TALARI Networks
the Trusted SD-WAN Leader

Talari with Zscaler Cloud Security Gateway

Solution Deployment Guide

June 23, 2017

Table of Contents

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 ZIA Public Service Edge 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. To learn more about Talari, please visit:

https://www.talari.com

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

Audience

This document was designed for network administrators & architects who are familiar with Talari and need to tunnel Internet-bound traffic to Zscaler.

References

The following documents are available on the Talari Support site (www.talari.com/support):

- *Talari 7.0 New Feature Guide*

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us (support@talari.com).

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).

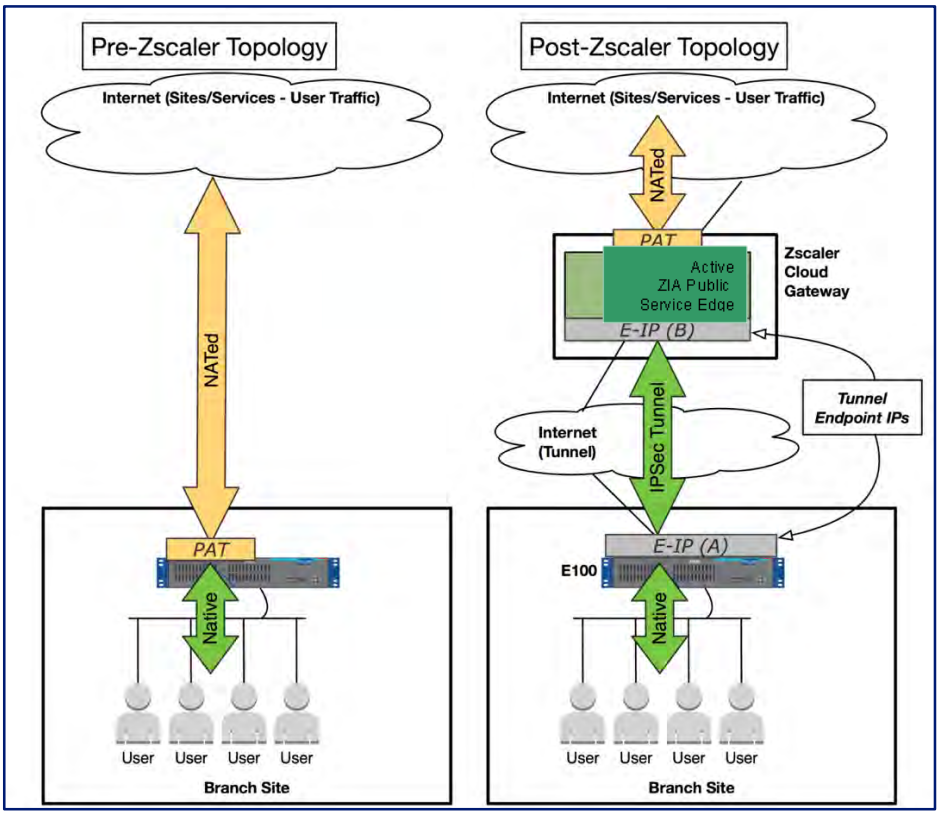

Figure 1: Pre/Post Topologies

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 ZIA Public Service Edge 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 Internet-destined traffic leaving the branch directly to Zscaler for cloud security filtering of traffic to-and-from the Internet:

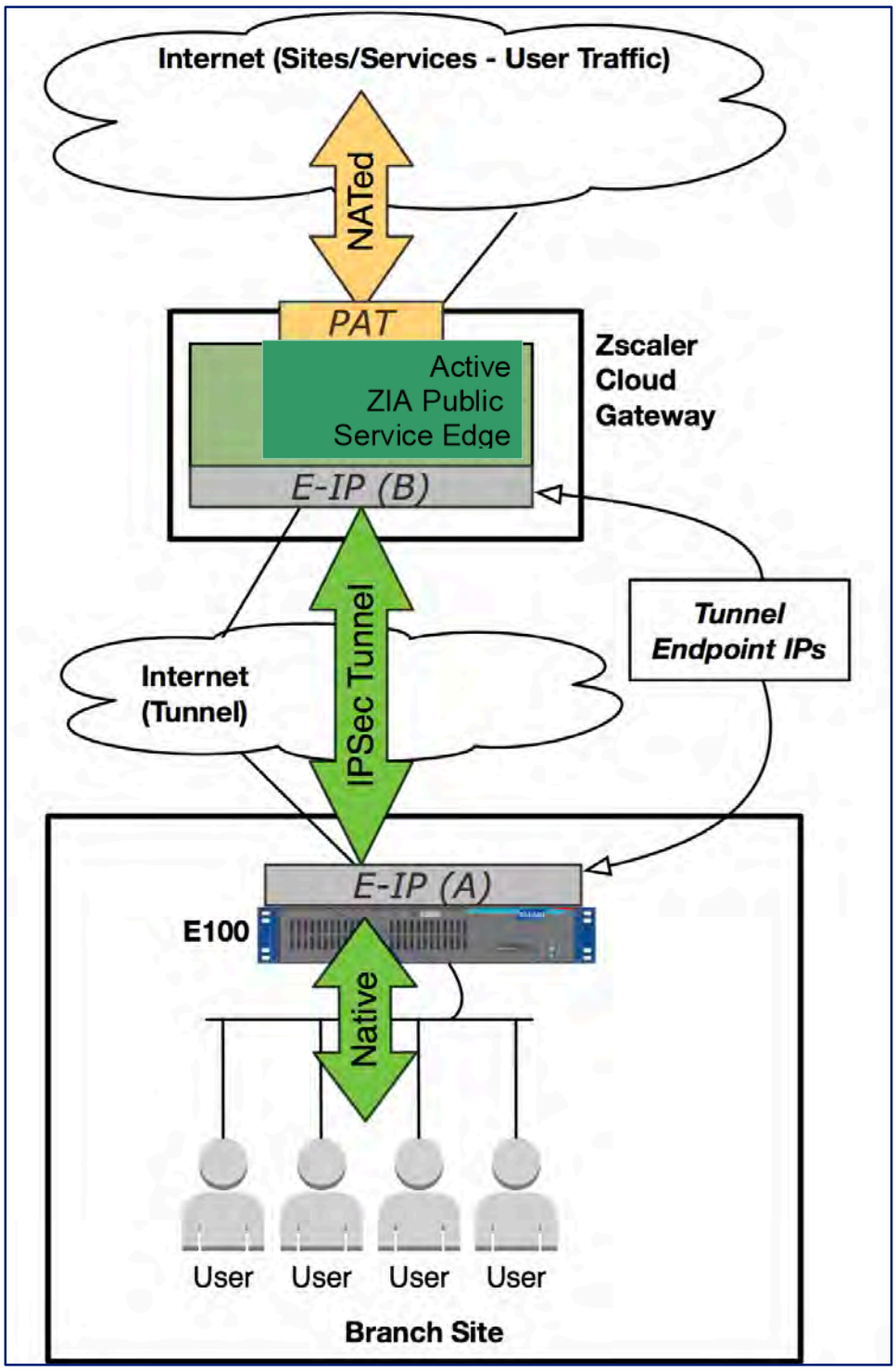

Figure 2: Zscaler Enabled Branch Office

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 ZIA Public Service Edge 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.
- 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

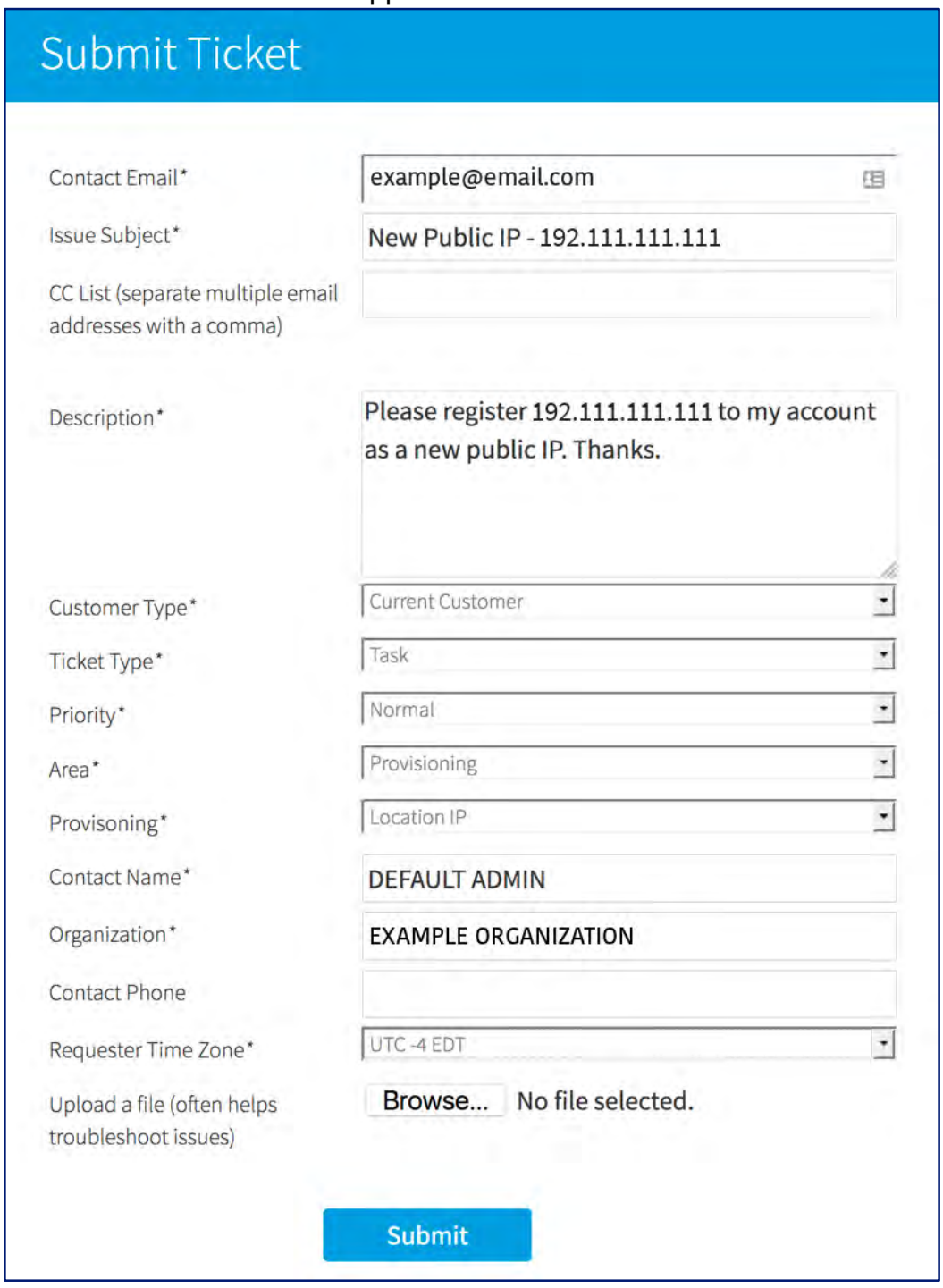

Figure 4: Submit a Zscaler Support Ticket

2. Add VPN credentials for branch office.
    - Location: Zscaler Portal > Administration > Resources > VPN Credentials > Add VPN Credential

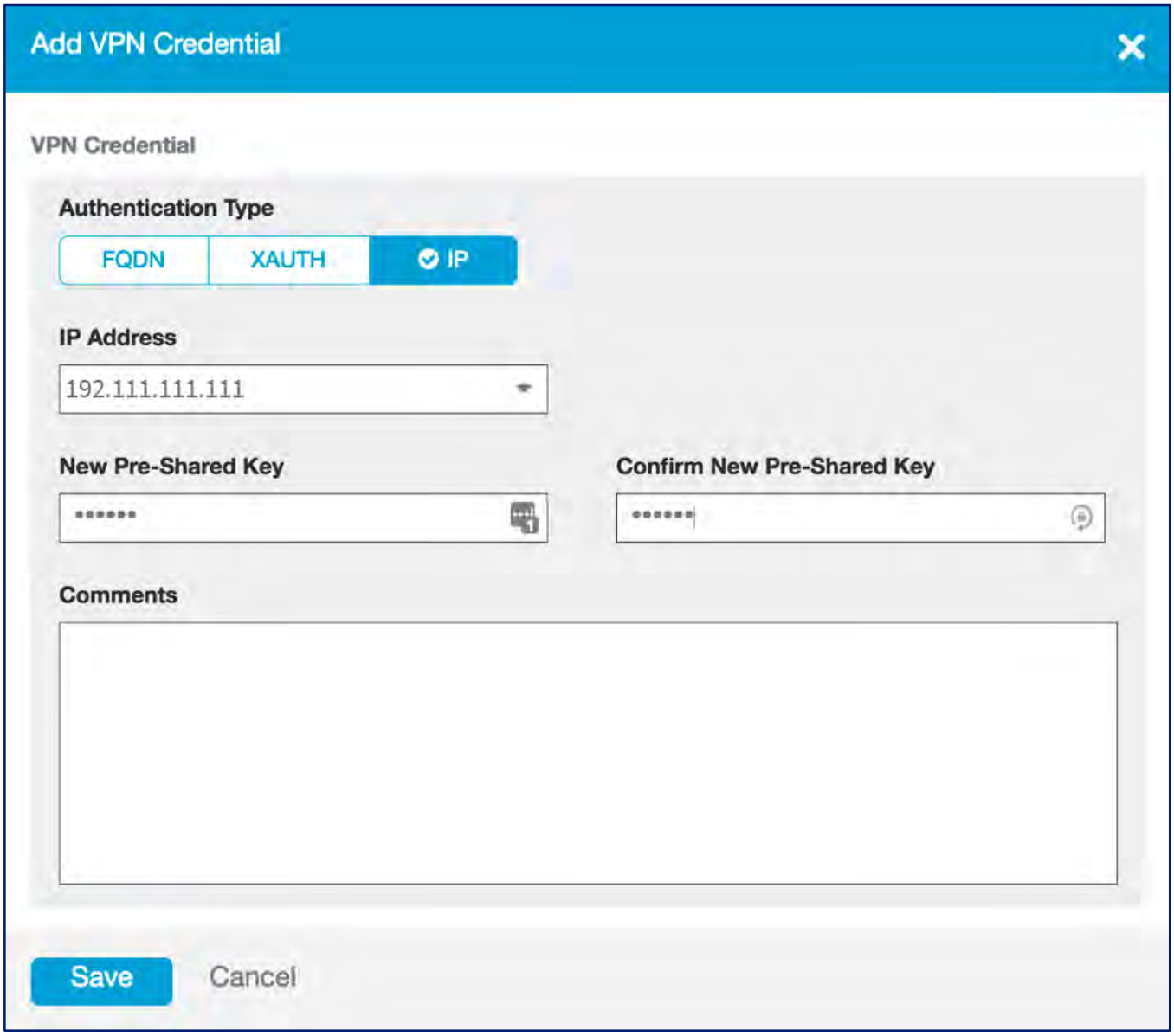

Figure 5: Add VPN Credentials to Zscaler Admin

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.

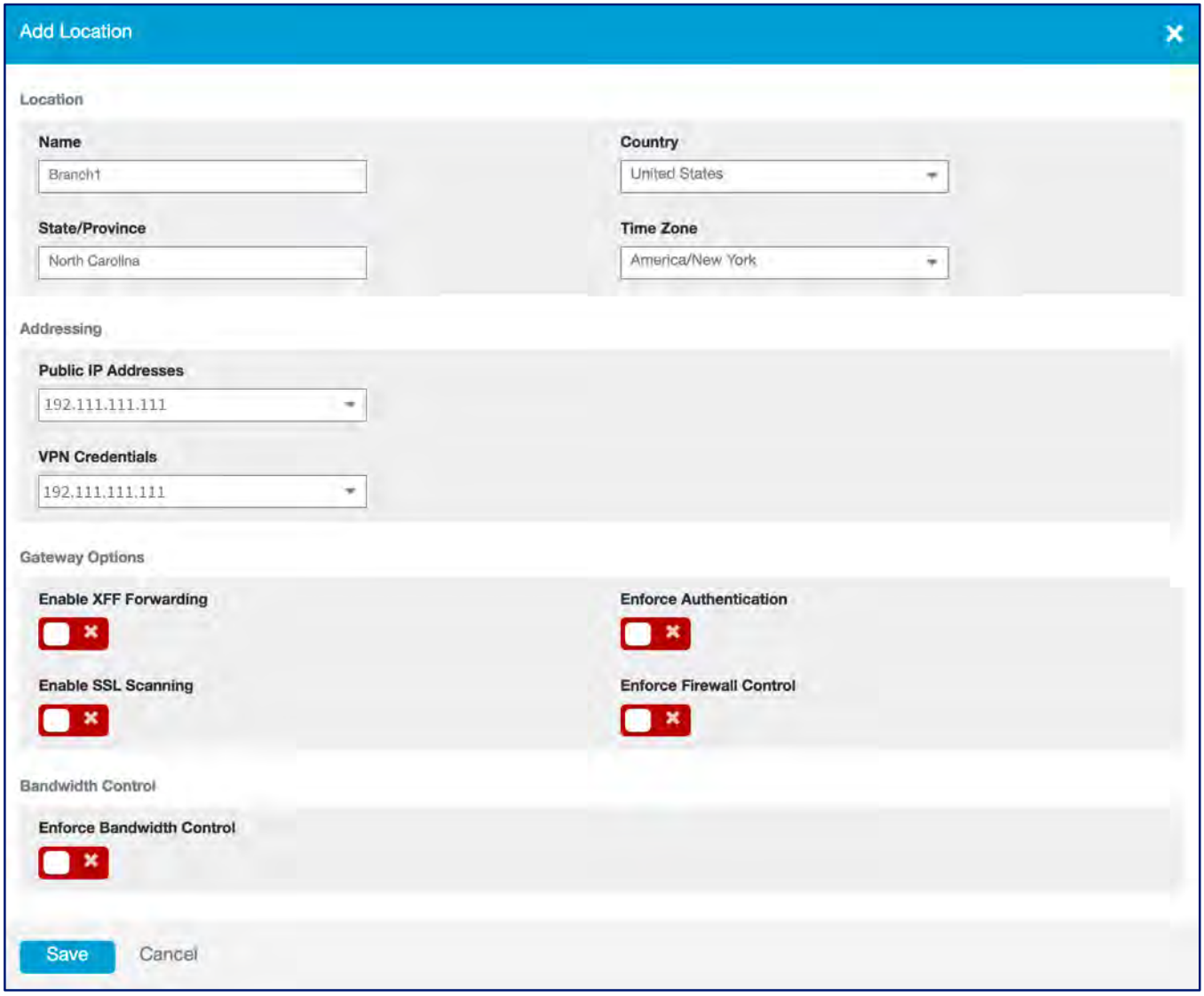

Figure 6: Edit Location Settings in Zscaler

4. Gather ZIA Public Service Edge endpoint IP address.

   Please check the Zscaler portal for your ZIA Public Service Edge endpoint IP address.

5. 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

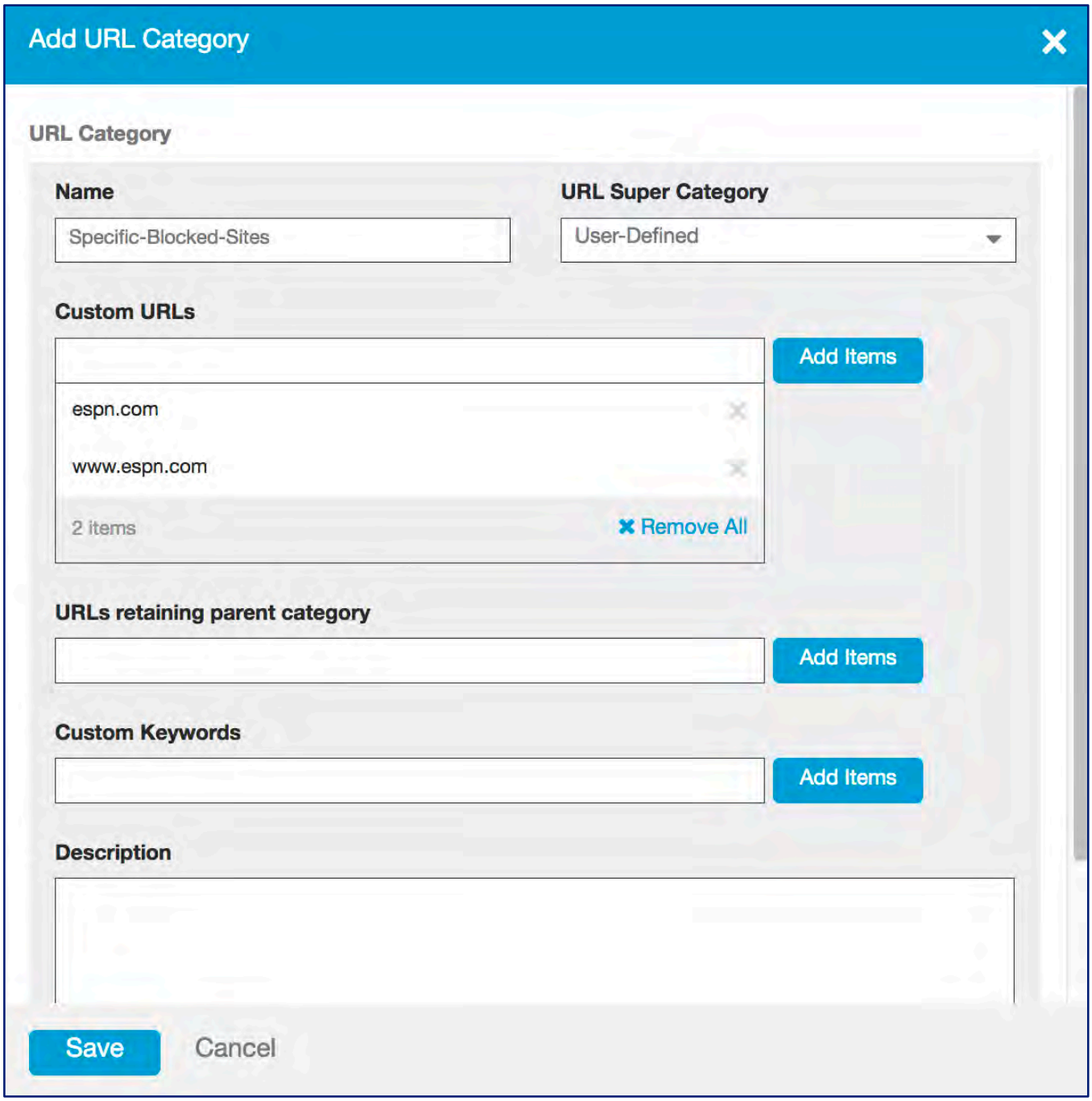

Figure 7: Add a URL Category to Zscaler

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.

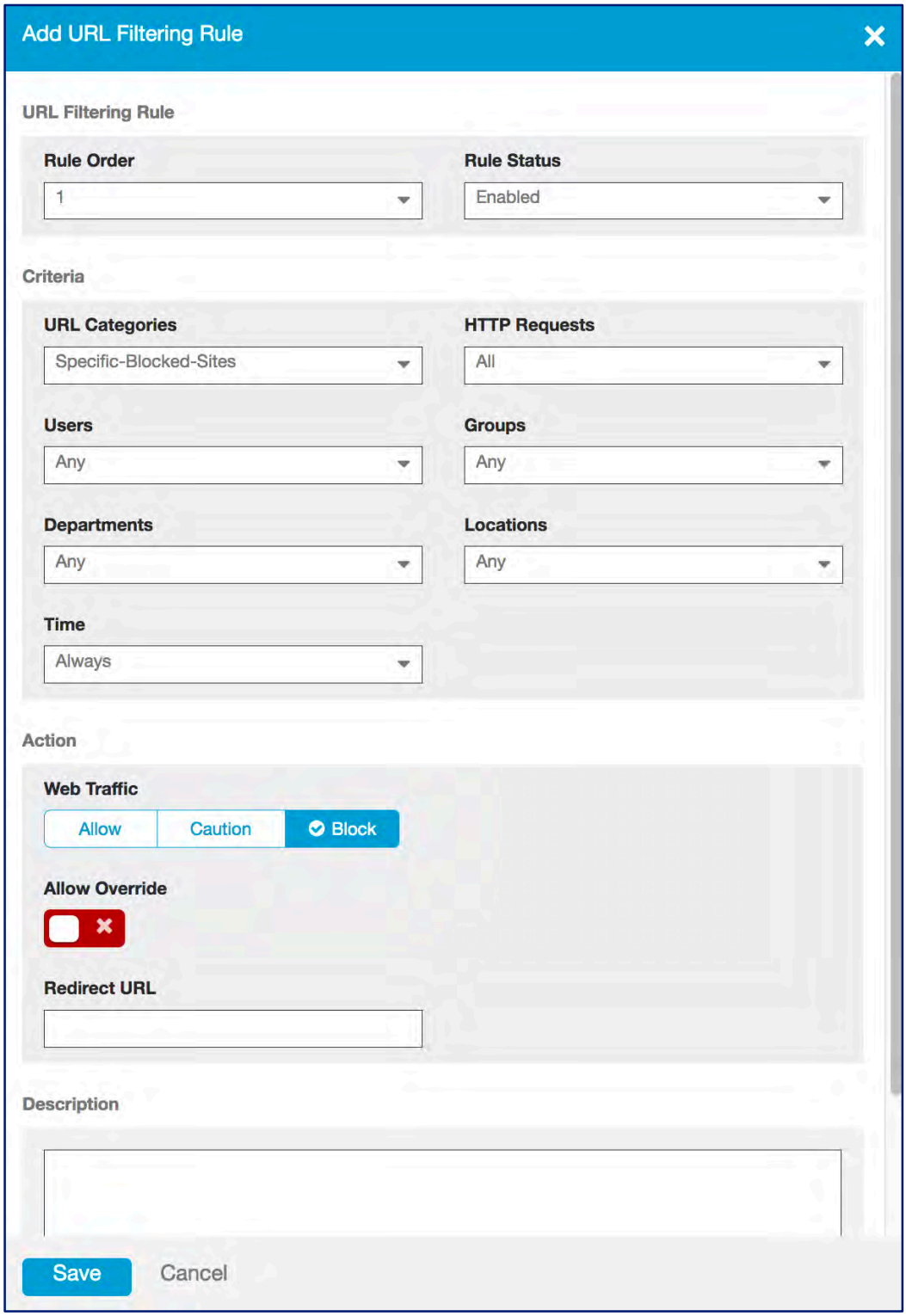

Figure 8: Add URL Filtering Rule to Zscaler

Talari APNA Configuration

1. 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 the ZIA Public Service Edge IP address and IKE Pre-Shared-Key, click Apply.

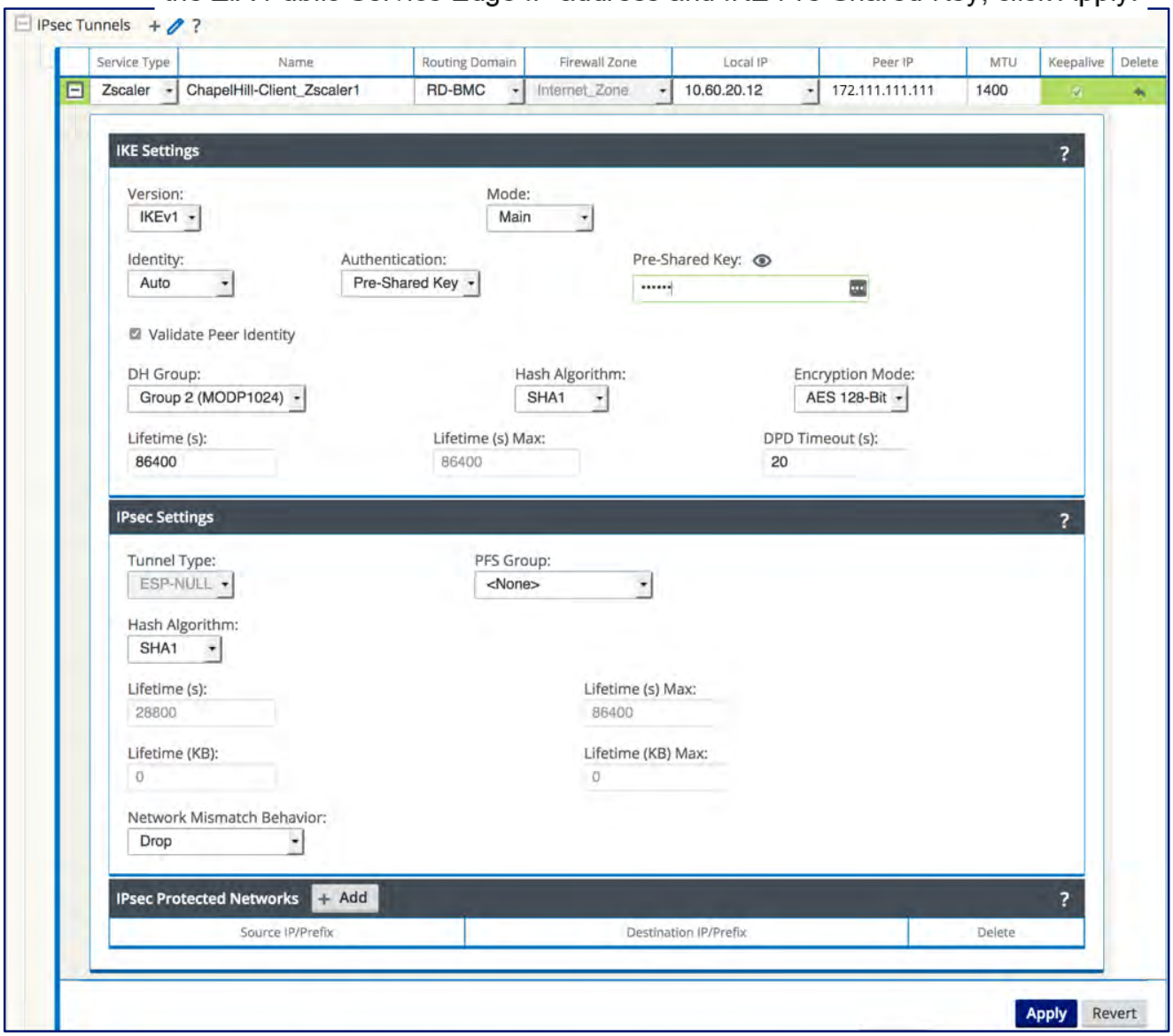

Figure 9: Talari IPSec Tunnel Configuration

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**

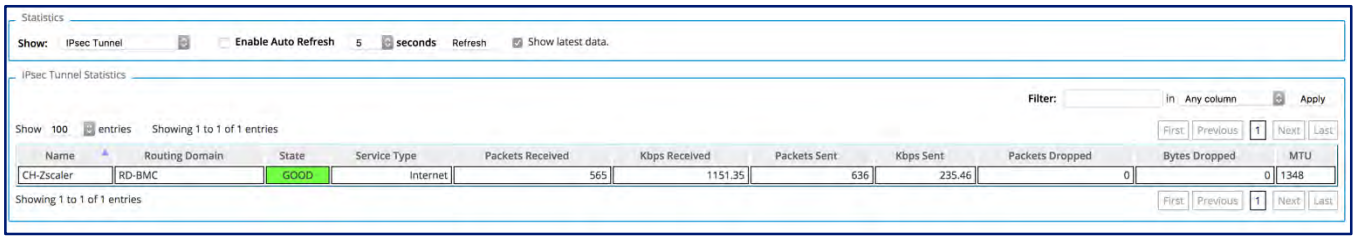

Figure 10: Talari IPSec Tunnel Verification

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

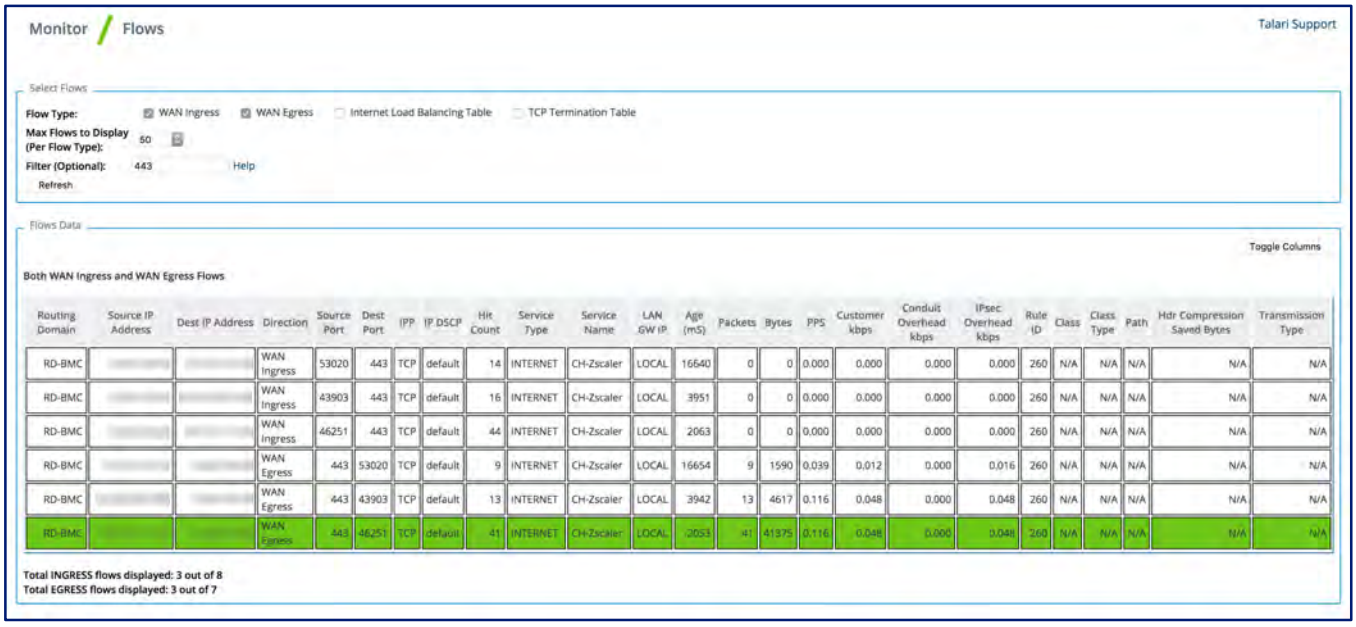

Figure 11: Talari to Zscaler Flow Verification

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

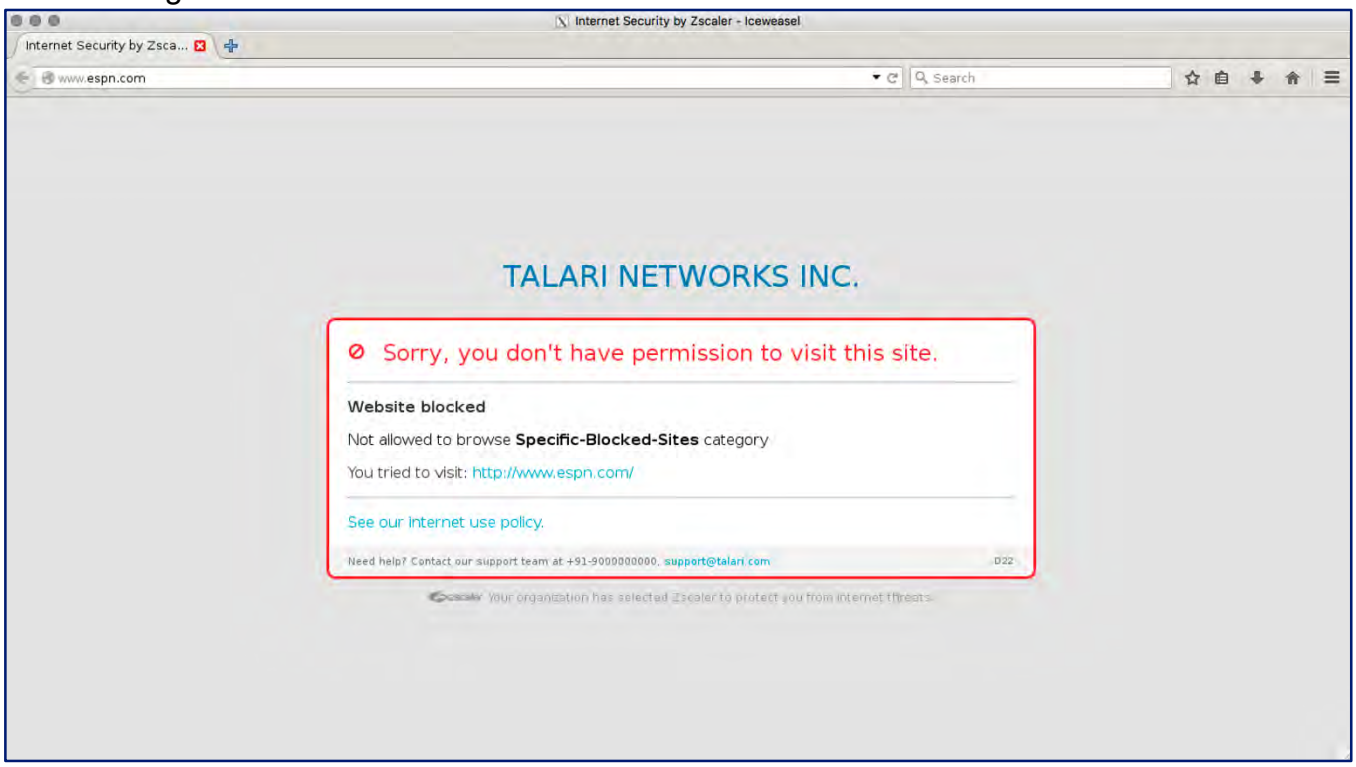

Figure 12: Zscaler Success

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

TALARI Networks

About Talari

Talari Networks, the trusted SD-WAN technology and market leader, engineers the internet and branch for maximum business impact by designing failsafe WANs that deliver superior business-critical application reliability and resiliency, while unlocking the simplification and cost reduction benefits of branch consolidation.

Passionate and committed to their customers, Talari has incorporated eight years of innovation into five generations of product and is successfully deployed across thousands of sites in over 40 countries.

www.talari.com