Illumio® Plugin for Netskope Cloud Exchange

Integration Guide

The integration of Illumio and Netskope extends Zero Trust security principles to remote access architectures. By using Illumio's Zero Trust Segmentation (ZTS) and Netskope's Security Service Edge (SSE) capabilities, this architecture ensures dynamic access controls and security across hybrid and multi-cloud environments.

Table of Contents

Introducing the Illumio Plugin for Netskope Cloud Exchange 4
Architecture Components 4
Data Flow and Integration 4
Data Collection 4
Data Aggregation 4
Policy Enforcement 5
Deployment Topology 5
Installing and Configuring 5
Troubleshooting 7
Testing and Verification 7

Introducing the Illumio Plugin for Netskope Cloud Exchange

The integration of Illumio and Netskope extends Zero Trust security principles to remote access architectures. By using Illumio's Zero Trust Segmentation (ZTS) and Netskope's Security Service Edge (SSE) capabilities, this architecture ensures dynamic access controls and security across hybrid and multi-cloud environments.

Architecture Components

Three components are part of the architecture:

- Illumio Policy Compute Engine (PCE)
  - Central management point to define and enforce security policies for workloads and endpoints.
  - Collects telemetry data from various endpoints and network segments.
  - Central management for defining and managing labels.
- Netskope One
  - Provides secure access to cloud services, applications, and the internet.
  - Enforces security policies based on user identity, device posture, and real-time threat intelligence.
- Netskope Cloud Exchange
  - Facilitates the exchange of data between Netskope and other security platforms.
  - The Illumio Plugin is published in Cloud Exchange.

Data Flow and Integration

This section provides an overview about the data flow and integration process.

Data Collection

- The Illumio PCE gathers telemetry and security data such as Illumio labels and policies from protected workloads and endpoints.
- Netskope collects data on user activities, application usage, and network traffic.

Data Aggregation

- The Illumio PCE and Netskope SSE share relevant security data through secure API.
- The combined data is used to enhance security policies and enforcement across the infrastructure.

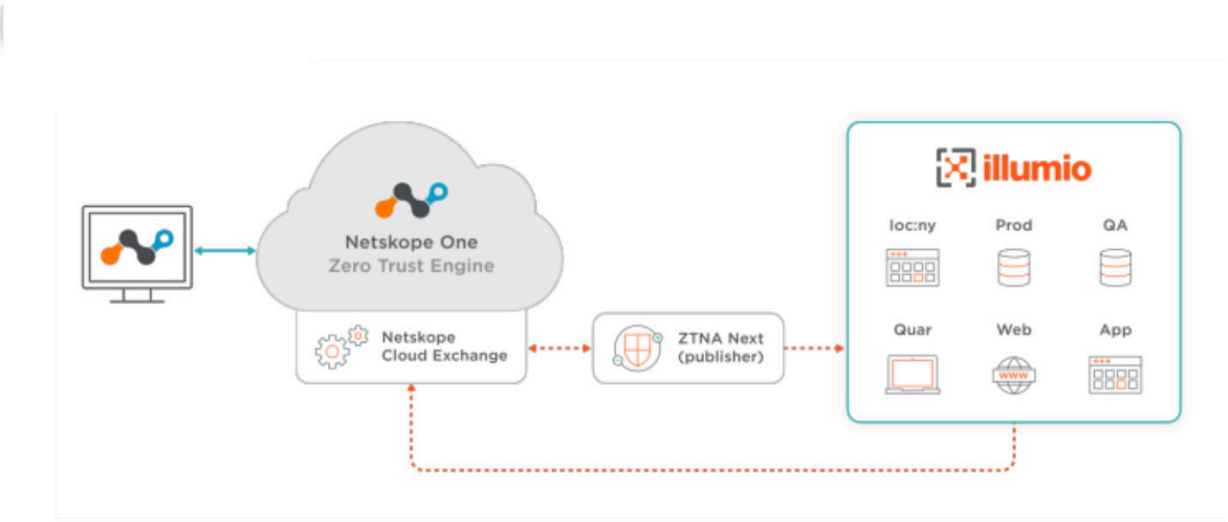
Policy Enforcement

- Netskope One enforces access policies based on real-time label data from the Illumio PCE.
- Netskope applies adaptive access controls and threat protection, informed by Illumio's segmentation policies.

Deployment Topology

The deployment topology for Illumio and Netskope integration provides data collection and policy enforcement across the entire IT infrastructure.

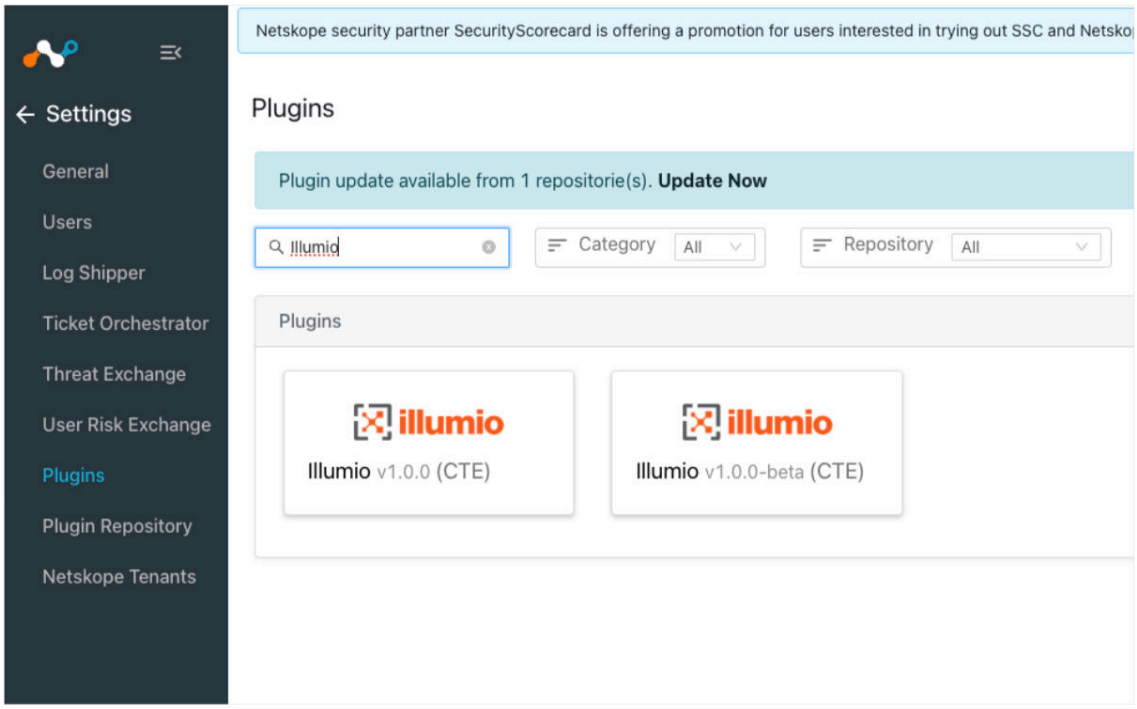
This diagram shows a high-level architecture flow.



Installing and Configuring

This section provides step-by-step installation and configuration instructions.

1. Access the Illumio Plugin for Netskope Cloud Exchange through the Cloud Exchange by navigating to Home > Settings > Plugins and search for Illumio.



2. Click Plugin and define the following parameters.

Parameters	Description
Configuration Name	Pick any reference name for the configuration. For example, IllumioConfig.
Sync Interval	Define the Sync Interval based on the organizational requirements. This would normally be the same as how often you update labels for your workloads. For example, 10 minutes.
Aging Criteria	Define how often the oldest data will be deleted.
Override Reputation	Leave this parameter empty.

3. Check Enable SSL Verification and click Next.
4. On the Next Page, enter your Illumio Credentials.

Parameters	Description
PCE URL	This is your Illumio PCE URL. Ensure that Cloud Exchange has network connectivity and access to PCE.For example, https://my.pce.com
PCE Port Number	Define the Illumio API Port number. The default port is 443. Change it to the desired port number if it is different from the default port number.
PCE Organization ID	Find Org ID by navigating to “My profile” after logging into the PCE. For example, 65865.
API Authentication Username	Create a new API key by navigating to “My API Keys” in the PCE and Click Add. Copy Authentication Username.
API Secret	Copy the Secret from previous output and paste it here.

Parameters	Description
Label Scope	Define the label scope in key value pairs to pull IPs against these labels from the PCE. Here are some examples: • app: HR • app: HR, loc: AWS • app: HR, loc: AWS • app: HR, loc: AWS • role: DC app: HR loc: AWS, role: DC, env: QA
Enable Tagging	Select Yes to enable tagging.

5. Click Save.
6. To configure information fetched by the plugin to pass it to Netskope for policies, follow these steps to define Business Rules and Sharing config.

Troubleshooting

Keep track of errors when you click save during the final step of installing the plugin. If any of the following parameters are incorrect, you will not be able to save the configuration.

Here are some examples of common errors you may see.

- API credentials are specified incorrectly.
- The port number or URL is configured incorrectly.
- The Organization ID is configured incorrectly.

Testing and Verification

This section provides a list of tests you can perform to verify that you have installed the plugin correctly.

1. After you configure the plugin, verify the configuration by navigating to Logging on the bottom left area of Netskope Cloud Exchange.
   Based on the sync intervals defined in the configuration, this section shows a message indicating how many indicators (IPs) were fetched against the configured labels.
2. Verify the correct functionality by navigating to Threat Exchange > Plugins.
   It should show the last run value and the current Status.
3. Verify the IP addresses that are being retrieved from the PCE against the configured labels by navigating to: Threat Exchange > Filter > IoCs By Sources. Check Tags > Any In > app:ZTNA (Defined Tag in plugin Configuration).
4. Apply Filter.