

Discontinuation of Automatic Third-Level Failover for IPsec Tunnels

Contents

[Introduction](#)

[Overview](#)

[Why are we making this change?](#)

[What happens to the disaster recovery data centers?](#)

[What if I still want to use third-level of data center failover?](#)

Introduction

This document describes the discontinuation of automatic third-level failover for IPsec tunnels.

Overview

Starting January 18th, 2023, Cisco Umbrella has stopped supporting automatic third-level failover (disaster recovery) for IPsec tunnels in the United States, Canada, Brazil, and Mexico.

Changes in Europe, Africa, Asia, and Australia are to follow.

Why are we making this change?

When Cisco Umbrella first introduced IPsec tunnel support for Secure Internet Gateway we made architectural decisions to maximize service reliability while minimizing configuration complexity. Some key features included anycast based IPsec failover with data center pairs, as well as third-level failover to disaster recovery data centers if both data centers in a pair become unavailable.

Due to continued investment in operations and architecture of our systems, third-level failover is no longer appropriate as a default configuration.

What happens to the disaster recovery data centers?

The three data centers previously dedicated to third-level IPsec failover are to be repurposed as regular IPsec data centers, available for primary or backup IPsec tunnels.

Dallas–Fort Worth is already available for use with primary or backup IPsec tunnels. Amsterdam, and Osaka are to follow. More information is available at [Connect to Cisco Umbrella Through Tunnel](#).

What if I still want to use third-level of data center failover?

For most customers we recommend configuring two tunnels, one to each DC in a region, with unique IPsec tunnel IDs per tunnel, however customers can choose to set up one, two, three, or even four IPsec tunnels from a given site. One tunnel provides redundancy via automatic anycast based failover.