Nexus 7000 и 7700 коммутаторов серии оптимизированный пример конфигурации регистрации ACL

Содержание

Введение

Этот документ описывает, как настроить Оптимизированную Регистрацию Списка контроля доступа (ACL) (OAL) на коммутаторах Серии Cisco Nexus 7000 и 7700.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с конфигурациями Nexus с основными ACL перед попыткой конфигурации, которая описана в этом документе.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного

обеспечения:

- Коммутаторы Cisco Nexus серии 7000
- Коммутаторы Серии Cisco Nexus 7700

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

ACL logging enabled предоставляют понимание трафика, поскольку это пересекает сеть или отброшено сетевыми устройствами. К сожалению, Регистрация ACL может быть сом интенсивной загрузкой ЦПУ и может негативно влиять на другие функции сетевого устройства. Для сокращения циклов ЦПУ коммутатор Cisco Nexus серии 7000 использует OAL.

Использование OAL предоставляет аппаратную поддержку для Регистрации ACL. OAL разрешает или пакеты отбрасываний в аппаратных средствах и использует оптимизированную подпрограмму для передачи информации к Супервизору так, чтобы это могло генерировать сообщения регистрации. Например, когда пакет поражает ACL logging enabled, в то время как это передано в аппаратных средствах, копия пакета создана в аппаратных средствах, и пакет плывется на плоскодонке к Супервизору для регистрации в соответствии с временным интервалом, который настроен.

Настройка

Этот раздел предоставляет сведения, который можно использовать для настройки коммутатора Nexus для использования OAL.

В примере, который описан в этом разделе, существует хост в IP-адресе 10.10.10.1, который передает трафик к другому хосту в IP-адресе 172.16.10.10 через Nexus интерфейс серии 7000, который имеет ACL с регистрацией настроенного.

Схема сети

Соединение между хостами и Коммутатором Cisco Nexus серии 7000 происходит согласно этой топологии:

Конфигурации

Выполните эти шаги для настройки коммутатора для использования OAL:

1. Настройте эти команды global для включения OAL:
```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
```

```
logging ip access-list cache threshold 0
```
Например:
```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. Примените эту конфигурацию для регистрации:
```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```
Например:
```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level 5
Nexus-7000(config)# logging logfile acllog 5
```

3. Настройте ACL чтобы к enable logging. Записи должны быть настроены с **регистрационным** включенным ключевым словом, как показано в данном примере:
```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
Nexus-7000(config-acl)#
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
10 permit ip 10.10.10.1/32 172.16.10.10/32 log
20 deny ip any any log
Nexus-7000(config-acl)#
```

4. Примените ACL, который вы настроили в предыдущем шаге в соответствующий интерфейс:
```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
Nexus-7000(config-if)#
Nexus-7000(config-if)# show run int ethernet 4/1
!Command: show running-config interface Ethernet4/1
!Time: Mon Jun 30 16:30:38 2014
version 6.2(6)
interface Ethernet4/1
 ip access-group test1 in
 ip access-group test1 out
 ip address 10.10.10.2/24
 no shutdown
Nexus-7000(config-if)#
```

Проверка

Используйте информацию, которая предоставлена в этом разделе, чтобы проверить, что ваша конфигурация работает должным образом.

В примере, который используется в этом документе, эхо-запрос инициируется от хоста в IP-адресе 10.10.10.1 к хосту в IP-адресе 172.16.10.1. Введите **команду show logging ip access-list cache** в CLI для проверки трафика:

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
```

```
-------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

Вы видите регистрацию каждые 300 секунд, поскольку это - интервал времени по умолчанию:

```
Nexus-7000# show logging logfile
2014 Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog)
cleared by user
2014 Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on console0
2014 Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 2589
2014 Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 4561
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Примечания по конфигурации

Этот раздел предоставляет дополнительные сведения о конфигурации, которая описана в этом документе.

Подробная регистрация ACL

В Операционной системе Nexus (NX-OS) Освобождают 6.2 (6) и позже, *подробная* Регистрация ACL доступна. Функция регистрирует эту информацию:

- IP-адреса источника и получателя
- Источник и порты назначения
- Source interface
- Протокол
- Название ACL
- Действие списка прав доступа (ACL) (permit or deny)
- Прикладной интерфейс
- Packet count

Войдите **ip access-list регистрации детализировал** команду в CLI для включения подробной регистрации. Например:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

Вот регистрация вывода в качестве примера, после того, как детализировано, регистрация

включена:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

Глобальные описания команды OAL

В этом разделе описываются глобальные команды OAL, которые используются для настройки Коммутатора Cisco Nexus серии 7000 для использования OAL.

Команда	Описание
Коммутатор (config) # logging ip access-list cache {{записи number_of_entries} | {секунды интервала} | {rate-limit number_of_packets} | {порог number_of_packets}}	Это наборы команд глобальные параметры OAL.
Коммутатор (config) # никакой кэш ip access-list регистрации {записи | интервал | rate-limit | порог}	Эта команда возвращается глобальные параметры OAL к настро по умолчанию.
записи num_entries	Эти параметры задают максимальное число записей журнала, которые кэшируются в программном обеспечении. Диапазон от 0 1,048,576. Значение по умолчанию является 8,000 записей.
интервал секунды	Эти параметры задают интервал максимального времени, прежд запись будет передана системному журналу. Диапазон 5 - 86,400 Значение по умолчанию составляет 300 секунд.
threshold num_packets	Эти параметры задают количество пакетных соответствий (соответствия), прежде чем запись будет передана системному журналу. Диапазон от 0 до 1,000,000. Значение по умолчанию является 0 пакетами (ограничение скорости выключено), что означает, что системный журнал не инициирован количеством пакетных соответствий.

Примечание: *Никакая* форма этих команд CLI только не возвращается параметры к настройкам по умолчанию, если они были изменены; это не удаляет конфигурацию, поскольку Коммутатор Cisco Nexus серии 7000 только имеет опцию OAL.

Описания команды Регистрации

В этом разделе описываются команды регистрации, которые используются для настройки Коммутатора Cisco Nexus серии 7000 для использования OAL.

Команда	Описание
коммутатор (config) # acllog журнал соответствия - номер уровня Пример: коммутатор (config) # acllog журнал соответствия -	Эта команда задает уровень регистрации, с которым нужно совп прежде чем записи зарегистрированы в журнале ACL (acllog). Диапазон от 0 до 7. По умолчанию является значением, 6.

уровень 3 Коммутатор (config) # никакой acllog журнал соответствия - номер уровня Пример: коммутатор (config) # никакой acllog журнал соответствия - уровень 6	Эта команда возвращается уровень регистрации к настройке по умолчанию (6).
Коммутатор (config) # уровень важности средства уровня регистрации Пример: коммутатор (config) # уровень регистрации acllog 3	Эта команда включает сообщения регистрации от указанного средства, которые имеют указанный уровень важности или выше примере, который используется в этом документе, *acllog* уровень установлен в 3, тогда как настройка по умолчанию равняется 2.
Коммутатор (config) # никакой уровень регистрации [уровень важности средства] Пример: коммутатор (config) # никакой уровень регистрации acllog 3	Эта команда перезагружает уровень важности регистрации для указанного средства к его уровню по умолчанию. Если вы не зад средство и степени серьезности ошибки уровень, устройство перезагружает все средства к их уровням по умолчанию. В примере, который используется в этом документе acllog вернулся к по умолчанию (2).
Коммутатор (config) # уровень важности названия файла журнала logging logfile [байты размера] Пример: коммутатор (config) # logging logfile acllog 3	Эта команда настраивает название файла журнала, который используется для хранения системных сообщений и минимальн уровня серьезности, прежде чем произойдет регистрация. Можн дополнительно задать максимальный размер файла. Уровень важности по умолчанию равняется 5, и размер файла по умолча 10,485,760.
Коммутатор (config) # никакой logging logfile [уровень важности названия файла журнала [байты размера]] Пример: коммутатор (config) # никакой logging logfile acllog 3	Эта команда отключает регистрацию к файлу журнала.

Примечание: Для сообщений журнала, которые будут введены в журналы, уровень регистрации для средства журнала ACL (acllog) и уровня важности регистрации для файла журнала должен быть больше, чем или равным значению *регистрационного уровня соответствия* журнала ACL.

Рекомендации и ограничения

Вот некоторые важные рекомендации и ограничения, которые необходимо рассмотреть перед применением конфигурации, которая описана в этом документе:

- Nexus 7000 и 7700 коммутаторов Серии поддерживают только OAL.
- Регистрация ACL не работает с функцией Перехвата ACL.
- *Регистрационная* опция в выходных ACL не поддерживается для пакетов групповой адресации.
- Подробная поддержка регистрации не доступна для пакетов IPv6.

- Уровень регистрации для *acllog* средства и степеней серьезности ошибки *logging logfile* должен быть настроен таким образом, что они больше, чем или равны *acllog* значению *регистрационного уровня соответствия*.

- Не используйте **аппаратную** команду **перехвата access-list**, в то время как используется OAL. Когда эта команда используется вместе с OAL, и вы включаете перехват ACL, предупреждающее сообщение появляется, чтобы сообщить вам, что Регистрация ACL отключается для всех Контекстов Виртуального устройства (VDC). При отключении перехвата ACL Регистрация ACL включена. Для этого процесса для работы должным образом отключите с использованием **никакой аппаратной** команды **перехвата access-list**.