Troubleshoot SD-WAN Auto Tunneling

Contents

Introduction

Overview

Details

Troubleshooting and FAQ

- Q: What happen if I cannot see the Tunnel register on Umbrella Dashboard?
- Q: Why is the IPSec auto tunnel is connecting to DC outside of the region?
- Q: What happens if I rename the Tunnel name on Umbrella Dashboard to reflect a customer's site?

Introduction

This document describes how SD-WAN Auto Tunneling works.

Overview

This article explains how SD-WAN router Auto-Tunneling works.

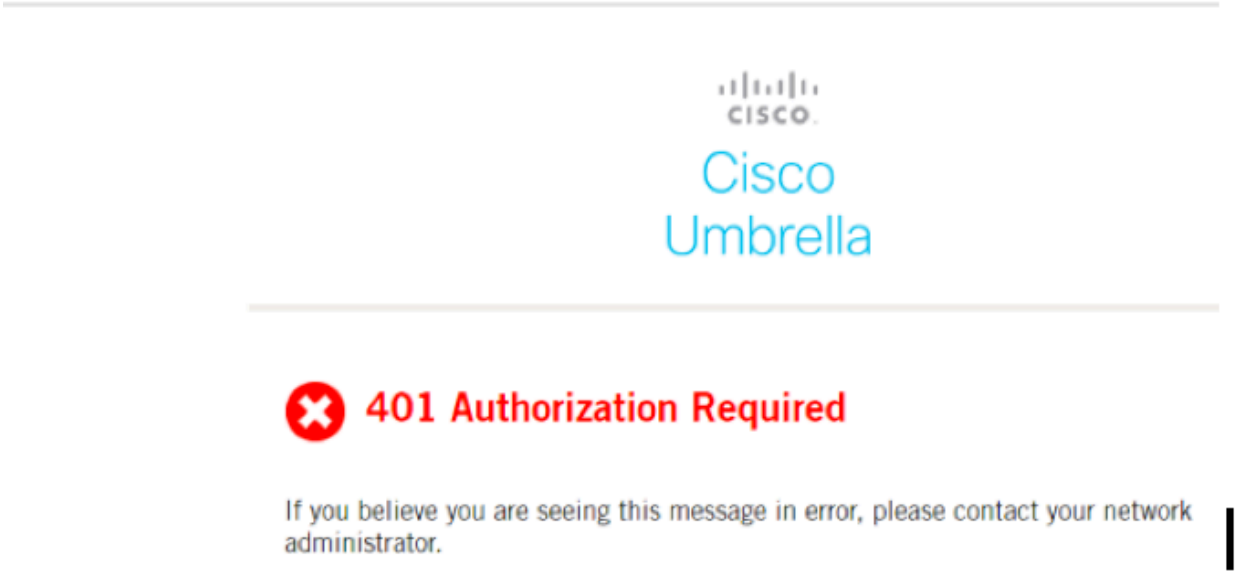
Prerequisite and configuration guide is available:

- Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.x
- Security Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20

Details

Once the configuration is completed on Cisco vManage, the template is pushed down to SD-WAN router:

- The SD-WAN router makes an API call (to **management.api.umbrella.com with Key + Secret**) to create the tunnel on Umbrella Dashboard
- Next, SD-WAN router (prior to v17.5) resolves the hardcoded FQDN and determine closest DC:
  - **global-a.vpn.sig.umbrella.com**
  - **global-b.vpn.sig.umbrella.com**
- On v17.5 or newer, vManage provides the option to choose the Umbrella Tunnel DC. This is helpful when the hardcoded FQDN resolve to an undesired Umbrella Tunnel DC.



screenshot.png

- SD-WAN router initiates IPsec connection to Umbrella VPN head-end

Troubleshooting and FAQ

Q: What happen if I cannot see the Tunnel register on Umbrella Dashboard?

A: Check if the Umbrella Management API Key and Secret are correct. Ensure there is nothing blocking connection to management.api.umbrella.com over TCP 443

Q: Why is the IPSec auto tunnel is connecting to DC outside of the region?

A: Here is the list of Umbrella Tunnel DC: Connect to Cisco Umbrella Through Tunnel. Umbrella uses Anycast technology to determine the closest DC. The chosen DC might not be geographically closest.

If the connected Umbrella Tunnel DC is not ideal, please upgrade the SD-WAN router to v17.5 or use the manual method: cEdge vEdge

Q: What happens if I rename the Tunnel name on Umbrella Dashboard to reflect a customer's site?

A: It is not recommended because under certain condition (such as router reboot), the SD-WAN router makes an API call to Umbrella Dashboard to check if tunnel exists or new tunnel provision is required. If the default Tunnel name has been renamed, the API calls provision a new tunnel and customer needs to associate the new tunnel with the appropriate policy.