Содержание

Вопрос:

Как я настраиваю Маршрутизацию на основе политик (PBR) на Многоуровневом коммутаторе Cisco или маршрутизаторе для передачи трафика к WSA?

Среда: Cisco Web Security Appliance (WSA), прозрачный режим - коммутатор L4

Когда WSA настроен в прозрачном режиме с помощью коммутатора L4, никакая конфигурация не необходима на WSA. Перенаправление управляется коммутатором L4 (или маршрутизатор).

Возможно использовать Маршрутизацию на основе политик (PBR) для перенаправления веба - трафика к WSA. Это достигнуто, совпав с правильным трафиком (на основе портов tcp) и дав маршрутизатору/коммутатору команду перенаправить этот трафик к WSA.

В следующем примере интерфейс данных/прокси WSA (или M1 или P1 в зависимости от конфигурации) находится на интерфейсе выделенной сети VLAN многоуровневого коммутатора / маршрутизатор (Vlan 3), и Интернет-маршрутизатор находится на интерфейсе выделенной сети VLAN также (Vlan4). Клиенты находятся на Vlan1 и Vlan2.

Начальная конфигурация (только отображенные соответствующие части)
interface VLAN1 ПОЛЬЗОВАТЕЛЬСКАЯ LAN desc 1 ip address 10.1.1.1 255.255.255.0 ! интерфейсный Vlan2 ПОЛЬЗОВАТЕЛЬСКАЯ LAN desc 2 IP-адрес 10.1.2.1 255.255.255.0 ! интерфейсный Vlan3 desc Cisco выделенная сеть VLAN WSA IP-адрес 192.168.1.1 255.255.255.252 ! интерфейсный Vlan4 выделенная сеть VLAN Интернет-маршрутизатора desc IP-адрес 192.168.2.1 255.255.255.252 ! ip route 0.0.0.0 0.0.0.0 192.168.2.2

Данный вышеупомянутый пример и Cisco WSA наличие IP-адреса 192.168.1.2, вы добавили бы следующие команды для устанавливания Маршрутизации на основе политик (PBR):

Шаг 1: Определите Веб - трафик
! Трафик HTTP соответствия tcp разрешения на access-list 100 10.1.1.0 0.0.0.255 любых eq 80 tcp разрешения на access-list 100 10.1.2.0 0.0.0.255 любых eq 80 *! Совпадите с Трафиком HTTPS* tcp разрешения на access-list 100 10.1.1.0 0.0.0.255 любых eq 443 tcp разрешения на access-list 100 10.1.2.0 0.0.0.255 любых eq 443
Шаг 2: Определите Карту маршрутизации для управления, где выведены пакеты.
разрешение на route-map ForwardWeb 10 match ip address 100 set ip next-hop 192.168.1.2
Шаг 3: Примените Карту маршрутизации к корректному интерфейсу.
! Обратите внимание на то, что это должно быть применено к исходному интерфейсу (клиентская сторона) interface VLAN1 ip policy route-map ForwardWeb ! интерфейсный Vlan2 ip policy route-map ForwardWeb

Примечание: Этот метод переадресации трафика (PBR) имеет некоторые ограничения. Основная проблема с этим методом - то, что трафик будет всегда перенаправляться к WSA, даже если устройство не будет достижимо (из-за проблем сети, например). Так, нет никакой опции переключения при отказе.

Для обхождения этого дефицита можно настроить любое из придерживающегося:

1. **PBR с отслеживанием опций** при использовании маршрутизаторов Cisco. Эта функция использована для проверки доступности следующего перехода прежде, чем перенаправить трафик.

   Больше подробных данных о следующей статье:
   Пример конфигурации маршрутизации на основе политик с функцией отслеживания по нескольким параметрам
2. Отслеживающие опции не доступны для коммутаторов Cisco Catalyst. Однако существует усовершенствованный обходной путь, доступный для достижения того же поведения.

   Подробные данные могут быть найдены на следующей Cisco Wiki:
   Маршрутизация на основе политик (PBR) с отслеживанием для Catalyst 3xxx коммутаторы - обходной путь с помощью EEM