Переадресация трафика ISE на коммутаторе серии Catalyst 3750

Содержание

Введение

Эта статья описывает, как перенаправление трафика пользователя работает и условия, которые необходимы для перенаправления пакета коммутатором.

Предварительные условия

Требования

Cisco рекомендует иметь опыт с платформой Cisco Identity Services Engine (ISE) конфигурация и базовые знания об этих темах:

- Развертывания ISE и потоки Центральной веб-аутентификации (CWA)

- Конфигурация интерфейса командой строки коммутаторов Cisco Catalyst

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Microsoft Windows 7
- Cisco Catalyst программное обеспечение коммутатора серии 3750X, версии 15.0 и позже
- Программное обеспечение ISE, версии 1.1.4 и позже

Общие сведения

Перенаправление трафика пользователя на коммутаторе является критически важным компонентом для большинства развертываний с ISE. Все эти потоки включают использование переадресации трафика коммутатором:

- CWA
- Клиент, настраивающий (CPP)
- Регистрация устройства (DRW)
- Собственный соискатель, настраивающий (NSP)
- Управление мобильными устройствами (MDM)

Неправильно настроенное перенаправление является причиной нескольк проблем с развертываниями. Типичным результатом является Агент Network Admission Control (NAC), который не появляется правильно или неспособность отобразить Гостевой Портал.

Для сценариев, в которых коммутатор не имеет того же коммутируемого виртуального интерфейса (SVI) как клиентская VLAN, обратитесь к последним трем примерам.

Устранение неполадок

Сценарий проверки

Тесты выполнены на клиенте, который должен быть перенаправлен к ISE для инициализации (CPP). Пользователь аутентифицируется через Обход проверки подлинности MAC (MAB) или 802.1x. ISE возвращает профиль авторизации с названием Списка контроля доступа (ACL) перенаправления (REDIRECT_POSTURE) и URL перенаправления (перенаправления к ISE):

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface: GigabitEthernet1/0/2
         MAC Address: 0050.5699.36ce
          IP Address: 192.168.1.201
           User-Name: cisco
              Status: Authz Success
              Domain: DATA
     Security Policy: Should Secure
     Security Status: Unsecure
      Oper host mode: single-host
```

```
    Oper control dir: both
       Authorized By: Authentication Server
         Vlan Policy: 10
             ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
    URL Redirect ACL: REDIRECT_POSTURE
        URL Redirect: https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A8000100000D5D015F1B47
     Acct Session ID: 0x00011D90
              Handle: 0xBB000D5E

Runnable methods list:
      Method  State
      dot1x   Authc Success
```

Загружаемый список ACL (DACL) разрешает весь трафик на данном этапе:

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1 (per-user)
   10 permit ip any any
```

ACL перенаправления позволяет этот трафик без перенаправления:

- Весь трафик к ISE (10.48.66.74)
- Система доменных имен (DNS) и трафик Протокола ICMP

Весь другой трафик должен быть перенаправлен:

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (10 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

Коммутатор имеет SVI в той же VLAN как пользователь:

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
```

В следующих разделах это модифицируется для представления потенциального воздействия.

Трафик не достигает ACL перенаправления

Когда вы пытаетесь пропинговать любой хост, необходимо получить ответ, потому что не перенаправлен тот трафик. Для подтверждения выполните эту отладку:

```
debug epm redirect
```

Для каждого пакета ICMP, передаваемого клиентом, отладки должны представить:

```
Jan 9 09:13:07.861: epm-redirect:IDB=GigabitEthernet1/0/2: In
epm_host_ingress_traffic_qualify ...
Jan 9 09:13:07.861: epm-redirect:epm_redirect_cache_gen_hash:
IP=192.168.1.201 Hash=562
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: CacheEntryGet Success
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: Ingress packet on
[idb= GigabitEthernet1/0/2] didn't match with [acl=REDIRECT_POSTURE]
```

Для подтверждения исследуйте ACL:

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (4 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

Трафик достигает ACL перенаправления

Сценарий 1 - Адресат находится в Той же VLAN, Существует и является SVI 10 UP

Когда вы инициируете трафик к IP-адресу, который является непосредственно Уровнем 3 (L3), достижимый коммутатором (сеть для коммутатора имеет интерфейс SVI), вот то, что происходит:

1. Клиент инициирует запрос разрешения Протокола ARP об адресате (192.168.1.20) в той же VLAN и получает ответ (трафик ARP никогда не перенаправляется).

2. Точки пересечения коммутатора, которые открывают сеанс, даже когда IP - адрес назначения не настроен на том коммутаторе. Квитирование TCP между клиентом и коммутатором закончено. На данном этапе никакие другие пакеты не переданы за пределами коммутатора. В этом сценарии клиент (192.168.1.201) инициировал сеанс TCP с другим хостом, который существует в той VLAN (192.168.1.20) и для которого коммутатор имеет интерфейс SVI UP (с IP-адресом 192.168.1.10):

3. После того, как сеанс TCP установлен, и запрос HTTP передается, коммутатор возвращает Ответ HTTP с перенаправлением к ISE (Заголовок местоположения).

   Эти шаги подтверждены отладками. Существует несколько соответствий ACL:

   ```
   epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2]
   matched with [acl=REDIRECT_POSTURE]
   epm-redirect:Fill in URL=https://10.48.66.74:8443/guestportal/gateway?sessionId=
   C0A8000100000D5D015F1B47&action=cpp for redirection
   epm-redirect:IP=192.168.1.201: Redirect http request to https:
   //10.48.66.74:8443/guestportal/gateway?sessionId=C0A8000100000D5D015F1B47&action=cpp
   epm-redirect:EPM HTTP Redirect Daemon successfully created
   ```

   Это может также быть подтверждено более подробными отладками:

   ```
   debug ip http all

   http_epm_http_redirect_daemon: got redirect request
   HTTP: token len 3: 'GET'
   http_proxy_send_page: Sending http proxy page
   http_epm_send_redirect_page: Sending the Redirect page to ...
   ```

4. Клиент соединяется с ISE непосредственно (сеанс Уровня защищенных сокетов (SSL) к 10.48.66.74:8443). Этот пакет не инициирует перенаправление:

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] didn't
match with [acl=REDIRECT_POSTURE]
```

Примечание: Сеанс перехвачен коммутатором, и таким образом что трафик может быть перехвачен на коммутаторе со встроенной функцией захвата пакетов (EPC). Предыдущий перехват был взят с EPC на коммутаторе.

Сценарий 2 - Адресат находится в Той же VLAN, Не Существует и является SVI 10 UP

Если адресат 192.168.1.20 не работает (не отвечает), клиент не получает ответ ARP (коммутатор не перехватывает ARP), и клиент не передает SYN TCP. Перенаправление никогда не происходит.

Это - то, почему Агент NAC использует шлюз по умолчанию для обнаружения. Шлюз по умолчанию должен всегда отвечать и инициировать перенаправления.

Сценарий 3 - Адресат находится в Другой VLAN, Существует и является SVI 10 UP

Вот то, что происходит в этом сценарии:

1. Клиент пытается обратиться к HTTP://8.8.8.8.

2. Та сеть не находится ни на каком SVI на коммутаторе.
3. Клиент передает SYN TCP за тем сеансом к шлюзу по умолчанию 192.168.1.10 (известный MAC - адрес назначения).

4. Перенаправление инициировано точно таким же образом как в первом примере.

5. Точки пересечения коммутатора, которые открывают сеанс и возвращают Ответ HTTP, который перенаправляет к серверу ISE.

6. Доступы клиента сервер ISE без проблем (что трафик не перенаправлен).

Примечание: Если шлюз по умолчанию находится на том же коммутаторе или на устройстве восходящего потока данных, не имеет значения. Только необходимо получить ответ ARP от того шлюза для инициирования процесса перенаправления. Кроме того, необходимо, чтобы была разрешена доступность ISE через шлюз по умолчанию. Обратите особое внимание, если межсетевой экран находится на исправлении, особенно если это - Уровень 2 (L2), межсетевой экран и пакеты L2 пересекают другие ссылки (тогда, обход состояния TCP мог бы быть необходимым на межсетевом экране).

Сценарий 4 - Адресат находится в Другой VLAN, Не Существует и является SVI 10 UP

Этот сценарий является точно тем же как Сценарием 3. Если адресат в удаленной VLAN существует или нет, не имеет значения.

Сценарий 5 - Адресат находится в Другой VLAN, Существует и является ВЫКЛЮЧЕННЫМ SVI 10

Если коммутатор не имеет SVI UP в той же VLAN как клиент, это может все еще выполнить перенаправление, но только когда совпадают с особыми условиями.

Проблема для коммутатора состоит в том, как возвратить ответ клиенту от другого SVI. Трудно определить, какой источник с MAC-адресом должен использоваться.

Поток отличается от того, когда SVI подключен UP:

1. Клиент передает SYN TCP к хосту в другой VLAN (192.168.2.20) с набором MAC - адреса назначения к шлюзу по умолчанию, который определен на восходящем коммутаторе. Тот пакет достигает ACL перенаправления, который показывают отладки.
2. Коммутатор проверяет, имеет ли он маршрутизацию назад клиенту. Помните, что SVI 10 не работает.
3. Если коммутатор не имеет другого SVI, который имеет маршрутизацию назад клиенту, тот пакет не перехвачен или перенаправлен, даже когда журналы Менеджера политики предприятия (EPM) указывают, что достигнут ACL. Удаленный хост мог бы возвратить ACK SYN, но коммутатор не имеет маршрутизации назад клиенту (VLAN10) и отбрасывает пакет. Пакет не может только быть коммутирован назад (L2), потому что это достигло ACL перенаправления.
4. Если коммутатор действительно имеет маршрутизацию к клиентской VLAN через другой SVI, это перехватывает тот пакет и выполняет перенаправление, как обычно. Ответ с перенаправлением URL не идет непосредственно к клиенту, но через другой коммутатор/маршрутизатор на основе решения о маршрутизации.

Заметьте асимметрию здесь:

- Трафик, полученный от клиента, перехвачен локально коммутатором.
- Ответ, для который, который включает перенаправление HTTP, передается через восходящий коммутатор на основе маршрутизации.
- Это - когда типичные проблемы с межсетевым экраном могли бы произойти, и обход TCP требуется.
- Трафик к ISE, который не перенаправлен, симметричен. Только само перенаправление асимметрично.

Сценарий 6 - Адресат находится в Другой VLAN, Не Существует и является ВЫКЛЮЧЕННЫМ SVI 10

Этот сценарий является точно тем же как Сценарием 5. Не имеет значения, что существует удаленный хост. Корректная маршрутизация - то, что важно.

Сценарий 7 - Сервис HTTP не работает

Как представлено в Сценарии 6, Процесс HTTP на коммутаторе играет важную роль. Если

сервис HTTP отключен, EPM показывает, что пакет достигает ACL перенаправления:

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] matched
with [acl=REDIRECT_POSTURE]
```

Однако перенаправление никогда не происходит.

Сервис HTTPS на коммутаторе не требуется для перенаправления HTTP, но это требуется для перенаправления HTTPS. Агент NAC может использовать обоих для обнаружения ISE. Поэтому рекомендуется включить обоим.

ACL перенаправления - неправильные протоколы и порт, никакое перенаправление

Заметьте, что коммутатор может только перехватить трафик HTTP или Трафик HTTPS, который работает на стандартные порты (TCP/80 и TCP/443). Если HTTP/HTTPS работает на нестандартный порт, он может быть настроен с командой **http ip port-map**. Кроме того, коммутатор должен иметь свой сервер HTTP, слушают на том порту **(ip http port)**.

Дополнительные сведения

- Центральная веб-аутентификация с коммутатором и примером конфигурации платформы Identity Services Engine
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация