Содержание

Введение

Этот документ описывает, как позволить трафик с низкими Находящимися на web очками репутации (WBRS) через Cisco Web Security Appliance (WSA) с продолжительным использованием Антивирусной программы.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с устройствами WSA.

Используемые компоненты

Сведения в этом документе являются ядром на устройствах WSA, которые выполняют Версии AsyncOS 5.6 и позже.

Проблема

Сайт заблокирован из-за низкого WBRS. Вы желаете позволить трафик через, но все еще просмотреть трафик с Антивирусной программой.

Решение

Если вы желаете позволить трафик этому назначению, необходимо создать специальную Идентичность/Политику доступа, которая совпадает с запросом. Например, если **www. пример. com** имеет счет-6.0 и в настоящее время блокируется, необходимо сначала создать пользовательскую категорию URL для этого URL. Затем необходимо связать новую категорию с идентичностью, связать идентичность с политикой доступа, и наконец модифицировать диапазон блока WBRS для политики доступа.

Выполните эти шаги для создания пользовательской категории URL:

1. Войдите в свой WSA, перейдите **веб-Менеджеру безопасности> Пользовательские категории URL** и **нажмите Add Пользовательскую Категорию....**

2. Создайте запись, подобную этому:

   Название категории: **обход. WBRS**Узлы: **www. пример. com**
3. Отправьте запись, как только конфигурация завершена.

Выполните эти шаги для привязки новой категории с идентичностью:

1. Перейдите **веб-Менеджеру безопасности> Личности** и **нажмите Add Идентичность....**

2. Создайте идентичность, подобную этому:

   Name: **Обход. WBRS.id**Вставка выше: **1**Усовершенствованные категории URL: **обходной WBRS**

3. Настройте другие поля, как желаемый. Например, если вы требуете аутентификации, затем включаете аутентификацию для этой идентичности.

4. Отправьте идентичность, как только конфигурация завершена.

Выполните эти шаги для привязки новой идентичности с политикой доступа:

1. Перейдите **веб-Менеджеру безопасности> Политика доступа** и **нажмите Add Политику....**

2. Создайте политику, подобную этому:

   Policy-name: **Обход. WBRS.policy**Вставка выше политики: **1**Личности и пользователи: **выберите One или More Identities**Идентичность: **обход. WBRS.id**

3. Настройте другие поля, как желаемый.

4. Отправьте политику, как только конфигурация завершена.

Выполните эти шаги для изменения диапазона блока WBRS для этой новой политики доступа:

1. Перейдите **веб-Менеджеру безопасности> Политика доступа> Обход. WBRS.policy> веб-фильтрация Репутации и Антивируса** и щелчок **(глобальная политика)**.

2. Измените **веб-**выбор **Параметров настройки Репутации и Антивируса** для **Определения веб-Пользовательских настроек Репутации и Антивируса**. Это позволяет вам изменять веб-настройки Репутации.

3. Переместите стрелку, которая задает **БЛОЧНЫЙ Диапазон** и устанавливает его так, чтобы были запуски для блокирования в**-7.0**. Этот шаг необходим так, чтобы просмотр не происходил через полный диапазон, в случае, если страница является вирусной и

уменьшения счета еще больше.

4. Отправьте изменение и передачу, как только конфигурация завершена.

С этой настройкой, когда пользователь отправляет запрос к **www. пример. com**, WSA назначает этот запрос **Обход. WBRS.id**. Начиная с **Обхода. WBRS.policy** связан с **Обходом. WBRS.id**, WSA применяет политику, которая настроена для **Обхода. WBRS.policy**. WBRS, устанавливающий в этой политике, настроен так, чтобы это начало блокироваться в**-7.0**, таким образом, запрос позволен через.

Примечание: При использовании **Обход.** Категория **WBRS** и настраивает Действие для **Разрешения** в категории URL, это обходит Антивирусный/Вредоносный просмотр. Вместо этого заставьте Действие **Контролировать**.