Руководство по интеграции контроллера беспроводной LAN и IPS

Содержание

Введение

Унифицированная система обнаружения вторжения (IDS) / система предотвращения вторжений (IPS) Cisco представляет собой компонент комплекса Cisco SDN и является первым интегрированным решением для защиты проводных и беспроводных сетей в отрасли. Cisco Унифицированный IDS/IPS проявляет комплексный подход к безопасности — в беспроводном краю, соединенном проводом краю, краю глобальной сети (WAN), и через ЦОД. То, когда связанный клиент передает вредоносный трафик через единую беспроводную сеть Cisco (UWN), Cisco соединила Устройство IDS проводом, обнаруживает атаку и передает, избегают запросов к контроллерам беспроводной локальной сети Cisco (WLC), которые тогда разъединяют устройство клиента.

Cisco IPS является встроенным, сетевым решением, разработанным, чтобы точно определить, классифицировать, и остановить вредоносный трафик, включая червей, шпионское ПО / рекламное ПО, сетевые вирусы и злоупотребление приложения, прежде чем они будут влиять на непрерывность бизнеса.

С использованием версии программного обеспечения 5 датчика Cisco IPS решение для Cisco IPS комбинирует встроенные сервисы предотвращения с инновационными технологиями для улучшения точности. Результатом является общая уверенность в обеспеченной защите вашего решения системы IPS без страха перед отбрасываемым легальным трафиком. Решение для Cisco IPS также предлагает всестороннюю защиту вашей сети через ее уникальную способность сотрудничать с другими ресурсами сетевой безопасности и предоставляет упреждающий подход защите вашей сети.

Решение для Cisco IPS помогает пользователям останавливать большие угрозы с большей уверенностью с помощью этих функций:

- Точные встроенные технологии предотвращения — Предоставляют непараллельную уверенность для принятия превентивных мер против более широкого диапазона угроз без риска понижающегося легального трафика. Интеллектуальный, автоматизированный, контекстный анализ предложения этих уникальных технологий ваших данных и справка гарантируют получение большинства из решения для предотвращения вторжений.
- Идентификация угрозы мультивектора — Защищает вашу сеть от нарушений политики, эксплуатации уязвимости и аномального действия посредством подробного контроля трафика в Уровнях 2 до 7.
- Совместная работа уникальной сети — Улучшает масштабируемость и упругость через сетевую совместную работу, включая эффективные способы перехвата трафика, распределяя нагрузку возможности и видимость в зашифрованный поток данных.
- Всесторонние решения для развертываний — Предоставляют решения для всех сред от малых и средних компаний (SMB) и местоположения филиала компании к установкам поставщика услуг и крупному предприятию.
- Мощное управление, корреляция событий и службы поддержки — Включают полное решение, включая конфигурацию, управление, корреляцию данных и усовершенствованные службы поддержки. В особенности Мониторинг Cisco Security, Анализ и Система ответа (MARS) определяют, изолируют и рекомендуют удаление точности оскорбления элементов для сетевого широкого решения для предотвращения вторжений. И система управления инцидентами Cisco Incident Control System предотвращает нового червя и вспышки вируса, позволяя сети быстро адаптировать и предоставить распределенный ответ.

Когда объединено, эти элементы предоставляют всестороннее встроенное решение для предотвращения и вселяют в вас веру, чтобы обнаружить и остановить самый широкий диапазон вредоносного трафика, прежде чем это будет влиять на непрерывность бизнеса. Инициатива Cisco SDN призывает к интегрированной и встроенной безопасности для сетевых решений. Текущий Протокол LWAPP - базирующиеся системы беспроводной ЛВС только поддерживают основные функции IDS вследствие того, что это - по существу система Уровня 2, и это ограничило питание для обработки линии. Релизы Cisco новый код своевременно для включения новых расширенных характеристик в новые коды. Выпуск 4.0 имеет последние функции, которые включают интеграцию основанной на LWAPP системы беспроводной ЛВС с линейкой продуктов/IP Cisco IDS. В этом выпуске цель состоит в том, чтобы позволить системе/IP Cisco IDS давать WLC команду блокировать определенных

клиентов от доступа до беспроводных сетей, когда атака обнаружена где угодно от Уровня 3 через Уровень 7, который вовлекает клиента в рассмотрение.

Предварительные условия

Требования

Гарантируйте соответствие этим минимальным требованиям:

- Версия микропрограммы 4.x WLC и позже
- Знание о том, как настроить Cisco IPS и WLC Cisco, выбираемо.

Используемые компоненты

WLC Cisco

Эти контроллеры включены с выпуском ПО 4.0 для модификаций IDS:

- Cisco WLC серии 2000
- Cisco WLC серии 2100
- WLC Cisco серии 4400
- Сервисный модуль беспроводной связи Cisco (WiSM)
- Cisco Catalyst унифицированный коммутатор доступа серии 3750G
- Cisco Wireless LAN Controller Module (WLCM)

Точки доступа

- Точки доступа облегченных серий AG Cisco Aironet 1100
- Точки доступа облегченных серий AG Cisco Aironet 1200
- Облегченные точки доступа Cisco Aironet серии 1300
- Облегченные точки доступа Cisco Aironet серии 1000

Менеджмент

- Система беспроводного управления Cisco Wireless Control System (WCS)
- Cisco датчик серии 4200
- Менеджмент Cisco IDS - менеджер устройств Cisco IDS (IDM)

Cisco Унифицированные Платформы IDS/IPS

- Сенсоры Cisco IPS серии 4200 с ПО датчика Cisco IPS 5.x или позже.
- SSM10 и SSM20 для многофункциональных устройств защиты Cisco ASA серии 5500 с ПО датчика Cisco IPS 5. x
- Многофункциональные устройства защиты Cisco ASA серии 5500 с ПО датчика Cisco IPS 5. x
- Сетевой модуль Cisco IDS (CID NM) с ПО датчика Cisco IPS 5. x
- Cisco Catalyst модуль 2 (IDSM-2) системы обнаружения проникновения серии 6500 с ПО датчика Cisco IPS 5. x

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Обзор Cisco IDS

Основные компоненты Cisco IDS (Версия 5.0):

- **Приложение датчика** — Выполняет захват пакета и анализ.
- **Менеджмент Хранения событий и Модуль Действий** — Предоставляют хранилище нарушений политики.
- **Обработка изображений, Установка и Модуль Запуска** — Загрузки, инициализирует и запускает все системное программное обеспечение.
- **Модуль поддержки Интерфейсов пользователя и UI** — Предоставляет встроенный CLI и IDM.
- **Датчик ОС** — Хостовая операционная система (на основе Linux).

Приложение Датчика (программное обеспечение IPS) состоит из:

- **Главное приложение** — Инициализирует систему, запускает и останавливает другие приложения, настраивает ОС и ответственно за обновления. Это содержит эти компоненты:**Сервер Контрольной сделки** — Позволяет Датчикам передавать контрольные сделки, которые используются для включения Контроллера Ответа Атаки (раньше известный как Контроллер Доступа к сети) Ведущее устройство, Блокирующее возможность Датчика.**Хранилище события** — индексируемое хранилище использовало хранить события IPS (ошибки, статус и сообщения системы предупреждений), который доступен через CLI, IDM, Менеджер устройств адаптивной безопасности (ASDM) (ASDM) или Протокол обмена удаленных данных (RDEP).
- **Интерфейсное Приложение** — Обрабатывает обходные и физические параметры настройки и определяет соединенные интерфейсы. Физические параметры настройки состоят из скорости, дуплекса и административных состояний.
- **Регистрационное Приложение** — Пишет сообщения журнала приложения к файлу журнала и сообщения об ошибках к Хранилищу События.
- Когда аварийное событие имело место, **Контроллер ответа атаки (ARC) (раньше известный как Контроллер Доступа к сети)** — Управляет удаленными сетевыми устройствами (межсетевые экраны, маршрутизаторы, и коммутаторы) для обеспечения запирающих способностей. ARC создает и применяет списки контроля доступа (ACL) на устройство управляемой сети или использует **избегать** команду (межсетевые экраны).
- **Приложение уведомления** — Передает trap-сообщения SNMP, когда инициировано предупреждением, статусом и событиями ошибки. Приложение Уведомления использует агента SNMP общественного достояния чтобы для этого. GET SNMP предоставляют сведения о состоянии Датчика.**Web-сервер (сервер HTTP RDEP2)** — Предоставляет интерфейс веба - пользователя. Это также предоставляет средство связаться с другими устройствами IPS через RDEP2 с помощью нескольких servlet для предоставления сервисов IPS.**Опознавательное Приложение** — Проверяет, что

пользователи авторизуются выполнить CLI, IDM, ASDM или действия RDEP.
- **Приложение датчика (Аналитический Механизм)** — Выполняет захват пакета и анализ.
- **CLI** — интерфейс, который выполнен, когда пользователи успешно входят к Датчику через Telnet или SSH. Все учетные записи, созданные через CLI, используют CLI в качестве своей оболочки (кроме учетной записи сервиса - только одна учетная запись сервиса позволена). Позволенные команды CLI зависят от привилегии пользователя.

Все приложения IPS связываются друг с другом через распространенное применение Программный интерфейс (API) под названием IDAPI. Удаленные приложения (другие Датчики, приложения управления сетью и ПО независимого поставщика) связываются с Датчиками через протоколы стандарта Security Device Event Exchange (SDEE) и RDEP2.

Это должно быть обращенный внимание, что Датчик имеет эти разделы диска:

- **Раздел установки приложения** — Содержит полный образ системы IPS.
- **Разделение обслуживания** — образ IPS специального назначения использовал повторно захватывать образ раздел установки приложения IDSM-2. Повторно захватывание образ разделения обслуживания приводит к потерянным параметрам конфигурации.
- **Раздел восстановления** — образ специального назначения используется для восстановления Датчика. Начальная загрузка в раздел восстановления позволяет пользователям полностью повторно захватить образ раздел установки приложения. Настройки сети сохранены, но потеряны все другие конфигурации.

Cisco IDS и WLC – обзор интеграции

Версия 5.0 Cisco IDS представляет способность настроить, запрещают действия, когда обнаружены нарушения политики (подписи). На основе пользовательской конфигурации в системе IDS/IPS избегать запрос может быть отправлен к межсетевому экрану, маршрутизатору или WLC для блокирования пакетов от определенного IP - адреса.

С Выпуском ПО единой беспроводной сети Cisco (UWN) 4.0 для Контроллеров беспроводной связи Cisco, избегать запрос должен быть отправлен к WLC для инициирования клиентского поведения помещения в черный список или исключения, доступного на контроллере. Интерфейс использование контроллера для получения избегать запроса является интерфейсом команд и управления на Cisco IDS.

- Контроллер позволяет до пяти сенсоров IDS быть настроенными на данном контроллере.
- Каждый настроенный сенсор IDS определен его IP-адресом или квалифицированным сетевым именем и учетными данными авторизации.
- Каждый сенсор IDS может быть настроен на контроллере со скоростью уникального запроса в секундах.

Избегающий IDS

Контроллер делает запрос Датчика на настроенной скорости запроса для получения всех избегать событий. Данный избегает запроса, распределен всюду по всей группе мобильности контроллера, который получает запрос из сенсора IDS. Каждый избегает запроса о IP-адресе клиента, в действительности для указанного секундного значения

таймаута. Если значение таймаута указывает бесконечное время, то избегать событие заканчивается, только если избегать запись удалена на IDS. Даже если кто-либо из контроллеров перезагружены, клиентский статус, которого избегают, поддержан на каждом контроллере в группе мобильности.

Примечание: Решение избежать клиента всегда принимается сенсором IDS. Контроллер не обнаруживает атаки Уровня 3. Это - намного более сложный процесс, чтобы решить, что клиент запускает злонамеренную атаку на Уровне 3. Клиент аутентифицируется на Уровне 2, который достаточно хорош для контроллера для предоставления доступа Уровня 2.

Примечание: Например, если клиент добирается, предыдущее оскорбление (избежало) назначенного IP-адреса, это до таймаута Датчика для разблокирования доступа Уровня 2 для этого нового клиента. Даже если контроллер предоставляет доступ на Уровне 2, трафик клиента мог бы быть заблокирован в маршрутизаторах в Уровне 3 так или иначе, потому что Датчик также сообщает маршрутизаторам избегать события.

Предположите, что у клиента есть IP-адрес A. Теперь, когда контроллер опрашивает IDS для, избегают событий, IDS отправляет избегать запрос к контроллеру с IP-адресом как целевой IP - адрес. Теперь, черные списки контроллера этот клиент A. На контроллере клиенты отключены на основе MAC-адреса.

Теперь, предположите, что клиент изменяет его IP-адрес от до B. Во время следующего опроса контроллер получает список клиентов, которых избегают, на основе IP-адреса. На этот раз снова IP-адрес A находится все еще в списке, которого избегают. Но так как клиент изменил его IP-адрес от до B (который не находится в списке, которого избегают, IP-адресов), этот клиент с новым IP-адресом B освобожден, как только таймаут черных перечисленных клиентов достигнут на контроллере. Теперь, контроллер начинает позволять этому клиенту с новым IP-адрес B (но MAC - адрес клиента остается тем же).

Поэтому невзирая на то, что клиент остается отключенным на время времени исключения контроллера и повторно исключен, если это повторно устанавливает соединение свой предыдущий адрес DHCP, тот клиент больше не отключается, если IP-адрес клиента, которого избегают изменения. Например, если не истекаются клиентские подключения к той же сети и таймауту аренды DHCP.

Контроллеры только поддерживают соединение с IDS для клиента, избегающего запросов, которые используют порт управления на контроллере. Контроллер подключает с IDS для проверки пакетов через применимые интерфейсы виртуальной локальной сети (VLAN) тот трафик беспроводного клиента переноса.

На контроллере страница Disable Clients показывает каждому клиенту, который был отключен через запрос сенсора IDS. **Команда показа** CLI также отображает список помещенных в черный список клиентов.

На WCS исключенные клиенты отображены под подзакладкой Безопасности.

Вот шаги для придержаний для завершения интеграции WLC Cisco и датчиков Cisco IPS.

1. Установите и подключите Устройство ids на том же коммутаторе, где находится контроллер беспроводной локальной сети.
2. Зеркало (SPAN) порты WLC, которые несут трафик беспроводного клиента к Устройству ids.

3. Устройство ids получает копию каждого пакета и осматривает трафик на Уровне 3 до 7.
4. Устройство ids предлагает загружаемый Файл цифровой подписи, который может также быть настроен.
5. Устройство ids генерирует сигнал тревоги с действием события, избегают, когда обнаружена подпись атаки.
6. WLC опрашивает IDS для сигналов тревоги.
7. Когда сигнал тревоги с IP-адресом беспроводного клиента, который привязан к WLC, обнаружен, это помещает клиента в список исключения.
8. Trap-сообщение генерируется WLC, и WCS уведомлен.
9. Пользователь удален из списка исключения после указанного периода времени.

Дизайн сетевой архитектуры

WLC Cisco связан с гигабитными интерфейсами на Catalyst 6500. Создайте port-channel для гигабитных интерфейсов и включите Агрегирование каналов (LAG) на WLC.

```
(Cisco Controller) >show interface summary Interface Name Port Vlan Id IP Address Type Ap Mgr -- ------------------------------ ---- -------- --------------- ------- ------ ap-manager LAG untagged 10.10.99.3 Static Yes management LAG untagged 10.10.99.2 Static No service-port N/A N/A 192.168.1.1 Static No virtual N/A N/A 1.1.1.1 Static No vlan101 LAG 101 10.10.101.5 Dynamic No
```

Контроллер подключен к интерфейсному гигабиту 5/1 и гигабиту 5/2 на Catalyst 6500.

```
cat6506#show run interface gigabit 5/1 Building configuration... Current configuration : 183 bytes ! interface GigabitEthernet5/1 switchport switchport trunk encapsulation dot1q switchport trunk native vlan 99 switchport mode trunk no ip address channel-group 99 mode on end
cat6506#show run interface gigabit 5/2 Building configuration... Current configuration : 183 bytes ! interface GigabitEthernet5/2 switchport switchport trunk encapsulation dot1q switchport trunk native vlan 99 switchport mode trunk no ip address channel-group 99 mode on end
cat6506#show run interface port-channel 99 Building configuration... Current configuration : 153 bytes ! interface Port-channel99 switchport switchport trunk encapsulation dot1q switchport trunk native vlan 99 switchport mode trunk no ip address end
```

Интерфейсы считывания Сенсора IPS могут работать индивидуально в **Случайном режиме**, или можно соединить их для создания встроенных интерфейсов для **Встроенного режима Считывания**.

В Случайном режиме пакеты не текут через Датчик. Датчик анализирует копию отслеживаемого трафика, а не фактического переданного пакета. Преимущество работы в Случайном режиме состоит в том, что Датчик не влияет на поток пакетов с переданным трафиком.

Примечание: Схема архитектуры является просто настройкой в качестве примера интегрированной архитектуры IPS и WLC. Пример конфигурации, показанный здесь, объясняет IDS, снимающий показания интерфейс, действующий в Случайном режиме. Схема архитектуры показывает интерфейсы считывания, соединяемые вместе для действия во Встроенном Парном режиме. См. Встроенный Режим для получения дополнительной информации о Встроенном Интерфейсном режиме.

В этой конфигурации предполагается, что считывание взаимодействует действия в Случайном режиме. Контролирующий интерфейс Датчика Cisco IDS связан с гигабитным интерфейсом 5/3 на Catalyst 6500. Создайте сеанс монитора на Catalyst 6500, где интерфейс порт-канала является источником пакетов, и назначение является гигабитным интерфейсом, где связан контролирующий интерфейс датчика Cisco IPS. Это реплицирует весь вход, и выходной трафик от контроллера соединил интерфейсы проводом к IDS для

Уровня 3 посредством контроля Уровня 7.

```
cat6506#show run | inc monitor monitor session 5 source interface Po99 monitor session 5
destination interface Gi5/3 cat6506#show monitor session 5 Session 5 --------- Type : Local
Session Source Ports : Both : Po99 Destination Ports : Gi5/3 cat6506#
```

Настройте датчик Cisco IDS

Начальная конфигурация Датчика Cisco IDS сделана от консольного порта или путем соединения монитора и клавиатуры к Датчику.

1. Войдите к устройству:Подключите консольный порт с Датчиком.Подключите монитор и клавиатуру к Датчику.
2. Введите свое имя пользователя и пароль в приглашении регистрации.**Примечание:** По умолчанию действует имя пользователя «cisco» с паролем «cisco». Вам предлагают изменить их первоначально, вы входите к устройству. Необходимо сначала ввести пароль UNIX, который является Cisco. Затем необходимо ввести новый пароль дважды.`login: cisco Password: ***NOTICE*** This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please contact us by sending email to export@cisco.com. ***LICENSE NOTICE*** There is no license key installed on the system. Please go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet (registered customers only) to obtain a new license or install a license.`
3. Настройте IP-адрес, маску подсети и список доступа на Датчике.**Примечание:** Это - интерфейс команд и управления на IDS, используемом для передачи с контроллером. Этот адрес должен быть маршрутизуемым к интерфейсу управления контроллера. Интерфейсы считывания не требуют адресации. Список доступа должен включать адрес интерфейса управления контроллера (контроллеров), а также допустимые адреса для управления IDS.`sensor#configure terminal sensor(config)#service host sensor(config-hos)#network-settings sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1 sensor(config-hos-net)#access-list 10.0.0.0/8 sensor(config-hos-net)#access-list 40.0.0.0/8 sensor(config-hos-net)#telnet-option enabled sensor(config-hos-net)#exit sensor(config-hos)#exit Apply Changes:?[yes]: yes sensor(config)#exit sensor# sensor#ping 192.168.5.1 PING 192.168.5.1 (192.168.5.1): 56 data bytes 64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms 64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms 64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms 64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms --- 192.168.5.1 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.3/0.6/1.0 ms sensor#`
4. Можно теперь настроить Сенсор IPS от GUI. Укажите браузер к управлению IP-адресами Датчика. Это выводы образа выборка, где Датчик настроен с 192.168.5.2..
5. Добавьте пользователя что использование WLC для доступа к событиям IPS Sensor.
6. Включите контролирующие интерфейсы.Контролирующие интерфейсы должны быть добавлены к Аналитическому Механизму, поскольку это окно показывает:
7. Выберите подпись 2004 года (Эхо-запрос протокола ICMP) для выполнения быстрой проверки настройки.Подпись должна быть включена, набор Серьезности оповещений к **Высокому** и набор Действия События для **Создания Хоста Блока Предупреждения** и **Запроса** к этому шагу проверки, который будет завершен.

Настройте WLC

Выполните эти шаги для настройки WLC:

1. Как только устройство IPS настроено и готово быть добавленным в контроллере, выбрать **Security> CIDS> Sensors> New**.
2. Добавьте IP-адрес, номер порта TCP, имя пользователя и пароль, которое вы создали на предыдущем этапе.Для получения отпечатка пальца из Сенсора IPS выполните эту команду в Сенсоре IPS и добавьте отпечаток пальца SHA1 на WLC (без двоеточия). Это используется для обеспечения связи опроса контроллера к IDS.`sensor#`**`show tls fingerprint`** `MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19 SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42`
3. Проверьте статус соединения между Сенсором IPS и WLC.
4. Как только вы устанавливаете подключение с датчиком Cisco IPS, удостоверьтесь, что конфигурация WLAN корректна и что вы включаете **Клиентское Исключение**.Клиентское значение таймаута исключения по умолчанию составляет 60 секунд. Также обратите внимание, что независимо от клиентского таймера исключения, клиентское исключение сохраняется, пока клиентский блок, вызванный IDS, остается активным. Блочное время по умолчанию в IDS составляет 30 минут.
5. Можно инициировать событие в системе Cisco IPS или когда вы делаете Просмотр NMAP к определенным устройствам в сети или когда вы делаете эхо-запрос к некоторым хостам, проверенным датчиком Cisco IPS. Как только сигнал тревоги инициирован в Cisco IPS, перейдите **к Блокам Мониторинга и Активного узла** для проверки подробных данных о хосте.Список Клиентов, которого Избегают, в контроллере теперь заполнен с IP и MAC-адресом хоста.Пользователь добавлен к Клиентскому списку Исключения.Журнал trap-сообщения генерируется, поскольку клиент добавлен к избегать списку.Журнал сообщений также генерируется для события.Некоторые дополнительные события генерируются в датчике Cisco IPS, когда просмотр NMAP сделан на устройстве, это контролирует.Это окно показывает события, генерируемые в датчике Cisco IPS.

Пример конфигурации датчика Cisco IDS

Это - выходные данные из сценария программы установки от установки:

```
sensor#show config ! ------------------------------ ! Version 5.0(2) ! Current configuration
last modified Mon Apr 03 15:32:07 2006 ! ------------------------------ service host network-
settings host-ip 192.168.5.2/25,192.168.5.1 host-name sensor telnet-option enabled access-list
10.0.0.0/8 access-list 40.0.0.0/8 exit time-zone-settings offset 0 standard-time-zone-name UTC
exit exit ! ------------------------------ service notification exit ! -------------------------
----- service signature-definition sig0 signatures 2000 0 alert-severity high status enabled
true exit exit signatures 2001 0 alert-severity high status enabled true exit exit signatures
2002 0 alert-severity high status enabled true exit exit signatures 2003 0 alert-severity high
status enabled true exit exit signatures 2004 0 alert-severity high engine atomic-ip event-
action produce-alert|request-block-host exit status enabled true exit exit exit ! --------------
---------------- service event-action-rules rules0 exit ! ------------------------------ service
logger exit ! ------------------------------ service network-access exit ! ---------------------
--------- service authentication exit ! ------------------------------ service web-server exit !
------------------------------ service ssh-known-hosts exit ! ------------------------------
service analysis-engine virtual-sensor vs0 description default virtual sensor physical-interface
GigabitEthernet0/0 exit exit ! ------------------------------ service interface physical-
interfaces GigabitEthernet0/0 admin-state enabled exit exit ! ------------------------------
```

```
service trusted-certificates exit sensor#
```

Настройте ASA для IDS

В отличие от традиционного Датчика Обнаружения несанкционированного доступа, ASA должен всегда быть в пути данных. Другими словами, вместо того, чтобы охватить трафик от порта коммутатора к пассивному порту сниффинга на Датчике, ASA должен получить данные на одном интерфейсе, обработать его внутренне, и затем передать ему другой порт. Для IDS используйте модульную систему политик (MPF) для копирования, торгуют ASA, получает к внутреннему Усовершенствованному Модулю Сервисов безопасности Контроля и Предотвращения (SSM AIP) для контроля.

В данном примере используемый ASA уже является настройкой и передает трафик. Эти шаги демонстрируют, как создать политику, которая передает данные к SSM AIP.

1. Войдите в ASA с помощью ASDM. На успешную регистрацию в системе появляется окно ASA Main System.
2. Нажмите **Configuration** в верхней части страницы. Окно переключается на представление интерфейсов ASA.
3. Нажмите **Security Policy** на левой стороне окна. На результирующем окне выберите вкладку **Service Policy Rules**.
4. **Нажмите Add** для создания новой политики. Добавить Мастер Правила Политики обслуживания запускает в новом окне.Нажмите **Interface** и затем выберите корректный интерфейс из выпадающего списка для создания новой политики, которая связана с одним из интерфейсов, который передает трафик.Дайте политике название и описание того, что политика делает использование этих двух текстовых полей.Нажмите **Next** для перемещения в следующий шаг.
5. Создайте новый класс трафика для применения к политике.Разумно создать определенные классы для осмотра определенных типов данных, но в данном примере, Любой Трафик выбран для простоты. Нажмите **Next** для перехода.
6. Выполните эти шаги чтобы кдайте ASA команду направлять трафик к его SSM AIP.Проверка **Включает IPS для этого трафика** для включения обнаружения несанкционированного доступа.Установите режим в **Разнородный** так, чтобы копия трафика была передана модулю, внеполосному вместо того, чтобы разместить модуль, встроенный с потоком данных.Нажмите **трафик Permit**, чтобы гарантировать, что ASA переключается на открытое состояние сбоя, если отказывает SSM AIP.Нажмите **Finish** для фиксации изменения.
7. ASA теперь настроен для передачи трафика к Модулю ips. Нажмите **Save** на верхнем ряде для записи изменений в ASA.

Настройте SSM AIP для контроля трафика

В то время как ASA передает данные к Модулю ips, привяжите интерфейс SSM AIP к его действительному механизму Датчика.

1. Вход в систему к SSM AIP с помощью IDM.
2. Добавьте пользователя с, по крайней мере, привилегиями средства просмотра.
3. Включите интерфейс.
4. Проверьте конфигурацию виртуального датчика.

Настройте WLC для опроса SSM AIP для клиентских блоков

Выполните эти шаги, как только Датчик настроен и готов быть добавленным в контроллере:

1. Выберите **Security> CIDS> Sensors> New** в WLC.
2. Добавьте IP-адрес, номер порта TCP, имя пользователя и пароль, которое вы создали в предыдущем разделе.
3. Для получения отпечатка пальца из Датчика выполните эту команду в Датчике и добавьте отпечаток пальца SHA1 на WLC (без двоеточия). Это используется для обеспечения связи опроса контроллера к IDS.`sensor#show tls fingerprint MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55`
4. Проверьте статус соединения между SSM AIP и WLC.

Добавьте блокирующуюся подпись к SSM AIP

Добавьте инспекционную подпись для блокирования трафика. Несмотря на то, что существует много подписей, которые могут сделать задание на основе доступных программных средств, данный пример создает подпись, которая блокирует ping - пакеты.

1. Выберите **подпись 2004 года (Эхо-запрос протокола ICMP)** для выполнения быстрой проверки настройки.
2. Включите подпись, заставьте Серьезность оповещений в **Высокий** и Действие События набора **Производить Хост Блока Предупреждения** и **Запроса** для завершения этого шага проверки. Обратите внимание на то, что действие Хоста Блока Запроса является ключом к сигнализации WLC для создания клиентских исключений.
3. Нажмите **OK** для сохранения подписи.
4. Проверьте, что подпись активна и что она собирается выполнить блокирующее действие.
5. Нажмите **Apply** для передачи подписи модулю.

Блокирование монитора и события с IDM

Выполните следующие действия:

1. Когда подпись срабатывает успешно, существует два места в IDM для замечания на это.Первый метод показывает активные блоки, что SSM AIP установил. Нажмите **Monitoring** вдоль верхнего ряда действий. В рамках списка элементов, который появляется на левой стороне, выберите **Active Host Blocks**. Каждый раз, когда подпись эхо-запроса инициирует, окно Active Host Blocks показывает IP-адрес преступника, адрес устройства под огнем, и время, которое остается, для которого блок в действительности. Время блокирования по умолчанию составляет 30 минут и является настраиваемым. Однако изменение этого значения не обсуждено в этом документе. Консультируйтесь с документацией по конфигурации ASA по мере необходимости для получения информации о том, как изменить этот параметр. Удалите блок сразу, выберите его из списка и затем нажмите **Delete**.Второй метод для просмотра инициированных подписей использует буфер события AIP-SSM. От страницы IDM

Monitoring выберите **Events** в списке элементов на левой стороне. События ищут, утилита появляется. Установите соответствующие условия поиска и нажмите **View....**
2. Просмотр событий тогда появляется со списком событий, которые совпадают с данными критериями. Просмотрите список путем прокрутки и найдите подпись Эхо-запроса протокола ICMP модифицируемой в шагах предыдущей конфигурации.Посмотрите в столбце Events для названия подписи или иначе ищите идентификационный номер подписи под столбцом Sig ID.
3. После того, как вы определяете местоположение подписи, дважды нажимаете запись для открытия нового окна. Новое окно содержит подробные сведения на событии, которое инициировало подпись.

Контролируйте клиентское исключение в контроллере беспроводной локальной сети

Список Клиентов, которого Избегают, в контроллере заполнен на этом этапе времени с IP и MAC-адресом хоста.

Пользователь добавлен к Клиентскому списку Исключения.

Следите за развитием событий в WCS

События связанное с безопасностью, которые инициируют блок в SSM AIP, заставляют контроллер добавлять адрес преступника к клиентскому списку исключения. Событие также генерируется в WCS.

1. Используйте утилиту **Monitor> Alarms** из главного меню WCS для просмотра события исключения. WCS первоначально отображает все несброшенные аварийные сигналы и также представляет ищущую функцию на левой стороне окна.
2. Модифицируйте условия поиска для обнаружения клиентского блока. При Степенях серьезности ошибки выберите **Minor**, и также установите Категорию аварийных сигналов в **Безопасность**.
3. **Нажмите кнопку «Search» (Поиск).**
4. Окно предупреждения тогда перечисляет только аварийные сигналы защиты с незначительными степенями серьезности ошибки. Укажите мышь в событии, которое инициировало блок в SSM AIP.В частности WCS показывает MAC-адрес станции клиента, которая вызвала сигнал тревоги. Путем обращения в верном адресе WCS появляется маленькое окно с подробными данными события. Щелкните по ссылке, чтобы посмотреть эти те же детали на другом окне.

Пример конфигурации Cisco ASA

```
ciscoasa#show run : Saved : ASA Version 7.1(2) ! hostname ciscoasa domain-name cisco.com enable
password 2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0/0 nameif outside security-level
0 ip address 10.10.102.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100
ip address 172.16.26.2 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-
level no ip address ! interface Management0/0 nameif management security-level 100 ip address
192.168.1.1 255.255.255.0 management-only ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive
dns server-group DefaultDNS domain-name cisco.com pager lines 24 logging asdm informational mtu
inside 1500 mtu management 1500 mtu outside 1500 asdm image disk0:/asdm512-k8.bin no asdm
```

```
history enable arp timeout 14400 nat-control global (outside) 102 interface nat (inside) 102
172.16.26.0 255.255.255.0 nat (inside) 102 0.0.0.0 0.0.0.0 route inside 0.0.0.0 0.0.0.0
172.16.26.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00
sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 10.1.1.12
255.255.255.255 inside http 0.0.0.0 0.0.0.0 inside http 192.168.1.0 255.255.255.0 management no
snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup
linkdown coldstart telnet 0.0.0.0 0.0.0.0 inside telnet timeout 5 ssh timeout 5 console timeout
0 dhcpd address 192.168.1.2-192.168.1.254 management dhcpd lease 3600 dhcpd ping_timeout 50
dhcpd enable management ! class-map inside-class match any ! ! policy-map inside-policy
description IDS-inside-policy class inside-class ips promiscuous fail-open ! service-policy
inside-policy interface inside Cryptochecksum:699d110f988e006f6c5c907473939b29 : end ciscoasa#
```

Пример конфигурации датчика системы предотвращения вторжений Cisco (IPS)

```
sensor#show config ! ------------------------------ ! Version 5.0(2) ! Current configuration
last modified Tue Jul 25 12:15:19 2006 ! ------------------------------ service host network-
settings host-ip 172.16.26.10/24,172.16.26.1 telnet-option enabled access-list 10.0.0.0/8
access-list 40.0.0.0/8 exit exit ! ------------------------------ service notification exit ! --
--------------------------- service signature-definition sig0 signatures 2004 0 engine atomic-
ip event-action produce-alert|request-block-host exit status enabled true exit exit exit ! -----
------------------------ service event-action-rules rules0 exit ! ------------------------------
- service logger exit ! ------------------------------ service network-access exit ! -----------
------------------- service authentication exit ! ------------------------------ service web-
server exit ! ------------------------------ service ssh-known-hosts exit ! -------------------
---------- service analysis-engine virtual-sensor vs0 description default virtual sensor
physical-interface GigabitEthernet0/1 exit exit ! ------------------------------ service
interface exit ! ------------------------------ service trusted-certificates exit sensor#
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

- Установка и Использование менеджера устройств системы предотвращения вторжений Cisco (IPS) 5.1
- Многофункциональные устройства защиты Cisco ASA серии 5500 - руководства по конфигурации
- Настройка датчик системы предотвращения вторжений Cisco (IPS) Использование интерфейса командной строки 5.0 - интерфейсы Настройки
- Руководство по конфигурации WLC 4.0
- Беспроводная техническая поддержка
- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Решения по обеспечению безопасности Настройки
- Cisco Systems – техническая поддержка и документация