Oracle® SD-WAN

Zscaler Cloud Security Gateway Solution Deployment Guide

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document 3
Talari Overview 3
Zscaler Overview 4
Audience 4
References 4
Introduction 5
Industry Trend 5
Talari Customer and Zscaler Relationship 5
Functional Business Requirements 6
Talari and Zscaler Solution Overview (Branch Office) 7
Solution Integration 8
Prerequisites 8
Integration Tasks 9
Zscaler Configuration 9
Talari APNA Configuration 14
Solution Verification 16
Verification Tasks 16
Appendix A: 18
Talari References: 18
Zscaler References 18
Zscaler Knowledge Base 18
Zscaler Tools 18
Zscaler Training and Certification 18
Zscaler Submit a Ticket 18

About This Document

The purpose of this document is to provide the reader with an understanding of how to configure a Talari Appliance to tunnel Internet-bound traffic to a Zscaler Enforcement Node (ZEN) via a standard IPSec tunnel for the purposes of Cloud Security Services.

Talari Overview

Talari is an innovator in next-generation SD-WAN technology, helping multi-site organizations redefine their remote and branch-office networks by intelligently allocating more bandwidth at less cost, while delivering superior QoS for greater business continuity, operational agility, and application control.

Talari provides a truly failsafe Software Defined WAN (SD-WAN) solution offering dynamic capacity, improved reliability, and higher quality of experience. Our patented hardware and virtual solutions have proven so effective at delivering guaranteed remote uptime that Talari is trusted to broker real-time emergency cloud-voice traffic in large metro 911 call centers.

Whatever your mission-critical network traffic, Talari provides the most resilient and responsive network, delivering stable, complex traffic across the widest area networks and hybrid-cloud IT infrastructures, regardless of the underlying transport technology or application architecture.

Zscaler Overview

Zscaler was started in 2008 when industry veterans, including CEO Jay Chaudhry, came together to create the next step in network security. Zscaler was built on several foundational observations, including the fact that business and personal applications had begun moving to the cloud, Web 2.0 was leading to the evolution of web-based apps, and that the adoption of mobility meant that users could be working from anywhere.

Today, Zscaler protects more than 15 million users at more than 5,000 of the world’s leading enterprises and government organizations worldwide against cyberattacks and data breaches while staying fully compliant with corporate policies. For more information on Zscaler, please visit:

https://www.zscaler.com/products/zscaler-overview

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.

2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
    - For technical issues such as creating a new Service Request (SR), select 1.
    - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Click the Oracle Communications link.

   Under the SD-WAN header, select a product.
4. Select the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available: *Talari 7.0 New Feature Guide*

Introduction

This deployment guide details how to integrate a Talari Appliance with the Zscaler Cloud Security Gateway via IPSec tunneling, for the purposes of tunneling Internet-destined traffic to Zscaler for cloud-hosted filtering and security services.

Industry Trend

An industry trend has developed in the past few years in which branch offices have fewer traditional Next-Generation Firewall (NGFW) security appliances and are migrating towards a cloud-security vendor architecture, essentially outsourcing NGFW functions to the cloud. Figure 1 shows the pre/post topologies, with and without a cloud-security vendor (Zscaler).

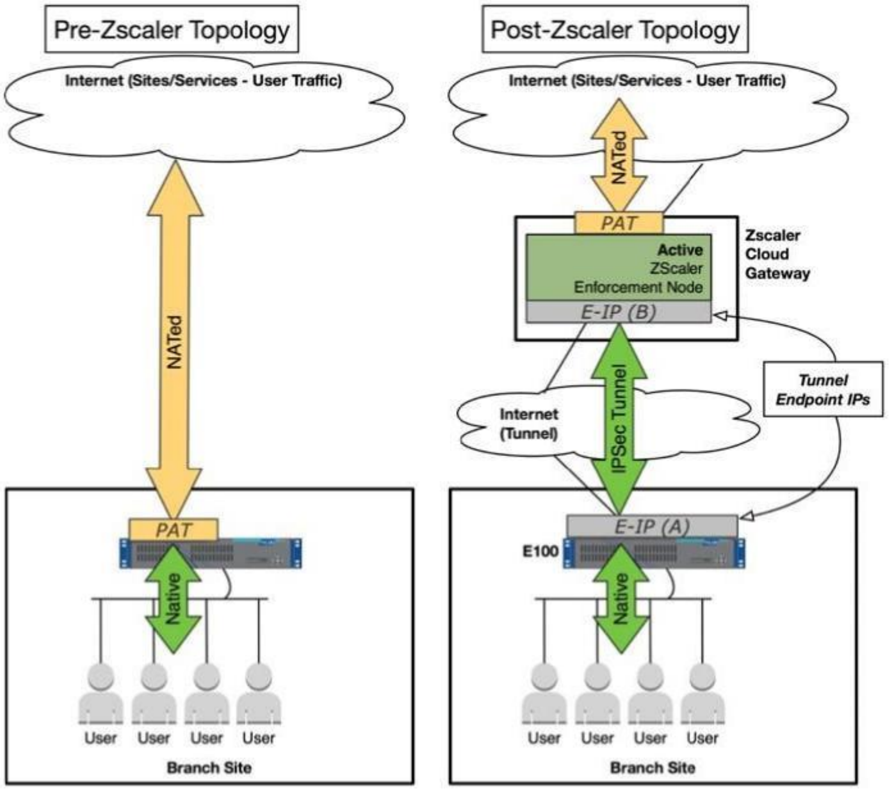


Figure 1: Pre/Post Topologies

Talari Customer and Zscaler Relationship

The relationship between a Talari customer and Zscaler is one of security-customer and security-vendor, respectively. By leveraging Zscaler, the customer is outsourcing functions and features that were traditionally done on a Next Generation Firewall (NGFW).

Aside from the integration of the Talari Appliance with Zscaler via IPSec tunnel (and associated configuration), all Zscaler configuration, management, and monitoring is done via the Zscaler self-service customer portal.

Functional Business Requirements

This solution is for customers seeking to deploy Zscaler Cloud Security Services in conjunction with Talari Appliances deployed at Branch Offices.

The use can be tested via building a IPSec tunnel to a Zscaler Enforcement Node (ZEN) from a Talari, and generating user-traffic destined for the tunnel.

Success is defined by validating the security functionality of Zscaler by blocking an individual website.

Talari and Zscaler Solution Overview (Branch Office)

In Figure 2, the Zscaler enabled Branch Office scenario, the administrator tunnels all Internetdestined traffic leaving the branch directly to Zscaler for cloud security filtering of traffic to-andfrom the Internet:

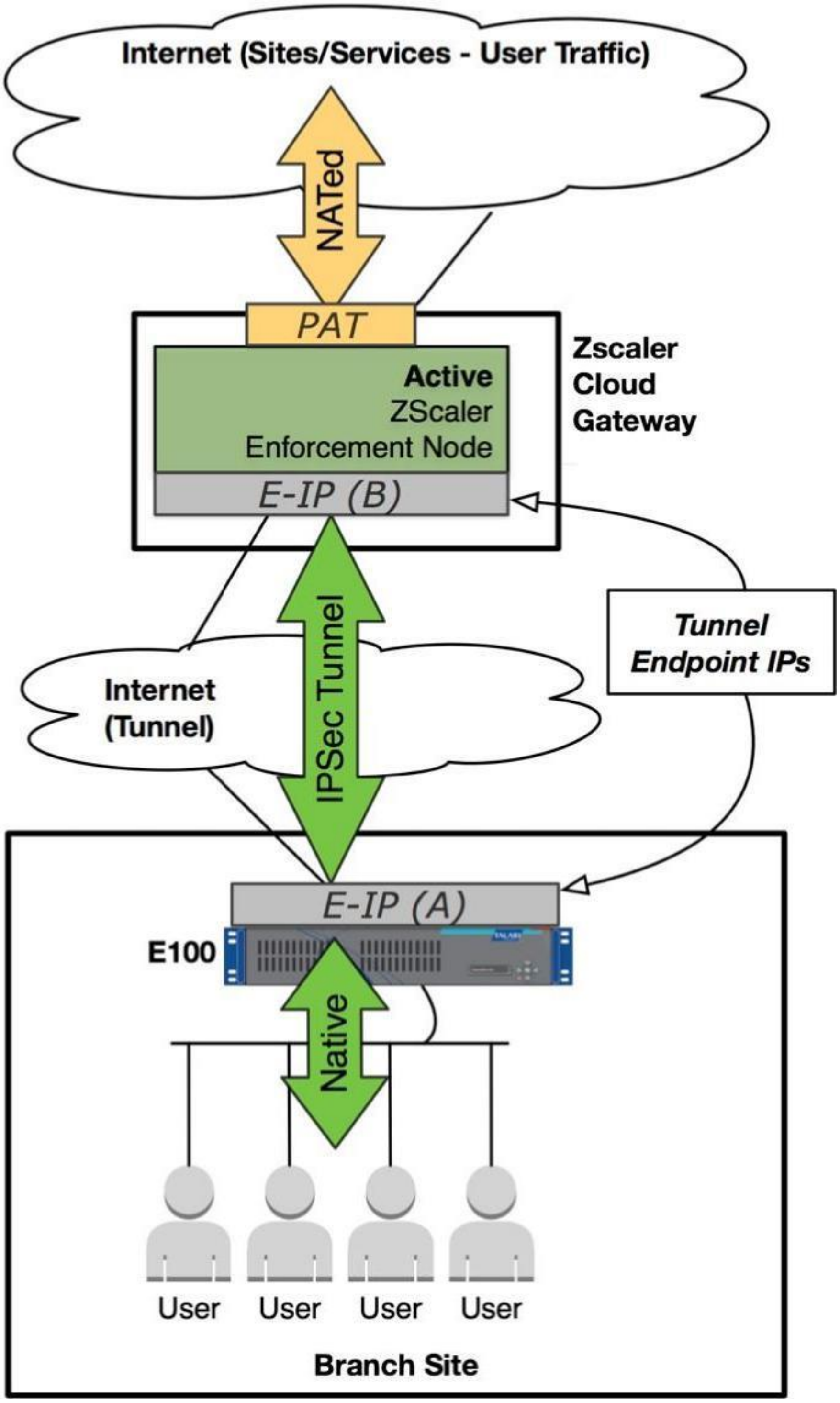


Figure 2: Zscaler Enabled Branch Office

The solution to tunnel Internet-destined traffic from a branch office to Zscaler for cloud-security services consists of a standard IPSec tunnel with specific attributes and behaviors. Figure 3 shows the preferred IPSec settings between Talari and Zscaler :

□ Single IPSec tunnel from a Talari Appliance to Zscaler Enforcement

□ Node. Talari Appliance will always initiate the tunnel.

□ IKE Settings (Phase 1):

- Version: IKEv1
- Mode: Main
- Peer Identity: Auto
- Pre-Shared Key
- DH Group: 2
- Hash: SHA1
- Encryption: AES-128
- SA Lifetime 86400 seconds. (24 hours)
- IKE Identity: ID_IPv4_ADDR* + PSK (Pre-Shared Key)
- Dead Peer Detection: 20 seconds (for immediate re-attempt on failure)

□ IPSec Settings (Phase 2):

- Tunnel Type (Cipher): ESP-NULL
- Perfect Forward Secrecy Group: None Hash: SHA1
- SA Lifetime: 28800 seconds. (8 hours)
- SA (default): 0.0.0.0/0 <-> 0.0.0.0/0

Figure 3: Zscaler IPsec Preferred Settings

Note Regarding RFC 2407: Talari currently supports ID_IPv4_ADDR (1.1.1.1) authentication to IKE peers. Talari will support ID_USER_FQDN (user@domain.tld) authentication to IKE peers in a future release.

Solution Integration

Prerequisites

The following requirements must be met before deploying the solution:

- Minimum of 2 Talari appliances for a minimal functional APN, one to be used for Zscaler testing.
- Must be running APN software 7.0 or later.
- Must be able to communicate with the Zscaler Enforcement Node (ZEN) via ESP, UDP/500, and UDP/4500.
- Security recommendation: configure Internet port as Untrusted / Fail-to-Block.

  - **Note:** Although it is recommended that the interface for Zscaler be configured as Untrusted/Fail-to-Block due to security implications if the device is powered off, it is not required.

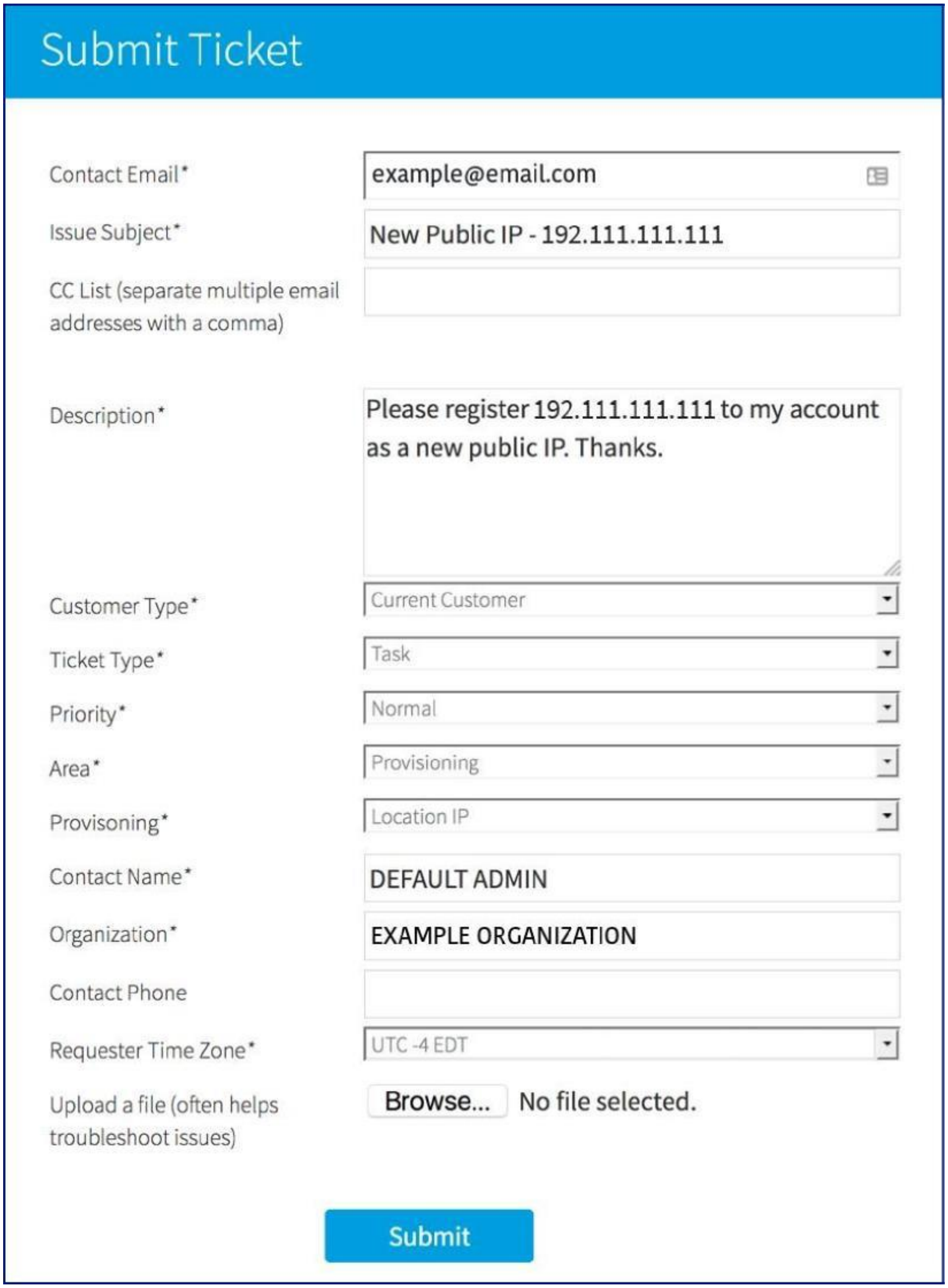
- Must have Internet access added to site and Internet Service configured.
- Static public IP address for WAN link associated with Internet Service.
  - **Note**: The public IP Address of the WAN link associated with the Internet Service must be static, as IP+PSK authentication is supported, but FQDN is not.
- Linux or Windows host on LAN side of Talari to generate Internet traffic.

At this point, the user can configure and deploy the Zscaler tunnel configuration.

Integration Tasks

Zscaler Configuration

1. Register Branch Office IP Address via support ticket.
   - ▯ Location: Zscaler Portal > Support > Submit a Ticket



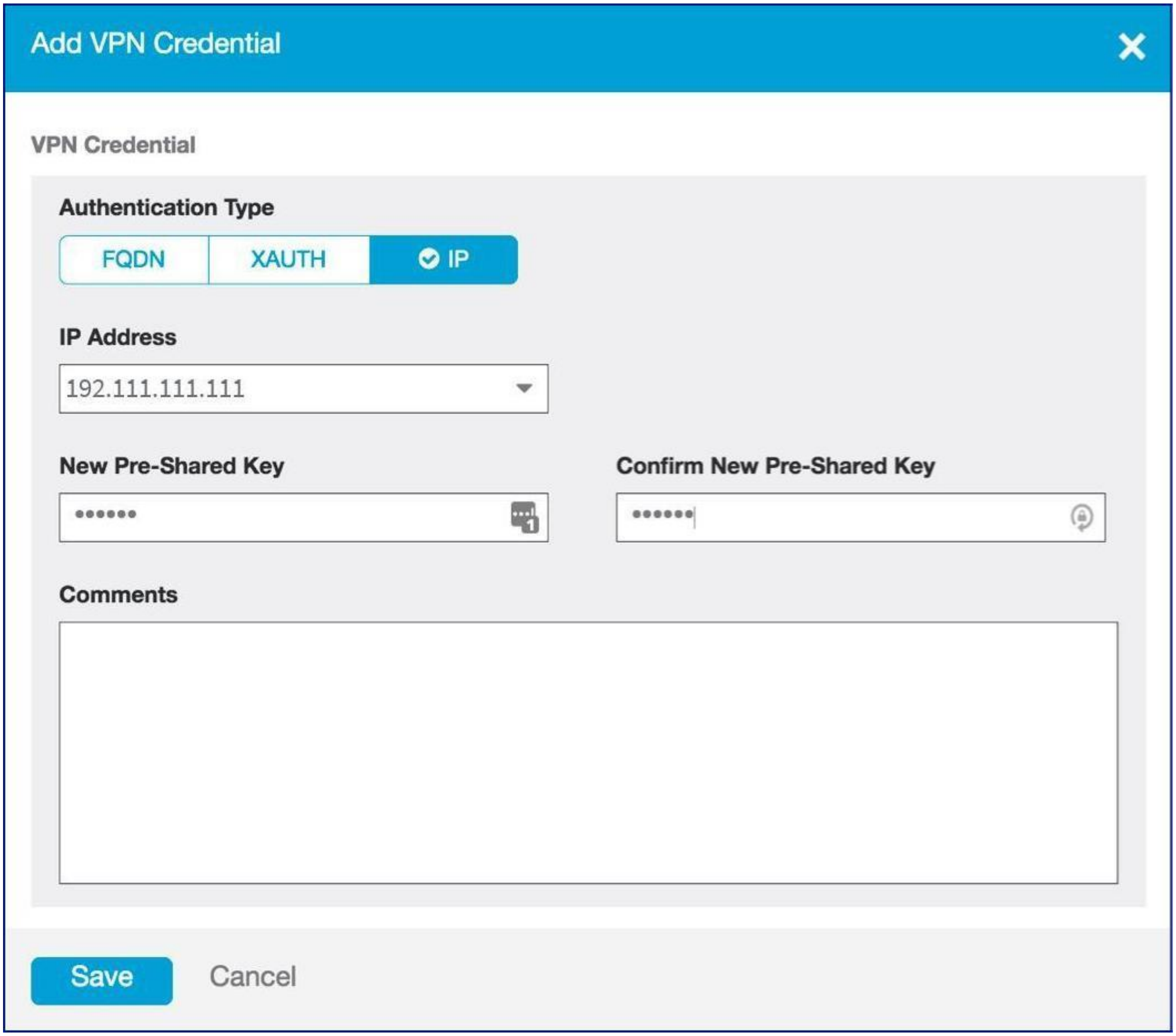
Submit Ticket

Contact Email*	example@email.com
Issue Subject*	New Public IP - 192.111.111.111
CC List (separate multiple email addresses with a comma)	
Description*	Please register 192.111.111.111 to my account as a new public IP. Thanks.
Customer Type*	Current Customer
Ticket Type*	Task
Priority*	Normal
Area*	Provisioning
Provisoning*	Location IP
Contact Name*	DEFAULT ADMIN
Organization*	EXAMPLE ORGANIZATION
Contact Phone	
Requester Time Zone*	UTC -4 EDT
Upload a file (often helps troubleshoot issues)	Browse... No file selected.

Figure 4: Submit a Zscaler Support Ticket

2. Add VPN credentials for branch office.

- Location: Zscaler Portal > Administration > Resources > VPN Credentials > Add VPN Credential



Authentication Type: IP

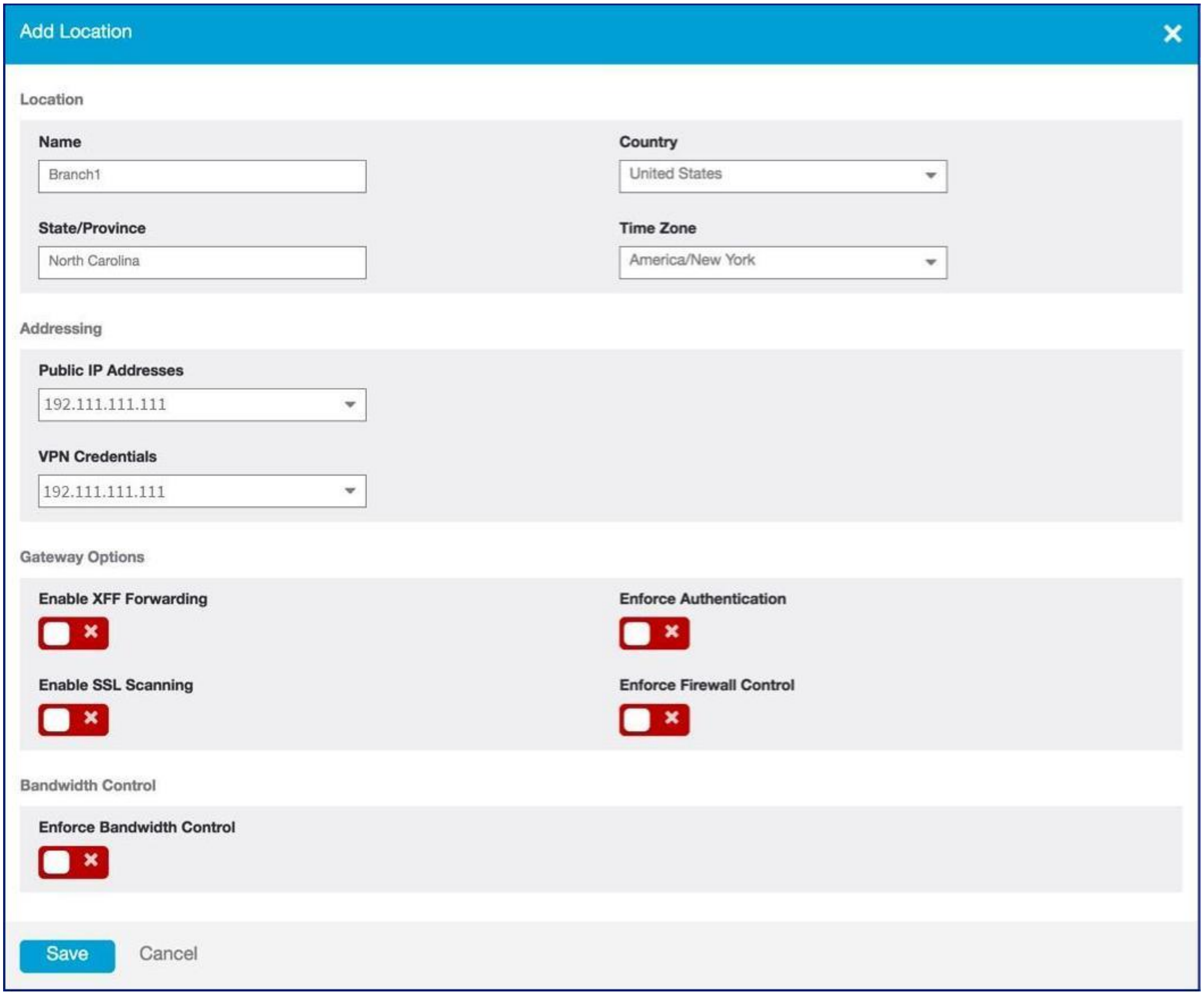
IP Address: 192.111.111.111

New Pre-Shared Key: ••••••

Confirm New Pre-Shared Key: ••••••

Figure 5 : Add VPN Credentials to Zscaler Admin

3. Add location for branch office and assign VPN credentials and IP address.
    - Location: Zscaler Portal > Administration > Resources > Locations > Add Location
    - Fill in Name, Country, State, Timezone, Public IP, and VPN Credential.



Add Location

Location

Name: Branch1

Country: United States

State/Province: North Carolina

Time Zone: America/New York

Addressing

Public IP Addresses: 192.111.111.111

VPN Credentials: 192.111.111.111

Gateway Options

Enable XFF Forwarding: ✕

Enforce Authentication: ✕

Enable SSL Scanning: ✕

Enforce Firewall Control: ✕

Bandwidth Control

Enforce Bandwidth Control: ✕

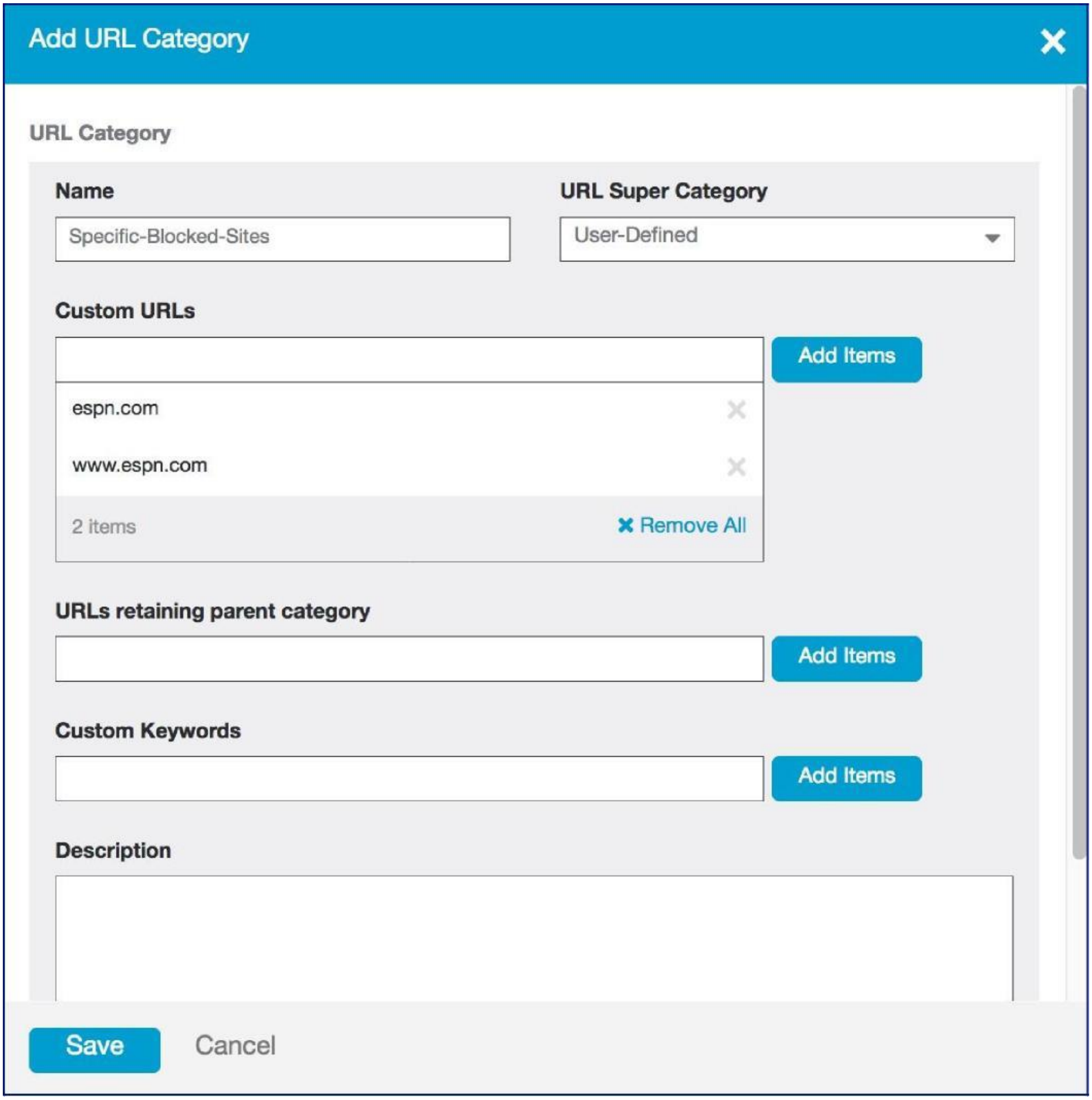
Figure 6 : Edit Location Settings in Zscaler

4. Gather ZEN endpoint IP address.

Please check the Zscaler portal for your ZEN endpoint IP address. For information on how to find your ZEN endpoint, please see the following Zscaler support article:

https://support.zscaler.com/hc/en-us/articles/211692786-How-do-I-locate-the-ZEN-IPaddresses-for-my-IPsec-VPN-tunnels-

1. Add custom URL category. (For this example, we will use espn.com.)
    - Location: Zscaler Portal > Administration > Resources > URL
       Categories > Add Fill in Name, URL Super Category, and Custom URLs fields



Add URL Category

URL Category

Name: Specific-Blocked-Sites

URL Super Category: User-Defined

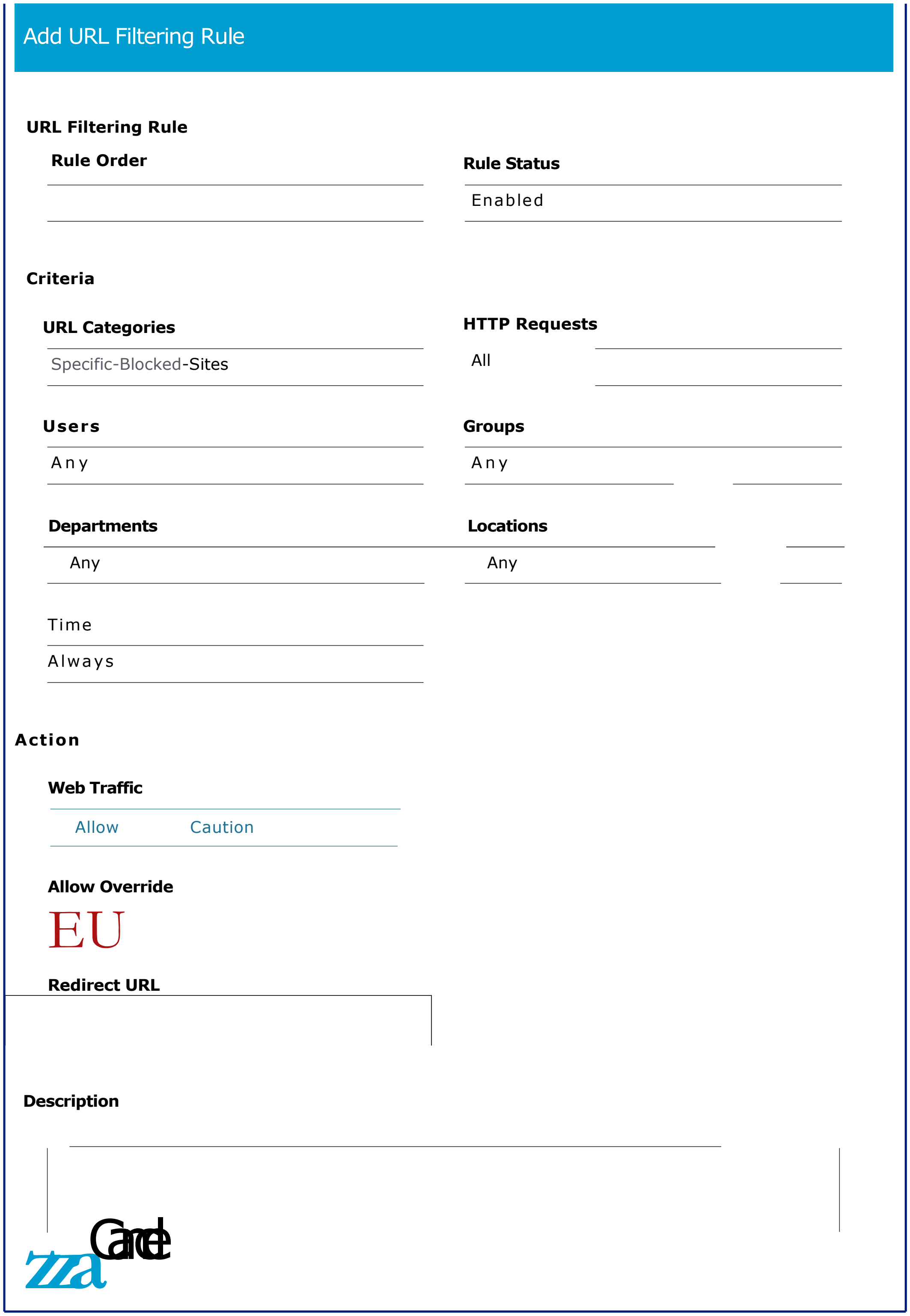
Custom URLs

- espn.com
- www.espn.com

2 items

Figure 7 : Add a URL Category to Zscaler

6. Add URL filtering rule referencing created custom URL category.
    - Location: Zscaler Portal > Policy > Web > URL & Cloud App Control > □ Add URL Categories: Select the previously created category from step 5.
    - Change Action > Web Traffic to Block.



Add URL Filtering Rule

URL Filtering Rule

Rule Order	**Rule Status**
	Enabled

Criteria

URL Categories	**HTTP Requests**
Specific-Blocked-Sites	All
Users	**Groups**
Any	Any
Departments	**Locations**
Any	Any
Time	
Always	

Action

Web Traffic

Allow Caution

Allow Override

EU

Redirect URL

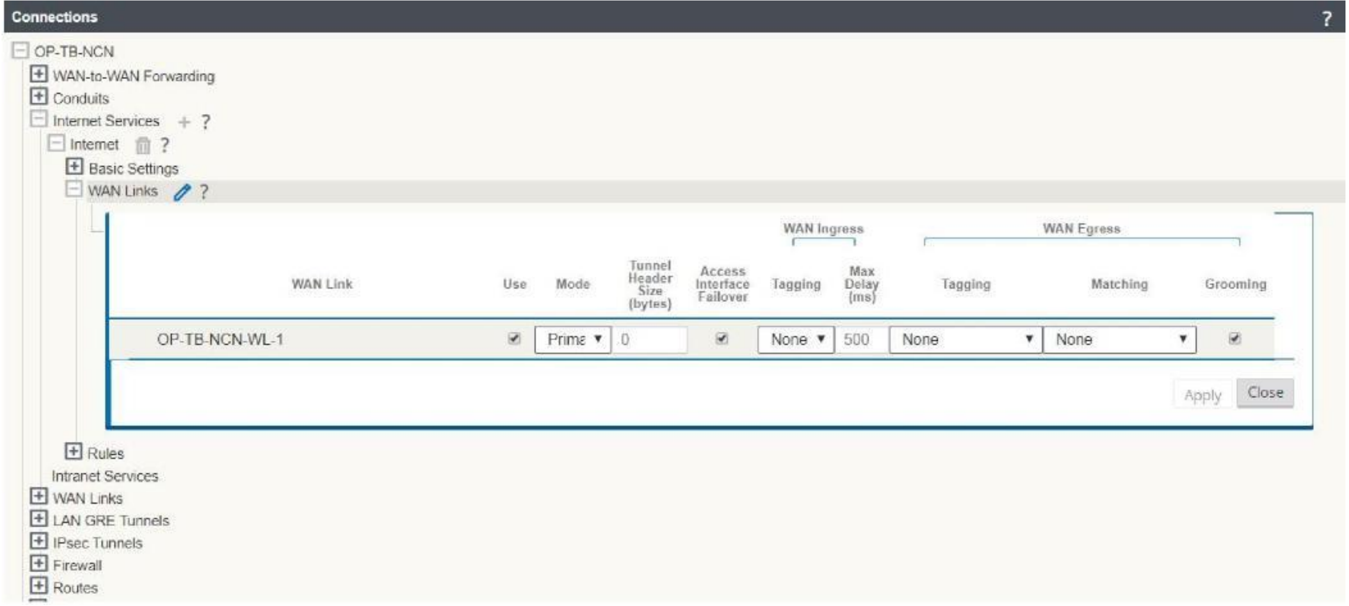
Description

Figure 8: Add URL Filtering Rule to Zscaler

Talari APNA Configuration

1. Add Internet Service to configuration

- Location: **Manage Network > APN Configuration Editor > Advanced > Connections > [Site] > Internet Services**
- Click the **Add** icon to create a new Internet Service.
- Click the **Edit** pencil, choose the desired WAN Link, check **Use** box, click **Apply**.

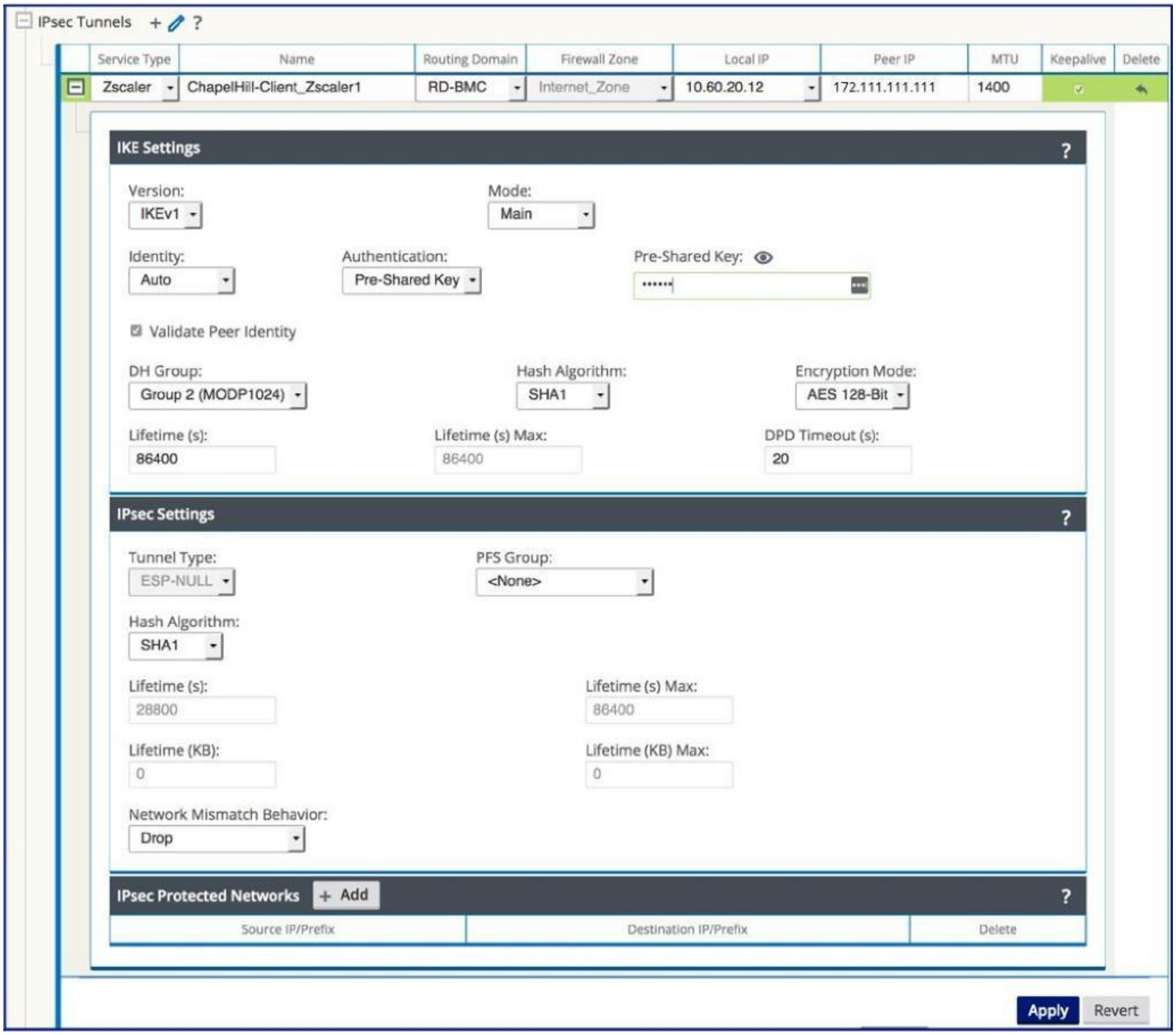


					WAN Ingress		WAN Egress		
WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	Tagging	Max Delay (ms)	Tagging	Matching	Grooming
OP-TB-NCN-WL-1	☑	Prima ▾	0	☑	None ▾	500	None ▾	None ▾	☑

Figure 9: Add Internet Service to APN

Note: The public IP Address of the WAN link associated with the Internet Service must be static, as IP+PSK authentication is supported, but FQDN is not.

2. Add Zscaler IPSec tunnel to configuration.
   - Location: **Manage Network > APN Configuration Editor > Advanced > Connections >** [Site] **> IPSec Tunnels > Add**
   - Select "Zscaler" Service Type tunnel, select local tunnel-endpoint VIP, fill in ZEN IP address and IKE Pre-Shared-Key, click **Apply**.



IPsec Tunnels

Service Type	Name	Routing Domain	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
Zscaler	ChapelHill-Client_Zscaler1	RD-BMC	Internet_Zone	10.60.20.12	172.111.111.111	1400	☑	

IKE Settings

Version: IKEv1

Mode: Main

Identity: Auto

Authentication: Pre-Shared Key

Pre-Shared Key: ••••••

☑ Validate Peer Identity

DH Group: Group 2 (MODP1024)

Hash Algorithm: SHA1

Encryption Mode: AES 128-Bit

Lifetime (s): 86400

Lifetime (s) Max: 86400

DPD Timeout (s): 20

IPsec Settings

Tunnel Type: ESP-NULL

PFS Group: <None>

Hash Algorithm: SHA1

Lifetime (s): 28800

Lifetime (s) Max: 86400

Lifetime (KB): 0

Lifetime (KB) Max: 0

Network Mismatch Behavior: Drop

IPsec Protected Networks

Source IP/Prefix	Destination IP/Prefix	Delete

Figure 10 : Talari IPSec Tunnel Configuration

Note: When you add an IPSec tunnel with a Service Type of “Zscaler”, the following default configurations will be applied:
Firewall – Add Deny policy from Default_LAN_Zone to Untrusted_Internet_Zone.
NAT – Delete default outbound PAT policy, if exists.
Routing – Adds 0/0 over Zscaler tunnel. Also adds /32 host-route of tunnel peer IP to gateway.

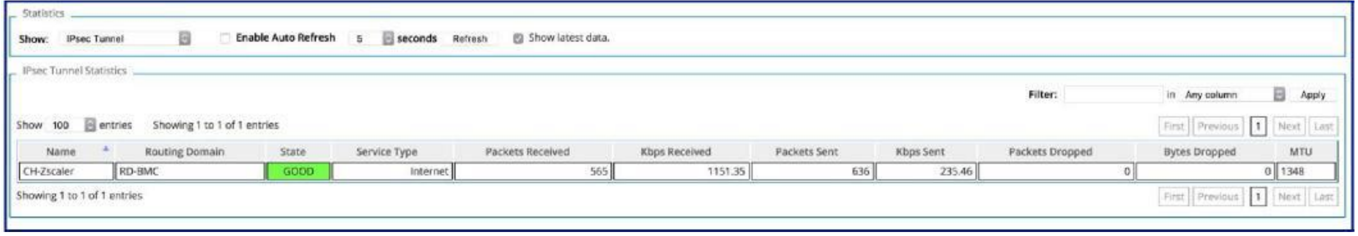
Save the configuration, then export it to the Change Management inbox. From Change Management, stage and activate the configuration.

Solution Verification

Verification Tasks

1. Generate Internet traffic from host.
    - HTTP or HTTPS to public website of choice.

2. Verify Zscaler IPSec tunnel status.
    - Location: On that Talari Appliance, **Monitor > Statistics > IPSec Tunnel**



Statistics

Show: IPsec Tunnel □ Enable Auto Refresh 5 seconds Refresh ☑ Show latest data.

IPsec Tunnel Statistics

Filter: in Any column Apply

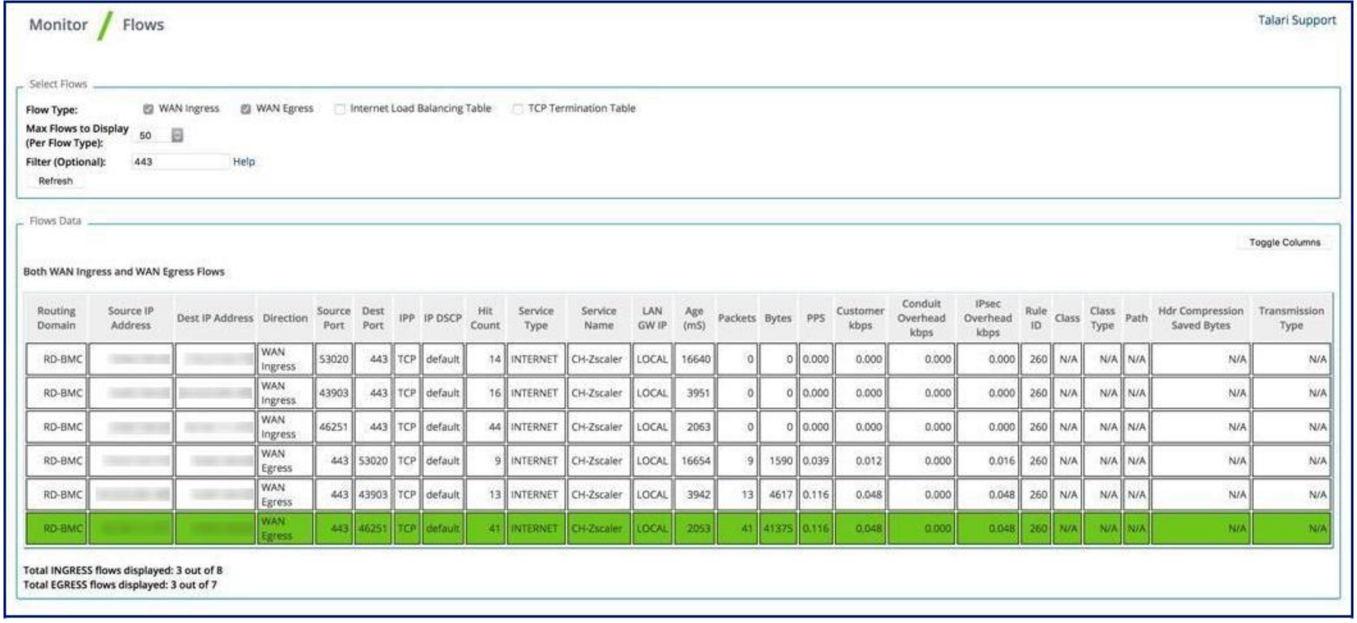
Show 100 entries Showing 1 to 1 of 1 entries

Name	Routing Domain	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
CH-Zscaler	RD-BMC	GOOD	Internet	565	1151.35	636	235.46	0	0	1348

Showing 1 to 1 of 1 entries

Figure 11 : Talari IPSec Tunnel Verification

3. Verify flows status.
    - Location: On the Talari Appliance, **Monitor > Flows** Verify the flows are Service Type INTERNET.



Monitor / Flows

Select Flows

Flow Type: ☑ WAN Ingress ☑ WAN Egress □ Internet Load Balancing Table □ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): 443 Help

Flows Data

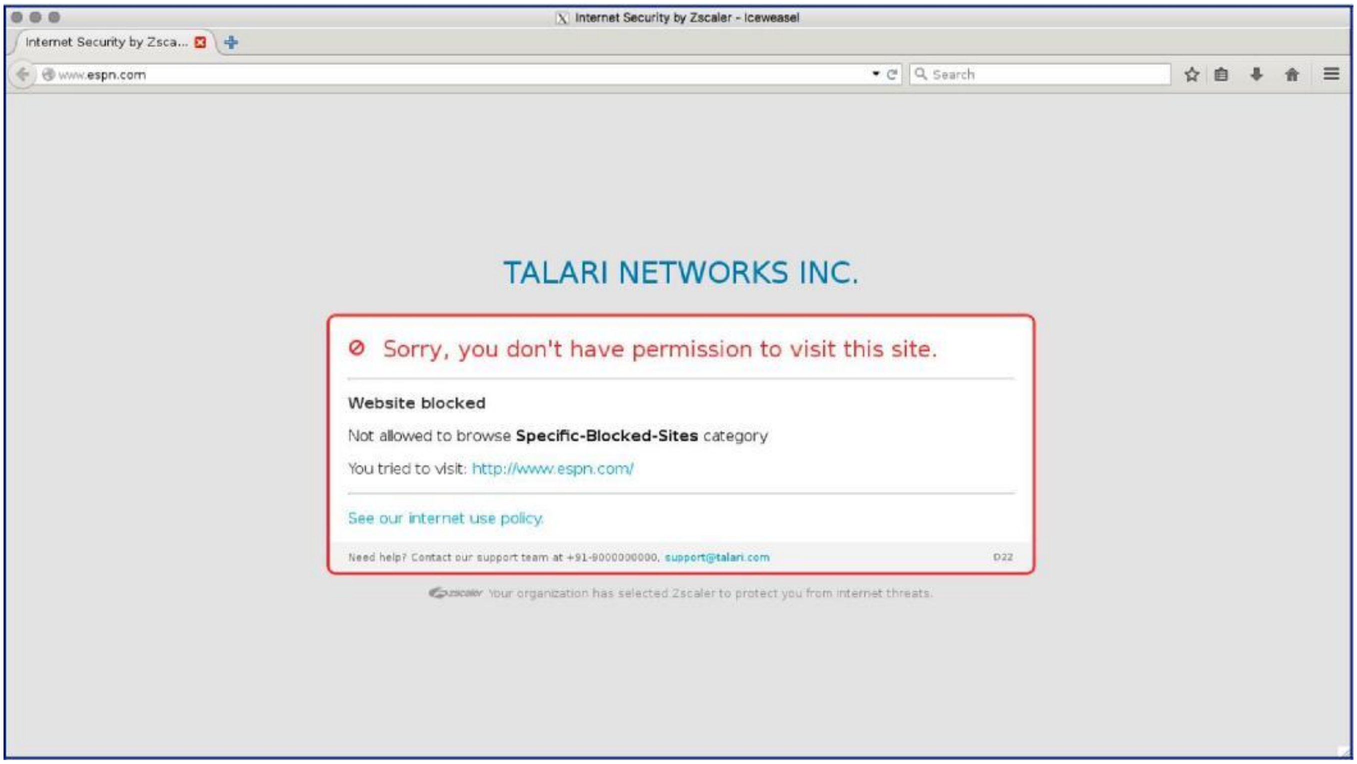
Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
RD-BMC	[redacted]	[redacted]	WAN Ingress	53020	443	TCP	default	14	INTERNET	CH-Zscaler	LOCAL	16640	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	[redacted]	[redacted]	WAN Ingress	43903	443	TCP	default	16	INTERNET	CH-Zscaler	LOCAL	3951	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	[redacted]	[redacted]	WAN Ingress	46251	443	TCP	default	44	INTERNET	CH-Zscaler	LOCAL	2063	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	[redacted]	[redacted]	WAN Egress	443	53020	TCP	default	9	INTERNET	CH-Zscaler	LOCAL	16654	9	1590	0.039	0.012	0.000	0.016	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	[redacted]	[redacted]	WAN Egress	443	43903	TCP	default	13	INTERNET	CH-Zscaler	LOCAL	3942	13	4617	0.116	0.048	0.000	0.048	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	[redacted]	[redacted]	WAN Egress	443	46251	TCP	default	41	INTERNET	CH-Zscaler	LOCAL	2053	41	41375	0.116	0.048	0.000	0.048	260	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 3 out of 8
Total EGRESS flows displayed: 3 out of 7

Figure 12 : Talari to Zscaler Flow Verification

4. Verify Zscaler is blocking the URL previously configured in Step 5 of Zscaler configuration.


Internet Security by Zscaler - Iceweasel
Internet Security by Zsca...
www.espn.com
Search

TALARI NETWORKS INC.

Sorry, you don't have permission to visit this site.

Website blocked

Not allowed to browse **Specific-Blocked-Sites** category

You tried to visit: http://www.espn.com/

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@talari.com D22

Your organization has selected Zscaler to protect you from internet threats.

Figure 13 9 : Zscaler Success

Appendix A:

Talari References:

For more information on configuring additional Talari capabilities, please go to https://www.talari.com/support/support-portal.

Zscaler References

For more information on configuring additional Zscaler capabilities, please go to:

Zscaler Knowledge Base

https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools

https://www.zscaler.com/tools

Zscaler Training and Certification

https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket

https://help.zscaler.com/submit-ticket