Настройте сервисы исправления с интеграцией FirePower и ISE

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Настройка
Схема сети
Центр управления FireSight (оборонный центр)
Модуль исправления ISE
Политика корреляции
ASA
ISE
Настройте сетевое устройство доступа (NAD)
Включите адаптивное управление сетью
Карантинный DACL
Профиль авторизации для карантина
Правила авторизации
Проверка
AnyConnect инициирует сеанс VPN ASA
Соответствие политики корреляции FireSight
ISE выполняет карантин и передает CoA
Сеанс VPN Разъединен
Устранение неполадок
FireSight (оборонный центр)
ISE
Дефекты
Дополнительные сведения

Введение

Этот документ описывает, как использовать модуль исправления на устройстве Cisco FireSight, чтобы обнаружить атаки и автоматически повторно добиться атакующего с использованием Идентификационного механизма сервиса (ISE) Cisco как сервер политик. Пример, который предоставлен в этом документе, описывает метод, который используется для исправления удаленного пользователя VPN, который аутентифицируется через ISE, но это может также использоваться для соединенного проводом 802.1x/MAB/WebAuth или пользователь беспроводной связи.

Примечание: Модуль исправления, на который ссылаются в этом документе, официально не поддерживается Cisco. Это разделено на портале сообщества и может использоваться любым. В Версиях 5.4 и позже, существует также более новый модуль исправления, доступный, который основывается *на pxGrid* протоколе. Этот модуль не поддерживается в Версии 6.0, но запланирован, чтобы поддерживаться в последующих версиях.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Устройство адаптивной защиты Cisco (ASA) конфигурация VPN
- Конфигурация Защищенного мобильного клиента Cisco AnyConnect Secure Mobility
- Базовая конфигурация Cisco FireSight
- Базовая конфигурация Cisco FirePower
- Конфигурация Cisco ISE

Используемые компоненты

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

- Microsoft Windows 7
- Версия 9.3 Cisco ASA или позже
- Версии программного обеспечения Cisco ISE 1.3 и позже
- Версии Защищенного мобильного клиента Cisco AnyConnect Secure Mobility 3.0 и позже
- Версия 5.4 центра управления Cisco FireSight
- Версия 5.4 (виртуальная машина (VM)) Cisco FirePower

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

Используйте информацию, которая предоставлена в этом разделе для настройки системы.

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

Схема сети

Пример, который описан в этом документе, использует эту сетевую установку:

Вот поток для этой сетевой установки:

1. Пользователь инициирует удаленный сеанс VPN с ASA (через AnyConnect Cisco Безопасная Версия 4.0 Мобильности).

2. Пользователь пытается обратиться *к http://172.16.32.1*. (Трафик перемещается через FirePower, который установлен на VM и управляется FireSight.)

3. FirePower настроен так, чтобы он заблокировался (встраивают) тот определенный трафик (политика доступа), но он также имеет Политику Корреляции, которая инициирована. В результате это инициирует исправление ISE через Прикладной программный интерфейс (API) REST (метод *QuarantineByIP*).

4. Как только ISE получает остальных вызов API, он ищет сеанс и передает изменение авторизации RADIUS (CoA) к ASA, который завершает тот сеанс.

5. ASA разъединяет пользователя VPN. Так как AnyConnect настроен с *Постоянным* доступом VPN, новый сеанс установлен; однако, на этот раз с другим Правилом авторизации ISE совпадают (для изолированных хостов), и ограниченный доступ к сети предоставлен. На данном этапе не имеет значения, как пользователь соединяется и аутентифицируется на сети; пока ISE используется для проверки подлинности и авторизация, пользователь ограничил доступ к сети, должный изолировать.

Как ранее упомянуто, этот сценарий работает для любого типа аутентифицируемого сеанса (VPN, проводной 802.1x/MAB/Webauth, беспроводной 802.1x/MAB/Webauth) как долго, поскольку ISE используется для аутентификации и поддержек устройств доступа к сети RADIUS CoA (все современные устройства Cisco).

> **Совет:** Для перемещения пользователя из карантина можно использовать GUI ISE. Последующие версии модуля исправления могли бы также поддержать его.

FirePower

> **Примечание:** Устройство VM используется для примера, который описан в этом

документе. Только начальная конфигурация выполнена через CLI. Вся политика настроена от Оборонного Центра Cisco. Для получения дополнительной информации обратитесь к Разделу связанных сведений этого документа.

VM имеет три интерфейса, один для управления и два для встроенного (внутреннего/внешнего) контроля.

Весь трафик от пользователей VPN перемещается через FirePower.

Центр управления FireSight (оборонный центр)

Политика контроля доступа

После того, как вы устанавливаете корректные лицензии и добавляете устройство FirePower, перешли к **Политике> Управление доступом** и создаете Политику доступа, которая используется для отбрасывания трафика HTTP к 172.16.32.1:

Весь другой трафик принят.

Модуль исправления ISE

Текущая версия модуля ISE, который разделен на портале сообщества, является *бетой 1.3.19 ISE 1.2 Исправления*:

Перейдите к **Политике> Действия> Исправления> Модули** и установите файл:

Корректный экземпляр должен тогда быть создан. Перейдите к **Политике> Действия> Исправления> Экземпляры** и предоставьте IP-адрес Узла администрирования политик (PAN), наряду с ISE административные учетные данные, которые необходимы для остальных API (отдельному пользователю с ролью *Admin ERS* рекомендуют):

IP - адрес источника (атакующий) должен также использоваться для исправления:

Политика корреляции

Необходимо теперь настроить определенное правило корреляции. Это правило инициировано в начале соединения, которое совпадает ранее *правило (DropTCP80)* контроля за настроенным адресом. Для настройки правила перейдите к **Политике> Корреляция> менеджмент Правила**:

Это правило используется в Политике Корреляции. Перейдите к **Политике> Корреляция> Управление политиками**, чтобы создать новую политику, и затем добавить настроенное правило. Нажмите **Remediate** справа и добавьте два действия: **исправление для sourceIP** (настроил ранее), и **системный журнал**:

Гарантируйте включение политики корреляции:

ASA

ASA, который действует как Шлюз VPN, настроен для использования ISE для аутентификации. Также необходимо позволить считать и RADIUS CoA:

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
 address-pool POOL-VPN
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy POLICY

aaa-server ISE protocol radius
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
 key *****

webvpn
 enable outside
 enable inside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable
```

ISE

Настройте сетевое устройство доступа (NAD)

Перейдите к **администрированию> Сетевые устройства** и добавьте ASA, который действует как Клиент RADIUS.

Включите адаптивное управление сетью

Перейдите к **администрированию> Система> Параметры настройки> Адаптивное Управление сетью** для включения карантинного API и функциональности:

> **Примечание:** В Версиях 1.3 и ранее, эту функцию называют *Службой защиты Оконечной точки*.

Карантинный DACL

Для создания Загружаемого списка контроля доступа (DACL), который используется для изолированных хостов, перейдите к **Политике> Результаты> Авторизация> Загружаемый список ACL**.

Профиль авторизации для карантина

Перейдите к **Политике> Результаты> Авторизация> Профиль Авторизации** и создайте профиль авторизации с новым DACL:

Правила авторизации

Необходимо создать два правила авторизации. Первое правило (VPN ASA) предоставляет полный доступ для всех сеансов VPN, которые завершены на ASA. *ASA-VPN_quarantine* правила поражен для повторно аутентифицируемого сеанса VPN, когда хост уже находится в карантине (ограниченный доступ к сети предоставлен).

Для создания этих правил перейдите к **Политике> Авторизация**:

Проверка

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

AnyConnect инициирует сеанс VPN ASA

ASA создает сеанс без любого DACL (полный доступ к сети):

```
asav# show vpn-sessiondb details anyconnect

Session Type: AnyConnect

Username     : cisco                  Index       : 37
Assigned IP : 172.16.50.50           Public IP   : 192.168.10.21
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     : 18706                  Bytes Rx    : 14619
Group Policy : POLICY                 Tunnel Group : SSLVPN-FIRESIGHT
Login Time   : 03:03:17 UTC Wed May 20 2015
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN        : none
Audt Sess ID : ac10206400025000555bf975
Security Grp : none

.......
DTLS-Tunnel:
 <some output omitted for clarity>
```

Пользователь делает попытку доступа

Как только пользователь пытается обратиться к http://172.16.32.1, политика доступа поражена, трафик, который соответствует, заблокирован встроенный, и сообщение системного журнала передается от управления IP-адресами FirePower:

```
May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine
(cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User:
```

```
Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown,
 Access Control Rule Name: DropTCP80, Access Control Rule Action: Block,
Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation:
Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2,
Security Zone Ingress: Internal, Security Zone Egress: External, Security
Intelligence Matching IP: None, Security Intelligence Category: None, Client Version:
(null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0,
NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes:
66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A,
SSL Cipher Suite: N/A, SSL Certificate: 0000000000000000000000000000000000000000,
SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org:
N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org:
N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server
Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server
Name: (null), SSL URL Category: N/A, SSL Session ID:
0000000000000000000000000000000000000000000000000000000000000000, SSL Ticket Id:
00000000000000000000000000000000000000, {TCP} 172.16.50.50:49415 -> 172.16.32.1:80
```

Соответствие политики корреляции FireSight

Управление FireSight (Оборонный Центр) Политика Корреляции поражена, о котором сообщает сообщение системного журнала, которое передается от Оборонного Центра:

```
May 24 09:37:10 172.16.31.206 SFIMS: Correlation Event:
CorrelateTCP80Block/CorrelationPolicy at Sun May 24 09:37:10 2015 UTCConnection Type:
FireSIGHT 172.16.50.50:49415 (unknown) -> 172.16.32.1:80 (unknown) (tcp)
```

На данном этапе Оборонный Центр использует остальных API (карантин) вызов к ISE, который является сеансом HTTPS и может быть дешифрован в Wireshark (с плагином Уровня защищенных сокетов (SSL) и секретным ключом PAN административный сертификат):

В запросе GET о IP-адресе атакующего передан (172.16.50.50), и тот хост изолирован ISE.

Перейдите к **Анализу> Корреляция> Статус** для подтверждения успешного исправления:

ISE выполняет карантин и передает CoA

На данном этапе ISE *prrt-management.log* уведомляет, что должен быть передан CoA:

```
DEBUG [RMI TCP Connection(142)-127.0.0.1][] cisco.cpm.prrt.impl.PrRTLoggerImpl
-:::- send() - request instanceof DisconnectRequest
       clientInstanceIP = 172.16.31.202
       clientInterfaceIP = 172.16.50.50
       portOption = 0
       serverIP = 172.16.31.100
       port = 1700
       timeout = 5
       retries = 3
       attributes = cisco-av-pair=audit-session-id=ac10206400021000555b9d36
Calling-Station-ID=192.168.10.21
Acct-Terminate-Cause=Admin Reset
```

Время выполнения (prrt-server.log) передает CoA *окончечное* сообщение к NAD, который завершает сеанс (ASA):

```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
```

```
    [4] NAS-IP-Address - value: [172.16.31.100]
    [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
    [49] Acct-Terminate-Cause - value: [Admin Reset]
    [55] Event-Timestamp - value: [1432457729]
    [80] Message-Authenticator - value:
[00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00]
    [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
```

ise.psc передает уведомление, подобное этому:

```
INFO  [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -::::- PrrtManager
disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50
AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202
NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault
```

Когда вы перешли к **Операциям> Аутентификация**, она должна показать *Динамическую Авторизацию, за которой следуют*.

Сеанс VPN Разъединен

Конечный пользователь передает уведомление, чтобы указать, что сеанс разъединен (для проводного/беспроводного 802.1X/MAB/ГОСТЯ, этот процесс прозрачен):

Подробные данные от журналов AnyConnect Cisco показывают:

```
10:48:05 AM Establishing VPN...
10:48:05 AM Connected to 172.16.31.100.
10:48:20 AM Disconnect in progress, please wait...
10:51:20 AM The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: COA initiated
```

Сеанс VPN с ограниченным доступом (карантин)

Поскольку *постоянная VPN* настроена, новый сеанс сразу создан. На этот раз правило *ASA-VPN_quarantine* ISE поражено, который предоставляет ограниченный доступ к сети:

> **Примечание:** DACL загружен в отдельном Запросе RADIUS.

Сеанс с ограниченным доступом может быть проверен на ASA с **anyconnect** командой CLI **подробности покажите vpn-sessiondb**:

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username    : cisco                 Index       : 39
Assigned IP : 172.16.50.50          Public IP   : 192.168.10.21
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    : 11436                 Bytes Rx    : 4084
Pkts Tx     : 8                     Pkts Rx     : 36
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : POLICY                Tunnel Group : SSLVPN-FIRESIGHT
Login Time  : 03:43:36 UTC Wed May 20 2015
```

```
Duration    : 0h:00m:10s
Inactivity  : 0h:00m:00s
VLAN Mapping : N/A                    VLAN        : none
Audt Sess ID : ac10206400027000555c02e8
Security Grp : none

......
DTLS-Tunnel:
 <some output ommited for clarity>
 Filter Name : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

Устранение неполадок

Этот раздел предоставляет сведения, который можно использовать для устранения проблем конфигурации.

FireSight (оборонный центр)

Сценарий исправления ISE находится в этом местоположении:

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
_lib_ ise-instance ise-test.pl ise.pl module.template
```

Это - простой сценарий *жемчуга*, который использует стандартный Sourcefire (SF) подсистема регистрации. Как только исправление выполняется, можно подтвердить результаты через*/var/log/messages*:

```
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin
```

ISE

Важно, чтобы вы включили Адаптивный сервис Управления сетью на ISE. Для просмотра подробного, входит в процесс во время выполнения (*prrt-management.log* и *prrt-server.log*), необходимо включить Уровень отладки для Ааа во время выполнения. Перейдите к **администрированию> Система> Регистрация> Конфигурация Журнала Отладки** для включения отладок.

Можно также перейти к **Операциям> Отчёты> Оконечная точка и Пользователи> Адаптивный Аудит Управления сетью** для просмотра информации для каждой попытки и результата карантинного запроса:

Дефекты

См. идентификатор ошибки Cisco CSCuu41058 (Карантинное несоответствие оконечной точки ISE 1.4 и сбой VPN) для получения информации о дефекте ISE, который отнесен к сбоям сеанса VPN (802.1x/MAB хорошо работает).

Дополнительные сведения

- Настройте интеграцию WSA с ISE для TrustSec осведомленные сервисы
- Версия 1.3 ISE pxGrid Интеграция с IPS pxLog Приложение
- Руководство администратора платформы Cisco Identity Services Engine, выпуск 1.4 – устанавливает адаптивное управление сетью
- Справочное руководство API платформы Cisco Identity Services Engine, выпуск 1.2 – введение к внешнему API сервисов RESTful
- Справочное руководство API платформы Cisco Identity Services Engine, выпуск 1.2 – введение к контролирующим API REST
- Руководство администратора платформы Cisco Identity Services Engine, выпуск 1.3
- Техническая поддержка и документация – C i s c o S y s t e m s