Настройте интеграцию WSA с ISE для TrustSec осведомленные сервисы

Содержание

Введение

Этот документ описывает, как интегрировать Web Security Appliance (WSA) с платформой Identity Services Engine (ISE). Версия 1.3 ISE поддерживает новый API, названный pxGrid. Эта современная и гибкая аутентификация поддержек протокола, шифрование и

привилегии (группы), который обеспечивает простую интеграцию с другими решениями по обеспечению безопасности.

Версия 8.7 WSA поддерживает pxGrid протокол и в состоянии получить идентификационную информацию контекста из ISE. В результате WSA позволяет вам создавать политику на основе групп тега группы безопасности (SGT) TrustSec, полученных из ISE.

Предварительные условия

Требования

Cisco рекомендует иметь опыт с конфигурацией Cisco ISE и базовыми знаниями об этих темах:

- Развертывания ISE и Конфигурация авторизации
- Конфигурация интерфейса командой строки Устройства адаптивной защиты (ASA) для TrustSec и доступа VPN
- Конфигурация WSA
- Основное понимание развертываний TrustSec

Используемые компоненты

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

- Microsoft Windows 7
- Версия программного обеспечения 1.3 Cisco ISE и позже
- AnyConnect Cisco Мобильная Версия 3.1 Безопасности и позже
- Версия 9.3.1 Cisco ASA и позже
- Cisco Версия 8.7 WSA 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.

Настройка

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

Диаграмма сети и поток трафика

Метки TrustSec SGT назначены ISE, используемым в качестве сервера проверки подлинности для всех типов пользователей, которые обращаются к корпоративной сети.

Это включает проводной / пользователи беспроводной связи, которые аутентифицируются через 802.1x или гостевые порталы ISE. Кроме того, удаленные пользователи VPN, которые используют ISE для аутентификации.

Для WSA не имеет значения, как пользователь обратился к сети.

Данный пример представляет удаленный сеанс завершения пользователей VPN на VPN ASA. Тем пользователям назначили определенная метка SGT. Весь трафик HTTP к Интернету будет перехвачен FW ASA (межсетевой экран) и перенаправлен к WSA для контроля. WSA использует профиль идентификации, который позволяет ему классифицировать пользователей на основе метки SGT и доступа сборки или политики расшифровки на основе этого.

Подробный поток:

1. Пользователь VPN AnyConnect завершает сеанс Уровня защищенных сокетов (SSL) на VPN ASA. VPN ASA настроена для TrustSec и использует ISE для аутентификации пользователей VPN. Проверенному пользователю назначают значение метки SGT = 2 (название = IT). Пользователь получает IP-адрес от 172.16.32.0/24 сети (172.16.32.50 в данном примере).
2. Пользователь пытается обратиться к веб-странице в Интернете. FW ASA настроен для протокола WCCP, который перенаправляет трафик к WSA.
3. WSA настроен для интеграции ISE. Это использует pxGrid для загрузки информации от ISE: пользовательский IP-адрес 172.16.32.50 был назначен, SGT помечает 2.
4. WSA обрабатывает запрос HTTP от пользователя и поражает политику доступа PolicyForIT. Та политика настроена для блокирования трафика к спортивным узлам. Все другие пользователи (которые не принадлежат SGT 2) поражают политику доступа по умолчанию и имеют полный доступ к спортивным узлам.

VPN ASA

Это - Шлюз VPN, настроенный для TrustSec. Подробная конфигурация вне области этого документа. См. эти примеры:

- ASA и коммутатор Catalyst серии 3750X — пример конфигурации TrustSec и руководство по устранению неполадок
- VPN версии ASA 9.2 классификация SGT и пример конфигурации осуществления

FW ASA

Межсетевой экран ASA ответственен за перенаправление WCCP к WSA. Это устройство не знает о TrustSec.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.110 255.255.255.0
```

```
access-list wccp-routers extended permit ip host 172.16.32.204 any
access-list wccp-redirect extended deny tcp any host 172.16.32.204
access-list wccp-redirect extended permit tcp any any eq www
access-list wccp-redirect extended permit tcp any any eq https

wccp 90 redirect-list wccp-redirect group-list wccp-routers
wccp interface inside 90 redirect in
```

ISE

ISE является центральной точкой в развертываниях TrustSec. Это назначает метки SGT на всех пользователей, которые обращаются и аутентифицируются на сети. Шаги, требуемые для базовой конфигурации, перечислены в этом разделе.

Шаг 1. SGT для IT и другой группы

Выберите **Policy>> Security Results Группы> Security Группового доступа** и создайте SGT:

Шаг 2. Правило авторизации для доступа VPN, который назначает SGT = 2 (IT)

Выберите **Policy> Authorization** и создайте правило для удаленного доступа VPN. Все VPN-подключения, установленные через VPN ASA, получат полный доступ (PermitAccess) и будут назначены, SGT помечает 2 (IT).

Шаг 3. Добавьте сетевое устройство и генерируйте файл PAC для VPN ASA

Для добавления VPN ASA к домену TrustSec необходимо генерировать файл автоматического config прокси (PAC) вручную. Тот файл будет импортирован на ASA.

Это может быть настроено от **администрирования> Сетевые устройства**. После того, как ASA добавлен, прокрутите вниз к параметрам настройки TrustSec и генерируйте файл PAC. Подробные данные, для которых описаны в отдельном документе на который (ссылаются).

Шаг 4. . Включите pxGrid Роль

Выберите **Administration> Deployment** для включения pxGrid роли.

Шаг 5. . Генерируйте Сертификат для администрирования и pxGrid Роли

pxGrid протокол использует проверку подлинности сертификата и для клиента и для сервера. Очень важно настроить корректные сертификаты и для ISE и для WSA. Оба сертификата должны включать Полное доменное имя (FQDN) в Предмет и x509 расширения для Аутентификации клиента и Проверки подлинности сервера. Кроме того, удостоверьтесь корректный DNS, запись создана и для ISE и для WSA и совпадает с соответствующим FQDN.

Если оба сертификата подписаны другим Центром сертификации (CA), важно включать те CAs в доверяемое хранилище.

Для настройки сертификатов выберите **Administration> Certificates**.

ISE может генерировать запрос подписи сертификата (CSR) для каждой роли. Для pxGrid роли экспортируйте и подпишите CSR с внешним CA.

В данном примере Microsoft CA использовалась с этим шаблоном:

Конечный результат мог бы быть похожим:

Не забывайте создавать DNS записи для ise14. пример. com и pxgrid. пример. com та точка к 172.16.31.202.

Автоматическая регистрация

Шаг 6. pxGrid

По умолчанию ISE автоматически не зарегистрирует pxGrid абонентов. Это должно быть вручную утверждено администратором. Те настройки должны быть изменены для интеграции WSA.

Выберите **Administration> pxGrid Сервисы** и установите **, Включают Авторегистрацию**.

WSA

Шаг 1. Прозрачный режим и перенаправление

В данном примере WSA настроен только с интерфейсом управления, прозрачным режимом и перенаправлением от ASA:

Шаг 2. Генерация сертификата

WSA должен доверить CA для подписания всех сертификатов. Выберите**> Certificate Management Network** для добавления сертификата CA:

Также необходимо генерировать сертификат, который WSA будет использовать для аутентификации на pxGrid. Выберите **Network> Identity Services Engine> WSA Client certificate**, чтобы генерировать CSR, подписать его с корректным шаблоном CA (ISE-pxgrid) и импортировать его назад.

Кроме того, для "Сертификата Admin ISE" и "сертификата ISE pxGrid", импортируют сертификат CA (для доверия pxGrid сертификату, представленному ISE):

Шаг 3. Тестовое подключение ISE

Выберите **Network> Identity Services Engine** для тестирования соединения с ISE:

Шаг 4. . Идентификационные профили ISE

Выберите **Web Security Manager> профили Identification** для добавления нового профиля для ISE. Для "*Идентификации и Опознавательного*" использования "*Прозрачно определяют пользователей с ISE".*

Шаг 5. . Обратитесь к политике на основе метки SGT

Выберите **Web Security Manager> Access Policies** для добавления новой политики. Членство использует профиль ISE:

Для Selected Groups и Пользователей SGT помечает 2, будет добавлен (IT):

Политика запрещает доступ ко всем спортивным узлам для пользователей, которые принадлежат SGT IT:

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Шаг 1. Сеанс VPN

Пользователь VPN инициирует сеанс VPN к VPN ASA:

VPN ASA использует ISE для аутентификации. ISE создает сеанс и назначает метку SGT 2 (IT):

После успешной аутентификации VPN ASA создает сеанс VPN с меткой SGT 2 (возвратился в Access-Accept Радиуса в Cisco-av-pair):

```
asa-vpn# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username    : cisco                 Index       : 2
Assigned IP : 172.16.32.50          Public IP   : 192.168.10.67
Protocol    : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License     : AnyConnect Essentials
Encryption  : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx    : 12979961              Bytes Rx    : 1866781
Group Policy : POLICY                Tunnel Group : SSLVPN
Login Time  : 21:13:26 UTC Tue May 5 2015
Duration    : 6h:08m:03s
```

```
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                    VLAN        : none
Audt Sess ID : ac1020640000200055493276
Security Grp : 2:IT
```

Начиная со ссылки между VPN ASA и FW ASA не включенный TrustSec, VPN ASA передает кадры без разметки за тем трафиком (не был бы в состоянии к GRE, инкапсулируют Фреймы Ethernet с введенным полем CMD/TrustSec).

Шаг 2. Информация о сеанса, полученная WSA

На данном этапе WSA должен получить сопоставление между IP-адресом, именем пользователя и SGT (по pxGrid протоколу):

Шаг 3. Переадресация трафика к WSA

Пользователь VPN инициирует соединение с sport.pl, который перехвачен FW ASA:

```
asa-fw# show wccp

Global WCCP information:
   Router information:
       Router Identifier:                  172.16.33.110
       Protocol Version:                   2.0

   Service Identifier: 90
       Number of Cache Engines:            1
       Number of routers:                  1
       Total Packets Redirected:           562
       Redirect access-list:               wccp-redirect
       Total Connections Denied Redirect:  0
       Total Packets Unassigned:           0
       Group access-list:                  wccp-routers
       Total Messages Denied to Group:     0
       Total Authentication failures:      0
       Total Bypassed Packets Received:    0

asa-fw# show access-list wccp-redirect
access-list wccp-redirect; 3 elements; name hash: 0x9bab8633
access-list wccp-redirect line 1 extended deny tcp any host 172.16.32.204 (hitcnt=0)
0xfd875b28
access-list wccp-redirect line 2 extended permit tcp any any eq www (hitcnt=562)
0x028ab2b9
access-list wccp-redirect line 3 extended permit tcp any any eq https (hitcnt=0)
0xe202a11e
```

и туннелировал в GRE к WSA (заметьте, что router-id WCCP является самый высокий настроенный IP-адрес):

```
asa-fw# show capture
capture CAP type raw-data interface inside [Capturing - 70065 bytes]
 match gre any any

asa-fw# show capture CAP

525 packets captured

  1: 03:21:45.035657      172.16.33.110 > 172.16.32.204: ip-proto-47, length 60
  2: 03:21:45.038709      172.16.33.110 > 172.16.32.204: ip-proto-47, length 48
```

```
3: 03:21:45.039960      172.16.33.110 > 172.16.32.204: ip-proto-47, length 640
```

WSA продолжает квитирование TCP - подключения и обрабатывает запрос GET. В результате политика под названием PolicyForIT поражена, и трафик заблокирован:

Это подтверждено Отчётом о WSA:

Заметьте, что ISE отображает имя пользователя.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Неправильные сертификаты

Когда WSA правильно не инициализируется (сертификаты), тест для ошибки подключения ISE:

ISE pxgrid-cm.log отчёты:

```
[2015-05-06T16:26:51Z] [INFO ] [cm-1.jabber-172-16-31-202]
[TCPSocketStream::_doSSLHandshake] [] Failure performing SSL handshake: 1
```

Основания для сбоя могут видеться с Wireshark:

Для сеанса SSL, используемого для защиты Расширяемого Протокола Обмена сообщениями и Присутствия (XMPP) обмен (используемый pxGrid), Клиент сообщает о сбое SSL из-за неизвестной цепочки сертификатов, представленной сервером.

Корректный сценарий

Для корректного сценария, ISE pxgrid-controller.log журналы:

```
2015-05-06 18:40:09,153 INFO [Thread-7][] cisco.pxgrid.controller.sasl.SaslWatcher
-::::::- Handling authentication for user name wsa.example.com-test_client
```

Кроме того, GUI ISE представляет WSA как абонента с корректными возможностями:

Дополнительные сведения

- Положение VPN версии ASA 9.2.1 с примером конфигурации ISE
- Пользовательское WSA 8.7 руководство
- ASA и коммутатор Catalyst серии 3750X — пример конфигурации TrustSec и руководство по устранению неполадок
- Руководство конфигурации коммутатора Cisco TrustSec: понимание Cisco TrustSec
- Настройка внешний сервер для авторизации пользователя на устройстве безопасности
- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.1
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация