

Konfiguration für sicheren Zugriff Kennwortgeschützter ZIP-Datei-Download

Inhalt

Problem

Nach der Migration zu Cisco Secure Access können die Benutzer keine kennwortgeschützten (verschlüsselten) ZIP-Dateien herunterladen. Die Downloads schlagen fehl, wenn versucht wird, über den Secure Access-Dienst auf verschlüsselte Dateiinhalte zuzugreifen. Dieses Problem tritt auf, obwohl auf einem C8200-Gerät Richtlinien für den Internetdatenverkehr mit mehreren Sicherheitsregeln konfiguriert wurden, darunter kategoriebasierte Blockierung, SSL-Überprüfungskontrollen und Sandbox-Funktionalität.

Bei dem Versuch, auf kennwortgeschützte ZIP-Dateien zuzugreifen, auf die vor der Migration zu Secure Access zugegriffen werden konnte, treten vollständige Downloadfehler auf. Das Problem besteht über mehrere Tunnelgruppen hinweg fort und betrifft alle 15 konfigurierten Standorte.

Umwelt

- Cisco Secure Access (Secure Access, Organisations-ID: 8320925)
- C8200-Gerät zur Verwaltung internetgebundener Datenverkehrsrichtlinien
- Mehrere Tunnelgruppen an 15 Standorten (TK-TG und andere)
- SSL-Überprüfungsrichtlinien mit aktivierten und deaktivierten Konfigurationen
- Aktivierung von Sandbox-Sicherheitsprofilen für bestimmte Richtlinien
- Konfiguration von IPS-Profilen nach spezifischen Zugriffsregeln

Auflösung

Die Lösung für das Zulassen kennwortgeschützter ZIP-Datei-Downloads in Cisco Secure Access besteht darin, die Einstellung "Zugriff auf verschlüsselte Dateien zulassen" zu konfigurieren und bei Bedarf entsprechende Problemumgehungen zu implementieren.

Primäre Konfigurationsmethode

Schritt 1: Zugriff auf die Konfiguration der Cisco Sicherheitszugriffsrichtlinie

Navigieren Sie in Ihrem Cisco Secure Access Dashboard zu der spezifischen Zugriffsrichtlinie, die den betroffenen Datenverkehr behandelt.

Phase 2: Verschlüsselten Dateizugriff aktivieren

Suchen Sie in der Richtlinie "Erweiterte Einstellungen" die Option Zugriff auf verschlüsselte Dateien zulassen, und aktivieren Sie sie. Diese Einstellung wird auf Regelbasis konfiguriert und steuert, ob über diese spezifische Richtlinie auf verschlüsselte Inhalte zugegriffen werden kann.

Schritt 3: Anwenden der Konfiguration

Speichern und anwenden Sie die Richtlinienänderungen, um sie für den Benutzerdatenverkehr zu aktivieren.

Alternative Lösungsmethode

Wenn das Problem durch die primäre Methode nicht behoben wird, implementieren Sie die Problemumgehung, die in den nächsten Abschnitten beschrieben wird.

Schritt 1: Betroffene URLs ermitteln

Bestimmen Sie die URLs oder Domänen, auf denen kennwortgeschützte ZIP-Dateien gehostet werden, und verursachen Sie Downloadfehler.

Phase 2: Liste "Nicht entschlüsseln" konfigurieren

Fügen Sie die identifizierten URLs der Liste Nicht entschlüsseln in der Cisco Secure Access-Konfiguration hinzu. Dadurch wird die SSL-Überprüfung dieser spezifischen URLs verhindert.

Schritt 3: Erstellen einer Richtlinie für die SSL-Überprüfung

Stellen Sie sicher, dass eine Zugriffsrichtlinie mit deaktivierter SSL-Überprüfung konfiguriert ist, um den Datenverkehr zu diesen URLs zu verarbeiten.

Diese Richtlinie muss folgende Anforderungen erfüllen:

- SSL-Überprüfung deaktiviert
- Alle Sicherheitsprofile deaktiviert
- Höhere Priorität als Richtlinien mit SSL-Überprüfung

Referenz zur Richtlinienkonfiguration

Die in den nächsten Unterabschnitten beschriebene Reihenfolge der Richtlinien und die entsprechenden Konfigurationen können als Referenz für die ordnungsgemäße Verarbeitung des Datenverkehrs verwendet werden.

Richtlinie 1: Kategoriebasierte Sperrregel

- Policy-Name: IA-To-InternetContentBlock
- IPS-Profil: None

- Zweck: Blockieren bestimmter Inhaltskategorien
- Ziel: Alle Tunnelgruppen

Richtlinie 2: SSL-Überprüfung - Regel deaktiviert

- Policy-Name: IA-SSL-Inspektion-MUKOU
- IPS-Profil: Deaktiviert
- Sicherheitsprofile: Alle deaktiviert
- Ziel: Alle Tunnelgruppen

Richtlinie 3: Regel für SSL-Überprüfung aktiviert

- Policy-Name: IA-SSL-Überprüfung
- IPS-Profil: Aktiviert
- Sicherheitsprofile: Sandbox-Funktion aktiviert
- Ziel: Alle Tunnelgruppen

Wichtige Konfigurationshinweise

Für die Funktion "Zugriff auf verschlüsselte Dateien zulassen" ist keine Entsprechung der globalen Einstellungen vorhanden. Diese Einstellung muss bei Bedarf für individuelle Zugriffsrichtlinien konfiguriert werden. Für jede Richtlinie, für die verschlüsselter Dateizugriff erforderlich ist, muss diese Einstellung in der Konfiguration für erweiterte Einstellungen explizit aktiviert sein.

Planen Sie beim Testen von Konfigurationsänderungen ausreichend Zeit für die Richtlinienweitergabe in der gesamten Cisco Secure Access-Infrastruktur ein, bevor Sie die Funktionalität überprüfen. Servicevorfälle oder Wartungsfenster können die Testergebnisse beeinflussen und müssen bei der Fehlerbehebung berücksichtigt werden.

Ursache

Das Problem tritt auf, weil Cisco Secure Access den Zugriff auf verschlüsselte Dateien standardmäßig blockiert. Wenn die SSL-Überprüfung aktiviert ist und auf kennwortgeschützten oder verschlüsselten Inhalt trifft, verhindert der Dienst den Download, es sei denn, er ist explizit für diesen Zugriff konfiguriert. Die Einstellung Zugriff auf verschlüsselte Dateien zulassen in den erweiterten Einstellungen der Zugriffsrichtlinien steuert dieses Verhalten. Wenn diese Einstellung nicht aktiviert ist, werden verschlüsselte ZIP-Dateien und ähnliche Inhalte während des Downloads blockiert.

Darüber hinaus können SSL-Überprüfungsrichtlinien verschlüsselte Dateidownloads stören, wenn der Überprüfungsprozess den verschlüsselten Inhalt nicht ordnungsgemäß handhaben kann. Dies erfordert entweder die Einstellung für den verschlüsselten Dateizugriff oder die Umgehung der SSL-Überprüfung für betroffene URLs.

Verwandte Inhalte

- [Erweiterte Sicherheitskontrollen](#)
- [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.