WSA permite el flujo de tráfico bajo WBRS sin la pérdida de protección del antivirus

Contenido

Introducción

Este documento describe cómo permitir el tráfico con las calificaciones basadas en web bajas de la reputación (WBRS) a través del dispositivo de seguridad de la red de Cisco (WSA) con el uso continuo de un programa de antivirus.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de los dispositivos WSA.

Componentes Utilizados

La información en este documento es baja en los dispositivos WSA que funcionan con las versiones 5.6 de AsyncOS y posterior.

Problema

Un sitio es bloqueado debido a un WBRS bajo. Usted desea de permitir el tráfico a través, pero todavía analiza el tráfico con un programa de antivirus.

Solución

Si usted desea de permitir el tráfico a este destino, usted debe crear una identidad/una política de

acceso especiales que haga juego la petición. Por ejemplo, si **www.example.com** tiene una calificación de -6.0 y se bloquea actualmente, usted debe primero crear una categoría de la aduana URL para este URL. Entonces usted debe atar la nueva categoría a una identidad, ata la identidad a una política de acceso, y finalmente modifica el rango del bloque WBRS para la política de acceso.

Complete estos pasos para crear una categoría de la aduana URL:

1. El registro en su WSA, navega al **administrador de seguridad de la red > las categorías de encargo URL**, y el tecleo **agrega la categoría de encargo….**

2. Cree una entrada similar a esto:

   Nombre de la categoría: **Bypass.WBRS**Sitios: **www.example.com**
3. Someta el entrada una vez que la configuración es completa.

Complete estos pasos para atar la nueva categoría a una identidad:

1. Navegue al **administrador de seguridad > a las identidades de la red** y el tecleo **agrega la identidad….**

2. Cree una identidad similar a esto:

   Nombre: **Bypass.WBRS.id**Inserte arriba: **1**Categorías avanzadas URL: **Puente WBRS**

3. Configure los otros campos según lo deseado. Por ejemplo, si usted requiere la autenticación, después habilite la autenticación para esta identidad.

4. Someta la identidad una vez que la configuración es completa.

Complete estos pasos para atar la nueva identidad a una política de acceso:

1. Navegue al **administrador de seguridad > a las políticas de acceso de la red** y el tecleo **agrega la directiva….**

2. Cree una directiva similar a esto:

   Nombre de la directiva: **Bypass.WBRS.policy**Inserte sobre la directiva: **1**Identidades y usuarios: **Seleccione una o más identidades**Identidad: **Bypass.WBRS.id**

3. Configure los otros campos según lo deseado.

4. Someta la directiva una vez que la configuración es completa.

Complete estos pasos para modificar el rango del bloque WBRS para esta nueva política de acceso:

1. Navegue al **administrador de seguridad de la red > a las políticas de acceso > a Bypass.WBRS.policy > a la reputación Web y a la filtración anti-Malware y haga clic (política global**).

2. Cambie la **reputación Web y la** selección **anti-Malware de las configuraciones para definir la**

reputación Web y las configuraciones personalizadas antis-Malware. Esto permite que usted cambie las configuraciones de la reputación Web.

3. Mueva la flecha que especifica el **rango del BLOQUE** y lo fija de modo que sea el comienzo a bloquear en **-7.0**. Este paso es necesario de modo que la exploración no ocurra a través del alcance total, en caso de que la página sea viral y las disminuciones de la calificación incluso más futuras.

4. Someta el cambio y confíelo una vez que la configuración es completa.

Con esta configuración, cuando un usuario envía una petición a **www.example.com**, el WSA asigna a esta petición el **Bypass.WBRS.id. Puesto que el Bypass.WBRS.policy** está limitado al **Bypass.WBRS.id, el WSA aplica las** directivas **que se configuran** para el Bypass.WBRS.policy. La configuración WBRS en esta directiva es el configuredso **que comienza** a bloquear en -7.0, así que la petición se permite a través.

Note: Si usted utiliza la categoría **Bypass.WBRS** y configura la acción **para permitir** en la categoría URL, desvía la exploración del antivirus/de Malware. En lugar, fije la acción **para monitorear**.