Sicherer Zugriff Anwendungsprotokollblockierung verhindert Internetverbindungen

Inhalt

Problem

Umwelt

Auflösung

Schritt 1: Identifizieren der Blockierungsregel

Phase 2: Anwendungseinstellungen ändern

Schritt 3: Änderungen anwenden und überprüfen

Ursache

Verwandte Inhalte

- Problem
- Umwelt
- Auflösung
  - Schritt 1: Identifizieren der Blockierungsregel
  - Phase 2: Anwendungseinstellungen ändern
  - Schritt 3: Änderungen anwenden und überprüfen
- Ursache
- Verwandte Inhalte

Problem

Nach der Migration zu Cisco Secure Access wurde die Internetverbindung blockiert, wenn versucht wurde, auf Webdienste zuzugreifen. Das spezifische Symptom besteht darin, dass der HTTP-Datenverkehr durch die Sicherheitsrichtlinie blockiert wird und so der Zugriff auf legitime Websites und Anwendungen verhindert wird.

Die Details des Blockierungsereignisses zeigten folgende Merkmale:

- Aktion: Gesperrt
- Grund für Ereignisblockierung: AC_REGEL_ÜBEREINSTIMMUNG_BLOCKIEREN
- Ziel: http://www.bing.com/api/shopping/v1/user/shoppingsettings

- Ziel-Port: 443
- Kategorien: Nicht kategorisiert
- Anwendungskategorie: Suche
- Anwendungsprotokoll: Hypertext Transfer Protocol
- Protokolle: TCP

Umwelt

- Cisco Secure Access-Bereitstellung
- Aktive Sicherheitsrichtlinie mit Einschränkungen für Anwendungsprotokolle

Auflösung

Die Lösung besteht darin, die Konfiguration der Sicherheitsregeln so zu ändern, dass HTTP-Anwendungsprotokollverkehr zugelassen wird, während der Sicherheitsstatus für wirklich nicht vertrauenswürdige Anwendungen erhalten bleibt.

Schritt 1: Identifizieren der Blockierungsregel

Suchen Sie in der Verwaltungsschnittstelle für sicheren Zugriff nach der Regel, die den Block verursacht:

- Regelname: Test
- Aktuelle Konfiguration: Verwenden von Anwendungseinstellungen Block als Ziel.

Phase 2: Anwendungseinstellungen ändern

Greifen Sie auf die Regelkonfiguration zu, und überprüfen Sie den Namen der Anwendungseinstellungen unter Ziel:

- Navigieren Sie zu Ressourcen > Internet- und SaaS-Ressourcen > Anwendungslisten. Klicken Sie dann auf die Anwendung.
- Suchen Sie nach den Einstellungen für das Anwendungsprotokoll.
- Deaktivieren oder entfernen Sie HTTP aus der Liste der blockierten Anwendungsprotokolle.
- Stellen Sie sicher, dass für nicht vertrauenswürdige Anwendungen andere Sicherheitskontrollen vorhanden sind.

Schritt 3: Änderungen anwenden und überprüfen

Speichern Sie die Regeländerungen, und testen Sie die Verbindung:

1.- Übernehmen der Konfigurationsänderungen auf die aktive Richtlinie

2.- Testen der Internetverbindung zu zuvor blockierten Zielen

3.- Sicherheitsprotokolle überwachen, um sicherzustellen, dass legitimer HTTP-Datenverkehr zugelassen wird.

4.- Überprüfen Sie, ob andere Sicherheitsmaßnahmen wirksam bleiben.

Ursache

Die Ursache dafür war eine zu restriktive Sicherheitsregelkonfiguration in Cisco Secure Access. Die Regel wurde so konfiguriert, dass der gesamte HTTP-Anwendungsprotokollverkehr blockiert wurde, wodurch legitimes Surfen im Internet und der Zugriff auf Anwendungen verhindert wurden. Die weit verbreitete Anwendung der HTTP-Protokollblockierung wirkte sich auf die normale Internetverbindung für Benutzer aus, die auf legitime Webdienste und Anwendungen zugreifen, die HTTP/HTTPS-Protokolle verwenden.

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.