Konfigurieren des Dateiinspektors, um kennwortgeschützte und andere nicht bösartige Dateien zuzulassen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie verhindert werden kann, dass eine nicht schädliche Datei durch die Dateiprüfung blockiert wird.

Problem

Bei Aktivierung der "Dateiprüfung" werden in einigen Fällen nicht schädliche Dateien blockiert. Zu diesen Dateitypen gehören:

- Kennwortgeschützte Dateien
- Dateien mit potenziell unerwünschten Anwendungen (beschädigt)

Diese Dateien werden von Umbrella blockiert, da sie von unserem Antivirus-Tool nicht dekomprimiert und gescannt werden können. Passwortgeschützte Dateien können unter der Kategorie "Geschützte Datei" blockiert erscheinen. Beschädigte Dateien können Dateien mit verschlüsseltem Inhalt, archivierten Inhalten, die nicht extrahiert werden können, ungültigen komprimierten Daten oder einem ungültigen Archiv-Header enthalten oder einfach komprimiert oder in einem nicht unterstützten Format archiviert werden. Obwohl diese Dateien nicht schädlich sein können, werden sie von Umbrella als Vorsichtsmaßnahme blockiert, da die Dateien nicht gescannt werden können.

Lösung

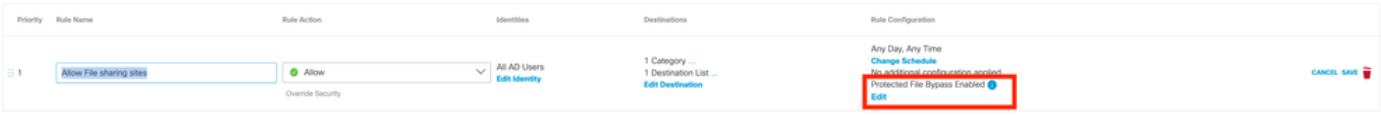
Wenn Sie eine nicht-bösartige Datei kennen, die aus einem der oben genannten Gründe blockiert wurde, können Sie dies umgehen, indem Sie geschützte Dateien zulassen. Das Verhalten zum Blockieren geschützter Dateien kann jetzt auf globaler Ebene oder in einer individuellen Webregel geändert werden.

- Regel (empfohlen) - Schützte Dateien für eine Identität und/oder ein Ziel zulassen. Führen Sie diesen Schritt aus, wenn Sie geschützten Dateien eines bestimmten Ziels vertrauen oder

das Verhalten eines einzelnen Benutzers oder einer Gruppe überschreiben möchten.
- Global - Geschützte Dateien für alle Benutzer in allen Regeln/Regelsätzen zulassen. Führen Sie diesen Schritt aus, wenn Sie das Risiko geschützter Dateidownloads akzeptieren und diese Option dem Verwaltungsaufwand durch detailliertere Ausnahmen vorziehen.

Regel

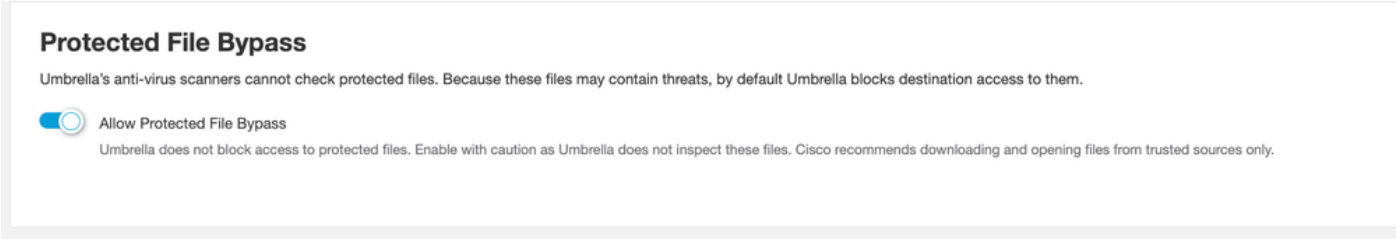
Sie können die Funktionalität ändern, indem Sie eine Webregel auf der Seite Policies > Web Policies (Richtlinien > Webrichtlinien) bearbeiten.



10588971481748

Global

Die Funktionalität kann unter Richtlinien > Webrichtlinien > Globale Einstellungen geändert werden.

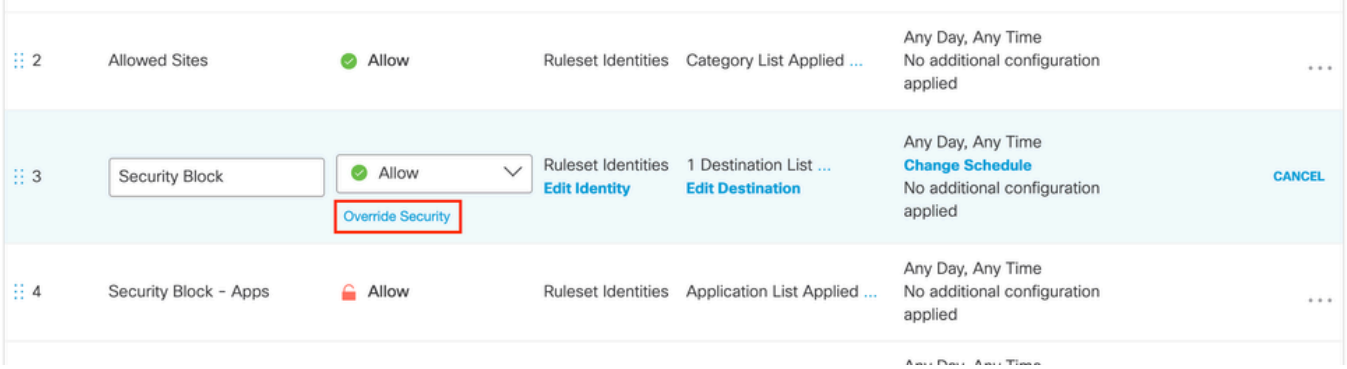


10589018672020

Alternative Lösung

Es ist auch möglich, Probleme mit der Dateiinspektion mit der Option Sicherheit außer Kraft setzen in jeder Web-Richtlinie zu umgehen. Diese Option muss mit Vorsicht verwendet werden, da sie alle anderen Sicherheitseinstellungen deaktiviert, einschließlich des Blockierens schädlicher Dateien.

- Verwenden Sie für geschützte Dateien stattdessen eine der in diesem Dokument beschriebenen Lösungen.
- Verwenden Sie diese Option nur, wenn Sie dem Ziel absolut sicher vertrauen und keine andere Möglichkeit haben, das Problem zu umgehen.
- Bei Fehlalarmen für Anti-Virus erhalten Sie eine Bestätigung, dass die Datei von Cisco Talos bereinigt wurde, bevor Sie Workarounds implementieren.



Screen_Shot_2021-10-07_at_2,59,04_PM.png

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.