

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Пример конфигурации списков управления доступом \(ACL\)](#)

[Предупреждения](#)

[Дополнительные сведения](#)

Введение

Перехват Списка контроля доступа (ACL) предоставляет вам способность выборочно перехватить трафик на интерфейсе или виртуальной локальной сети (VLAN) при включении опции перехвата для правила списка прав доступа (ACL) пакеты, которые совпадают с этим правилом, или переданы или отброшены на основе указанного, permit or deny действие и может также быть скопирован к альтернативному порту назначения для дальнейшего анализа. Правило списка прав доступа (ACL) с опцией перехвата может быть применено:

1. В VLAN,
2. В направлении доступа на всех интерфейсах,
3. В выходном направлении на всех Интерфейсах уровня 3.

Эта функция поддерживается от выпуска 5.2 Nexus 7000 NX-OS и позже. Этот документ предоставляет пример как краткое справочное руководство о том, как настроить эту функцию.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Nexus 7000 с Выпуском 5.2.x и позже.
- Линейная карта серии M1.

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.

Условные обозначения

[Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Пример конфигурации списков управления доступом (ACL)

Вот пример конфигурации перехвата ACL, примененный к VLAN, также известной как Список контроля доступа виртуальной локальной сети (VACL) перехват. Определяемые анализаторы на десять гигабитов могут не быть выполнимыми для всех сценариев. Когда объемы трафика высоки, выборочный перехват трафика может быть очень полезным в таких сценариях особенно во время устранения проблем.

Можно также проверить программирование Ternary Content Addressable Memory (TCAM) списка доступа. Эти выходные данные для VLAN 500 для Модуля 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics
```

```
slot 1
=====
```

```
INSTANCE 0x0
-----
```

```
Tcam 1 resource usage:
-----
```

```
Label_b = 0x802
Bank 0
-----
```

```
IPv4 Class
```

```
Policies: VACL(VACL_TEST)
```

```
Netflow profile: 0
```

```
Netflow deny profile: 0
```

```
Entries:
```

```
[Index] Entry [Stats]
```

```
-----
```

```
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
```

```
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
```

```
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
```

```
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
```

```
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

Предупреждения

1. Только один сеанс перехвата ACL может быть активным в любое заданное время в системе через контексты виртуального устройства (VDC).
2. Nexus 7000 модули Серии F1 не поддерживает перехват ACL.
3. Nexus 7000 модули Серии F2 в настоящее время не поддерживают перехват ACL, но это могло бы быть в плане развития.
4. Перехват ACL на Nexus модули серии M2 7000 поддерживается с Выпуском 6.1 (1)

Cisco NX-OS и позже.

5. Перехват ACL на Nexus модули серии M1 7000 поддерживается с Выпуском 5.2 (1) Cisco NX-OS и позже.
6. Перехват ACL не совместим с Регистрацией ACL. Поэтому, если у вас есть ACL с **регистрационным** ключевым словом, они не работают после глобального ввода аппаратного перехвата **access-list**.
7. Из-за [дефекта CSCug20139](#) пример в этом документе задокументирован с **сеансом перехвата** на ACE вместо на ACL, пока не решен дефект.

Дополнительные сведения

- [Cisco Nexus руководство по конфигурации системы безопасности NX-OS серии 7000, выпуск 6.x, примеры конфигурации для ACL IP](#)
- [Cisco Systems – техническая поддержка и документация](#)