Фильтры VPN на примере конфигурации Cisco ASA

Содержание

Введение

Этот документ описывает фильтры VPN подробно и применяется к LAN-LAN (L2L), Cisco VPN Client и защищенный мобильный клиент Cisco AnyConnect Secure Mobility.

Фильтры состоят из правил, которые указывают пропускать или отклонять туннелируемые пакеты данных, проходящие через устройство защиты, на основании различных критериев, например адреса источника, адреса получателя и протокола. Вы настраиваете Списки контроля доступа (ACL) для permit or deny различных типов трафика. Фильтр может быть настроен на групповой политике, атрибутах имени пользователя или политике динамического доступа (DAP).

DAP заменяет значение, настроенное и под атрибутами имени пользователя и под групповой политикой. Значение атрибута имени пользователя заменяет значение групповой политики в случае, если DAP не назначает фильтра.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Конфигурация VPN-туннелей L2L
- Конфигурация Удаленного доступа (RA) Клиента VPN
- AnyConnect конфигурация RA

Используемые компоненты

Сведения в этом документе основываются на Версии 9.1 (2) Устройства адаптивной защиты (ASA) Cisco 5500-X Series.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Команда **sysopt connection permit-vpn** позволяет весь трафик, который поступает в устройство безопасности через VPN-туннель для обхода списков доступа к интерфейсам. К трафику продолжают применяться групповые политики и списки авторизации доступа на уровне отдельных пользователей.

Vpn-filter применен к постдешифрованному трафику после того, как это выходит из туннеля и к предварительно зашифрованному трафику, прежде чем это введет туннель. ACL, что isused для vpn-filter не должен также использоваться для интерфейсного access-group.

Когда vpn-filter применен к групповой политике, которая управляет клиентскими соединениями VPN для удаленного доступа, ACL должен быть настроен с клиентскими назначенными IP - адресами в src_ip позиции ACL и локальной сети в dest_ip позиции ACL. Когда vpn-filter применен к групповой политике , которая управляет VPN-подключением L2L, ACL должен быть настроен с удаленной сетью в src_ip позиции ACL и локальной сети в dest_ip позиции ACL.

Настройка

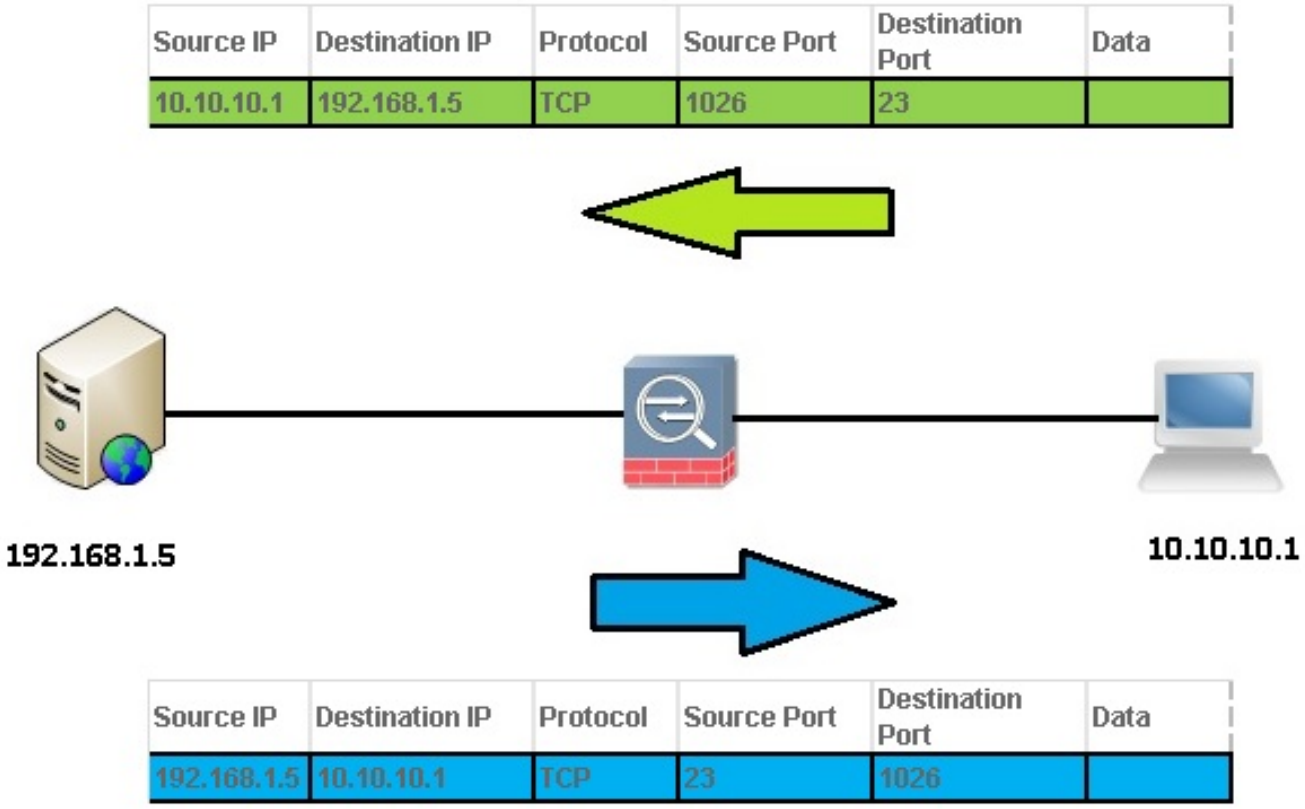
Фильтры VPN должны быть настроены во входящем направлении невзирая на то, что правила все еще применены двунаправленным образом. CSCsf99428 усовершенствования был открыт для поддержки однонаправленных правил, но он еще не планировался/передавался для реализации.

Пример 1. vpn-filter с AnyConnect или Клиентом VPN

Предположите, что клиентский назначенный IP - адрес является 10.10.10.1/24, и локальная сеть является 192.168.1.0/24.

Этот Элемент управления доступом (ACE) позволяет клиенту AnyConnect Telnet к локальной сети:

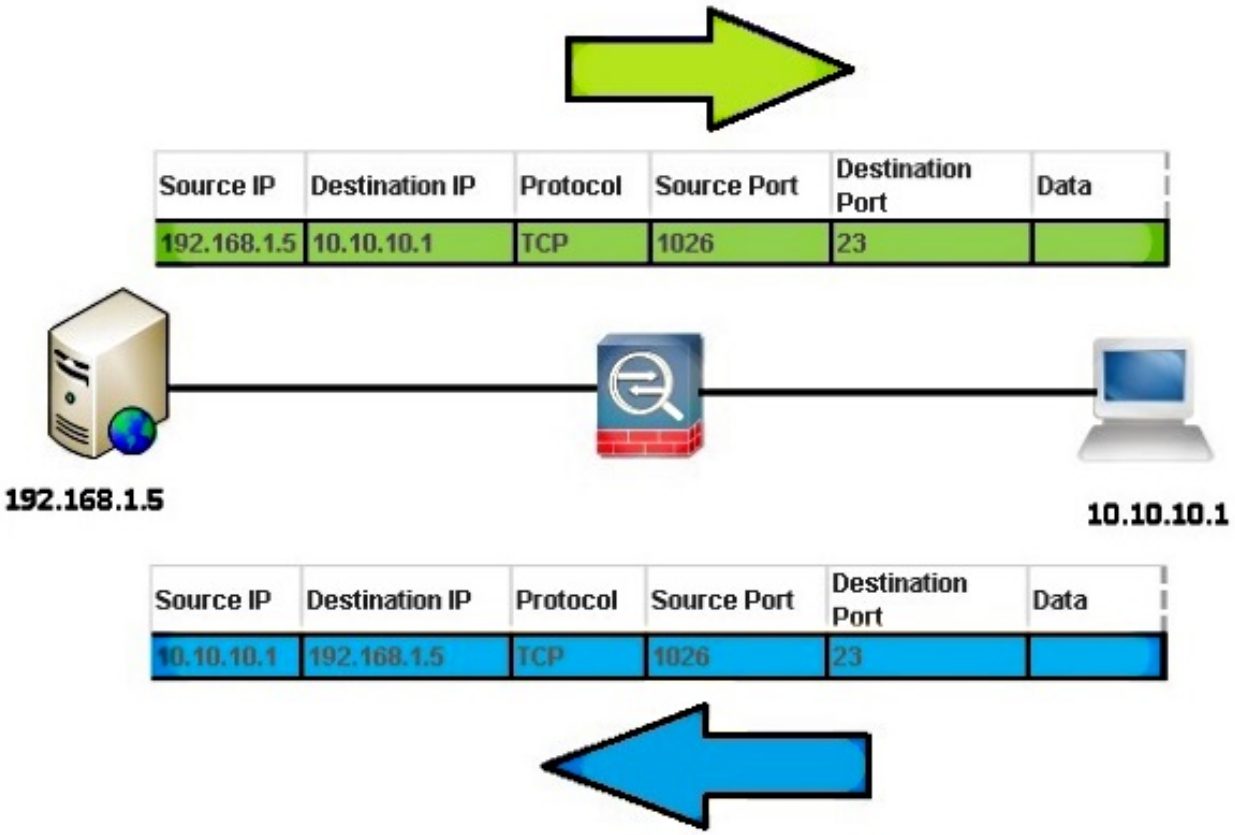
```
access-list vpnfilt-ra permit tcp

10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



Примечание: Первоклассный tcp разрешения vpnfilt-Pa access-list 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23 также позволяют локальной сети инициировать соединение с клиентом RA на любом порте TCP, если это использует исходный порт 23.

Этот ACE позволяет локальную сеть Telnet клиенту AnyConnect:

```
access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255
eq 23 192.168.1.0 255.255.255.0
```



Примечание: Первоклассный tcp разрешения vpnfilt-Pa access-list 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0 также позволяют клиенту RA инициировать соединение с локальной сетью на любом порте TCP, если это использует исходный порт 23.

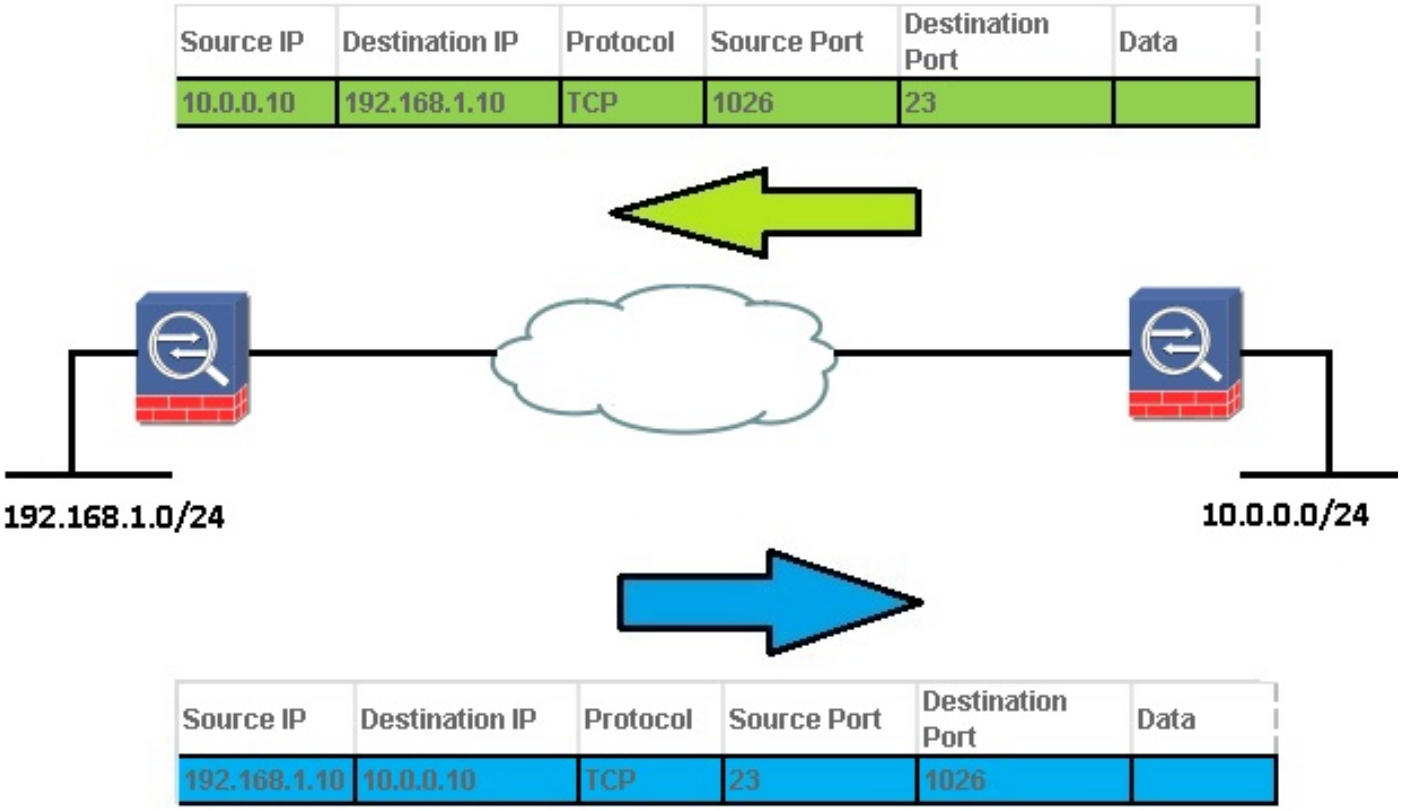
Внимание. : Функция vpn-filter обеспечивает трафик, который будет фильтроваться во входящем направлении только, и исходящее правило автоматически скомпилировано. Поэтому при создании access-list Протокола ICMP не задавайте тип ICMP в форматировании access-list, если вы хотите направляющие фильтры.

Пример 2. vpn-filter с VPN-подключением L2L

Предположите, что удаленная сеть является 10.0.0.0/24, и локальная сеть является 192.168.1.0/24.

Этот ACE позволяет удаленную сеть Telnet к локальной сети:

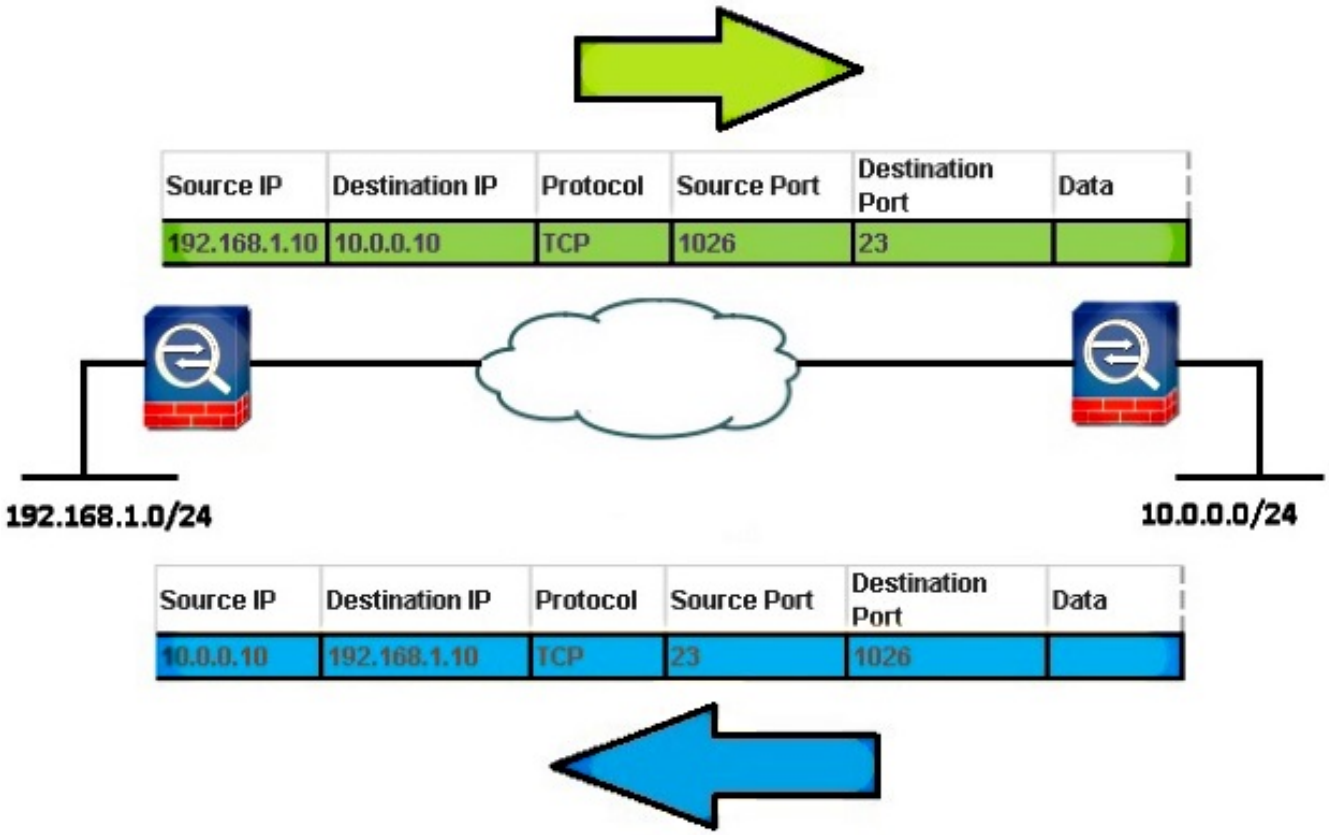
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



Примечание: Первоклассный tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23 разрешения на access-list vpnfilt-l2l также позволяет локальной сети инициировать соединение с удаленной сетью на любом порте TCP, если это использует исходный порт 23.

Этот ACE позволяет локальную сеть Telnet к удаленной сети:

```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```



Примечание: Первоклассный tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0 разрешения на access-list vpnfilt-l2l также позволяет удаленной сети инициировать соединение с локальной сетью на любом порте TCP, если это использует исходный порт 23.

Внимание. : Функция vpn-filter обеспечивает трафик, который будет фильтроваться во входящем направлении только, и исходящее правило автоматически скомпилировано. Поэтому при создании access-list ICMP не задавайте тип ICMP в форматировании access-list, если вы хотите направляющие фильтры.

Фильтры VPN и группы доступа замены для каждого пользователя

Трафик VPN не фильтруется интерфейсными ACL. Команда **никакой sysopt connection permit-vpn** не может использоваться для изменения поведения по умолчанию. В этом случае два ACL могут быть применены к трафику пользователя: интерфейсный ACL проверен сначала и затем vpn-filter.

Ключевое слово **замены для каждого пользователя** (только для списков контроля входящего доступа) позволяет динамические пользовательские ACL, которые загружены для авторизации пользователя для переопределения ACL, назначенного на интерфейс. Например, если интерфейсный ACL запрещает весь трафик от 10.0.0.0, но динамический ACL разрешает весь трафик от 10.0.0.0, то динамический ACL отвергает интерфейсный ACL для того пользователя, и трафик разрешен.

Примеры (когда **никакой sysopt connection permit-vpn** не настроен):

- никакая замена для каждого пользователя, никакой vpn-filter - с трафиком совпадают

против интерфейсного ACL

- никакая замена для каждого пользователя, vpn-filter - с трафиком совпадают сначала против интерфейсного ACL, затем против vpn-filter
- замена для каждого пользователя, vpn-filter - с трафиком совпадают против vpn-filter только

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show**. Используйте Cisco CLI Анализатор для **просматривания аналитику выходных данных команды show**.

- **покажите фильтр таблицы asp [access-list <*name*> *acl*] [соответствия]**

  Для отладки ускоренных таблиц фильтра пути безопасности используйте **команду фильтрации таблицы asp показа** в привилегированном режиме EXEC. Когда фильтр был применен к VPN-туннелю, правила фильтрации установлены в таблицу фильтра. Если туннелю задали фильтр, то таблица фильтра проверена до шифрования и после расшифровки, чтобы определить, должен ли внутренний пакет быть разрешен или запрещен.

```
USAGE
show asp table filter [access-list <acl-name>] [hits]
```


```
USAGE
show asp table filter [access-list <acl-name>] [hits]
```


- **очистите фильтр таблицы asp [access-list <*name*> *acl*]**

  Эта команда очищает счетчики попаданий для элементов таблицы фильтра ASP.

```
USAGE
clear asp table filter [access-list <acl-name>]
```


```
USAGE
clear asp table filter [access-list <acl-name>]
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show**. Используйте Cisco CLI Анализатор для **просматривания аналитику выходных данных команды show**.

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **фильтр acl отладки**

  Эта команда включает отладку фильтра VPN. Это может использоваться для помощи установкам/удалению устранения проблем фильтров VPN в таблицу Фильтра ASP. Для Примера 1. vpn-filter с AnyConnect или Клиентом VPN.

  Выходные данные отладки, когда соединяется user1:

```
 USAGE
clear asp table filter [access-list <acl-name>]
```

  Выходные данные отладки, когда user2 соединяется (после того, как user1 и тот же фильтр):

```
 USAGE
clear asp table filter [access-list <acl-name>]
```

  Выходные данные отладки, когда user2 разъединяет:

```
 USAGE
clear asp table filter [access-list <acl-name>]
```

  Выходные данные отладки, когда user1 разъединяет:

```
 USAGE
clear asp table filter [access-list <acl-name>]
```

- **покажите таблицу asp**

  Вот выходные данные **фильтра таблицы asp показа** до того, когда соединяется user1. Только неявные запрещают правила, установлены для IPv4 и IPv6 и в в и в направления.

```
 USAGE
```

clear asp table filter [access-list <acl-name>]