Use IP Allowlisting to enforce zero trust policies for specific SaaS Applications integrated with Okta

Use Network Zones and Sign-on Policies in Okta to ensure use of a Service Tunnel when authenticating to a SaaS Application like Salesforce

Updated on 5 minutes to read Contributors

ON THIS PAGE:

Overview
Steps
Step 1: Register a Service Tunnel for Public Domains
Step 2: Create a new network zone in Okta
Step 3: Update sign-on policy for all relevant applications

Overview

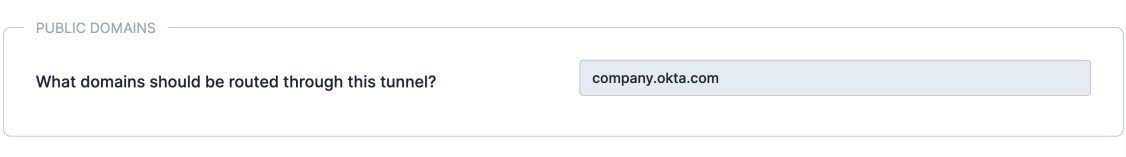
These steps outline how to use Network Zones and Sign-on Policies in Okta to require a user to have a Service Tunnel established in order to authenticate to the specified SaaS application(s).

Steps

Step 1: Register a Service Tunnel for Public Domains

1.1 Register a Service Tunnel for Public Domains.

1.2 Configure the Service Tunnel to include the relevant Okta domain used for authentication (e.g., `CSEsecurity.okta.com`).



Step 2: Create a new network zone in Okta

2.1 Create a network zone for the Access Tier(s).

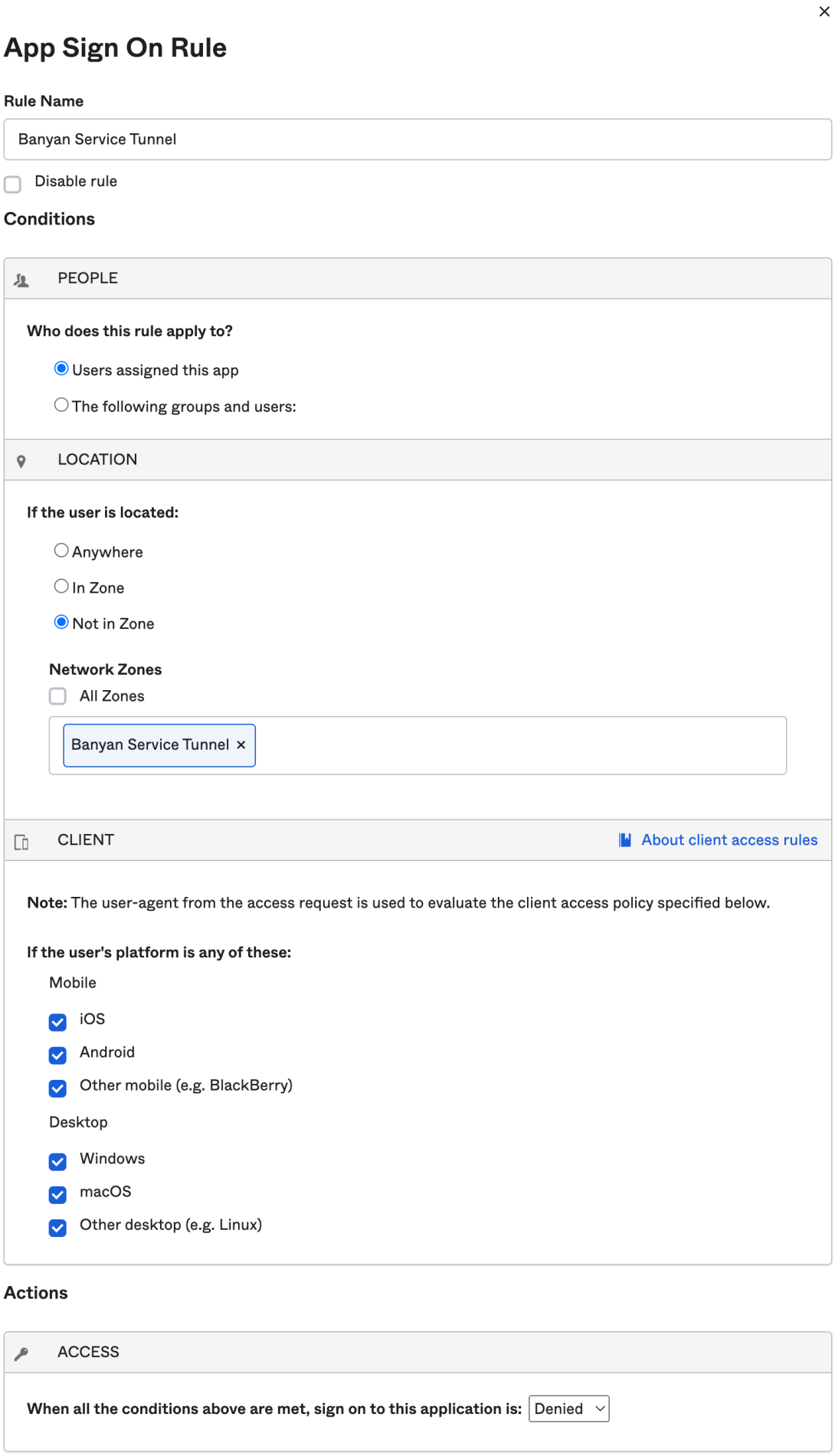
2.2 In the Okta Admin Console, navigate from **Security** > **Networks**. From the **Add Zone** dialog, select **IP Zone**.

2.3 In the **Zone Name** field, enter a name for the IP zone (e.g., `CSE Service Tunnel`).

2.4 In the Gateway IPs field, enter the IP Address(es) of the relevant Access Tiers

> **Note:** You can separate IPs and IP ranges with a new line or a comma.

2.5 Select **Save**.


App Sign On Rule
Rule Name
Banyan Service Tunnel
Disable rule
Conditions
PEOPLE
Who does this rule apply to?
Users assigned this app
The following groups and users:
LOCATION
If the user is located:
Anywhere
In Zone
Not in Zone
Network Zones
All Zones
Banyan Service Tunnel ×
CLIENT
About client access rules
Note: The user-agent from the access request is used to evaluate the client access policy specified below.
If the user's platform is any of these:
Mobile
iOS
Android
Other mobile (e.g. BlackBerry)
Desktop
Windows
macOS
Other desktop (e.g. Linux)
Actions
ACCESS
When all the conditions above are met, sign on to this application is:
Denied

Step 3: Update sign-on policy for all relevant applications

Configure an app sign-on policy to require a Service Tunnel to be registered before authenticating to specific SaaS application(s).

3.1 In the Okta Admin Console, navigate from **Applications** > **Applications**. Select the desired application.

3.2 Select the **Sign On** tab, and scroll down to the **Sign On Policy** section.

3.3 Create a Sign On rule, by which sign on to the application is denied if the user is not located in the CSE Service Tunnel zone.

Expected behaviour:

If the user **DOES NOT** have the Service Tunnel connection established, the user will receive an error message indicating that App Access is Locked. In addition, the user will be denied access from launching the application from the Okta End User Dashboard.

Error during SP-init flow:

App Access Locked

Access to this application is not allowed at this time due to a policy set by your administrator. If you're wondering why this is happening, please contact your administrator.
If it's any consolation, we can take you to your Okta home page.

Go to Homepage

SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

Concepts

Components

Release Notes

Guides

Quick Start Guides

Solutions

Feature Guides

API Guide