WSA permet un flux de trafic WBRS faible sans perte de protection antivirus

Contenu

Introduction

Ce document décrit comment autoriser le trafic avec de faibles scores de réputation Web (WBRS) via l'appareil de sécurité Web Cisco (WSA) avec l'utilisation continue d'un programme antivirus.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les périphériques WSA.

Components Used

Les informations de ce document sont basées sur les périphériques WSA qui exécutent AsyncOS versions 5.6 et ultérieures.

Problème

Un site est bloqué en raison d'un WBRS faible. Vous souhaitez autoriser le trafic à traverser, mais analysez toujours le trafic avec un programme antivirus.

Solution

Si vous souhaitez autoriser le trafic vers cette destination, vous devez créer une stratégie d'identité/d'accès spéciale qui correspond à la demande. Par exemple, si **www.example.com** a un

score de -6.0 et est actuellement bloqué, vous devez d'abord créer une catégorie d'URL personnalisée pour cette URL. Ensuite, vous devez lier la nouvelle catégorie à une identité, lier l'identité à une stratégie d'accès et enfin modifier la plage de blocs WBRS pour la stratégie d'accès.

Complétez ces étapes afin de créer une catégorie d'URL personnalisée :

1. Connectez-vous à votre WSA, accédez à **Gestionnaire de sécurité Web > Catégories d'URL personnalisées**, puis cliquez sur **Ajouter une catégorie personnalisée...**.

2. Créez une entrée similaire à celle-ci :

   Nom de la catégorie : **Ignorer.WBRS**Sites : **www.example.com**
3. Envoyez l'entrée une fois la configuration terminée.

Complétez ces étapes afin de lier la nouvelle catégorie à une identité :

1. Accédez à **Web Security Manager > Identities** et cliquez sur **Ajouter une identité ...**.

2. Créez une identité similaire à celle-ci :

   Name : **Contourner.ID.WBRS**Insérer au-dessus : **1**Catégories d'URL avancées : **Contourner WBRS**

3. Configurez les autres champs comme vous le souhaitez. Par exemple, si vous avez besoin d'une authentification, activez l'authentification pour cette identité.

4. Envoyez l'identité une fois la configuration terminée.

Complétez ces étapes afin de lier la nouvelle identité à une stratégie d'accès :

1. Accédez à **Gestionnaire de sécurité Web > Stratégies d'accès** et cliquez sur **Ajouter une stratégie ...**.

2. Créez une stratégie similaire à celle-ci :

   Nom de la stratégie : **Ignorer.Stratégie WBRS.WBRS**Insérer au-dessus de la stratégie : **1**Identités et utilisateurs : **Sélectionner une ou plusieurs identités**Identité : **Contourner.ID.WBRS**

3. Configurez les autres champs comme vous le souhaitez.

4. Envoyez la stratégie une fois la configuration terminée.

Complétez ces étapes afin de modifier la plage de blocs WBRS pour cette nouvelle stratégie d'accès :

1. Accédez à **Web Security Manager > Access Policies > Bypass.WBRS.policy > Web Reputation and Anti-Malware Filtering** et cliquez sur **(global policy)**.

2. Modifiez la sélection **Web Reputation and Anti-Malware Settings** pour **définir Web Reputation and Anti-Malware Custom Settings**. Vous pouvez ainsi modifier les paramètres de réputation

Web.

3. Déplacez la flèche qui spécifie la **plage BLOCK** et définissez-la de sorte qu'elle commence à bloquer à **-7.0**. Cette étape est nécessaire pour que l'analyse ne se fasse pas dans toute la plage, au cas où la page est virale et le score diminue encore plus.

4. Envoyez la modification et la validation une fois la configuration terminée.

Avec cette configuration, lorsqu'un utilisateur envoie une requête à **www.example.com**, le WSA attribue cette requête au **fichier Bypass.WBRS.id**. Étant donné que la **stratégie Bypass.WBRS.** est liée à la **stratégie Bypass.WBRS.id**, le WSA applique les stratégies configurées pour la **stratégie Bypass.WBRS.**. Le paramètre WBRS de cette stratégie est configuré de sorte qu'il commence à bloquer à **-7.0**, de sorte que la demande est autorisée à passer.

Note: Si vous utilisez la catégorie **Bypass.WBRS** et configurez l'action à **autoriser** dans la catégorie URL, elle ignore l'analyse antivirus/programmes malveillants. Définissez plutôt l'action sur **Surveillance**.