Inkonsistente Blockierungsseiten nach Umbrella- zu Cisco Secure Access-Migration

Inhalt

Problem

Nach der Migration von Umbrella zu Cisco Secure Access (SSE) mithilfe des Migrations-Tools wird blockierter Internetdatenverkehr inkonsistent auf die ältere Umbrella-Blockierungsseite umgeleitet, anstatt auf die Cisco Secure Access-Blockierungsseite. Das Problem tritt beim DNS-Schutz auf, wenn verschiedene Domänen Blockregeln auslösen, was zu unterschiedlichen Splash-Seiten und Blockursachen führt. Dies führt zu inkonsistenten Endbenutzer-Blockierungsbenachrichtigungen im gesamten Unternehmen.

Zu den beobachteten spezifischen Symptomen gehören:

- Blockierungsregeln leiten Benutzer an die alte Blockierungsseite für Umbrella anstatt an die neue Blockierungsseite für Cisco Secure Access weiter
- Unterschiedliche Domänen, die Blockregeln auslösen, zeigen unterschiedliche Splash-Seiten an.
- Inkonsistente Blockbegründung für Endbenutzer
- Das Verhalten beeinflusst die DNS-Abwehrfunktion nach der Migration.

Umwelt

- Technologie: Cisco Secure Access (SSE)
- Migration: Umbrella zu SSE mit Migrationstool
- Servicetyp: DNS-Abwehr
- Bereitstellung: Umgebung nach der Migration
- Web-Scanning: FTD-Geräte mit aktiviertem Web-Scanning

Auflösung

Web-Scanning auf FTD-Geräten beeinträchtigt die ordnungsgemäße Wiedergabe benutzerdefinierter Landing Pages für Cisco Secure Access. Um dieses Problem zu beheben, umgehen Sie das Web-Scanning auf den FTDs für die folgenden drei Domänen:

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

Mit dieser Problemumgehung können die Landing Pages von Cisco Secure Access korrekt gerendert werden, anstatt die vorhandenen Umbrella-Blockierungsseiten anzuzeigen.

Verifizierungsschritte

So überprüfen Sie die Effektivität der Problembehebung:

Schritt 1: Führen Sie Richtlinientests für Domänen aus, die zuvor ein inkonsistentes Verhalten aufwiesen.

Phase 2: Überprüfen des Verhaltens der blockierenden Seite nach der Implementierung der Problemumgehung

Bestätigen Sie, dass blockierter Datenverkehr jetzt konsistent die Seite für die Blockierung von Cisco Secure Access und nicht die Seite für ältere Umbrella-Geräte anzeigt.

Schritt 3: Validierung der konsistenten Blockbegründung

Stellen Sie sicher, dass alle gesperrten Domänen jetzt eine einheitliche Blockgrund-Benachrichtigung entsprechend den Cisco Secure Access-Standards anzeigen.

Ursache

Das Problem wird durch die Web-Scanning-Funktion auf FTD-Geräten verursacht, die die ordnungsgemäße Wiedergabe der benutzerdefinierten Landing Pages von Cisco Secure Access beeinträchtigt. Wenn Web-Scanning auf FTDs aktiviert ist, verhindert es die korrekte Anzeige der neuen Blockierungsseiten, sodass das System auf ältere Umbrella-Blockierungsseiten zurückgreift. Dies führt zu einer inkonsistenten Benutzererfahrung, bei der unterschiedliche Domänen unterschiedliche Formate für blockierende Seiten auslösen können.

Das Technikerteam hat dies als Problem auf Designebene identifiziert, das aus Sicht von Talos geändert werden muss. Bei der aktuellen Architektur muss für bestimmte Cisco Domänen das Web-Scanning umgangen werden, um die korrekte Funktion der Landing Page sicherzustellen.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.