Troubleshoot IP Layer Enforcement Enablement for Roaming Client

Contents

Introduction

This document describes how to troubleshoot IP Layer Enforcement enablement for the roaming client.

Overview

You can use this guide to troubleshoot issues with enabling IP Layer Enforcement in the roaming client. IP Layer Enforcement enables independently from the roaming client mode. Enabling or disabling this feature depends on policy synchronization and specific parameters returned from the sync server.

Expected Functionality

The roaming client enables IP Layer Enforcement regardless of the current client mode. This process is triggered by a policy sync.

- When the roaming client syncs, it sends the bundle ID to the sync server (Hydra).
- The Hydra server checks the policy associated with the bundle ID.
- The sync response includes**ipFilteringEnabled**(1 for true, 0 for false) and**iplKillSwitch**(1 for true, 0 for false).
- The**iplKillSwitch**value indicates if the feature is unavailable or limited.
    - This applies to all AnyConnect roaming clients unless the AnyConnect IP Layer Enforcement feature flag is enabled.
    - Without this flag, the feature does not activate even if the policy enables it.

Enable and Disable Triggers

The roaming client establishes an IP Layer Enforcement VPN tunnel if all conditions are met:

- **ipFilteringEnabled**is 1 (true)
- **iplKillSwitch**is 0 (false)

The roaming client does not enable IP Layer Enforcement if any of these are true:

- **ipFilteringEnabled**is 0 (false)
- **iplKillSwitch**is 1 (true)

Troubleshoot Common Issues

- If the client does not enable IP Layer Enforcement, but the final policy shows it as enabled, check that the kill switch is not on.
- There can be a 30-minute delay before activation.

- The policy bundle might not be sent during the initial sync if it is not available.
- IP Layer Enforcement enables after the next sync, which occurs about 25 minutes later.