WSA permite o baixo fluxo de tráfego WBRS sem a perda de proteção do Antivirus

Índice

Introdução

Este documento descreve como permitir o tráfego com as baixas contagens com base na Web da reputação (WBRS) através da ferramenta de segurança da Web de Cisco (WSA) com o uso continuado de um programa de Antivirus.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento de dispositivos WSA.

Componentes Utilizados

A informação neste documento é baixa nos dispositivos WSA que executam versões 5.6 e mais recente de AsyncOS.

Problema

Um local é obstruído devido a um baixo WBRS. Você deseja permitir completamente o tráfego, mas ainda faz a varredura do tráfego com um programa de Antivirus.

Solução

Se você deseja permitir o tráfego a este destino, você deve criar uma identidade/política de

acesso especiais que combine o pedido. Por exemplo, se **www.example.com** tem uma contagem de -6.0 e é obstruído atualmente, você deve primeiramente criar uma categoria do costume URL para esta URL. Então você deve ligar a categoria nova a uma identidade, liga a identidade a uma política de acesso, e altera finalmente a escala do bloco WBRS para a política de acesso.

Termine estas etapas a fim criar uma categoria do costume URL:

1. O log em seu WSA, navega ao **gerenciador de segurança da Web > categorias feitas sob encomenda URL**, e o clique **adiciona a categoria feita sob encomenda….**

2. Crie uma entrada similar a esta:

   Nome da categoria: **Bypass.WBRS**Locais: **www.example.com**
3. Submeta o a entrada uma vez que a configuração está completa.

Termine estas etapas a fim ligar a categoria nova a uma identidade:

1. Navegue ao **gerenciador de segurança > às identidades da Web** e o clique **adiciona a identidade….**

2. Crie uma identidade similar a esta:

   Nome: **Bypass.WBRS.id**Introduza acima: **1**Categorias avançadas URL: **Desvio WBRS**

3. Configurar os outros campos como desejados. Por exemplo, se você exige a autenticação, a seguir permita a autenticação para esta identidade.

4. Submeta a identidade uma vez que a configuração está completa.

Termine estas etapas a fim ligar a identidade nova a uma política de acesso:

1. Navegue ao **gerenciador de segurança > às políticas de acesso da Web** e o clique **adiciona a política….**

2. Crie uma política similar a esta:

   Nome da política: **Bypass.WBRS.policy**Introduza acima da política: **1**Identidades e usuários: **Selecione umas ou várias identidades**Identidade: **Bypass.WBRS.id**

3. Configurar os outros campos como desejados.

4. Submeta a política uma vez que a configuração está completa.

Termine estas etapas a fim alterar a escala do bloco WBRS para esta política de acesso nova:

1. Navegue ao **gerenciador de segurança da Web > às políticas de acesso > ao Bypass.WBRS.policy > à reputação e ao Anti-malware da Web que filtram e clique (**política **global**).

2. Mude a seleção dos **ajustes da reputação e do Anti-malware da Web para definir configurações personalizadas da reputação e do Anti-malware da Web**. Isto permite que

você mude os ajustes da reputação da Web.

3. Mova a seta que especifica a **escala do BLOCO** e a ajusta de modo que sejam os começos a obstruir em **-7.0**. Esta etapa está precisada de modo que a varredura não ocorra através da gama completa, caso que a página é viral e as diminuições da contagem mesmo mais adicionais.

4. Submeta a mudança e comprometa-a uma vez que a configuração está completa.

Com esta instalação, quando um usuário envia um pedido a **www.example.com**, o WSA atribui a este pedido o **Bypass.WBRS.id. Desde que o Bypass.WBRS.policy** é limitado ao **Bypass.WBRS.id, o WSA aplica as** políticas **que são configuradas** para o Bypass.WBRS.policy. O ajuste WBRS nesta política é o configuredso **que começa** obstruir em -7.0, assim que o pedido é permitido completamente.

Note: Se você usa a categoria **Bypass.WBRS** e configura a ação **para permitir na** categoria URL, contorneia a varredura do Antivirus/malware. Em lugar de, ajuste a ação **para monitorar**.