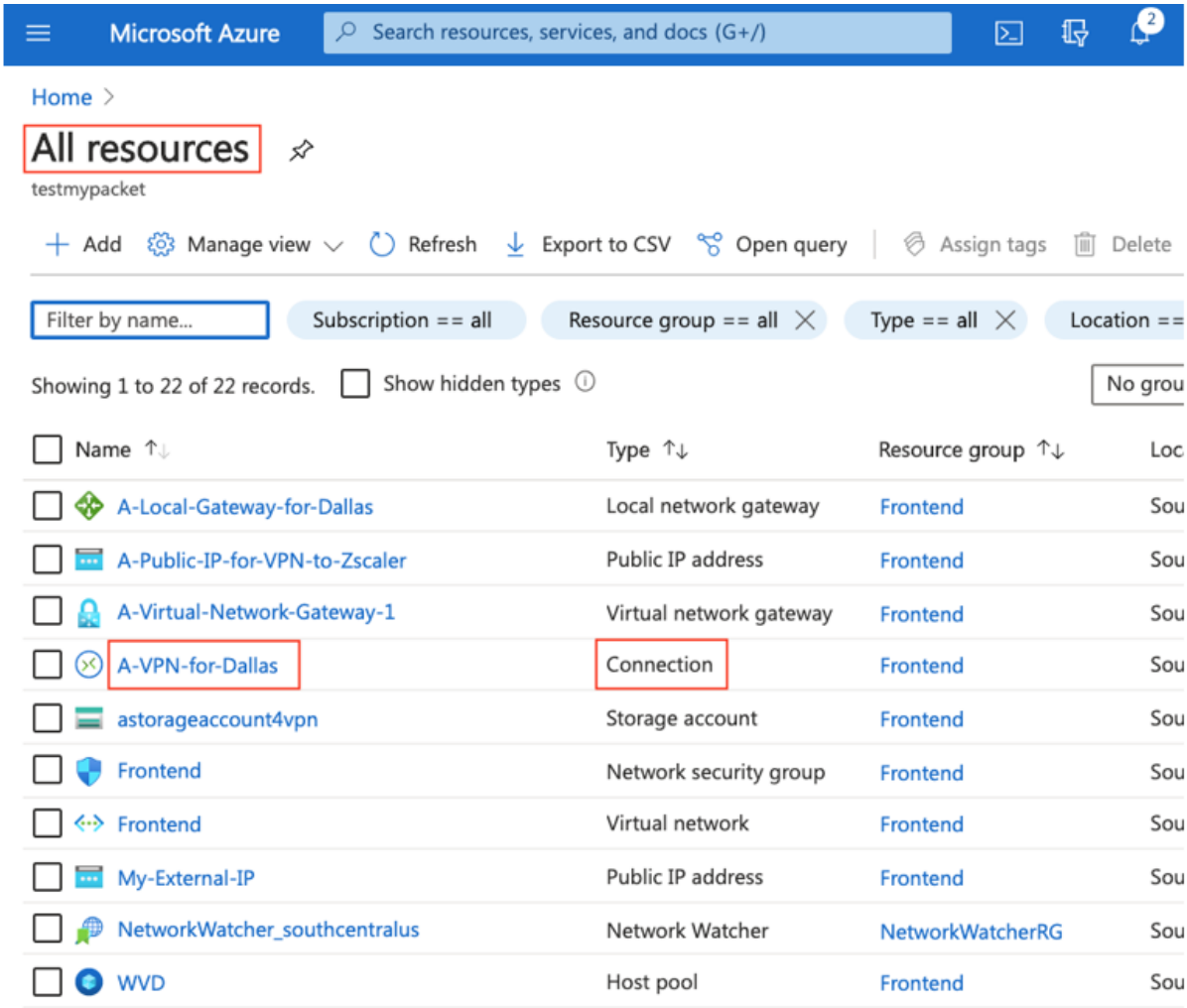

Figure 60. Select the connection

©2024 Zscaler, Inc. All rights reserved.

2. Select **Configuration** to bring up the configuration screen.
3. Under **IPsec / IKE policy**, select **Custom** to reveal the IPSec parameters. For **IKE Phase 1** set:
   - **Encryption** to **AES256**
   - **Integrity** and **PRF** to **SHA256**
   - **DH Group** to **DHGroup14**

   For **IKE Phase2 (IPsec)**, set:
   - **IPSec Encryption** to **none (Null Encryption)**
   - **IPSec Integrity** to **SHA256**
   - **PFS Group** to **none**
4. Click **Save**.

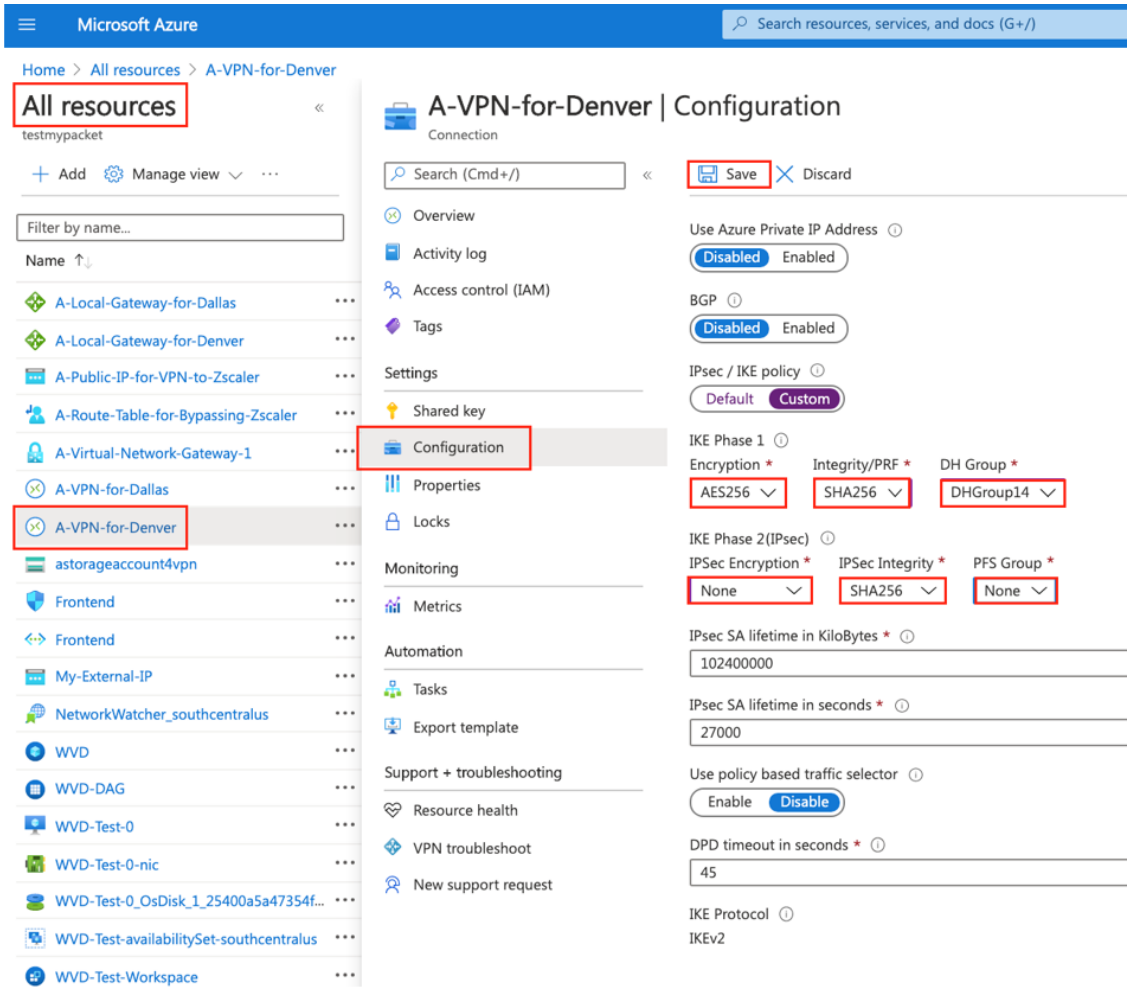

Figure 61. Configure IPSec parameters

You have finished the configuration of the redundant VPN connection. The final step required to complete installation is to create a Route Table.

©2024 Zscaler, Inc. All rights reserved.

Create a Route Table

You need to create a route table and assign the route table to the subnets that send traffic to Zscaler. The route table controls the flow of local traffic in Azure, controlling any internet traffic that needs to bypass Zscaler. The default action is to forward traffic to Zscaler.

To create a route table from all resources:

1. Select **Add**.

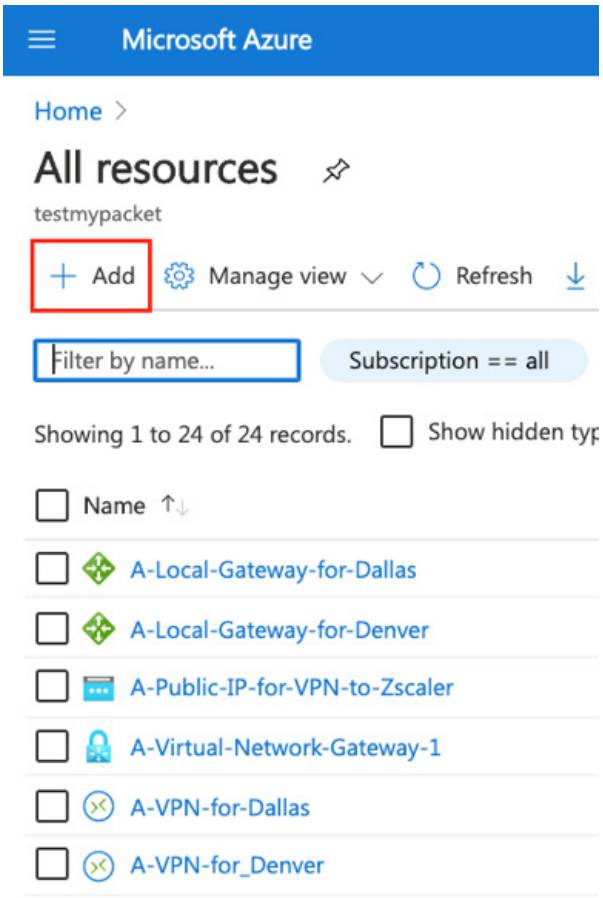

Figure 62. Add a resource

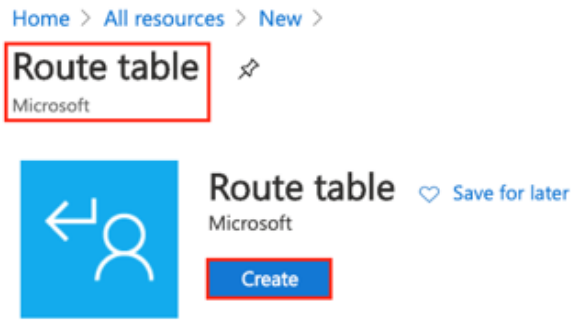

Figure 63. Create an application profile (1 of 2)

©2024 Zscaler, Inc. All rights reserved.

2. Configure the route table's basic features. Select:
   - The **Resource group** containing the subnets that must have traffic directed away from Zscaler.
   - The **Region** for the route table. Provide and intuitive name for the resource.
3. Select **No** to **Propagate gateway routes** to control the routes that are applied to the subnet.

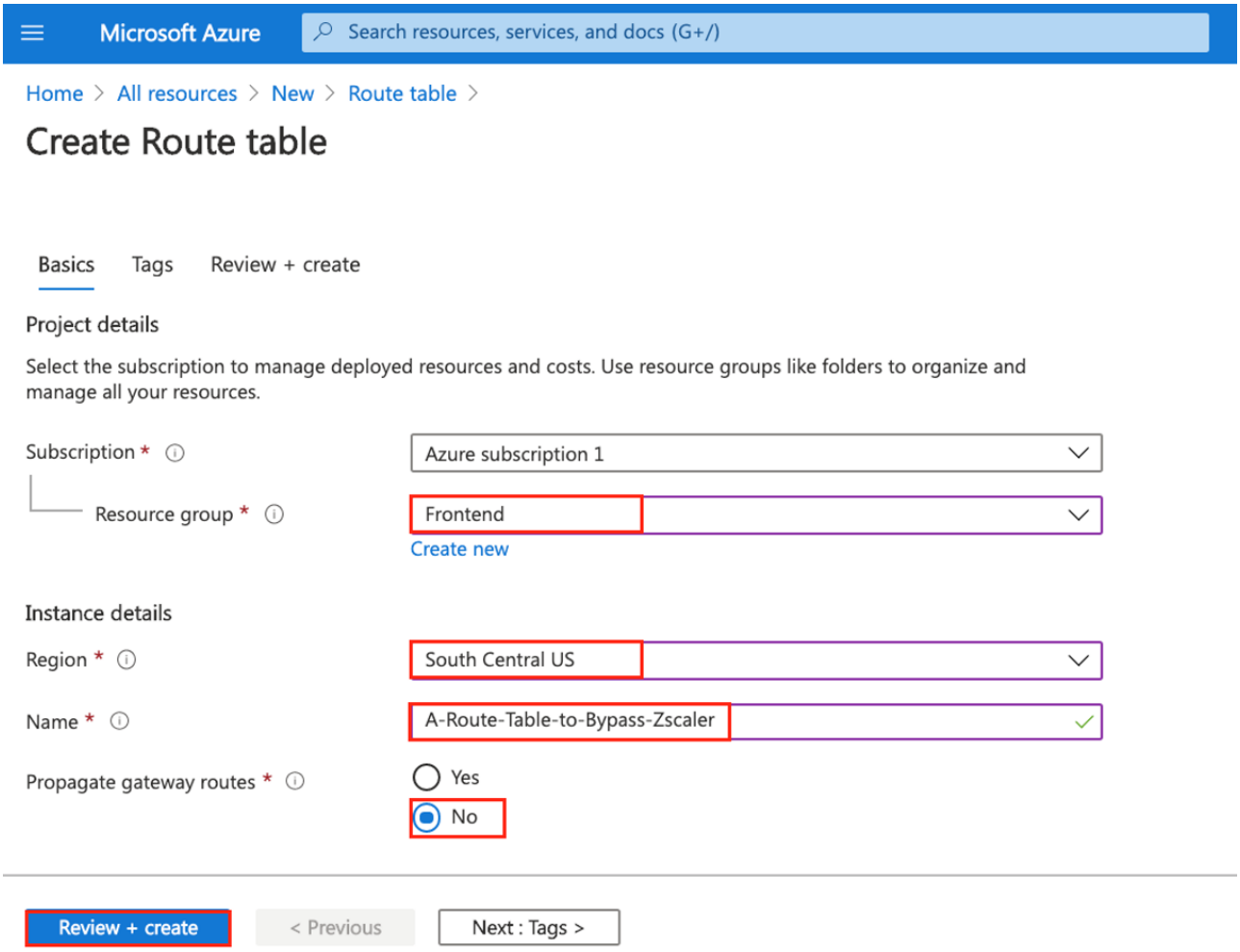

Figure 64. Create an application profile

©2024 Zscaler, Inc. All rights reserved.

Configure the Route Table

To configure the details of the route table, from **All resources**, select the **Route Table** that was just created. This brings up the route table configuration screen.

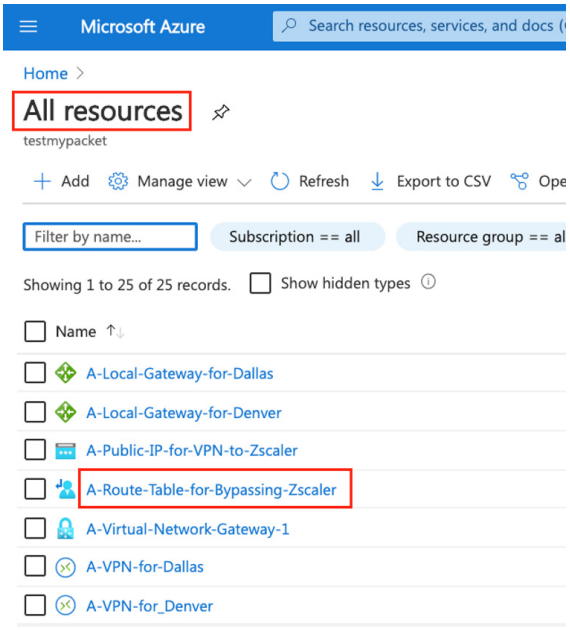

Figure 65. Select the route table to edit

To create the needed bypass routes, select **Routes** on the left, and then select **Add** to bring up the **Add route** screen.

Adding Routes

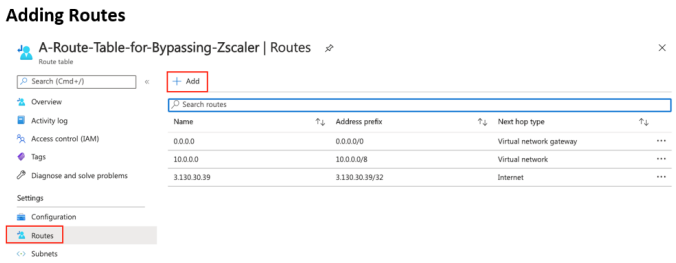

Figure 66. Add routes

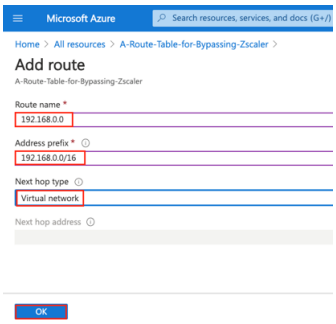

Figure 67. Creating a bypass route

Local traffic that must stay local or bypass Zscaler as it is sent out to the internet needs a route with a next hop type of virtual network or internet.

©2024 Zscaler, Inc. All rights reserved.

In the example, the 192.168.0.0/16 network is kept local. You must also add **the default route of 0.0.0.0/0 with a next hop of Zscaler's virtual network gateway**.

In the example, 3.130.30.39 goes directly to the internet site and bypasses Zscaler. Microsoft is releasing a new feature for bypassing routes based on a tag. This simulates FQDN bypasses. Currently route bypasses are destination-IP-based. To perform FQDN bypasses, you install a component such as the Microsoft firewall. FQDN bypasses are beyond of the scope of this document.

Applying the Route Table

Apply the route table to the subnet that contains the devices that talk to the internet. From **All resources**:

1. Select the **VNet** that contains our resources and select **Subnets**.
2. Select the **Subnets** that contain the devices that talk to internet resources.
3. Apply the route table that was just created.

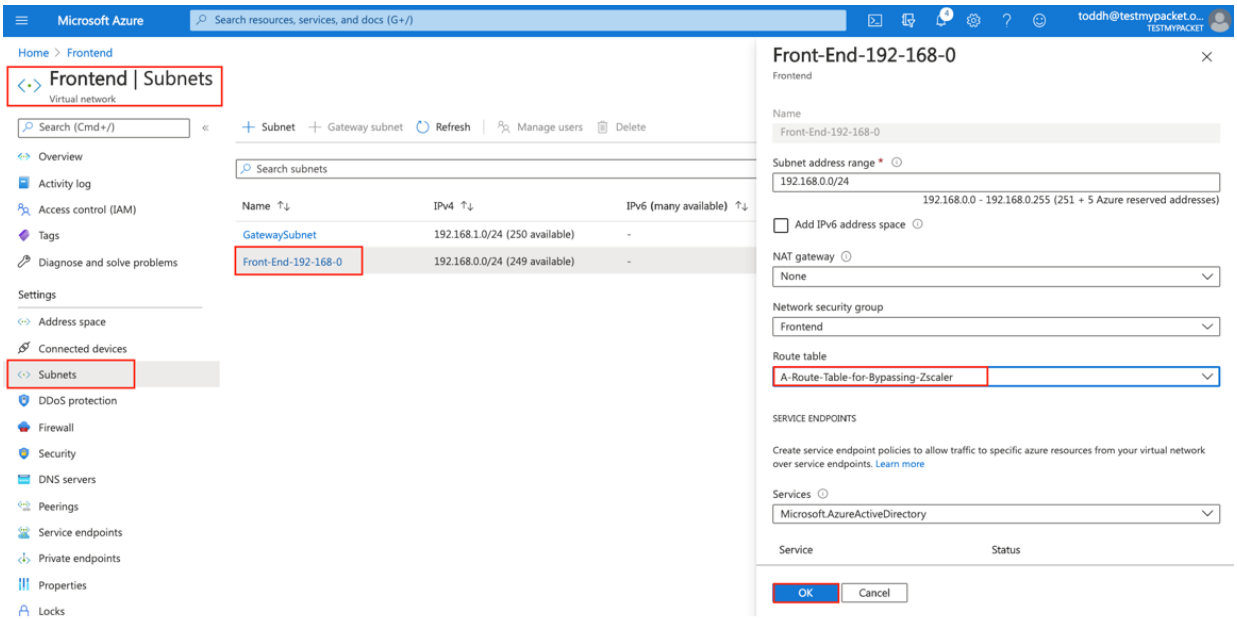

Figure 68. Apply the route table to a subnet

The configuration is now complete.

©2024 Zscaler, Inc. All rights reserved.

Appendix A: Troubleshooting

VPN Troubleshooting

There are a couple of tools to help troubleshoot the VPN connections:

- From Zscaler you can use Tunnel Insights (described in Check the Status of the VPN Connection) to check if the tunnel was initiated.
- You can also use the native VPN troubleshooting tool in Azure (located in the Virtual Network Gateway resource). To use this tool, you must create both Storage and a Container resources. You are prompted to select the resource or create the resource as you initiate troubleshooting.

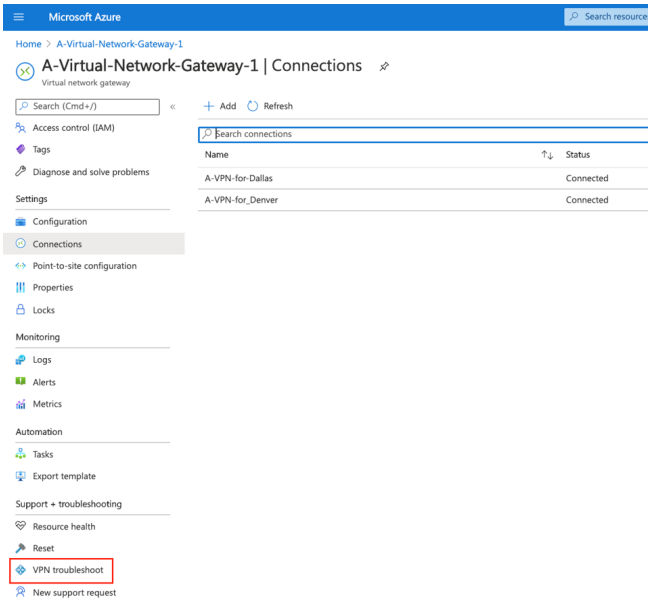

Figure 69. VPN troubleshooting

To start troubleshooting:

1. Select the storage and container.
2. Select the **Gateway** and the **Connection** to test.
3. Select **Start troubleshooting**.

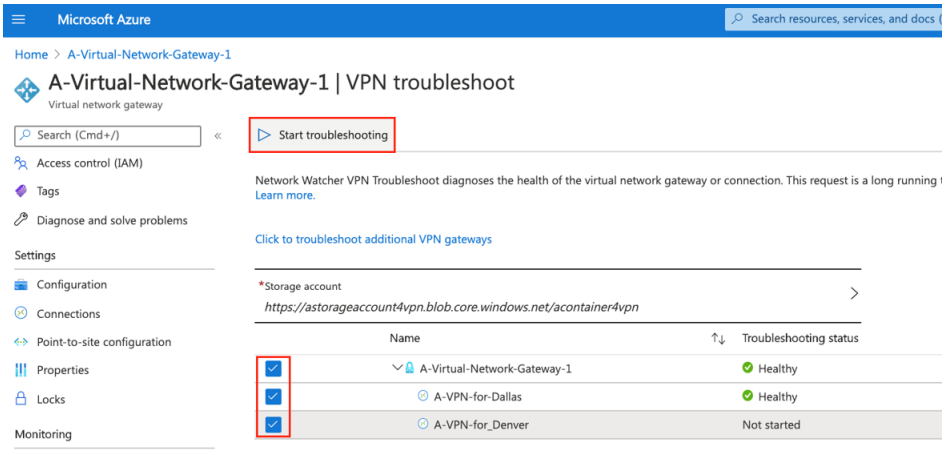

Figure 70. Troubleshooting a VPN

©2024 Zscaler, Inc. All rights reserved.

To get successful results, you might need to run the test twice. You must have a healthy connection before having a healthy gateway but you must run the gateway test first. Essentially, you must run the test twice to confirm that the traffic forwarding environment is healthy.

Troubleshooting from the VNet

From the VNet, you can issue an ICMP or TCP query to see if destinations are reachable. By issuing an ICMP probe to a Zscaler global IP, you can validate that destinations are reachable from the VNet.

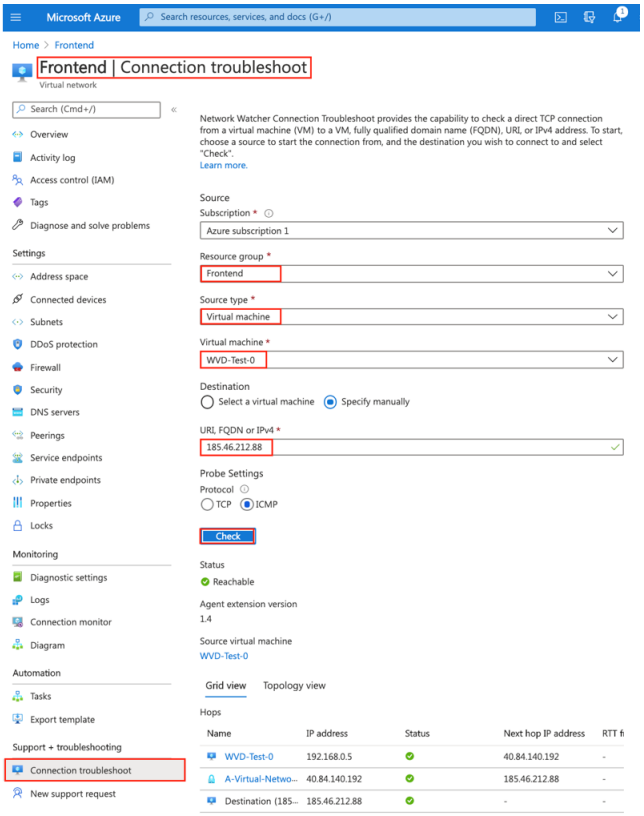

Figure 71. Sending an ICMP echo from a VM

©2024 Zscaler, Inc. All rights reserved.

Verify Traffic is Going Through the Tunnel to Zscaler

The simplest test to see if traffic is flowing through Zscaler is to open a browser and go to ip.zscaler.com. If traffic is flowing through the tunnel through Zscaler, this page tells you that traffic is received from a Zscaler location. The page also provides you the traffic source public IP address. In this case, traffic is flowing from your public IP Azure in Azure to the Zscaler Dallas facility.

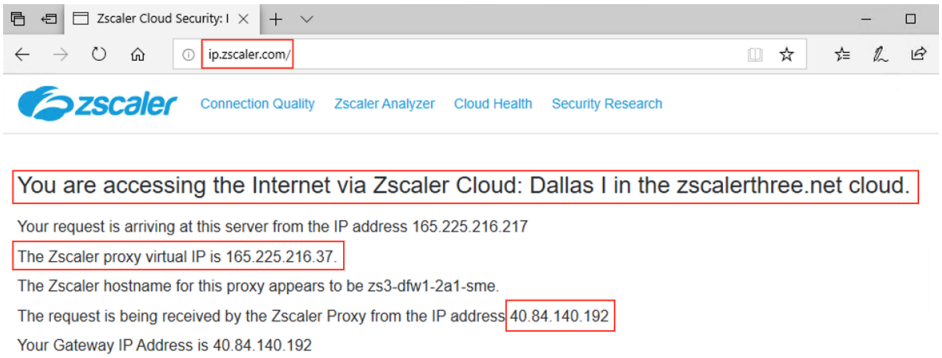

Figure 72. ip.zscaler.com

©2024 Zscaler, Inc. All rights reserved.

Appendix B: PAC Examples

APP PAC Example:

```
////////////////////////////////////////////////////////////////////////////////////////
/////

//

// Filename: App-Pac for Z-App for WVD Dedicated Machine

// Not for Shared WVD Environments

// Description: The is the Z-App App Pac File for Tunnel 2.0 and the WVD environment

// Allowing all port to be forwarded to the Zscaler Cloud Firewall

//

////////////////////////////////////////////////////////////////////////////////////////
/////


function FindProxyForURL(url, host) {


var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-
9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9.]+$/;

var resolved_ip = dnsResolve(host);


// Don’t send non-FQDN or private IP auths to us

if (isPlainHostName(host) || isInNet(resolved_ip, “192.0.2.0”,”255.255.255.0”) ||
privateIP.test(resolved_ip))

return “DIRECT”;


// FTP goes directly

if (url.substring(0,4) == “ftp:”)

return “DIRECT”;


// Updates are directly accessible

if ((localHostOrDomainIs(host, “trust.zscaler.com”)) && (url.substring(0,5) == “http:”
|| url.substring(0,6) == “https:”))

return “DIRECT”;
```

©2024 Zscaler, Inc. All rights reserved.

```
// Example Don’t send to Zscaler Internal Domains
//if (
//dnsDomainIs(host, “.name.of.customer.domain.to.bypass1.com”) ||
//dnsDomainIs(host, “.name.of.customer.domain.to.bypass2.com”))
//return “DIRECT”;

// Example Don’t send to Zscaler Customer Internal IP Addresses
//if (
//shExpMatch(host, “8.8.8.*”) ||
//shExpMatch(host, “4.4.4.*”))
//return “DIRECT”;

// Azure Bypass for Authentication
if (
dnsDomainIs(url, “.microsoftonline.com”) ||
dnsDomainIs(url, “.microsoftonline-p.net”) ||
dnsDomainIs(url, “.azure.com”))
return “DIRECT”;

// Azure and Microsoft Application Bypasses
if (
shExpMatch(url, “.microsoft.com”) ||
shExpMatch(url, “.windows.net”) ||
shExpMatch(url, “.sharepointonline.com”) ||
shExpMatch(url, “.office.com”) ||
shExpMatch(url, “.office.net”) ||
shExpMatch(url, “.onmicrosoft.com”) ||
shExpMatch(url, “.lync.com”) ||
shExpMatch(url, “.sfbassets.com”) ||
shExpMatch(url, “.trafficmanager.net”) ||
```

©2024 Zscaler, Inc. All rights reserved.

```
shExpMatch(url, ".msecnd.net") ||
shExpMatch(url, ".aspnetcdn.com") ||
shExpMatch(url, ".azure.net") ||
shExpMatch(url, ".secure.skypeassets.com") ||
shExpMatch(url, ".tenor.com") ||
shExpMatch(url, ".microsoftstream.com") ||
shExpMatch(url, ".skype.com") ||
shExpMatch(url, ".live.com") ||
shExpMatch(url, ".skypeforbusiness.com") ||
shExpMatch(url, ".office365.com"))
return "DIRECT";

// Specific to WVD
if (
shExpMatch(url, ".wvd.microsoft.com") ||
shExpMatch(url, ".core.windows.net") ||
shExpMatch(url, "login.windows.net") ||
shExpMatch(url, ".servicebus.windows.net") ||
shExpMatch(url, ".warmpath.msftcloudes.com") ||
shExpMatch(url, ".azureedge.net") ||
shExpMatch(url, ".events.data.microsoft.com") ||
shExpMatch(url, ".msftconnecttest.com") ||
shExpMatch(url, ".microsoftonline.com") ||
shExpMatch(url, ".prod.do.dsp.mp.microsoft.com") ||
shExpMatch(url, ".sfx.ms") ||
shExpMatch(url, ".digicert.com") ||
shExpMatch(url, "aka.ms") ||
shExpMatch(url, ".aka.ms") ||
shExpMatch(url, ".prod.cms.rt.microsoft.com"))
return "DIRECT";
```

©2024 Zscaler, Inc. All rights reserved.

```
// Send to Zscaler Cloud

//

return "PROXY ${COUNTRY_GATEWAY_FX}:80; PROXY ${COUNTRY_SECONDARY_GATEWAY_FX}:80;
DIRECT";

}
```

Forward PAC:

```
////////////////////////////////////////////////////////////////////////////////////
/////

//

// Filename: Fwd-Pac for Z-App for WVD Dedicated Machine

// Not for Shared WVD Enviroments

// Description: The is the Z-App FWD Pac File for Tunnel 2.0 and the WVD environment

// This provide a means for bypasses and must be added to both FWD and APP Pac.

//

////////////////////////////////////////////////////////////////////////////////////
/////



function FindProxyForURL(url, host) {


var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-
9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9.]+$/;

var resolved_ip = dnsResolve(host);


// Don't send non-FQDN or private IP auths to us

if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0","255.255.255.0") ||
privateIP.test(resolved_ip))

return "PROXY ${ZAPP_TUNNEL2_BYPASS}";


// FTP goes directly

if (url.substring(0,4) == "ftp:")

return "PROXY ${ZAPP_TUNNEL2_BYPASS}";
```

©2024 Zscaler, Inc. All rights reserved.

```
// Updates are directly accessible

if ((localHostOrDomainIs(host, "trust.zscaler.com")) && (url.
substring(0,5) == "http:" || url.substring(0,6) == "https:"))

return "PROXY ${ZAPP_TUNNEL2_BYPASS}";


// Example Don't send to Zscaler Internal Domains

//if (

//dnsDomainIs(host, ".name.of.customer.domain.to.bypass1.com") ||

//dnsDomainIs(host, ".name.of.customer.domain.to.bypass2.com"))

//return "PROXY ${ZAPP_TUNNEL2_BYPASS}";


// Example Don't send to Zscaler Customer Internal IP Addresses

//if (

//shExpMatch(host, "8.8.8.*") ||

//shExpMatch(host, "4.4.4.*"))

// return "PROXY ${ZAPP_TUNNEL2_BYPASS}";


// Azure Bypass for Authentication

if (

dnsDomainIs(url, ".microsoftonline.com") ||

dnsDomainIs(url, ".microsoftonline-p.net") ||

dnsDomainIs(url, ".azure.com"))

return "PROXY ${ZAPP_TUNNEL2_BYPASS}";


// Azure and Microsoft Application Bypasses

shExpMatch(url, ".microsoft.com") ||

shExpMatch(url, ".windows.net") ||

shExpMatch(url, ".sharepointonline.com") ||

shExpMatch(url, ".office.com") ||
```

©2024 Zscaler, Inc. All rights reserved.

```
shExpMatch(url, ".office.net") ||
shExpMatch(url, ".onmicrosoft.com") ||
shExpMatch(url, ".lync.com") ||
shExpMatch(url, ".sfbassets.com") ||
shExpMatch(url, ".trafficmanager.net") ||
shExpMatch(url, ".msecnd.net") ||
shExpMatch(url, ".aspnetcdn.com") ||
shExpMatch(url, ".azure.net") ||
shExpMatch(url, ".secure.skypeassets.com") ||
shExpMatch(url, ".tenor.com") ||
shExpMatch(url, ".microsoftstream.com") ||
shExpMatch(url, ".skype.com") ||
shExpMatch(url, ".live.com") ||
shExpMatch(url, ".skypeforbusiness.com") ||
shExpMatch(url, ".office365.com"))
return "PROXY ${ZAPP_TUNNEL2_BYPASS}";

// Specific to WVD
if (
shExpMatch(url, ".wvd.microsoft.com") ||
shExpMatch(url, ".core.windows.net") ||
shExpMatch(url, "login.windows.net") ||
shExpMatch(url, ".servicebus.windows.net") ||
shExpMatch(url, ".warmpath.msftcloudes.com") ||
shExpMatch(url, ".azureedge.net") ||
shExpMatch(url, ".events.data.microsoft.com") ||
shExpMatch(url, ".msftconnecttest.com") ||
shExpMatch(url, ".microsoftonline.com") ||
shExpMatch(url, ".prod.do.dsp.mp.microsoft.com") ||
shExpMatch(url, ".sfx.ms") ||
```

©2024 Zscaler, Inc. All rights reserved.

```
shExpMatch(url, ".digicert.com") ||
shExpMatch(url, "aka.ms") ||
shExpMatch(url, ".aka.ms") ||
shExpMatch(url, ".prod.cms.rt.microsoft.com"))
return "PROXY ${ZAPP_TUNNEL2_BYPASS}";

// Send to Zscaler Cloud
//
return "DIRECT";
}
```

Browser PAC:

```
////////////////////////////////////////////////////////////////////////////////
/////
//
// Filename: AzureWVD
// Description: PAC file for use in Azure Windows Virtual Desktop with
// Dedicated Proxy Port 10000. The Dedicated Proxy Port
// requires a Zscaler License and will be a unique port number.
//
////////////////////////////////////////////////////////////////////////////////
/////

function FindProxyForURL(url, host) {

var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-
9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9.]+$/;
var resolved_ip = dnsResolve(host);

// Don't send non-FQDN or private IP auths to us
if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0","255.255.255.0") ||
privateIP.test(resolved_ip))
return "DIRECT";
```

©2024 Zscaler, Inc. All rights reserved.

```
// FTP goes directly

if (url.substring(0,4) == "ftp:")

return "DIRECT";


// Updates are directly accessible

if ((localHostOrDomainIs(host, "trust.zscaler.com")) && (url.
substring(0,5) == "http:" || url.substring(0,6) == "https:"))

return "DIRECT";


// Example Don't send to Zscaler Internal Domains

//if (

//dnsDomainIs(host, ".name.of.customer.domain.to.bypass1.com")
||

//dnsDomainIs(host, ".name.of.customer.domain.to.bypass2.
com"))

//return "DIRECT";


// Example Don't send to Zscaler Customer Internal IP
Addresses

//if (

//shExpMatch(host, "8.8.8.*") ||

//shExpMatch(host, "4.4.4.*"))

//return "DIRECT";


// Azure Bypass for Authentication

if (

dnsDomainIs(url, ".microsoftonline.com") ||

dnsDomainIs(url, ".microsoftonline-p.net") ||

dnsDomainIs(url, ".azure.com"))

return "DIRECT";
```

©2024 Zscaler, Inc. All rights reserved.

```
// Azure and Microsoft Application Bypasses
if (
shExpMatch(url, ".microsoft.com") ||
shExpMatch(url, ".windows.net") ||
shExpMatch(url, ".sharepointonline.com") ||
shExpMatch(url, ".office.com") ||
shExpMatch(url, ".office.net") ||
shExpMatch(url, ".onmicrosoft.com") ||
shExpMatch(url, ".lync.com") ||
shExpMatch(url, ".sfbassets.com") ||
shExpMatch(url, ".trafficmanager.net") ||
shExpMatch(url, ".msecnd.net") ||
shExpMatch(url, ".aspnetcdn.com") ||
shExpMatch(url, ".azure.net") ||
shExpMatch(url, ".secure.skypeassets.com") ||
shExpMatch(url, ".tenor.com") ||
shExpMatch(url, ".microsoftstream.com") ||
shExpMatch(url, ".skype.com") ||
shExpMatch(url, ".live.com") ||
shExpMatch(url, ".skypeforbusiness.com") ||
shExpMatch(url, ".office365.com"))
return "DIRECT";

// Specific to WVD
if (
shExpMatch(url, ".wvd.microsoft.com") ||
shExpMatch(url, ".core.windows.net") ||
shExpMatch(url, "login.windows.net") ||
shExpMatch(url, ".servicebus.windows.net") ||
shExpMatch(url, ".warmpath.msftcloudes.com") ||
```

©2024 Zscaler, Inc. All rights reserved.

```
shExpMatch(url, ".azureedge.net") ||
shExpMatch(url, ".events.data.microsoft.com") ||
shExpMatch(url, ".msftconnecttest.com") ||
shExpMatch(url, ".microsoftonline.com") ||
shExpMatch(url, ".prod.do.dsp.mp.microsoft.com") ||
shExpMatch(url, ".sfx.ms") ||
shExpMatch(url, ".digicert.com") ||
shExpMatch(url, "aka.ms") ||
shExpMatch(url, ".aka.ms") ||
shExpMatch(url, ".prod.cms.rt.microsoft.com"))
return "DIRECT";


//
// Send to Zscaler Proxy
//
return "PROXY ${COUNTRY_GATEWAY_FX}:10000; PROXY ${COUNTRY_SECONDARY_GATEWAY_FX}:10000;
DIRECT";
}
```

©2024 Zscaler, Inc. All rights reserved.

Appendix C: Requesting Zscaler Support

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

To contact Zscaler support:

1. Go to **Administration > Settings** > and then click **Company profile**.

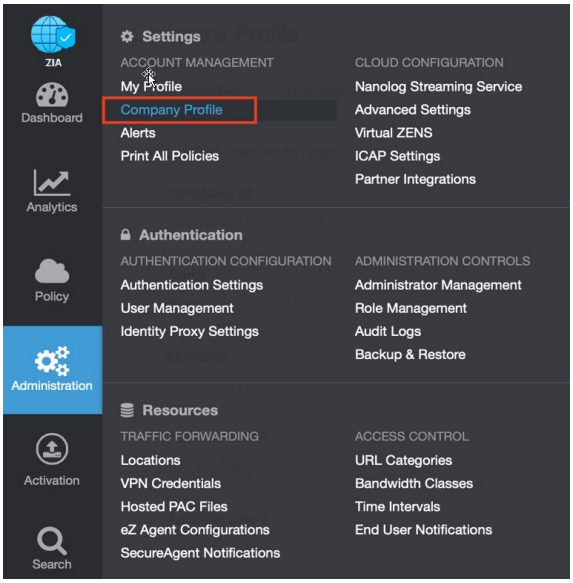

Figure 73. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

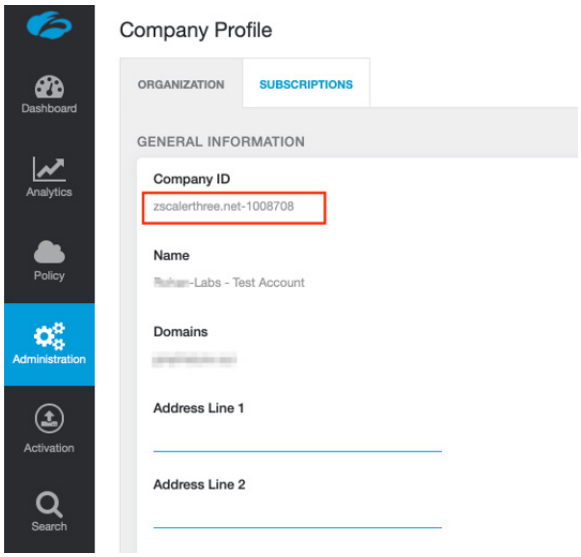

Figure 74. Company ID

©2024 Zscaler, Inc. All rights reserved.

3. With your company ID information, you can open a support ticket. Navigate to **Dashboard > Support > Submit a Ticket**.

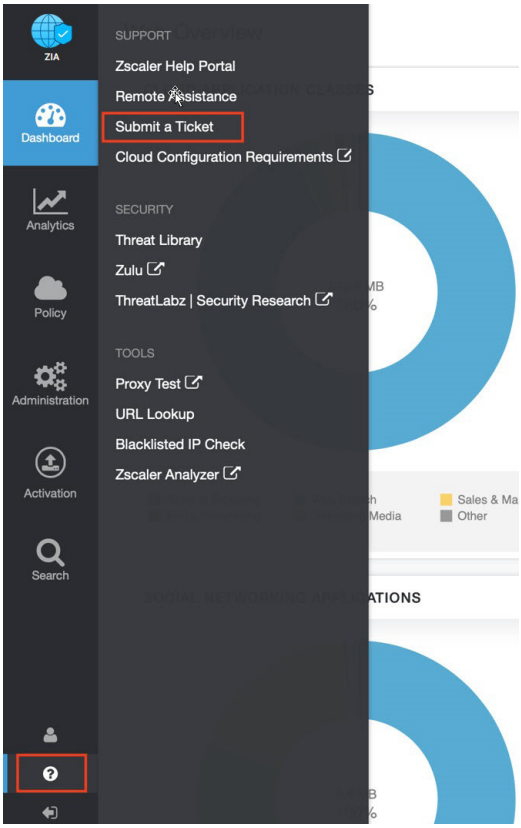

Figure 75. Submit a ticket

©2024 Zscaler, Inc. All rights reserved.