Inconsistent Blocking Pages After Umbrella to Cisco Secure Access Migration

Contents

Issue

After migrating from Umbrella to Cisco Secure Access (SSE) using the migration tool, blocked web traffic is inconsistently redirected to the legacy Umbrella blocking page instead of the Cisco Secure Access blocking page. The issue occurs with DNS Defense when different domains trigger block rules, resulting in different splash pages and block reason wording. This creates inconsistent end-user blocking notifications across the organization.

The specific symptoms observed include:

- Block rules redirect users to the old Umbrella blocking page instead of the new Cisco Secure Access blocking page
- Different domains triggering block rules display different splash pages
- Inconsistent block reason wording presented to end users
- The behavior affects DNS Defense functionality after migration

Environment

- Technology: Cisco Secure Access (SSE)
- Migration: Umbrella to SSE using migration tool
- Service Type: DNS Defense
- Deployment: Post-migration environment
- Web Scanning: FTD devices with web scanning enabled

Resolution

Web scanning on FTD devices interferes with the proper rendering of custom landing pages for Cisco

Secure Access. To resolve this issue, bypass web scanning on the FTDs for the following three domains:

- opendns.com
- cisco-secure.com
- sse.cisco.com

This workaround allows the custom Cisco Secure Access landing pages to render correctly instead of displaying the legacy Umbrella blocking pages.

Verification Steps

To verify the resolution effectiveness:

Step 1: Run policy tests for domains that previously showed inconsistent behavior

Step 2: Verify blocking page behavior after implementing the workaround

Confirm that blocked traffic now consistently displays the Cisco Secure Access blocking page instead of the legacy Umbrella page.

Step 3: Validate consistent block reason wording

Ensure that all blocked domains now display uniform block reason messaging aligned with Cisco Secure Access standards.

Cause

The issue is caused by web scanning functionality on FTD devices interfering with the proper rendering of Cisco Secure Access custom landing pages. When web scanning is enabled on FTDs, it prevents the correct display of the new blocking pages, causing the system to fall back to legacy Umbrella blocking pages. This creates inconsistent user experiences where different domains may trigger different blocking page formats.

The engineering team has identified this as a design-level issue that requires changes from the Talos perspective. The current architecture requires web scanning to be bypassed for specific Cisco domains to ensure proper custom landing page functionality.

Related Content

- Cisco Technical Support & Downloads