Zero Trust Access Profile Deletion Causing User Access Loss

Contents

Issue

After deleting a Zero Trust Access (ZTA) profile that was believed to be unused, all users with the ZTNA module experienced complete loss of access to both private resources and internet navigation. The deletion of this profile resulted in immediate service disruption for all ZTNA users, preventing them from accessing any resources through the Zero Trust Network Access infrastructure.

The affected users were unable to establish connections to:

- Private internal resources
- Internet navigation through the ZTNA module

Environment

- Secure Access (Zero Trust Network Access)
- ZTNA module deployed with multiple user profiles
- Default policy configured with ZTNA control
- Multiple ZTA profiles configured for user access management

Resolution

Understand ZTA Profile Matching Logic

Zero Trust Access profiles are applied based on a specific matching order and logic:

- **Profile Matching Order:** ZTA profiles are evaluated in order based on user and destination matching criteria
- **Default Profile Behavior:** When no specific profile matches the user or destination criteria, the system falls back to the default profile
- **Profile Dependencies:** Deleting a profile that serves as the effective default can cause service disruption even if it appears unused

The deleted profile was likely functioning as the effective default profile for user matching, despite appearing unused in the configuration interface. When this profile was removed, users lost their primary access path through the ZTNA infrastructure.

Validation Steps

To prevent similar issues in the future, this validation approach needs to be implemented:

1.- Review all configured ZTA profiles and their matching criteria before deletion.

2.- Identify which profile serves as the effective default for user access.

3.- Verify user-to-profile mapping through configuration screenshots and policy review.

4.- Test profile changes in a controlled manner before applying to production.

Cause

The root cause was the deletion of a ZTA profile that was functioning as the effective default profile for ZTNA user access, despite appearing unused in the configuration interface. When this profile was removed, the system lost the primary matching criteria for user access, causing all ZTNA users to lose connectivity to both private resources and internet navigation. The profile matching logic depends on having a valid default profile available for fallback when specific user or destination criteria are not met by other configured profiles.

Related Content

- Cisco Technical Support & Downloads