Neue Funktionen in Umbrella Dashboard

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

- [Anforderungen](#)
- [Verwendete Komponenten](#)

[Neue Funktionen](#)

[So nutzen Sie die Vorteile dieser Funktionen](#)

- [Dateiprüfung](#)
- [Testen der Dateiüberprüfung](#)
- [Sperren von URLs in den Ziellisten aktivieren](#)

[Berichterstellung](#)

[Umbrella-Feedback senden](#)

Einleitung

Dieses Dokument beschreibt die Dateiprüfung und die benutzerdefinierte URL-Blockierung über Ziellisten im Umbrella Dashboard.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Umbrella Dashboard.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

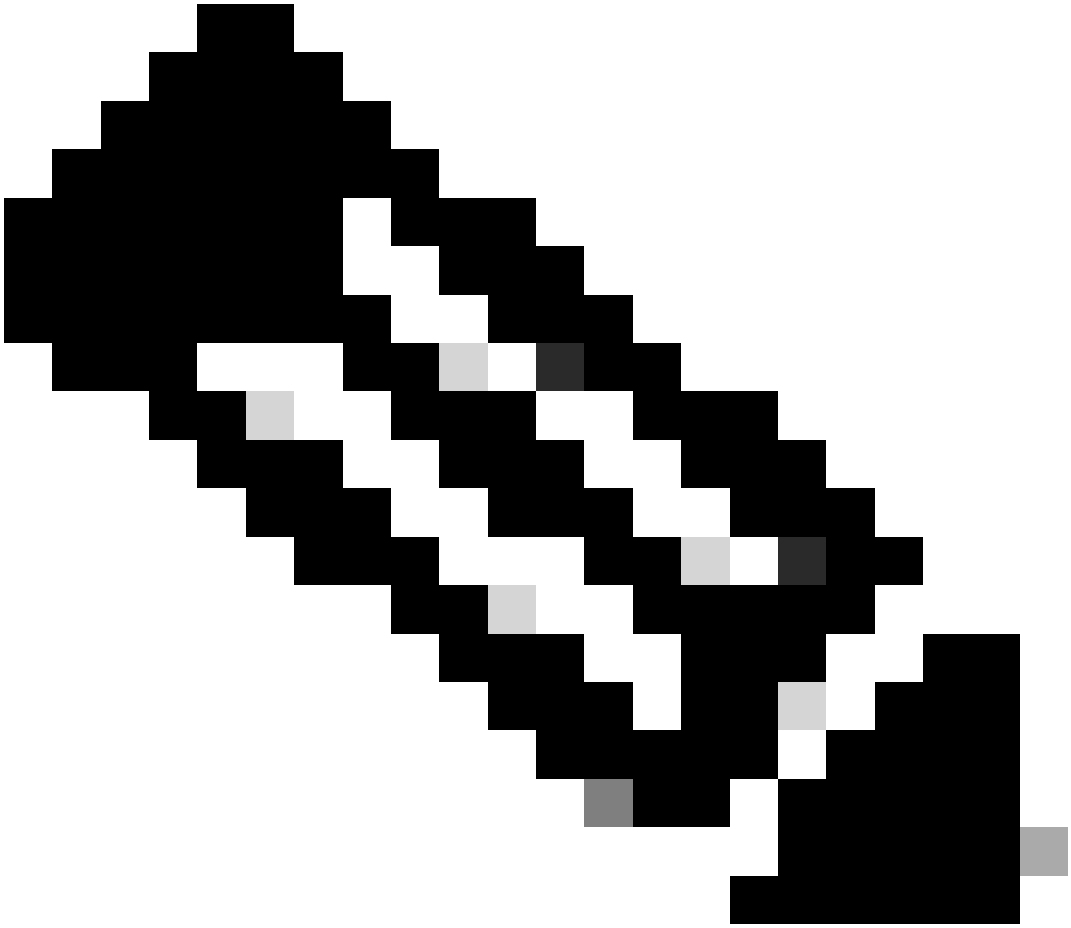
Neue Funktionen

Umbrella führt eine Reihe neuer Funktionen ein, die Ihre Funktionalität verbessern. Mit dieser Änderung sehen Sie jetzt zwei neue Funktionen in Ihrem Dashboard:

- Die Dateiprüfung überprüft die heruntergeladenen Dateien, um festzustellen, ob sie schädlichen Code enthalten, und blockiert diese, wenn sie dies tun.

- Durch benutzerdefinierte blockierte URLs können Sie Ihre eigenen URL-Sätze in einer Zielliste blockieren. So können Sie bestimmte Seiten jetzt flexibel blockieren, ohne ganze Domänen zu blockieren.

Damit Sie von dieser neuen Funktion profitieren können, können Sie die neuen und aktualisierten Berichte und eine neue Erfahrung bei der Erstellung von Richtlinien nutzen. Die Dateiinspektionsfunktion ist eine von mehreren geplanten Versionen für zukünftige Versionen, die auf der Weiterentwicklung der Intelligent Proxy-Infrastruktur aufbauen und Ihnen noch mehr Cloud-basierte Sicherheit bieten.



Anmerkung: Diese Funktionen werden unseren Kunden in kleinen Schritten zur Verfügung gestellt, und diese Updates sind im Zuge der Weiterentwicklung von Umbrella mit dieser Version nur begrenzt verfügbar. Wenn Sie in Ihrem Dashboard eine Benachrichtigung über diese Funktionen erhalten haben, verfügen Sie über diese. Wenn Sie mehr über diese Funktionen erfahren möchten, wenden Sie sich an umbrella-support@cisco.com.

Die Dateiprüfungsfunktion steht nur Kunden mit Umbrella Insights- oder Umbrella Platform-

Paketen zur Verfügung. Lesen Sie mehr über Pakete, und wenden Sie sich bei Fragen an Ihren Cisco Kundenbetreuer.

So nutzen Sie die Vorteile dieser Funktionen

Diese neuen Funktionen stehen an mehreren Stellen zur Verfügung: Mit dem Richtlinien-Assistenten können Sie die Dateiinspektion von der Zusammenfassungsseite aus aktivieren. Über Ziellisten können Sie benutzerdefinierte URLs zu den gesperrten Ziellisten hinzufügen. Darüber hinaus kann die benutzerdefinierte URL-Sperrung auch speziell über die Verwaltungsseite für Ziellisten verwaltet werden.

Auf der Berichtsseite wurde der Navigationsbereich "Berichte" des Umbrella Dashboards aktualisiert, sodass Sie die neuen und aktualisierten Berichte schnell finden können. In diesem Artikel erfahren Sie, wie Sie diese Funktionen aktivieren können, und sehen Sie sich einige Berichte an.

Dateiprüfung

Die Dateiprüfung ist eine Funktion des intelligenten Proxys, die dessen Umfang und Funktionalität erweitert, indem sie die Möglichkeit bietet, Dateien nach schädlichen Inhalten zu durchsuchen, die auf verdächtigen Domänen gehostet werden. Eine verdächtige Domäne ist weder vertrauenswürdig noch als schädlich bekannt.

Mit dem Umbrella Policy Wizard lässt sich die Dateiprüfung einfach implementieren. Navigieren Sie zu Policies > Policy List (Richtlinien > Richtlinienliste), und erweitern Sie eine Richtlinie, oder wählen Sie das Symbol + (Hinzufügen) aus, um eine neue Richtlinie zu erstellen. Stellen Sie im Richtlinien-Assistenten sicher, dass die Dateiinspektion auf der Zusammenfassungsseite aktiviert ist, oder wählen Sie in einer neuen Richtlinie die Option Dateien inspizieren, nachdem Sie den Intelligenten Proxy aktiviert haben (unter Erweiterte Einstellungen). Weitere Informationen finden Sie in der vollständigen Dokumentation zu dieser Funktion.

Testen der Dateiüberprüfung

Von einem Gerät, das bei aktivierter Dateiinspektion in einer Richtlinie registriert ist:

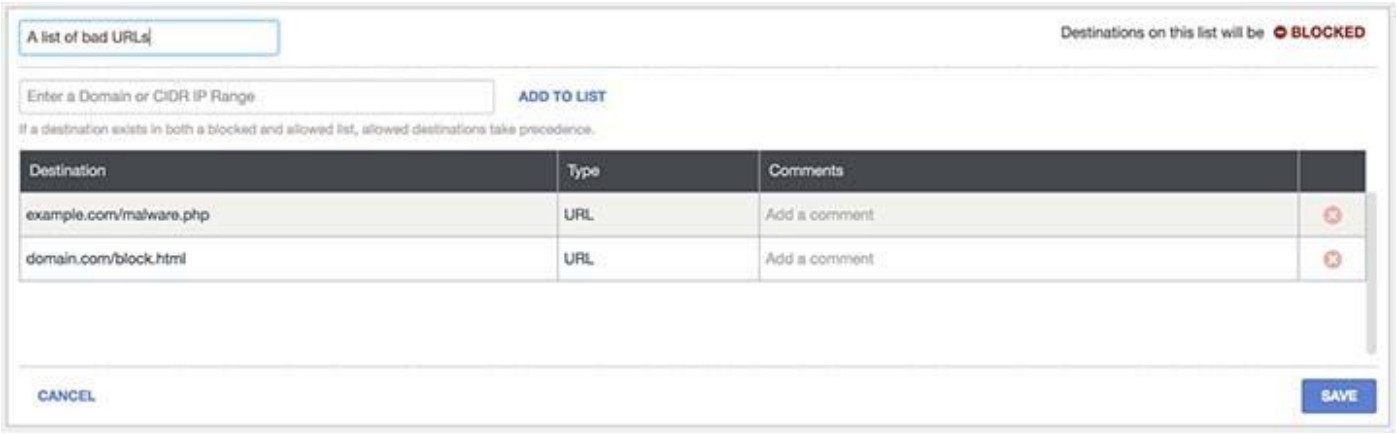
1. Navigieren Sie zu http://proxy.opendnstest.com/download/eicar.com.

2. Eine Blockseite wie dieser Screenshot wird angezeigt.

Umbrella blockiert Seite

Sperren von URLs in den Ziellisten aktivieren

Um eine URL zu blockieren, geben Sie sie einfach in eine Liste blockierter Ziele ein, oder erstellen Sie eine neue Liste blockierter Ziele nur für URLs. Navigieren Sie dazu zu Policies > Destination Lists (Richtlinien > Ziellisten), erweitern Sie eine Destination List (Zielliste), fügen Sie eine URL hinzu, und wählen Sie Save (Speichern) aus.



Liste der blockierten Umbrella-Ziele

Weitere Informationen finden Sie in der vollständigen Dokumentation zu dieser Funktion.

Damit die Umbrella-Infrastruktur eine URL untersuchen kann, um zu ermitteln, ob sie mit den in der Liste gesperrter Ziele definierten URLs übereinstimmt, müssen Sie über Folgendes verfügen:

- Intelligente Proxy- und SSL-Entschlüsselung müssen als Teil der Richtlinie aktiviert sein.

Weitere Informationen finden Sie in den Umbrella-Dokumenten.
- Die Cisco Umbrella Root-Zertifizierungsstelle muss mithilfe dieser Richtlinie auf den Computern installiert werden, damit auch HTTPS-Verbindungen gefiltert werden. Weitere Informationen finden Sie in den Umbrella-Dokumenten.

Es ist wichtig, eine URL korrekt anzugeben, damit die Informationen in der Richtlinie mit den Informationen übereinstimmen, auf die der Benutzer zuzugreifen versucht (und anschließend blockiert wird). Weitere Informationen zu den URLs, die Sie verwenden können oder nicht, finden Sie im Dokument Benutzerdefinierte URL-Zielliste - Gewusst wie.

Berichterstellung

Umbrella hat nun neue und verbesserte Berichte:

- Der Security Overview Report: bietet Ihnen eine einfach zu lesende Momentaufnahme Ihrer Netzwerkaktivitäten mithilfe von Diagrammen und Diagrammen. Sie können schnell Aktivitäten in Ihren Identitäten und deren Datenverkehr sehen, um zu veranschaulichen, wo Probleme auftreten können. Weitere Informationen hierzu finden Sie in den Umbrella-Dokumenten.
- Im Security Activity Report: Highlights Security-Events, die von Umbrella Threat Intelligence markiert, aber nicht notwendigerweise blockiert wurden. Dazu gehören auch Sicherheitsereignisse, die über den Intelligent Proxy gefiltert werden, und die Dateiprüfung. Weitere Informationen hierzu finden Sie in den Umbrella-Dokumenten.

- Aktivitätssuchbericht: Hilft Ihnen, das Ergebnis jeder DNS-, URL- und IP-Anforderung aus Ihren verschiedenen Identitäten zu finden, sortiert nach absteigendem Datum und Uhrzeit. Dieser Bericht kann alle sicherheitsrelevanten Aktivitäten innerhalb von Umbrella für den ausgewählten Zeitraum auflisten und ermöglicht Ihnen, Ihre Suche mithilfe von Filtern zu verfeinern, um nur das anzuzeigen, was Sie sehen möchten. Weitere Informationen hierzu finden Sie in den Umbrella-Dokumenten.

Auch diese Berichte sind leicht zu erhalten.

Umbrella-Feedback senden

Regenschirm würde gerne hören, was Sie über diese neuen Funktionen denken. Wenn Sie Fragen oder Kommentare haben, Umbrella möchte von Ihnen hören! Senden Sie Ihr Feedback an umbrella-support@cisco.com, und fügen Sie so viele Details wie möglich hinzu. Beispielsweise Screenshots, der verwendete Browser, Ihr Betriebssystem und das Szenario, in dem Sie diese Funktionen verwenden.

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.