Contenu

Introduction

Ce document décrit comment permettre le trafic avec les bas scores basés sur le WEB de réputation (WBRS) par l'appliance de sécurité Web de Cisco (WSA) avec l'utilisation continue d'un logiciel antivirus.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance des périphériques WSA.

Composants utilisés

Les informations dans ce document sont de base sur les périphériques WSA qui exécutent des versions 5.6 et ultérieures d'AsyncOS.

Problème

Un site est dû bloqué à un bas WBRS. Vous désirez permettre le trafic, mais balayez toujours le trafic avec un logiciel antivirus.

Solution

Si vous désirez permettre le trafic à cette destination, vous devez créer une stratégie spéciale d'identité/Access qui apparie la demande. Par exemple, si **www.example.com** a une vingtaine de -6.0 et est actuellement bloqué, vous devez d'abord créer une catégorie URL de coutume pour cet URL. Alors vous devez lier la nouvelle catégorie à une identité, liez l'identité à une stratégie d'accès, et modifiez finalement la plage de bloc WBRS pour la stratégie d'accès.

Terminez-vous ces étapes afin de créer une catégorie URL de coutume :

1. Connectez-vous dans votre WSA, naviguez vers le **gestionnaire de sécurité Web > des catégories faites sur commande URL**, et cliquez sur Add la **catégorie faite sur commande….**

2. Créez une entrée semblable à ceci :

   Nom de catégorie : **Bypass.WBRS**Sites : **www.example.com**
3. Soumettez la l'entrée une fois que la configuration est complète.

Terminez-vous ces étapes afin de lier la nouvelle catégorie à une identité :

1. Naviguez vers le **gestionnaire > les identités de sécurité Web** et cliquez sur Add l'**identité….**

2. Créez une identité semblable à ceci :

   Nom : **Bypass.WBRS.id**Insérez en haut : **1**Catégories avancées URL : **Contournement WBRS**

3. Configurez les autres champs comme désirés. Par exemple, si vous avez besoin de l'authentification, puis activez l'authentification pour cette identité.

4. Soumettez l'identité une fois que la configuration est complète.

Terminez-vous ces étapes afin de lier la nouvelle identité à une stratégie d'accès :

1. Naviguez vers le **gestionnaire de sécurité Web > les stratégies d'Access** et cliquez sur Add la **stratégie….**

2. Créez une stratégie semblable à ceci :

   Nom de stratégie : **Bypass.WBRS.policy**Insérez au-dessus de la stratégie : **1**Identités et utilisateurs : **Sélectionnez un ou plusieurs identités**Identité : **Bypass.WBRS.id**

3. Configurez les autres champs comme désirés.

4. Soumettez la stratégie une fois que la configuration est complète.

Terminez-vous ces étapes afin de modifier la plage de bloc WBRS pour cette nouvelle stratégie d'accès :

1. Naviguez vers le **gestionnaire de sécurité Web > les stratégies d'Access > le Bypass.WBRS.policy > la réputation et l'Anti-malware de Web filtrant et cliquez sur (**stratégie **globale**).

2. Changez la sélection de **configurations de réputation et d'Anti-malware de Web pour définir des paramètres personnalisés de réputation et d'Anti-malware de Web**. Ceci te permet pour changer les configurations de réputation de Web.

3. Déplacez la flèche qui spécifie la **plage de BLOC** et la place de sorte que soit les débuts à bloquer à **-7.0**. Cette étape est nécessaire de sorte que le balayage ne se produise pas par

la gamme complète, au cas où la page serait virale et les diminutions de score encore autres.

4. Soumettez la modification et la commettez une fois que la configuration est complète.

Avec cette installation, quand un utilisateur envoie une demande à **www.example.com**, le WSA assigne à cette demande le **Bypass.WBRS.id. Puisque le Bypass.WBRS.policy** est lié au **Bypass.WBRS.id, le WSA applique les** stratégies **qui sont configurées** pour le Bypass.WBRS.policy. La configuration WBRS dans cette stratégie est le configuredso **qu'elle commence** à bloquer à -7.0, ainsi on permet la demande.

Remarque: Si vous utilisez la catégorie **Bypass.WBRS** et configurez l'action **d'autoriser** dans la catégorie URL, elle saute le balayage d'antivirus/malware. Au lieu de cela, placez l'action **de surveiller**.