ZSCALER AND JUNIPER NETWORKS 128 TECHNOLOGY DEPLOYMENT GUIDE

AUGUST 2022, VERSION 2.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines 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)
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)
KNI	Kernel NIC Interface
LTE	Long-Term Evolution
MPLS	Multiprotocol Label Switching
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SSL	Secure Socket Layer (RFC6101)
VTI	Virtual Tunnel Interface
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the organizations and requirements of 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. Its flagship 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 or follow Zscaler on Twitter @zscaler.

Juniper Overview

Juniper (NYSE: JNPR) is dedicated to dramatically simplifying network operations and driving superior experiences for end users. Juniper solutions deliver industry-leading insight, automation, security, and AI to drive real business results. Juniper believes that powering connections brings us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality. To learn more, refer to the Juniper Networks website.

Juniper Networks announced its acquisition of SD-WAN provider 128 Technology (128T) in October 2020.

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, see:

- Zscaler Resources
- Juniper 128 Technology Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler Internet Access.

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 Juniper 128 Technology Introduction

The following are overviews of the Zscaler and Juniper 128 Technology applications described in this deployment 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, please 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 on-ramp—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 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 Browser Isolation, allowing you to 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.
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.

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.

Juniper 128 Technology SD-WAN Platform Overview

Juniper 128 Technology, which was founded by a team of network industry veterans and recently acquired by Juniper Networks, was the first company to apply session-based routing architecture to SD-WAN, which enables the creation of a simple platform that is tunnel-free and has no hardware-centric components. It enables agility with centralized management and a Zero Trust security model with the ability to scale to managing millions of segments simultaneously.

Components of the Juniper 128 Technology platform include a centralized orchestration and policy management solution enabled by a Conductor and a Session Smart Router. Together, these components form a distributed control plane and a data plane, both of which are stateful and session aware. Juniper's Session Smart SD-WAN platform creates a fabric of stateful sessions for each connection, allowing for tunnel-free encryptions across a variety of connection types, including MPLS, LTE, internet, and private IP. The Session Smart Router and the distributed control plane enable a variety of capabilities, including granular visibility and control of individual user experiences and policies based on business decisions. The Juniper platform also does service chaining of network functions such as a network-stateful firewall, network address translation (NAT), encryption/VPN, plus link and server load balancing. The Session Smart Router solution can be deployed in data centers, branch offices, or cloud locations, which, according to the company, allows for the creation of a multi-cloud fabric.

Juniper 128 Technology Resources

The following table contains links to Juniper 128 Technology support resources.

Name	Definition
128 Technology Online Help	Online help articles for 128 Technology SD-WAN.

Zscaler Configuration

The following sections describe how to configure Zscaler to work with 128 Technology SD-WAN.

Provision the Public IP Address of the 128T

First you must provision the public address from where the IPSec traffic is initiated towards Zscaler. The Zscaler endpoint tunnels are established to servers called Public Service Edges.

Open a support ticket with Zscaler listing the public IP addresses of all sites connected to Zscaler so that they can be allowed on the Zscaler side. After you have received word from Zscaler Support that this work is completed, you can move forward with the next steps.

Provision VPN Credentials

1. In the ZIA Admin Portal, go to **Administration** > **VPN Credentials**.

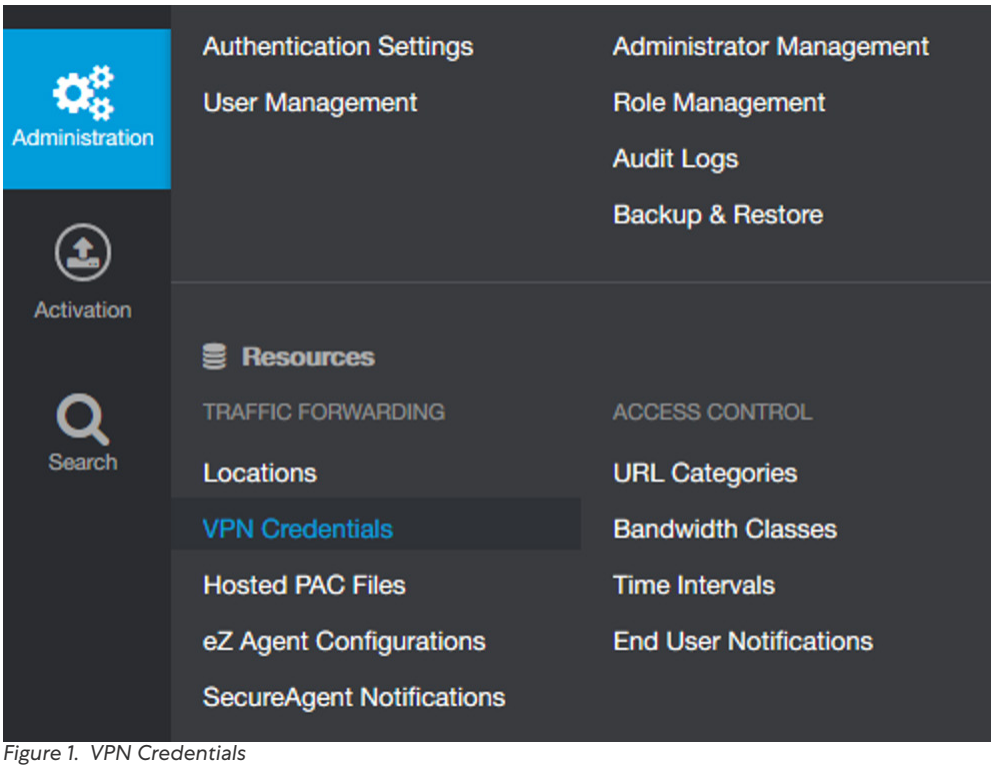

Figure 1. VPN Credentials

2. Click **VPN Credentials**.
3. For the authentication type, click **IP.**
4. You are prompted with a list of the public IP addresses you submitted in the previous step. Select the address for the site you want to set up.
5. Create a pre-shared key (PSK) that is used on both ends of the connection. Create a random string that does not use dictionary words. One method for creating a random key is to issue the following command on a Linux system with OpenSSL installed:

```
[root@west ~]# openssl rand -base64 48
```

6. Enter and confirm your PSK and save it somewhere for reference when you configure the 128T side, then click **Save**.

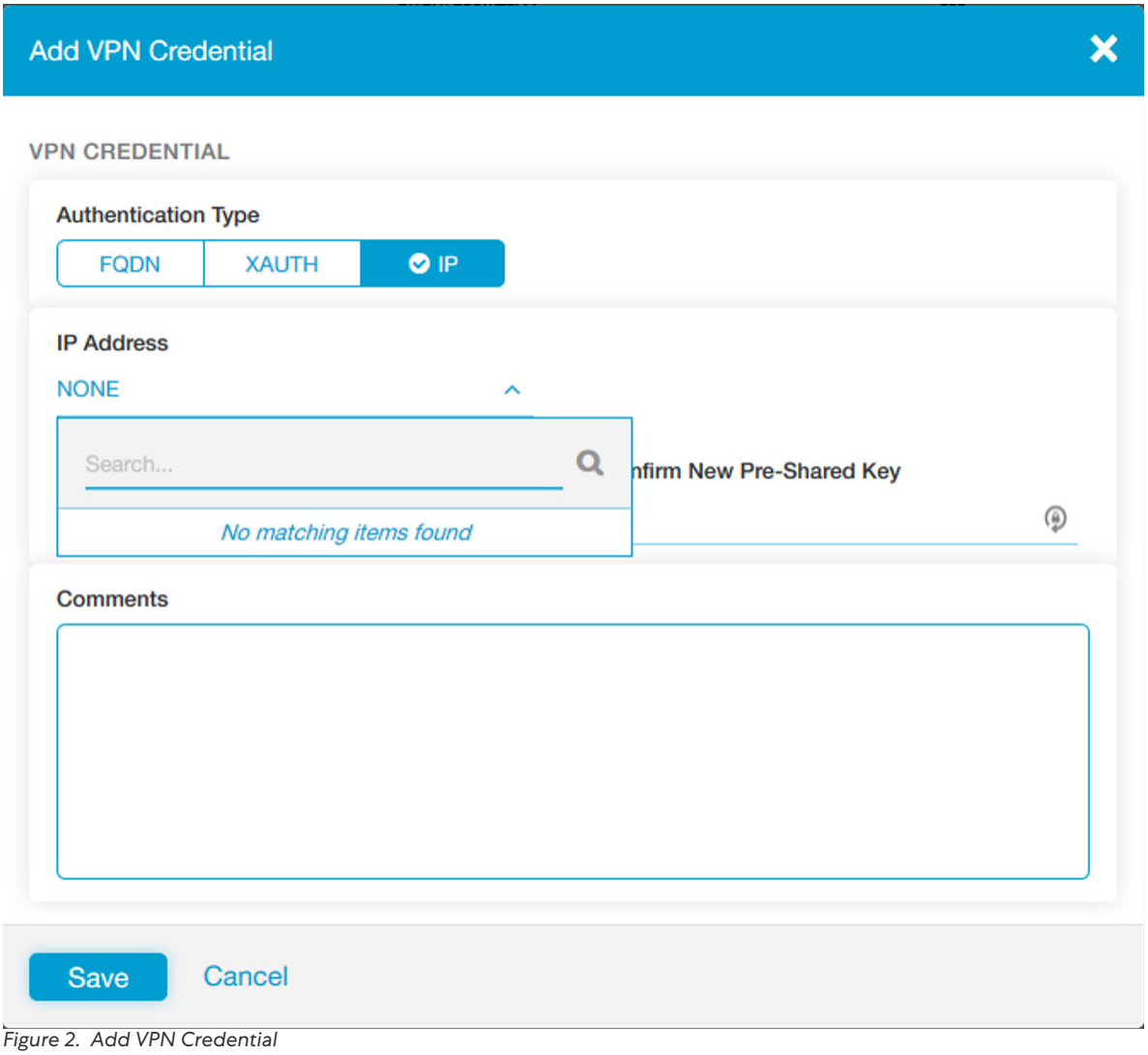

Figure 2. Add VPN Credential

Configure a Location

After you have created your VPN credentials, you can create a location in the ZIA Admin Portal to correspond to the site where the 128T resides.

1. From the ZIA Admin Portal, click **Location**.
2. Enter the appropriate information for your site. Select this site's public IP address from the list of available addresses and select the corresponding VPN Credentials to map to this site.
3. Click **Save**.

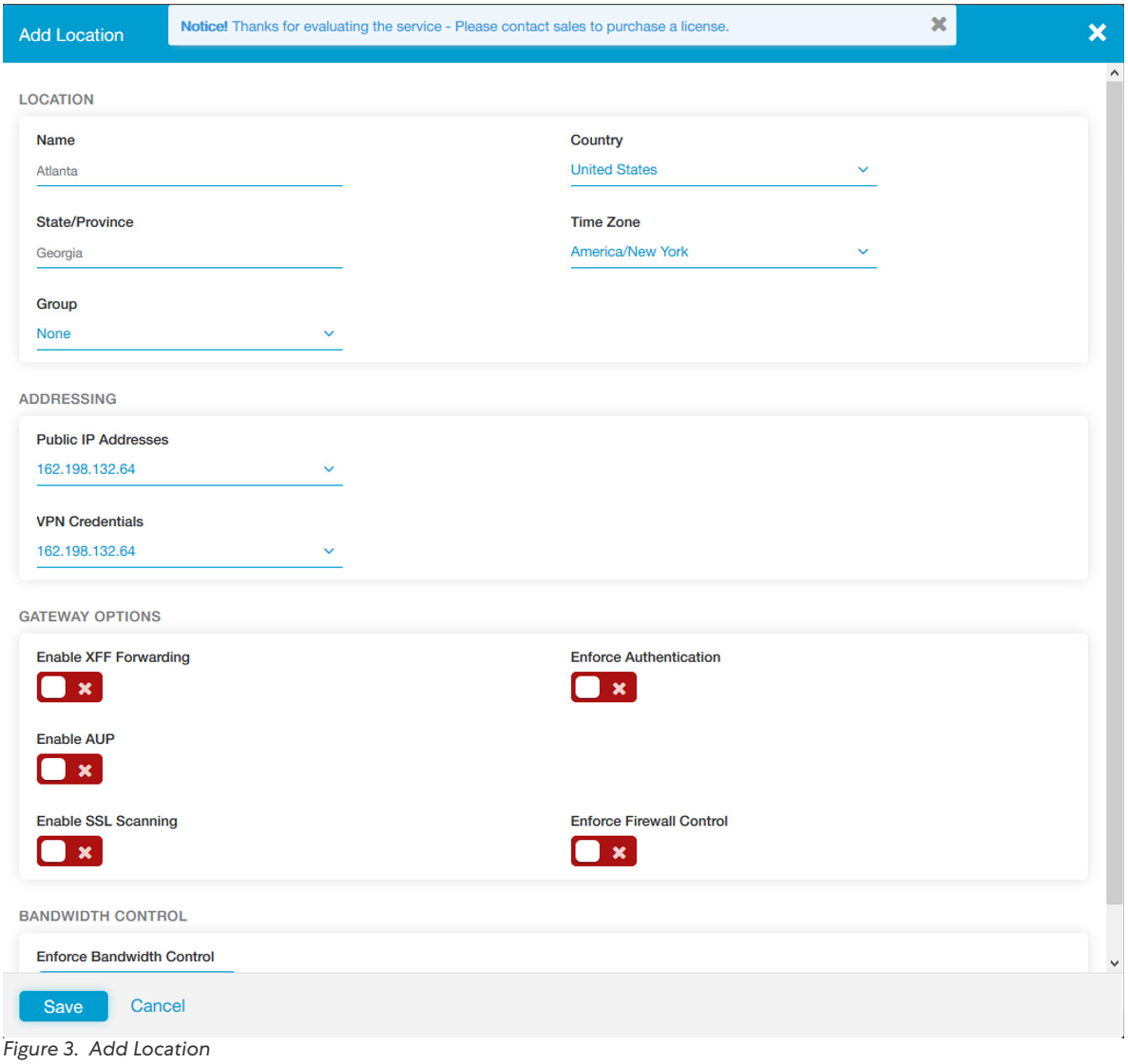

Figure 3. Add Location

Find the Addresses of the Tunnel Termination Public Service Egdes

Zscaler provides services on multiple cloud environments. When a customer is provisioned, they are provisioned in a specific cloud. This test provided access to Betacloud `https://admin.zscalerbeta.net`.

To find the correct Public Service Edges for your cloud environment, replace `admin` with `ips`, for example:

```
https://ips.zscalerbeta.net.
```

From there, click the **Cloud Enforcement Node Ranges** option from the left-side navigation.

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	VPN Host Name	Notes
Europe					Copy IP Addresses
Frankfurt IV	165.225.72.0/22	fra4.sme.zscalerbeta.net	165.225.72.38	fra4-vpn.zscalerbeta.net	
US & Canada					Copy IP Addresses
San Francisco IV	199.168.148.0/23	sunnyvale1.sme.zscalerbeta.net	199.168.148.131	sunnyvale1-vpn.zscalerbeta.net	
Washington DC	104.129.194.0/23	was1.sme.zscalerbeta.net	104.129.194.38	was1-vpn.zscalerbeta.net	

Figure 4. Cloud Enforcement Node Ranges

In this example, choose the **VPN Host Name** in the region that is closest to your site as the primary **PSE** (**was1-vpn.zscalerbeta.net**) and the other as the backup **PSE** (**sunnyvale1-vpn.zscalerbeta.net**).

Convert these names into IP addresses for later in the process. Use the following ping command from Linux:

```
[t128@localhost ~]$ ping was1-vpn.zscalerbeta.net

PING was1-vpn.zscalerbeta.net (104.129.194.39) 56(84) bytes of data.
```


128T Configuration

Use Linux to establish the IPSec tunnels. To pass the LAN traffic into the VPN tunnel and to allow the IPSec traffic out the WAN interface managed by 128T, service function chain the traffic through KNI interfaces as shown in the following drawing.

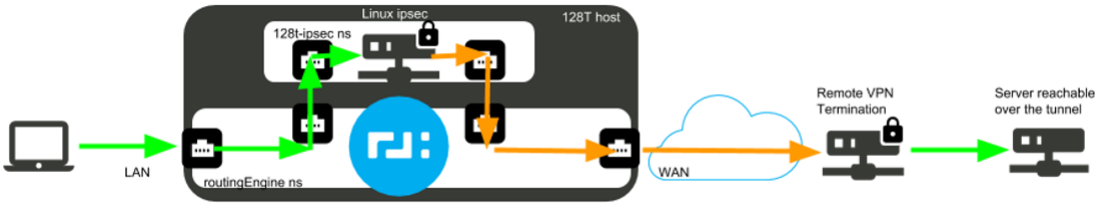

Figure 5. 128T traffic flow

To avoid conflicts with existing Linux routes, create a new namespace for this traffic. Create two KNI host interfaces and move them into the new namespace: one for customer traffic in, and one for IPSec traffic out.

The next section provides the low-level steps to set up and configure IPSec. This is the "phase 0" implementation of Zscaler Support.

Set Up Zscaler IPSec

This section describes the steps needed to set up Zscaler IPSec.

Install the libreswan Package

Install Libreswan with yum. This setup was tested and validated with libreswan-3.20-5.el7_4.x86_64.

```
[root@zscaler-128t ~]# yum install libreswan
```

Create the 128t-ipsec systemd Service

This service is used to launch the IKE daemon inside our 128t-ipsec namespace. Open the following file in your preferred text editor and paste in the contents:

```
/etc/systemd/system/128t-ipsec.service:

[Unit]

Description=Internet Key Exchange (IKE) Protocol Daemon for IPsec running in 128T man-
aged namespace

Wants=network-online.target

Documentation=man:ipsec(8) man:pluto(8) man:ipsec.conf(5)


[Service]

Type=notify

Restart=always

# backwards compatible with plutorestartoncrash=no
```



```
#RestartPreventExitStatus=137 143 SIGTERM SIGKILL

# Set WatchdogSec to the amount of time (in seconds) that systemd will wait

# before restarting an unresponsive pluto.

# EVENT_SD_WATCHDOG updates the heartbeat every 15 seconds, recommended values

# are 60, 90, 120. WatchdogSec=0 disables the action

NotifyAccess=all

WatchdogSec=200

# Check configuration file

ExecStartPre=/sbin/ip netns exec 128t-ipsec /usr/libexec/ipsec/addconn --config /etc/ip-
sec.conf --checkconfig

# Check for kernel modules

ExecStartPre=/sbin/ip netns exec 128t-ipsec /usr/libexec/ipsec/_stackmanager start

# Check for nss database status and migration

ExecStartPre=/sbin/ip netns exec 128t-ipsec /usr/sbin/ipsec --checknss

# Check for nflog setup

ExecStartPre=/sbin/ip netns exec 128t-ipsec /usr/sbin/ipsec --checknflog

# Start the actual IKE daemon

ExecStart=/sbin/ip netns exec 128t-ipsec /usr/libexec/ipsec/pluto --leak-detective
--config /etc/ipsec.conf --nofork

ExecStop=/sbin/ip netns exec 128t-ipsec /usr/libexec/ipsec/whack --shutdown

ExecStopPost=/sbin/ip netns exec 128t-ipsec /sbin/ip xfrm policy flush

ExecStopPost=/sbin/ip netns exec 128t-ipsec /sbin/ip xfrm state flush

ExecStopPost=/sbin/ip netns exec 128t-ipsec /usr/sbin/ipsec --stopnflog

ExecReload=/sbin/ip netns exec 128t-ipsec /usr/libexec/ipsec/whack --listen


[Install]
```


Set Up the Alternate Updown Script

The default updown script doesn't re-establish the routes to the VTI interfaces if the tunnels go down and come back up. You must create a new version of this file and reference it in the Zscaler IPSec configuration file.

1. Copy the original `/usr/libexec/ipsec/_updown.netkey` file to a new location:

```
[root@zscaler-128t ~]# cp /usr/libexec/ipsec/_updown.netkey /usr/libexec/ipsec_up-
down_route.sh
```

2. Using your favorite text editor, edit the new file and add the action `uproute` to the `up-client` command, which is called when the tunnel is re-established:

```
--- /usr/libexec/ipsec/_updown.netkey   2018-05-07 22:24:31.916720083 -0400

+++ /usr/libexec/ipsec_updown_route.sh  2018-05-07 10:12:45.166477846 -0400

@@ -676,6 +676,7 @@

         addcat

         addsource

         notifyNM connect

+         uproute

         ;;

      down-client)

         # connection to my client subnet going down
```

Note that the above output is the Linux diff command output comparing the old and new file. Open the file `/usr/libexec/ipsec_updown_route.sh` in your preferred text editor, go to line 752, look for the line that reads `notifyNM connect` and add a new line following that containing the text `uproute` aligned with the indentation above it.

Do not include the + sign.

Create the Zscaler IPSec Configuration File

This file defines two tunnels, one to each Public Service Edge identified in the first section of this document. Configure the tunnels to use the Zscaler-specified settings for encryption/authentication and phase2.

Setup **Dead Peer Detection** to the Zscaler-specified minimum timer of 10 seconds.

1. Open the file `/etc/ipsec.d/zscaler.conf` using your preferred text editor. Copy and paste the contents of the following text and change the highlighted values to match your setup (there are four places that must be changed). Each value for "right" must match one of the two remote Public Service Edge IP addresses.
2. Give the IP address of the closer location in the section for zscaler1 and the other IP address in the section for zscaler2. The value `leftid` in both locations must match this site's public IP address as configured in the VPN credentials portion of the Zscaler setup from the first section of this guide.

```
conn zscaler1

  authby=secret

  auto=start
```



```
  ike=aes128-sha1;MODP1024
  ikev2=insist
  keyexchange=ike
  ikelifetime=120m
  salifetime=30m
  phase2=esp
  phase2alg=null-md5;MODP1024
  replay-window=16384
  compress=no
  pfs=no
  type=tunnel
  mark=5/0xffffffff
  vti-interface=vti01
  vti-routing=yes
  vti-shared=no
  dpddelay=10
  dpdtimeout=15
  dpdaction=restart
  leftupdown="/usr/libexec/ipsec_updown_route.sh --route y"

  metric=100
  right=104.129.194.39
  rightsubnet=0.0.0.0/0
  left=169.254.32.2
  leftsubnet=0.0.0.0/0
  leftid=162.198.132.64


conn zscaler2
  authby=secret
```



```
auto=start

ike=aes128-sha1;MODP1024

ikev2=insist

keyexchange=ike

ikelifetime=120m

salifetime=30m

phase2=esp

phase2alg=null-md5;MODP1024

replay-window=16384

compress=no

pfs=no

type=tunnel

mark=6/0xffffffff

vti-interface=vti02

vti-routing=yes

vti-shared=no

dpddelay=10

dpdtimeout=15

dpdaction=restart

leftupdown="/usr/libexec/ipsec_updown_route.sh --route y"


metric=200

right=199.168.148.132

rightsubnet=0.0.0.0/0

left=169.254.32.2

leftsubnet=0.0.0.0/0

leftid=162.198.132.64
```


Set Up the IPSec Secrets File

1. Using your preferred text editor, open the file `/etc/ipsec.d/zscaler.secrets` and enter the following content, changing the highlighted values.

   The entries shown are word-wrapped because of length. Your file should contain only two lines, both starting with a `%` sign. On each line, replace the IP address with the IP address of one of the Public Service Edges (also used for the values of "right" in the configuration file from the previous section).

2. Replace the long string between the quotation marks with the appropriate PSK for this connection as recorded from the **Provision VPN Credentials** section of this document:

```
%any 104.129.194.39 : PSK "FAR5a/
JbBfB0WKt0y2kg5wJHTK4ELDk8p2+eVaBS5oZCa5xRxN9ra639Lg3RwuX5"

%any 199.168.148.132 : PSK "FAR5a/
JbBfB0WKt0y2kg5wJHTK4ELDk8p2+eVaBS5oZCa5xRxN9ra639Lg3RwuX5"
```

Configuring 128T for IPSec SFC

This section describes the steps needed to set up 128T IPSec.

Set Up the Plugin Scripts

Create two plugin scripts to make the 128t-ipsec namespace, move the interface into the namespace, and set up the interface address and any required routes.

1. Using your preferred text editor, open the file `/etc/128technology/plugins/network-scripts/host/zscaler-in/init` (create any non-existent directories in this path) and paste in the following contents:

```
#!/bin/bash

NAMESPACE=128t-ipsec

KNI_NAME=zscaler-in

KNI_ADDRESS=169.254.31.2

KNI_GATEWAY=169.254.31.1

KNI_MASK=30


# create namespace if it doesn't exist

if [ ! -e "/var/run/netns/$NAMESPACE" ]; then

  echo "$NAMESPACE namespace does not exist...creating it."

  ip netns add $NAMESPACE

  ip netns exec $NAMESPACE ip link set lo up

  echo "$NAMESPACE created."

  echo "Setting ip_forwarding in namespace $NAMESPACE."

  ip netns exec $NAMESPACE sysctl -w net.ipv4.ip_forward=1
```



```
    echo "Disabling send_redirects in namespace $NAMESPACE."
    ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.send_redirects=0
    echo "Disabling accept_redirects in namespace $NAMESPACE."
    ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.accept_redirects=0
    echo "Disabling Reverse Packet Filtering for $VPN_IN_KNI_NAME."
    ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.rp_filter=0
    ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.$VPN_IN_KNI_NAME.rp_filter=0
fi

# set up KNI if it exists in the default namespace
if [ -d "/sys/devices/virtual/net/$KNI_NAME" ]; then
    echo "$KNI_NAME found in default namespace."
    echo "Moving $KNI_NAME to $NAMESPACE namespace."
    ip link set $KNI_NAME netns $NAMESPACE
    ip netns exec $NAMESPACE ip a add $KNI_ADDRESS/$KNI_MASK dev $KNI_NAME
    ip netns exec $NAMESPACE ip l set $KNI_NAME up
    # Route RFC1918 space
    ip netns exec $NAMESPACE ip r add 10.0.0.0/8 via $KNI_GATEWAY dev $KNI_NAME
    ip netns exec $NAMESPACE ip r add 172.16.0.0/12 via $KNI_GATEWAY dev $KNI_NAME
    ip netns exec $NAMESPACE ip r add 192.168.0.0/16 via $KNI_GATEWAY dev $KNI_NAME
fi
```

2. Using your preferred text editor, open the file `/etc/128technology/plugins/network-scripts/host/zscaler-out/init` (create any non-existent directories in this path) and paste in the following contents:

```
#!/bin/bash
NAMESPACE=128t-ipsec
KNI_NAME=zscaler-out
KNI_ADDRESS=169.254.32.2
KNI_MASK=30
KNI_GATEWAY=169.254.32.1
IPSEC_PEER1_ADDRESS=104.129.194.39
IPSEC_PEER2_ADDRESS=199.168.148.132
```



```
# create namespace if it doesn't exist
if [ ! -e "/var/run/netns/$NAMESPACE" ]; then
  echo "$NAMESPACE namespace does not exist...creating it."
  ip netns add $NAMESPACE
  ip netns exec $NAMESPACE ip link set lo up
  echo "$NAMESPACE created."
  echo "Setting ip_forwarding in namespace $NAMESPACE."
  ip netns exec $NAMESPACE sysctl -w net.ipv4.ip_forward=1
  echo "Disabling send_redirects in namespace $NAMESPACE."
  ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.send_redirects=0
  echo "Disabling accept_redirects in namespace $NAMESPACE."
  ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.accept_redirects=0
  echo "Disabling Reverse Packet Filtering for $VPN_IN_KNI_NAME."
  ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.all.rp_filter=0
  ip netns exec $NAMESPACE sysctl -w net.ipv4.conf.$VPN_IN_KNI_NAME.rp_filter=0
fi

# set up KNI if it exists in the default namespace
if [ -d "/sys/devices/virtual/net/$KNI_NAME" ]; then
  echo "$KNI_NAME found in default namespace."
  echo "Moving $KNI_NAME to $NAMESPACE namespace."
  ip link set $KNI_NAME netns $NAMESPACE
  ip netns exec $NAMESPACE ip a add $KNI_ADDRESS/$KNI_MASK dev $KNI_NAME
  ip netns exec $NAMESPACE ip l set $KNI_NAME up
  ip netns exec $NAMESPACE ip r add $IPSEC_PEER1_ADDRESS via $KNI_GATEWAY dev
$KNI_NAME
  ip netns exec $NAMESPACE ip r add $IPSEC_PEER2_ADDRESS via $KNI_GATEWAY dev
$KNI_NAME
  systemctl start 128t-ipsec
fi
```


3. Change the two highlighted IP addresses to match the IP addresses of the two remote Public Service Edges you are using.
4. After you have saved both files, run the following two commands to ensure these scripts are executable:

```
[root@zscaler-128t ~]# chmod 744 /etc/128technology/plugins/network-scripts/host/zscaler-in/init

[root@zscaler-128t ~]# chmod 744 /etc/128technology/plugins/network-scripts/host/zscaler-out/init
```

Add the Required 128T Configuration Elements

1. Through the 128T CLI, add the following configuration elements to the "authority" level of your configuration.

```
tenant   zscaler
    name  zscaler
exit

service  zscaler-internet
    name                  zscaler-internet
    security              internal
    address               0.0.0.0/0

    access-policy         lan
            source  lan
    exit
    share-service-routes  false
exit

service  zscaler-ipsec
    name                  zscaler-ipsec
    security              internal
    address               199.168.148.132/32
    address               104.129.194.39/32

    access-policy         zscaler
            source  zscaler
```



```
        exit
        share-service-routes  false
    exit
```

2. Your access policy under the zscaler-internet service should match the name of the tenant (or tenants) on your LAN to which you want to grant access to the internet. Also, the two IP addresses in the zscaler-ipsec service should match the addresses of the two Public Service Edges to which you are connecting.
3. Next, configure the 128T KNI interfaces that connect to the 128t-ipsec namespace in order to service function chain with IPSec. Enter the following items under the node element in the router associated with the site you are configuring:

```
        device-interface  zscaler-out
          name               zscaler-out
          type               host

          network-interface  zscaler-out
                  name       zscaler-out
                  tenant     zscaler

                  address    169.254.32.1
                      ip-address     169.254.32.1
                      prefix-length  30
                      gateway        169.254.32.2
                  exit
          exit
        exit

        device-interface  zscaler-in
          name               zscaler-in
          type               host

          network-interface  zscaler-in
                  name       zscaler-in

                  address    169.254.31.1
```



```
                ip-address     169.254.31.1
                prefix-length  30
                gateway        169.254.31.2
            exit
        exit
    exit
```

4. Finally, create service routes to route the traffic associated with the zscaler-internet and Zscaler-ipsec service out the appropriate interfaces. Enter the following entries under the router object associated with the location you are configuring. Replace the highlighted IP address with the value for the next hop gateway to your ISP at this location. Also replace the node name with the correct node name for the system you are configuring.

```
service-route  internet
        name          internet
        service-name  zscaler-internet

        next-hop      zscaler-test-128t zscaler-in
            node-name   zscaler-test-128t
            interface   zscaler-in
            gateway-ip  169.254.31.2
        exit
    exit

    service-route  zscaler-ipsec
        name          zscaler-ipsec
        service-name  zscaler-ipsec

        next-hop      zscaler-test-128t wan
            node-name   zscaler-test-128t
            interface   wan
            gateway-ip  172.25.0.1
        exit
    exit
```


Zscaler Verification

After the configuration is completed, verify that your internet traffic is flowing through Zscaler. From a client on the LAN of your 128T router, browse to **https://ip.zscaler.com**.

If traffic is successfully flowing through Zscaler, you see a page that looks like the following image.

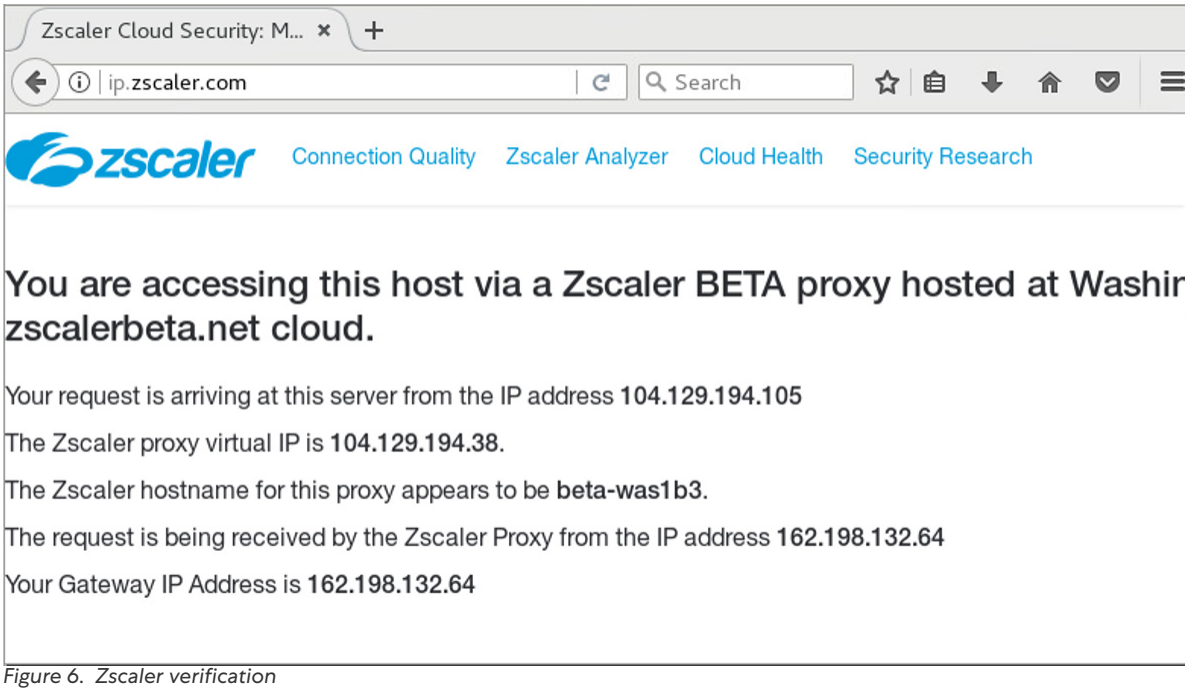

Figure 6. Zscaler verification

If the service is not working, the page won't load or you see a page that looks like the following image.

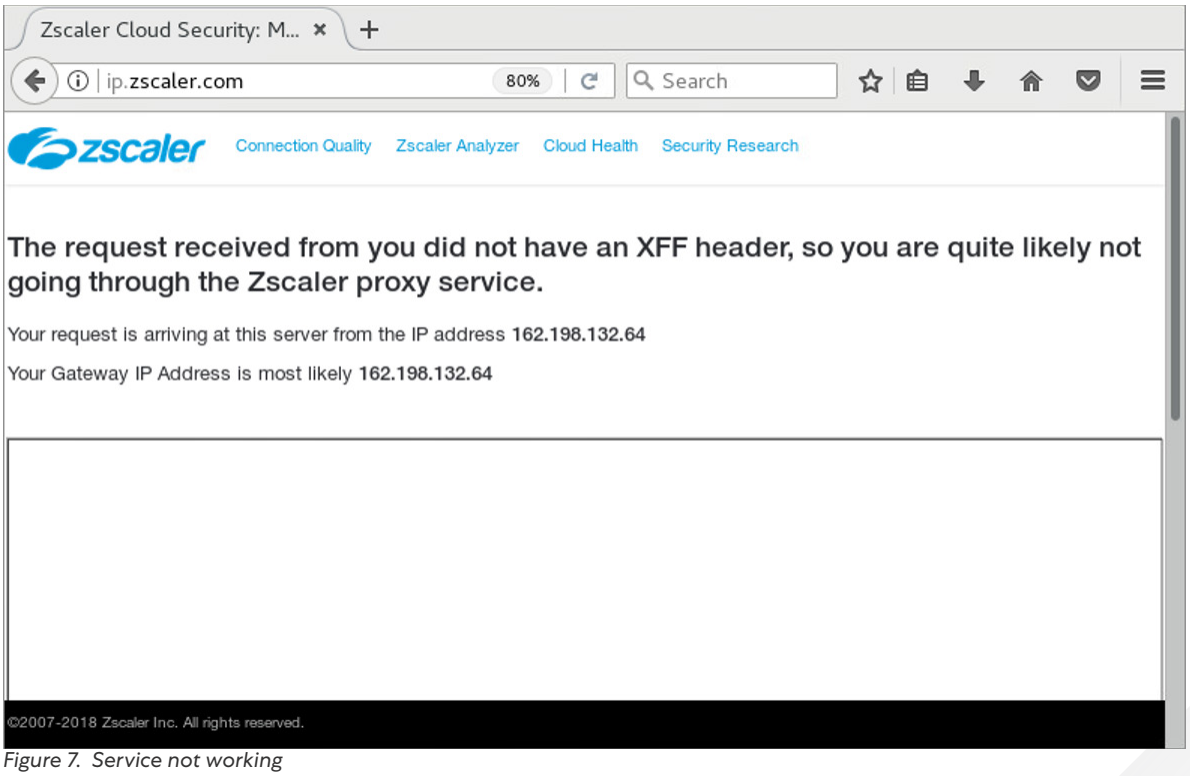

Figure 7. Service not working

Appendix A: Requesting Zscaler Support

You might need Zscaler Support to provision 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**.

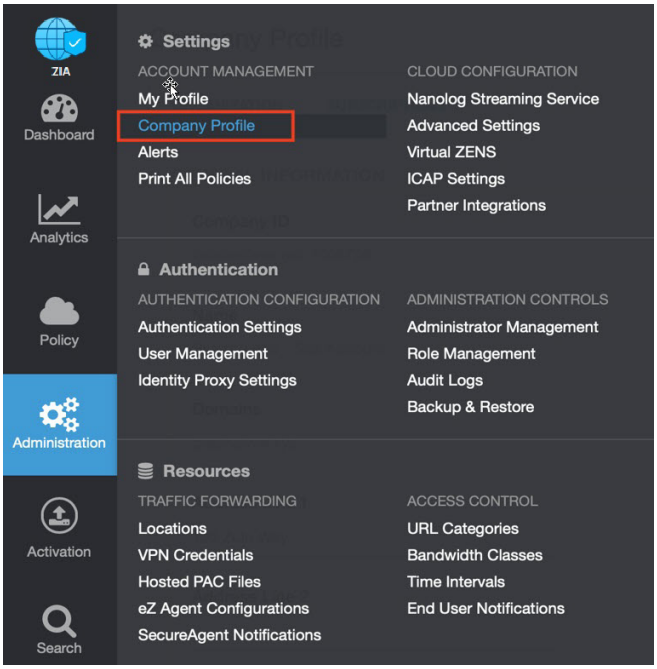

Figure 8. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

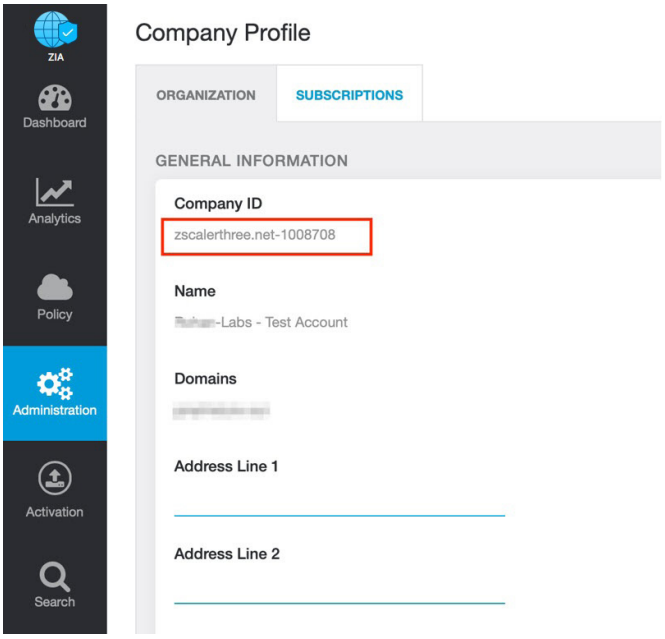

Figure 9. Company ID

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

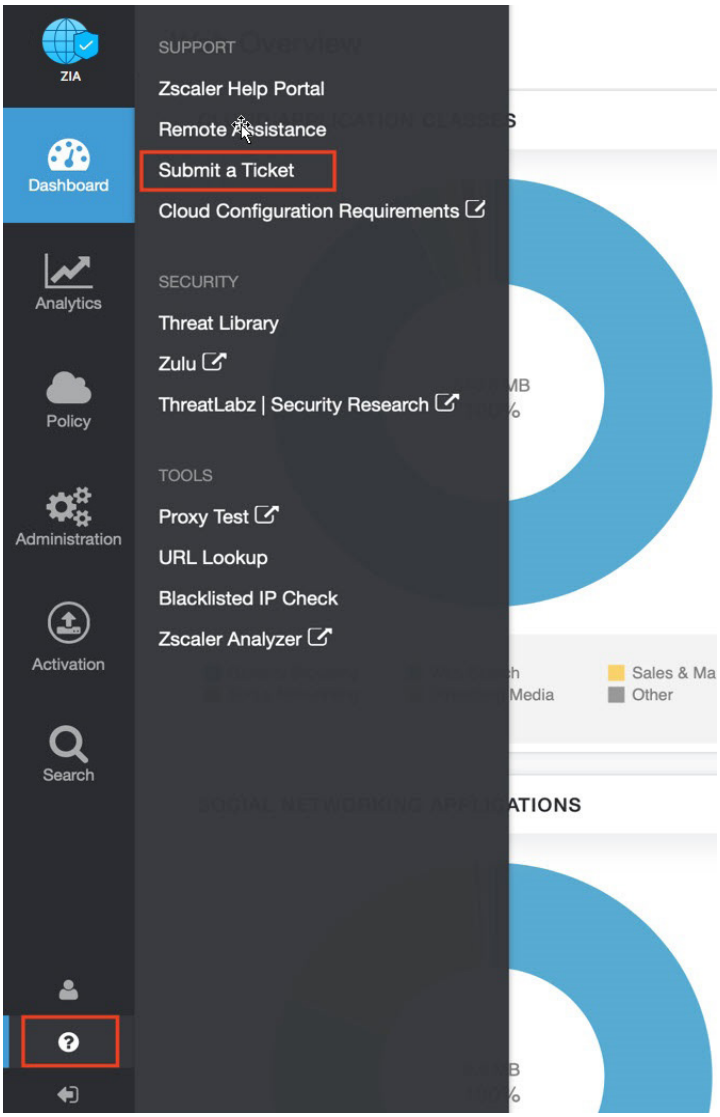

Figure 10. Submit a ticket

