Comprendre les nouvelles fonctionnalités du tableau de bord Umbrella

Table des matières

Introduction

Ce document décrit l'inspection de fichier et le blocage d'URL personnalisé via des listes de destinations dans le tableau de bord Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur le tableau de bord Umbrella.

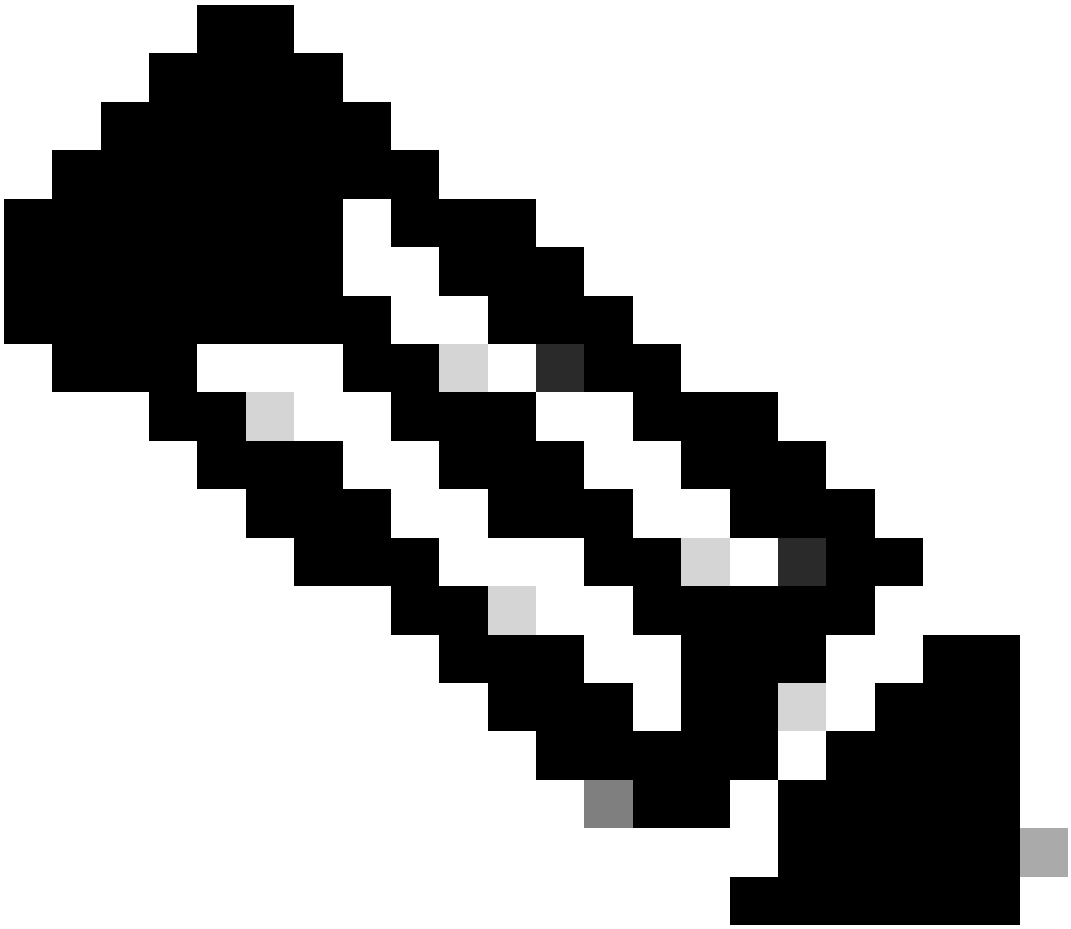
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Nouvelles fonctionnalités

Umbrella introduit un nouvel ensemble de fonctionnalités qui améliorent vos fonctionnalités. Avec cette modification, vous pouvez voir deux nouvelles fonctionnalités dans votre tableau de bord dès maintenant :

- L'inspection des fichiers analyse les fichiers que vos identités téléchargent pour voir s'ils contiennent du code malveillant et les bloquent le cas échéant.
- Les URL bloquées personnalisées vous permettent de bloquer votre propre ensemble d'URL dans une liste de destinations. Vous avez ainsi la possibilité de bloquer des pages spécifiques sans bloquer des domaines entiers.

Pour vous aider à tirer parti de cette nouvelle fonctionnalité, vous pouvez utiliser les rapports nouveaux et mis à jour et une nouvelle expérience de création de stratégie. La fonctionnalité d'inspection de fichier est l'une des nombreuses versions prévues pour les futures versions, qui s'articulent autour de l'infrastructure de proxy intelligent pour fournir encore plus de sécurité basée sur le cloud pour vous.



Remarque : Ces fonctionnalités sont déployées progressivement pour nos clients et ces mises à jour sont en disponibilité limitée à mesure que Umbrella progresse dans cette version. Si vous avez reçu une alerte sur ces fonctionnalités dans votre tableau de bord, vous les avez. Et si vous souhaitez en savoir plus sur ces fonctionnalités, contactez umbrella-support@cisco.com.

La fonction d'inspection des fichiers est uniquement disponible pour les clients disposant des packages Umbrella Insights ou Umbrella Platform. Pour en savoir plus sur les packages et pour toute question, contactez votre représentant Cisco.

Comment tirer parti de ces fonctionnalités

L'accès à ces nouvelles fonctionnalités est disponible dans quelques endroits : L'assistant de stratégie vous permet d'activer l'inspection des fichiers à partir de la page de résumé et, via les listes de destinations, vous pouvez ajouter des URL personnalisées à vos listes de destinations bloquées. En outre, le blocage d'URL personnalisé peut également être géré spécifiquement à partir de la page de gestion Listes de destinations.

Du côté des rapports, la section de navigation des rapports du tableau de bord Umbrella a été mise à jour afin que vous puissiez facilement trouver les nouveaux rapports et les rapports mis à jour. Pour en savoir plus sur l'activation de ces fonctionnalités et consulter certains rapports, lisez cet article.

Inspection des fichiers

L'inspection des fichiers est une fonctionnalité du proxy intelligent qui étend son étendue et ses fonctionnalités en ajoutant la possibilité d'analyser les fichiers à la recherche de contenu malveillant hébergé sur des domaines suspects. Un domaine suspect n'est ni fiable ni réputé malveillant.

Grâce à l'assistant de stratégie Umbrella, l'inspection des fichiers est facile à mettre en oeuvre. Accédez à Politiques > Liste des politiques et développez une politique ou sélectionnez l'icône + (Ajouter) pour créer une nouvelle politique. Dans l'assistant de stratégie, assurez-vous que l'inspection des fichiers est activée sur la page de résumé ou, à partir d'une nouvelle stratégie, sélectionnez Inspect Files après avoir activé le proxy intelligent (sous Advanced Settings). Pour en savoir plus, consultez la documentation complète de cette fonction.

Inspection des fichiers de test

À partir d'un périphérique inscrit dans une stratégie avec l'inspection des fichiers activée :

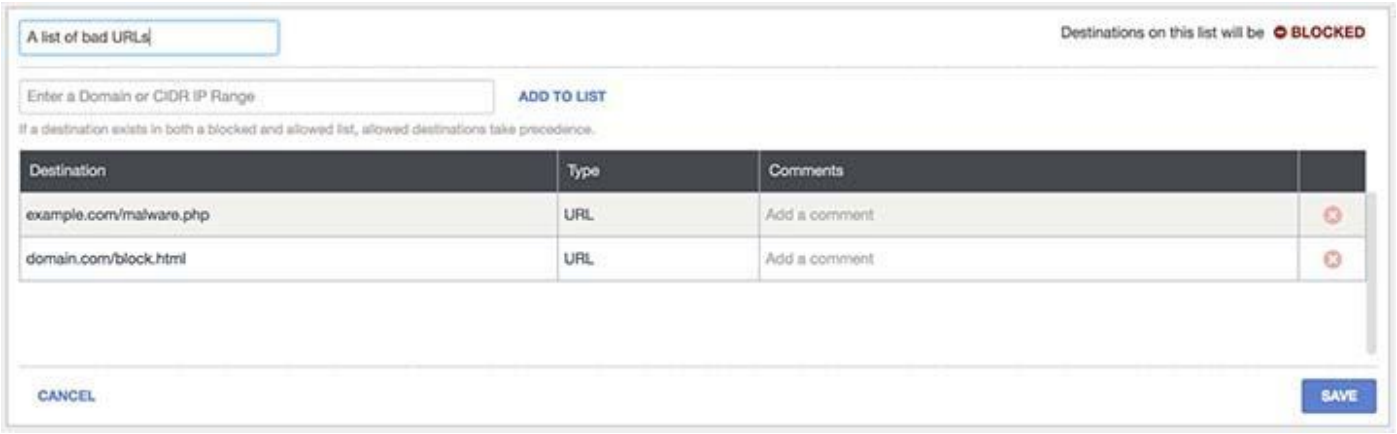
1. Accédez à http://proxy.opendnstest.com/download/eicar.com.

2. Une page de blocage telle que celle-ci apparaît.

Page de parapluie bloquée

Activer le blocage des URL dans vos listes de destinations

Pour bloquer une URL, il vous suffit de la saisir dans une liste de destinations bloquées ou de créer une nouvelle liste de destinations bloquées uniquement pour les URL. Pour ce faire, accédez à Politiques > Listes de destinations, développez une liste Destination, ajoutez une URL, puis sélectionnez Enregistrer.



Liste de destinations bloquées par parapluie

Pour en savoir plus, consultez la documentation complète de cette fonction.

Pour que l'infrastructure Umbrella inspecte une URL afin de déterminer si elle correspond à celles définies dans votre liste de destinations bloquées, vous devez disposer des éléments suivants :

- Le proxy intelligent et le déchiffrement SSL doivent être activés dans le cadre de la stratégie.

Pour plus d'informations, lisez les documents Umbrella.
- L'autorité de certification Cisco Umbrella Root doit être installée sur le ou les ordinateurs à l'aide de cette stratégie. Elle s'assure également que les connexions https sont filtrées. Pour plus d'informations, lisez les documents Umbrella.

Il est important de spécifier correctement une URL afin que ce qui est dans votre stratégie corresponde à ce à quoi l'utilisateur tente d'accéder (et est ensuite bloqué). Pour plus d'informations sur les URL que vous pouvez ou ne pouvez pas utiliser, veuillez lire Instructions relatives à la liste de destinations d'URL personnalisée.

Rapports

Umbrella propose désormais des rapports nouveaux et améliorés :

- Le rapport de présentation de la sécurité : vous offre un aperçu facile à lire de l'activité de votre réseau à l'aide de graphiques. Vous pouvez rapidement voir l'activité de vos identités et de leur trafic, en illustrant où les problèmes peuvent se produire. Pour en savoir plus, consultez les documents Umbrella.
- Rapport d'activité sur la sécurité : met en évidence les événements de sécurité signalés, mais pas nécessairement bloqués, par les informations sur les menaces d'Umbrella. Cela inclut les événements de sécurité filtrés via le proxy intelligent et l'inspection des fichiers. Pour en savoir plus, consultez les documents Umbrella.

- Rapport de recherche d'activité : vous aide à trouver le résultat de chaque requête DNS, URL et IP à partir de vos différentes identités, triées par date et heure décroissantes. Ce rapport peut répertorier toutes les activités liées à la sécurité dans Umbrella pour la période sélectionnée et vous permet d'affiner votre recherche à l'aide de filtres pour afficher uniquement ce que vous voulez voir. Pour en savoir plus, consultez les documents Umbrella.

Ces rapports sont également faciles à obtenir.

Envoi de commentaires Umbrella

Umbrella aimerait savoir ce que vous pensez de ces nouvelles fonctionnalités. Si vous avez des questions ou des commentaires, Umbrella veut vous entendre ! Envoyez vos commentaires à umbrella-support@cisco.com et fournissez autant de détails que possible. Par exemple, des captures d'écran, le navigateur que vous utilisez, votre système d'exploitation et le scénario dans lequel vous utilisez ces fonctionnalités.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.