Реализация усовершенствования функции SNMP ASA

Содержание

Введение

Этот документ описывает новые функции Протокола SNMP, которые доступны для устройства адаптивной защиты Cisco (ASA) Межсетевой экран серии 5500-X в выпуске ПО 9.1.5 и Версиях 9.2. (1) и позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Межсетевом экране Cisco ASA 5500-X Series, который выполняет Cisco ASA® Software Release 9.1.5 и Версии 9.2. (1) и позже.

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

В Версиях ASA 9.1.5 и 9.2.1 представлены эти усовершенствования SNMP:

- Поддержка 128 хостов SNMP добавлена.
- Поддержка Идентификаторов объекта SNMP cpmCPUTotal5minRev (OID) добавлена.
- Поддержка 1,472-байтовых сообщений SNMP добавлена.

Поддержка 128 хостов SNMP

Эта функция позволяет ASA поддерживать больше, чем текущие 32 хоста SNMP.

Цель

В настоящее время ASA имеет жесткий предел 32 общих количеств хостов SNMP. Это включает хосты, которые могут быть настроены для trap-сообщений и для опроса. Следующие разделы описывают влияние, которое эта функция имеет на режимах мультиконтекста и одиночном.

Режим одиночного контекста

- Позволяет значительно более высокому количеству записей (общие хосты) быть настроенным, вверх 4,096. Однако из этих записей, только 128 могут использоваться для trap-сообщений.
- Для опроса целей настройки до 4,096 хостов опроса и 128 узлам прерывания позволяют быть настроенными. Однако фактическое количество серверов, которые опрашивают систему, должно быть ограничено меньше чем 128, поскольку влияния на производительность от более высокого количества хостов неизвестны и не поддерживаемы.

Режим мультиконтекста

- Для целей настройки позволены до 4,000 хостов на контекст, и ограничение в масштабе всей системы 64,000 общих хостов наложено.

- Из общих настроенных хостов только 128 (на контекст) могут использоваться для trap-сообщений, и предел глобальной системы для trap-сообщений в режиме мультиконтекста 32,000.

- Несмотря на то, что можно настроить до 4,000 общих хостов на контекст, фактическое количество серверов, которые опрашивают любой контекст, должно быть ограничено 128.

Описание

Вы могли бы предпочесть контролировать сетевые устройства от большого бассейна хостов SNMP. Идеально, вы хотите способность задать диапазон IP и/или подсеть IP-адресов, которым позволяют контролировать сетевые устройства. ASA в настоящее время не предоставляет ту гибкость и ограничивает максимальные хосты SNMP 32.

Поддержка этой функции включает два аспекта:

- Предоставьте возможность ASA для обработки до 128 хостов SNMP.

- Предоставьте команды требуемой конфигурации так, чтобы можно было настроить значительно более высокое количество хостов, как детализировано в предыдущем разделе через одиночную команду.

Текущий дизайн на ASA таков, что отдельные хосты могут быть настроены через CLI. Для этой функции рассмотрели эти дополнительные требования к проектированию:

- Введение команды CLI **группы узлов snmp-server** с задержанием команды CLI **snmp-server host**.

- Способность к записям для прибытия и из **группы узлов snmp-server** и из команд CLI **snmp-server host**.

- Для SNMP Version 3, введения **snmp-server userlist** команда CLI с задержанием команды CLI **snmp-server user**.

- Наложение конфигурации должно также поддерживаться. Например, множественные команды **группы узлов** могут быть даны с хостами, которые накладываются в сетевых объектах. Точно так же можно задать хост с IP-адресом, который накладывается на текущие хосты или группу узлов. Это предоставляет механизм, который может использоваться для перезаписи параметров для нескольких хостов в группе без потребности реконфигурировать завершенную группу.

Некоторые ограничения ПО и предупреждения, которые привязаны к этой функции:

- Если **[trap|poll]** не задан, как часть команды **группы узлов snmp-server**, по умолчанию является **опросом**. Также важно обратить внимание, что для этой команды, и trap-сообщения и опрос не могут быть включены для той же группы узлов. Если это требуется, Cisco рекомендует использовать **команду snmp-server host** для соответствующих хостов.

- Можно задать сетевые объекты, которые накладываются в других командах **группы узлов**. Значения, которые заданы в последней группе узлов, вступают в силу для единого набора хостов в других сетевых объектах.

Например:

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

Введите **команду snmp-server host показа** для просмотра записей хоста:

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside poll version 3 cisco1
host ip = 64.103.236.37, interface = inside poll version 3 cisco1
host ip = 64.103.236.38, interface = inside poll version 3 cisco1
host ip = 64.103.236.39, interface = inside poll version 3 cisco1
host ip = 64.103.236.40, interface = inside poll version 3 cisco1
host ip = 64.103.236.41, interface = inside poll version 3 cisco1
host ip = 64.103.236.42, interface = inside poll version 3 cisco1
host ip = 64.103.236.43, interface = inside poll version 3 cisco1
host ip = 64.103.236.44, interface = inside poll version 3 cisco1
host ip = 64.103.236.45, interface = inside poll version 3 cisco1
host ip = 64.103.236.46, interface = inside poll version 3 cisco1
host ip = 64.103.236.47, interface = inside poll version 3 cisco1
host ip = 64.103.236.48, interface = inside poll version 3 cisco1
host ip = 64.103.236.49, interface = inside poll version 3 cisco1
host ip = 64.103.236.50, interface = inside poll version 3 cisco1
host ip = 64.103.236.51, interface = inside poll version 3 cisco1
host ip = 64.103.236.52, interface = inside poll version 3 cisco1
host ip = 64.103.236.53, interface = inside poll version 3 cisco1
host ip = 64.103.236.54, interface = inside poll version 3 cisco1
host ip = 64.103.236.55, interface = inside poll version 3 cisco1
```

Вот некоторые важные замечания об использовании этой функции:

- Если группа узлов или хост, который накладывается на другие группы узлов, удалены, хосты установлены снова со значениями, которые используются для настроенных групп узлов.

- Значения или параметры, которые привязаны к хостам, зависят от заказа, что выполняются команды.

- Список пользователей, который настроен, не может быть удален, если список используется группой определенного хоста.

- Если пользователь упомянут в списке индивидуального пользователя, пользователь SNMP не может быть удален.

- Сетевой объект не может быть удален, если он используется командой CLI **группы узлов**.

Настройка

Используйте информацию, которая описана в этом разделе для настройки ASA так, чтобы была внедрена эта новая характеристика.

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Команды CLI

Для SNMP Version 3 администратор может привязать различных пользователей к указанной группе хостов. Это полезно, если администратор хочет, чтобы ряд пользователей имел способность обратиться к ASA от группы хостов. Эта команда CLI используется для настройки списка пользователей для нескольких пользователей:

```
ASA(config)# [no] snmp-server user-list <list_name> username <user_name>
```

Для соединения списка пользователей к группе узлов введите эту команду в CLI:

```
[no] snmp-server host-group <interface> <network-object> [trap|poll]
[community [enc_type] <text>] [version {1 | 2c | 3 [user name | user-list
<list-name>]}] [udp-port <port_number>]
```

С этой одиночной командой можно задать сетевой объект для указания на множественные хосты, которые должны быть добавлены. С сетевым объектом можно задать или маску подсети или диапазон IP-адресов, которые должны быть добавлены с использованием одиночной команды. Все IP-адреса, которые перечислены как часть сетевого объекта, добавлены как записи хоста SNMP. Точно так же для каждого из пользователей, которые заданы в списке пользователей, существует отдельная запись хоста SNMP.

Эти команды используются, чтобы позволить администраторам очищать и просматривать новые параметры конфигурации для серверов SNMP:

- ясный настраивают список пользователей snmp-server
- ясный настраивают группу узлов snmp-server
- список пользователей snmp-server show running config
- группа узлов snmp-server show running config

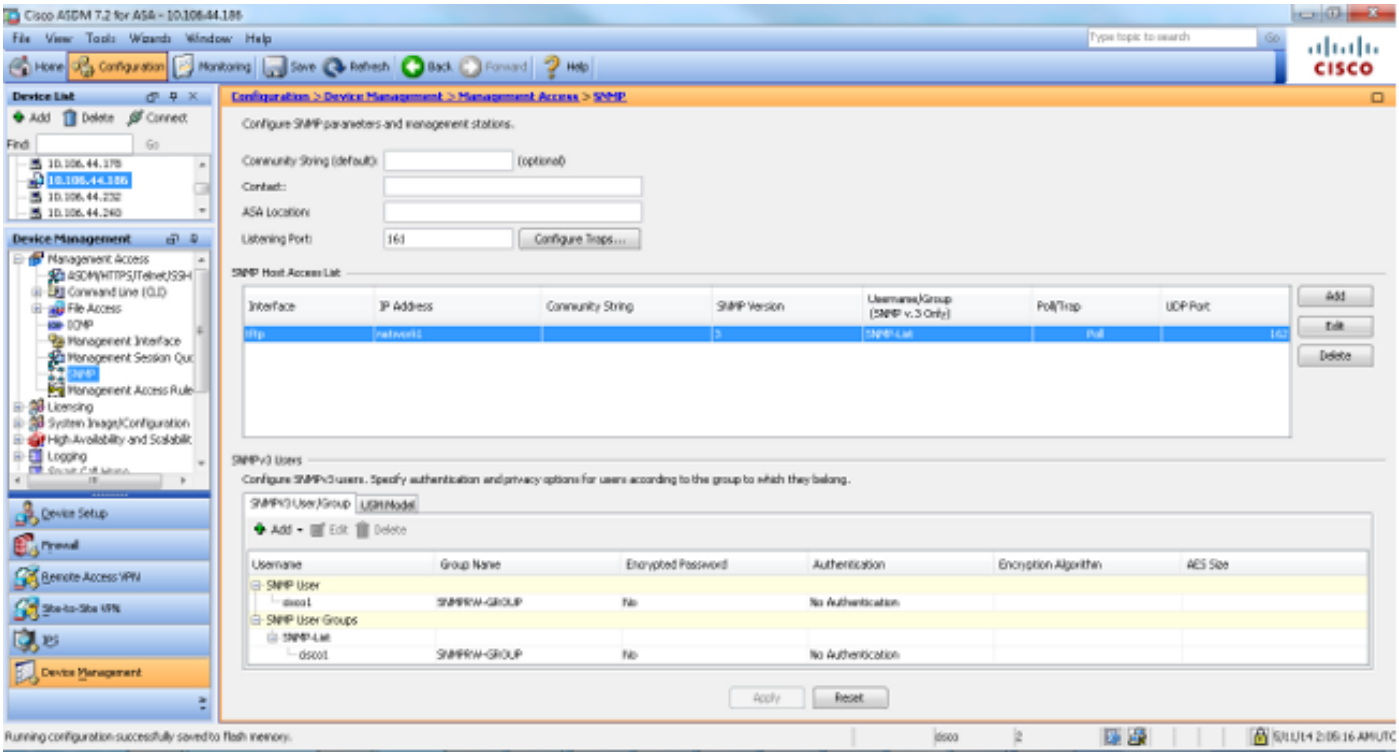
Пример конфигурации

Выполните эти шаги, чтобы использовать новые опции группы SNMP и создать группу узлов сервера SNMP для опроса Версии 2c:

1. Создайте сетевой объект:
   ```
   asa(config)# object network network1
   asa(config-network-object)# range 64.103.236.40 64.103.236.50
   ```
2. Определите группу узлов SNMP:
   ```
   asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
   ```
3. Определите группу SNMP Version 3:
   ```
   asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
   ```
4. Свяжите группы с пользователями:
   ```
   asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
   ```

```
asa(config)#snmp-server user-list SNMP-List username cisco1
asa(config)#snmp-server host-group inside network1 poll version 3 user-list SNMP-List
```

Этот образ иллюстрирует изменения, которые внесены в Cisco Adaptive Security Device Manager (ASDM):



Поддержка OID SNMP cpmCPUTotal5minRev

Эта функция позволяет ASA поддерживать OID SNMP **cpmCPUTotal5minRev**.

Цель

Эта функция добавляет поддержку **cpmCPUTotal5minRev** и OID **cpmCPUTotal1minRev** на ASA и осуждает поддерживаемый в настоящее время **cpmCPUTotal5min** OID и **cpmCPUTotal1min**. Цель этих OID состоит в том, чтобы контролировать использование ЦПУ. В то время как недавно поддерживаемые OID колеблются от 0 до 100, поддерживаемые в настоящее время OID колеблются от 1 до 100. Следовательно, поддержка была добавлена для более новых OID, поскольку они покрывают более широкий диапазон.

Следует отметить, что, так как осуждаемые OID (**cpmCPUTotal5min** и **cpmCPUTotal1min**) больше не поддерживаются на ASA, если ASA обновлен, и осуждаемые OID опрошены, ASA не возвращает информации для тех OID. После обновления ASA вы теперь обязаны контролировать **cpmCPUTotal5minRev** и **cpmCPUTotal1minRev** для использования ЦПУ.

Команды CLI

Нет никаких изменений CLI, начатых с этой новой характеристики.

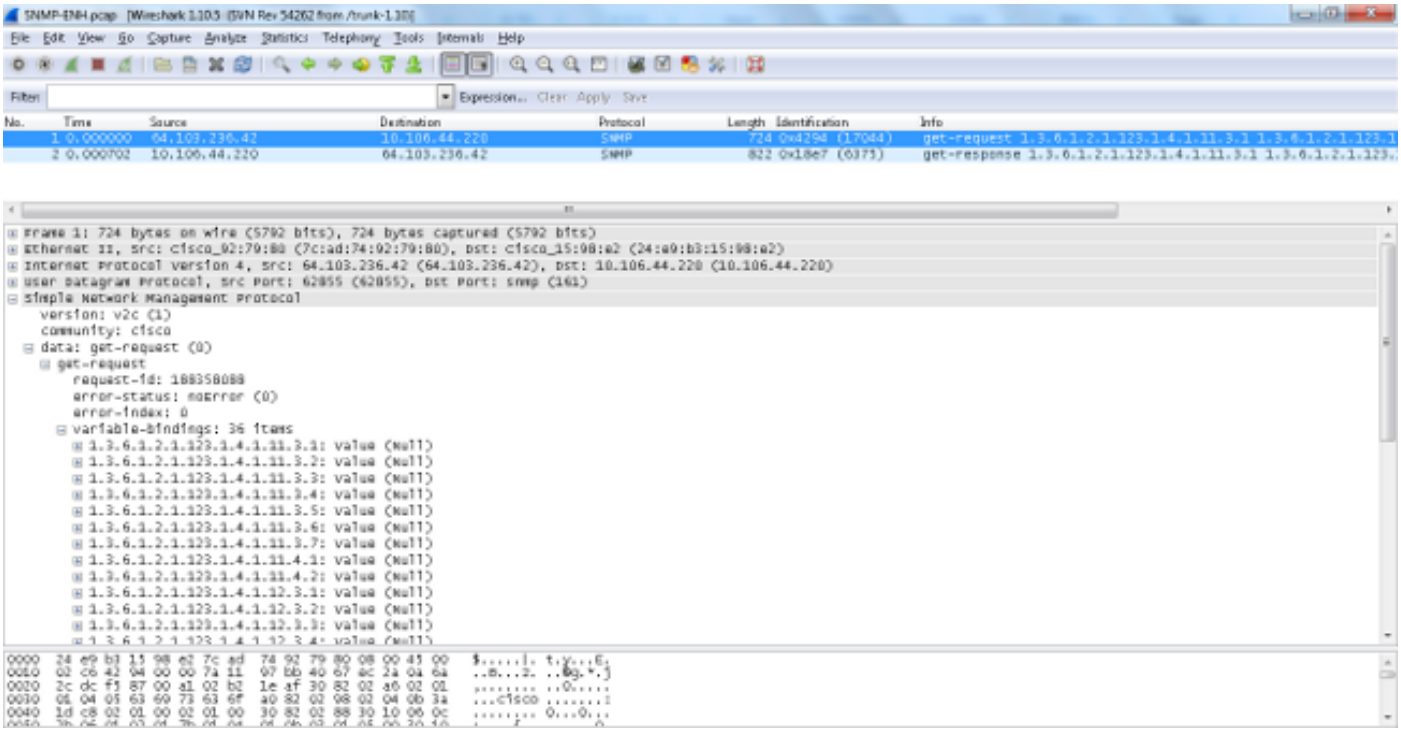
Новые OID

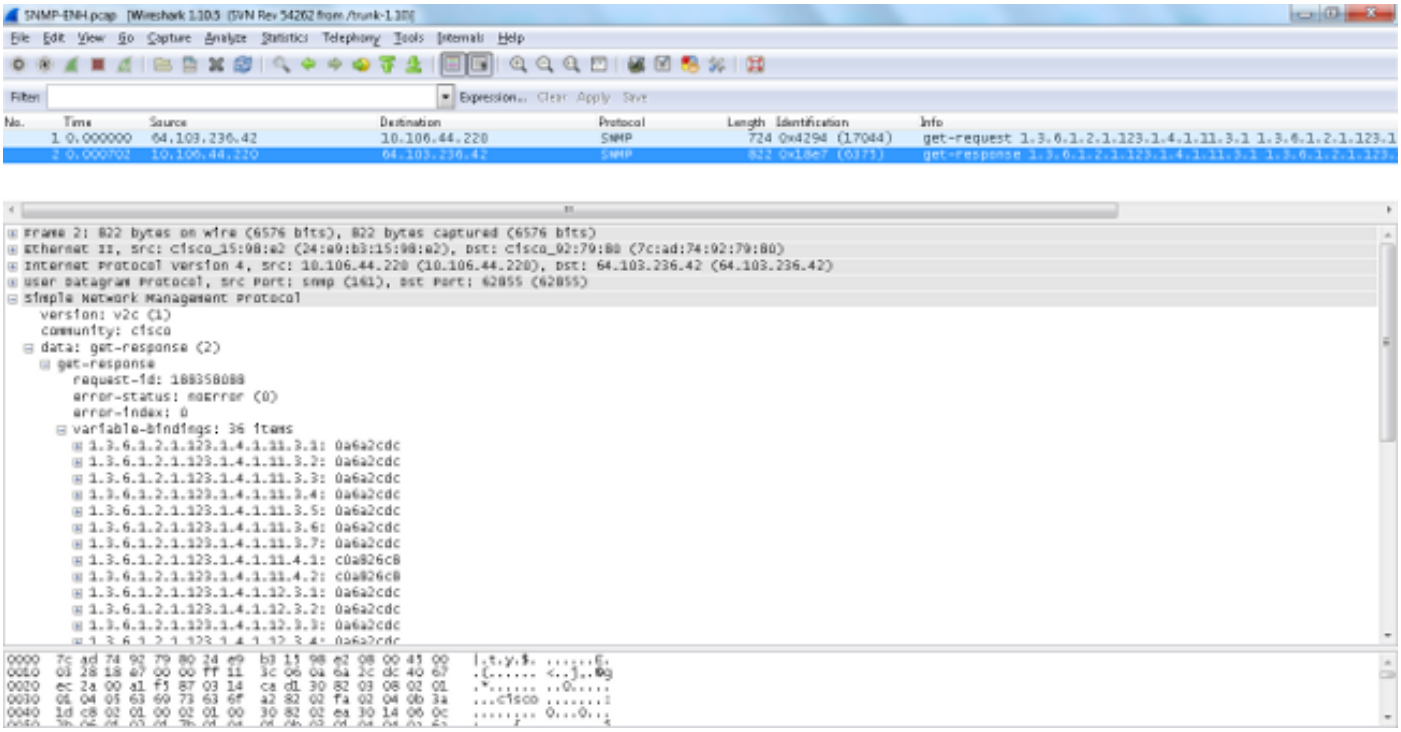
Это новые OID, которые добавлены с этой функцией:

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

Поддержка 1,472-байтовых сообщений SNMP

Платформы ASA ограничивают максимальный размер пакета для запросов SNMP к 512 байтам. Когда вы выполняете объемный запрос для большого числа OID MIB в рамках одиночного запроса SNMP, таймауты подключения SNMP и ошибочный системный журнал генерируется на ASA. RFC3417 предлагает, чтобы максимальный размер пакета для запросов SNMP составил 1,472 байта. Это - размер информационного наполнения SNMP для пакета. Кроме того, Заголовок ethernet и Размер IP - заголовка должны быть добавлены для вычислений общего размера пакета.





Примечание: И одиночный контекст и многоконтекстные режимы поддерживаются с этой функцией.

Устранение неполадок

Этот раздел предоставляет сведения, который можно использовать для решения системных проблем на ASA.

Команды "show"

Когда попытки предприняты для решения проблем на ASA, эти **команды показа** могут быть полезными:

- asa# **показывают выполненную группу узлов snmp-server**
  группа узлов snmp-server внутри network1 опрашивает Список SNMP списка пользователей версии 3

- asa# **показывают выполненный список пользователей snmp-server**
  имя пользователя Списка SNMP списка пользователей snmp-server cisco1

- asa# **показывают snmp-server host**

Эта команда CLI отображает записи, которые присутствуют в таблице адресов сервера SNMP, которая включает и хост и конфигурации группы узлов:

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
```

```
object network network3
range 64.103.236.60 64.103.236.70 ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside poll version 3 cisco1
host ip = 64.103.236.37, interface = inside poll version 3 cisco1
host ip = 64.103.236.38, interface = inside poll version 3 cisco1
host ip = 64.103.236.39, interface = inside poll version 3 cisco1
host ip = 64.103.236.40, interface = inside poll version 3 cisco1
host ip = 64.103.236.41, interface = inside poll version 3 cisco1
host ip = 64.103.236.42, interface = inside poll version 3 cisco1
```

Как показано эти команды показывают все хосты, которые настроены через команду **группы узлов**. Можно использовать эту команду, чтобы проверить, доступны ли все записи и также перекрестный проверяют группы узлов то наложение.