Пример конфигурации системного журнала ASA

Содержание

Введение

Этот документ предоставляет пример конфигурации, который демонстрирует, как настроить другие параметры регистрации на Устройстве адаптивной защиты (ASA), которое выполняет версию кода 8.4 или позже.

Версия ASA 8.4 представила очень гранулированные методы фильтрации, чтобы позволить только определенным указанным сообщениям системного журнала быть представленными. Основной раздел Системного журнала этого документа демонстрирует традиционную конфигурацию системного журнала. Усовершенствованный раздел Системного журнала этого документа показывает новые функции системного журнала в Версии 8.4. См. Руководство Сообщений журнала системы Cisco Security Appliance, Версию 8.x и 9.x для руководства сообщений журнала полной системы.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- ASA 5515 с версией программного обеспечения 8.4 ASA
- Cisco Adaptive Security Device Manager (ASDM) версия 7.1.6

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.

> **Примечание:** См. ASA 8.2: Настройте Системный журнал с помощью ASDM для получения дополнительной информации для подобных элементов конфигурации с версией 7.1 ASDM и позже.

Основной системный журнал

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

Введите эти команды, чтобы к enable logging, просмотрите журналы и просмотрите параметры конфигурации.

- **logging enable-** Включает передачу сообщений системного журнала ко всем выходным местоположениям.

- **никакой logging enable -** Не Отключает регистрацию ко всем выходным местоположениям.
- **show logging-** Перечисляет содержание буфера системного журнала, а также информации и статистических данных, которые принадлежат текущей конфигурации.

ASA может передать сообщения системного журнала различным назначениям. Введите команды в эти разделы для определения местоположений, которые вы хотели бы, чтобы сведения системного журнала были переданы:

Передайте регистрационную информацию к внутреннему буферу

```
logging buffered severity_level
```

Внешнее программное обеспечение или аппаратные средства не требуются при хранении сообщений системного журнала во внутреннем буфере ASA. Введите **команду show logging** для просмотра сохраненных сообщений системного журнала. Внутренний буфер имеет максимальный размер 1 МБ (конфигурируемый с командой **размера буфера регистрации**). В результате это могло бы перенестись очень быстро. Помните это при выборе уровня регистрации для внутреннего буфера, поскольку больше многословных уровней регистрации могло бы быстро заполниться, и обертка, внутренний буфер.

Передайте регистрационную информацию к серверу системного журнала

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number
```

Сервер, который выполняет приложение системного журнала, требуется для передачи сообщений системного журнала к внешнему хосту. ASA передает системный журнал на порту 514 UDP по умолчанию, но могут быть выбраны протокол и порт. Если TCP выбран в качестве протокола регистрации, это заставляет ASA передавать системные журналы через TCP - подключение к серверу системного журнала. Если сервер будет недоступен, или TCP - подключение к серверу не может быть установлен, то ASA, по умолчанию, заблокирует новые соединения ALL. Это поведение может быть отключено если вы **разрешение-hostdown на enable logging**. Посмотрите руководство по конфигурации для получения дополнительной информации о команде **разрешения-hostdown на регистрацию**.

Передайте регистрационную информацию как электронные почты

```
logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address
```

Сервер SMTP требуется при передаче сообщений системного журнала на электронных почтах. Корректная конфигурация на сервере SMTP необходима, чтобы гарантировать, что можно успешно передать электронные почты от ASA до указанного e-mail клиент. Если этот уровень регистрации установлен в очень многословный уровень, такой как *отладка* или *информационный,* вы могли бы генерировать значительное количество системных журналов начиная с каждого электронного письма, посланного этой конфигурацией журнала причины вверх четырех или больше журналов addtional, которые будут генерироваться.

Передайте регистрационную информацию к последовательной консоли

```
logging console severity_level
```

Вход через консоль позволяет сообщениям системного журнала отобразиться на консоли ASA (tty), как они происходят. Если вход через консоль настроен, вся регистрационная генерация на ASA является ratelimited к 9800 битам в секунду, скоростью последовательной консоли ASA. Это могло бы заставить системные журналы быть отброшенными всем назначениям, которые включают внутренний буфер. Не используйте вход через консоль для многословных системных журналов поэтому.

Передайте регистрационную информацию к сеансу telnet/SSH

```
logging monitor severity_level
terminal monitor
```

Logging monitor позволяет сообщениям системного журнала отобразиться, поскольку они происходят, когда вы обращаетесь к консоли ASA с Telnet или SSH, и **команда terminal monitor** выполняется от того сеанса. Для остановки печати журналов к сеансу не введите **команду terminal monitor**.

Сообщения журнала показа на ASDM

```
logging asdm severity_level
```

ASDM также имеет буфер, который может использоваться для хранения сообщений системного журнала. Введите **show logging asdm** команда для отображения содержания буфера системного журнала ASDM.

Передайте журналы к станции управления SNMP

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

Пользователям нужна существующая функциональная среда Протокола SNMP для передачи сообщений системного журнала с SNMP. Посмотрите Команды для Установки и Управления Адресами назначения для выходных данных для завершенной ссылки на командах, которые можно использовать, чтобы установить и управлять адресами назначения для выходных данных. См. сообщения, Перечисленные Уровнем важности для сообщений, перечисленных уровнем важности.

Добавьте метки времени к системным журналам

Чтобы помочь выравнивать и упорядочивать события, метки времени могут быть добавлены к системным журналам. Это рекомендуется, чтобы помочь отслеживать проблемы, основанные вовремя. Для включения меток времени введите **команду logging timestamp**. Вот два примера системного журнала, один без метки времени и один с:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
```

```
identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
442 TCP Reset-I
```

Пример 1

Эти выходные данные показывают пример конфигурации для того, чтобы войти **в буфер** с уровнем важности **отладки**.

```
logging enable
logging buffered debugging
```

Вот пример выходных данных.

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Настройте основной системный журнал с ASDM

Эта процедура демонстрирует конфигурацию ASDM для всех доступных назначений системного журнала.

1. Чтобы к enable logging на ASA, сначала настройте основные параметры регистрации. Выберите **Configuration> Features> Properties> Logging> Logging Setup**. Проверьте флажок **Enable logging** для включения системных журналов.
2. Для настройки внешнего сервера как назначение для системных журналов выберите **Syslog Servers in Logging** и **нажмите Add** для добавления сервера системного журнала. Введите подробные данные сервера системного журнала в Добавить коробку Сервера системного журнала и выберите **OK**, когда вы будете сделаны.
3. Выберите **E-Mail Setup in Logging** в заказе передать сообщения системного журнала как электронные почты определенным получателям. Задайте исходный адрес электронной почты в Исходной коробке АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ и выберите **Add** для настройки целевого адреса электронной почты получателей e-mail и степени важности сообщения. **Закончив все действия, нажмите кнопку OK.**
4. Выберите **Device Administration**, **Logging,** выберите **SMTP** и введите IP-адрес Основного сервера для определения IP-адреса сервера SMTP.
5. Если вы хотите передать системные журналы как trap-сообщения SNMP, необходимо сначала определить сервер SNMP. Выберите **SNMP** в в меню **Management Access** для определения адреса станций управления SNMP и их определенных свойств.
6. Выберите **Add** для добавления станции управления SNMP. Введите подробные данные хоста SNMP и нажмите **OK**.
7. Чтобы позволить журналам передаваться любому из предшествующих упомянутых назначений, выбирать **Logging Filters** в разделе регистрации. Это предоставляет вам каждое возможное конечное место регистрации и текущий уровень журналов, которые передаются тем назначениям. Выберите желаемое Конечное место регистрации и нажмите **Edit**. В данном примере модифицируется назначение 'Серверов системного журнала'.
8. Выберите соответствующие степени серьезности ошибки, в этом случае **Информационные,** от **Фильтра на** выпадающем списке **степеней серьезности ошибки**. **Закончив все действия, нажмите кнопку OK.**

9. Нажмите **Apply** после возврата к окну Logging Filters.

Передайте сообщения системного журнала по VPN к серверу системного журнала

Или в простом сквозном VPN-соединение дизайне или в более сложной схеме звезды, администратор мог бы хотеть контролировать все удаленные Межсетевые экраны ASA с сервером SNMP и сервером системного журнала, расположенным в центральном узле.

Для настройки конфигурации VPN защищенного взаимодействия между сетями Site-to-Site IPsec обратитесь к PIX/ASA 7.x и выше: Пример конфигурации VPN-туннеля OT PIX К PIX. Кроме конфигурации VPN, необходимо настроить SNMP и представляющий интерес трафик для сервера системного журнала и в центральном и в локальном узле.

Центральная конфигурация ASA

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514


logging enable
logging trap debugging

!--- Define logging host information.
logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.
snmp-server host inside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Удаленная конфигурация ASA

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
```

```
!--- interface to the SYSLOG server.
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514

!--- Define syslog server.
logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.
snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

См. Контролирующий Межсетевой экран ASA Cisco Secure Использование SNMP и Syslog через туннель VPN для получения дополнительной информации о том, как настроить Версию ASA 8.4

Усовершенствованный системный журнал

Версия ASA 8.4 предоставляет несколько механизмов, которые позволяют вам настроить и управлять сообщениями системного журнала в группах. Эти механизмы включают степень важности сообщения, класс сообщения, идентификатор сообщения или список пользовательского сообщения, который вы создаете. С использованием этих механизмов можно ввести одиночную команду, которая применяется к маленьким или большим группам сообщений. Когда вы устанавливаете системные журналы этот путь, вы в состоянии перехватить сообщения от указанной группы сообщений и больше все сообщения от тех же степеней серьезности ошибки.

Используйте список сообщений

Используйте список сообщений для включения только заинтересованных сообщений системного журнала уровнем важности и ID в группу, затем привяжите этот список сообщений к необходимому назначению.

Выполните эти шаги для настройки списка сообщений:

1. Введите **список регистрации** ***message_list | уровень severity_level [класс message_class]*** команда для создания списка сообщений, который включает сообщения с указанным уровнем важности или список сообщений.
2. Введите **список регистрации** ***message_list*** команда ***сообщения syslog_id-syslog_id2*** для добавления дополнительных сообщений к списку сообщений, просто созданному.
3. Введите ***конечное место регистрации message_list*** команда для определения назначения созданного списка сообщений.

Пример 2

Введите эти команды для создания списка сообщений, который включает все степени серьезности ошибки 2 (важных) сообщения с добавлением сообщения 611101 - 611323, и также передайте их к консоли:

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

Настройка посредством ASDM

Эта процедура показывает конфигурацию ASDM, например, 2 с использованием списка сообщений.

1. Выберите **Event Lists** под Регистрацией и **нажмите Add** для создания списка сообщений.
2. Введите имя списка сообщений в Поле имени. В этом случае **my_critical_messages** используется. **Нажмите Add** под Классом события / Фильтры серьезности.
3. Выберите **All** из выпадающего списка Класса события. Выберите **Critical** из выпадающего списка Степеней серьезности ошибки. **Закончив все действия, нажмите кнопку OK.**
4. **Нажмите Add** под Фильтрами Идентификатора сообщения, если требуются дополнительные сообщения. В этом случае необходимо вставить сообщения с ID 611101-611323.
5. Вставьте диапазон ID в коробке Идентификаторов сообщения и нажмите **OK**.
6. Вернитесь к меню **Logging Filters** и выберите **Console** в качестве назначения.
7. Выберите **my_critical_messages** из выпадающего списка **Списка событий Использования**. **Закончив все действия, нажмите кнопку OK.**
8. Нажмите **Apply** после возврата к окну Logging Filters.

Это завершает конфигурации ASDM с использованием списка сообщений как показано в Примере 2.

Используйте класс сообщения

Используйте класс сообщения для передачи всех сообщений, привязанных к классу к указанным выходным данным location. При определении порога уровня важности можно ограничить количество сообщений, передаваемых выходным данным location.

```
logging class message_class destination | severity_level
```

Пример 3

Введите эту команду для передачи всех сообщений класса CA с уровнем важности аварийных ситуаций или выше к консоли.

```
logging class ca console emergencies
```

Настройка посредством ASDM

Эта процедура показывает конфигурации ASDM, например, 3 с использованием списка сообщений.

1. Выберите меню **Logging Filters** и выберите **Console** в качестве назначения.
2. Нажмите **регистрацию Disable от всех классов события**.

3. Под Системными журналами от Классов Определенного события выберите Event Class и Severity, который вы хотите добавить.Эта процедура использует **приблизительно** и **Аварийные ситуации** соответственно.
4. **Нажмите Add**, чтобы добавить это в класс сообщения и нажать **OK**.
5. Нажмите **Apply** после возврата к окну Logging Filters. Консоль теперь собирает сообщение класса CA с Аварийными ситуациями уровня важности как показано на окне Logging Filters.

Это завершает конфигурацию ASDM, например, 3. См. сообщения, Перечисленные Уровнем важности для списка уровней важности сообщения журнала.

Передайте сообщения журнала отладки к серверу системного журнала

Для расширенных функций устранения проблем функция/протокол требуются определенные журналы отладки. По умолчанию эти сообщения журнала отображены на терминале (SSH/Telnet). Если отладки включены, зависящий от типа отладки и скорости генерируемых сообщений отладки, использование CLI могло бы оказаться трудным. Дополнительно, сообщения отладки могут перенаправляться к процессу системного журнала и генерироваться как системные журналы. Эти системные журналы могут быть переданы любому системному журналу desination, как был бы любой другой системный журнал. Для отклонения отладок к системным журналам введите команду **трассировки отладки регистрации**. Эта конфигурация передает выходные данные отладки, как системные журналы, к серверу системного журнала.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

Использование списка Регистрации и классов сообщения вместе

Введите команду **списка регистрации** для получения системного журнала для LAN-LAN и одних только сообщений IPSec VPN Удаленного доступа. Данный пример перехватывает всю VPN (IKE и IPsec) сообщения журнала системы классов с уровнем отладки или выше.

Пример

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Регистрационные соответствия ACL

Добавьте *журнал* к каждому элементу списка доступа (ACE), вы желаете для регистрации, когда поражен список доступа. Используйте этот синтаксис:

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Пример

```
ASAfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

ACL, по умолчанию, регистрируют каждый отклоненный пакет. Нет никакой потребности добавить регистрационную опцию, чтобы **запретить**, что ACL генерируют системные журналы для отклоненных пакетов. Когда *регистрационная* опция задана, она генерирует сообщение системного журнала `106100` для ACE, к которому она применена. Сообщение системного журнала `106100` генерируется для каждого соответствия, permit or deny первоклассный поток, который проходит через Межсетевой экран ASA. Первый match flow кэшируется. Последующие соответствия инкрементно увеличивают количество соответствия, отображенное в команде **show access-list**. Поведение регистрации списка доступа по умолчанию, которое является *регистрационным* ключевым словом, не заданным, состоит в том, что, если пакет запрещен, затем передать `106023` генерируется, и если пакет разрешен, то никакое сообщение системного журнала не генерируется.

Дополнительный уровень системного журнала (0 - 7) может быть задан для генерируемых сообщений системного журнала (`106100`). Если никакой уровень не задан, уровень по умолчанию равняется 6 (информационному) для нового ACE. Если ACE уже существует, то его текущий регистрационный уровень остается неизменным. Если *журнал отключает* опцию, задан, регистрация списка доступа полностью отключена. Никакое сообщение системного журнала, включая сообщение `106023`, не генерируется. *Регистрационный* параметр по умолчанию восстанавливает поведение регистрации списка доступа по умолчанию.

Выполните эти шаги, чтобы включить сообщению системного журнала `106100` для просмотра в выходных данных консоли:

1. Введите **команду logging enable** для включения передачи сообщений журнала системы ко всем выходным местоположениям. Необходимо привести в порядок местоположение регистрации вывода для просмотра любых журналов.
2. Введите **сообщение регистрации** *<message_number>* команда *<severity_level>* **уровня** для установки уровня важности определенного сообщения журнала системы.В этом случае введите команду **сообщения регистрации 106100**, чтобы включить сообщению `106100`.
3. Введите **консоль регистрации message_list | severity_level** команда, чтобы позволить сообщениям журнала системы отобразиться на консоли Устройства безопасности (tty), как они происходят. Установите `severity_level` от 1 до 7 или используйте название уровня. Можно также задать, какие сообщения передаются с переменной `message_list`.
4. Введите команду **сообщения show logging** для отображения списка сообщений сообщения журнала системы, которые модифицировались от настройки по умолчанию, которые являются сообщениями, которым назначили другой уровень важности и сообщения, которые были отключены.Это - пример выходных данных команды **сообщения show logging**:
```
ASAfirewall#show logging message 106100
syslog 106100: default-level informational (enabled)
ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Если вы хотите подавить определенное сообщение системного журнала, которое будет передаваться серверу системного журнала, то необходимо ввести команду как показано.

```
hostname(config)#no logging message <syslog_id>
```

См. команду logging message для получения дополнительной информации.

%ASA-3-201008: запрещение новых соединений

Сообщение об ошибках `%ASA-3-201008: Disallowing new connections.` замечено, когда ASA неспособен связаться с сервером системного журнала, и никакие новые соединения не позволены.

Решение

Это сообщение появляется, когда вы включили обмен сообщениями журнала системы TCP, и сервер системного журнала не может быть достигнут, или когда вы используете Сервер системного журнала Cisco ASA (PFSS), и диск в системе Windows NT полон. Выполните эти шаги для решения этого сообщения об ошибках:

- Отключите обмен сообщениями журнала системы TCP, если он включен.
- При использовании PFSS, свободный располагают с интервалами в системе Windows NT, где находится PFSS.
- Гарантируйте, что сервер системного журнала подключен, и можно пропинговать хост от консоли Cisco ASA.
- Запись сообщений в журнал системы TCP перезапуска для разрешения трафика.

Если сервер системного журнала выключается, и регистрация TCP настроена, или используйте команду разрешения-hostdown на регистрацию или коммутатор к регистрации UDP.

Дополнительные сведения

- Программное обеспечение межсетевого экрана Cisco ASA
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация