Secure Access Network Tunnel Group Internal Server Error Reverting Primary Peer IP

Contents

Issue

When attempting to modify the remote peer IP in a Network Tunnel Group (NTG) on Cisco Secure Access, users can encounter an "Internal Server Error" in the UI when trying to revert the primary tunnel IP back to a previously configured value. The specific scenario involves:

- An NTG initially configured with a primary tunnel IP and secondary IP, with both tunnels establishing successfully.
- The primary tunnel IP is changed to a different IP address for testing purposes, which is accepted without issue.
- When attempting to revert the primary tunnel IP back to the original value, the system fails to save the configuration and returns an "Internal Server Error" in the UI.
- This behavior is consistently reproducible and appears when trying to reuse a previously configured IP address.
- The original IP was previously working and there are no conflicts with the secondary tunnel IP.

Environment

- Cisco Secure Access (formerly Cisco Umbrella for SSE)
- Network Tunnel Group configuration for private access
- Dual tunnel configuration with primary and secondary peer IPs
- Web-based management interface

Resolution

This issue is caused by a backend validation/state problem where the original peer IP remains reserved or stuck in the backend system after configuration changes. The troubleshooting and resolution steps explained in the next section must be followed:

Step 1: Gather Diagnostic Information

Collect the following information for backend validation:

- Secure Access Organization ID
- Network Tunnel Group Name
- Tunnel ID for the affected primary tunnel
- Region/Data Center selected for the NTG
- Exact timestamp of a failed save attempt, including timezone
- Confirmation whether the original IP appears in any other NTG, current or previous
- Browser HAR capture of the failed save attempt

Step 2: Capture Browser HAR File

To collect diagnostic data for the failed save attempt:

- Open browser Developer Tools
- Go to the Network tab
- Enable Preserve log
- Reproduce the save failure
- Export the HAR file and attach it to the support case

**Note**: Sanitize/remove any session tokens or cookies before uploading the HAR file.

Step 3: Backend Validation and Cleanup

This issue requires backend intervention and cannot be resolved from the UI alone. The following actions must be performed by Cisco Technical Support:

- Engage Secure Access backend/SSE Platform team
- Validate for stale peer-IP reservation
- Check for orphaned tunnel objects
- Identify duplicate backend keys tied to the specific NTG configuration
- Clear stale tunnel peer reference for the original IP
- Force backend re-sync of NTG objects if necessary
- Release peer-IP allocation tied to the NTG UUID

Step 4: Alternative Resolution Method

If backend cleanup is not immediately available, try this procedure:

- Delete the Network Tunnel Group primary configuration
- Wait for 5 minutes
- Re-add the NTG with the required IP address

⚠ **Caution**: Possible. The details mentioned here appears to contain procedures or commands that could cause significant impact if executed. Please ensure the above procedures or commands have been evaluated by an SME or Business Unit before executing or recommending.

Step 5: Temporary Workaround

If the NTG is in production and cannot be removed:

- Continue using the secondary tunnel for connectivity
- Obtain an alternative public IP from your vendor/partner
- Update the NTG primary to use the alternative IP
- Acknowledge reduced redundancy until the backend issue is resolved

Cause

This issue is caused by a software bug in the Cisco Secure Access backend system. When a primary peer IP is changed and reverted back to its original value, the backend validation system incorrectly treats the original IP as still allocated or reserved, even if it ought to be available for reuse. This results in a backend validation failure that is masked by the UI as a generic "Internal Server Error." The backend system fails to properly clean up or release the IP reservation during the configuration change process, creating a persistent state issue that prevents the IP from being reused in the same NTG.

Related Content

- Troubleshoot and Collect Basic Information for Cisco Secure Access
- Cisco Technical Support & Downloads