Настройте положение версии 1.4 ISE с Microsoft WSUS

Содержание

Введение

Этот документ описывает, как настроить платформу Cisco Identity Services Engine (ISE) функциональность положения, когда это интегрировано с Microsoft Windows Server Update Services (WSUS).

Примечание: При доступе к сети вы перенаправлены к ISE для инициализации Версии 4.1 защищенного мобильного клиента Cisco AnyConnect Secure Mobility с модулем положения, который проверяет Состояние совместимости на WSUS и устанавливает необходимые обновления для станции, чтобы быть совместимым. Как только о станции сообщают как совместимой, ISE обеспечивает полный доступ к сети.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Развертывания Cisco ISE, аутентификация и авторизация
- Базовые знания о пути, которым действуют ISE и агент положения AnyConnect Cisco
- Конфигурация устройства адаптивной защиты Cisco (ASA)
- Основная VPN и знание 802.1x
- Конфигурация Microsoft WSUS

Используемые компоненты

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

- Версия 7 Microsoft Windows
- Версия 2012 Microsoft Windows с версией 6.3 WSUS
- Версии Cisco ASA 9.3.1 и позже
- Версии программного обеспечения Cisco ISE 1.3 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

В этом разделе описывается настроить ISE и отнесенные сетевые элементы.

Схема сети

Это - топология, которая используется для примеров всюду по этому документу:

Вот трафик, как проиллюстрировано в схеме сети:

1. Удаленный пользователь соединяется через AnyConnect Cisco для доступа VPN к ASA. Это может быть любым типом унифицированного доступа, такого как Обход 802.1X/ПРОРЕРКИ ПОЕЛИННОСТИ MAC (MAB) соединенный проводом сеанс, который завершен на коммутаторе или беспроводном сеансе, который завершен на Контроллере беспроводной локальной сети (WLC).

2. Как часть процесса проверки подлинности, ISE подтверждает, что статус положения конечной станции не равен совместимому (правило авторизации *ASA-VPN_quarantine*) и что атрибуты перенаправления возвращены в сообщении *Access-Accept Радиуса*. В результате ASA перенаправляет весь трафик HTTP к ISE.

3. Пользователь открывает web-браузер и вводит любой адрес. После перенаправления к ISE модуль Cisco AnyConnect 4 положения установлен на станции. Модуль положения тогда загружает политику от ISE (требование для WSUS).

4. Модуль положения ищет Microsoft WSUS и выполняет исправление.

5. После успешного исправления модуль положения передает отчёт ISE.

6. ISE выполняет изменение авторизации (CoA) Радиуса, которое предоставляет полный доступ к сети совместимому пользователю VPN (правило авторизации *ASA-VPN_compliant*).

   Примечание: Для исправления для работы (способность установить обновления Microsoft Windows на ПК) у пользователя должны быть локальные административные права.

Microsoft WSUS

> **Примечание:** Подробная конфигурация WSUS вне области этого документа. Для получения дополнительной информации обратитесь к Развернуть Windows Server Update Services в Вашей Организационной документации microsoft.

Сервис WSUS развернут через стандартный порт TCP 8530. Важно помнить, что для исправления, также используются другие порты. Это - то, почему безопасно добавить IP-адрес WSUS к Списку контроля доступа (ACL) перенаправления на ASA (описанный позже в этом документе).

Групповая политика для домена настроена для обновлений Microsoft Windows и точек к локальному серверу WSUS:

Это рекомендуемые обновления, которые включены для гранулированной политики, которая основывается на разных уровнях степеней серьезности ошибки:

Клиентское предназначение обеспечивает намного большую гибкость. ISE может использовать политику положения, которая основывается на другой Microsoft Active Directory (AD) компьютерные контейнеры. WSUS может утвердить обновления, которые основываются на этом членстве.

ASA

Простой доступ VPN Уровня защищенных сокетов (SSL) для удаленного пользователя используется (подробные данные которого вне области этого документа).

Вот пример конфигурации:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 10
 ip address 172.16.32.100 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.31.100 255.255.255.0

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

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

group-policy POLICY internal
group-policy POLICY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group SSLVPN type remote-access
tunnel-group SSLVPN general-attributes
 address-pool POOL-VPN
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy POLICY

ip local pool POOL-VPN 172.16.50.50-172.16.50.60 mask 255.255.255.0
```

Важно настроить access-list на ASA, который используется для определения трафика, который должен быть перенаправлен к ISE (для пользователей, которые еще не совместимы):

```
access-list Posture-redirect extended deny udp any any eq domain
access-list Posture-redirect extended deny ip any host 172.16.31.103
access-list Posture-redirect extended deny ip any host 172.16.31.202
access-list Posture-redirect extended deny icmp any any
access-list Posture-redirect extended permit tcp any any eq www
```

Только Система доменных имен (DNS), ISE, WSUS и трафик Протокола ICMP позволены

для не соответствующих стандарту пользователей. Весь другой трафик (HTTP) перенаправлен к ISE для инициализации AnyConnect 4, которая ответственна за положение и исправление.

ISE

> Инициализация **Примечание:** AnyConnect 4 и положение вне области этого документа. См. интеграцию AnyConnect 4.0 с Примером конфигурации Версии 1.3 ISE для получения дополнительной информации, такой как, как настроить ASA как сетевое устройство и установить приложение Cisco AnyConnect 7.

Исправление положения для WSUS

Выполните эти шаги для настройки исправления положения для WSUS:

1. Перейдите к **Политике> Условия> Положение> Восстановительные мероприятия> Исправление Windows Server Update Services** для создания нового правила.

2. Проверьте, что значение *Обновлений Microsoft Windows* установлено в **Уровень важности**. Если процесс исправления инициируется, эта часть ответственна за обнаружение.

Агент Обновления Microsoft Windows тогда соединяется с WSUS и проверяет, существуют ли какие-либо *Важные* обновления для того ПК, которые ждут установки:

Требование положения для WSUS

Перейдите к **Политике> Условия> Положение> Требования** для создания нового правила. Правило использует фиктивное условие, названное *pr_WSUSRule*, что означает, что с WSUS связываются для проверки для условия, когда исправление необходимо (*Важные* обновления).

Как только это условие соблюдают, WSUS устанавливает обновления, которые были настроены для того ПК. Они могут включать любой тип обновлений, и также тех с уровнями более низкой серьезности:

Профиль AnyConnect

Настройте профиль модуля положения, наряду с профилем AnyConnect 4 (как описано в интеграции AnyConnect 4.0 с Примером конфигурации Версии 1.3 ISE):

Клиент, настраивающий правила

Как только профиль AnyConnect готов, на него можно сослаться от *Клиента, Настраивающего* политику:

Целое приложение, наряду с конфигурацией, установлено на оконечной точке, которая перенаправлена Клиенту, Настраивающему страницу портала. AnyConnect 4 мог бы быть обновлен и дополнительный модуль установленное (положение).

Профили авторизации

Создайте профиль авторизации для перенаправления Клиенту, Настраивающему профиль:

Правила авторизации

Этот образ показывает правила авторизации:

Впервые, правило *ASA-VPN_quarantine* используется. В результате профиль авторизации *Положения* возвращен, и оконечная точка перенаправлена Клиенту, Настраивающему портал для AnyConnect 4 (с модулем положения) инициализация.

Однажды совместимый, правило *ASA-VPN_compliant* используется, и полный доступ к сети позволен.

Проверка

Этот раздел предоставляет сведения, который можно использовать, чтобы проверить, что вы конфигурация работаете должным образом.

ПК с обновленной политикой GPO

Политика домена с конфигурацией WSUS должна быть выдвинута после того, как ПК входит в домен. Это может произойти, прежде чем сеанс VPN установлен (внеполосный) или после если *Запуск Перед* функциональностью *Входа в систему* используется (это может также использоваться для проводного 802.1x / беспроводной доступ).

Как только у клиента Microsoft Windows есть корректная конфигурация, это может быть отражено от параметров настройки Windows Update:

В случае необходимости обновление Объекта групповой политики (GPO) и обнаружение Сервера агента Обновления Microsoft Windows могут использоваться:

```
C:\Users\Administrator>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.


C:\Users\Administrator>wuauclt.exe /detectnow

C:\Users\Administrator>
```

Утвердите важное обновление на WSUS

Процесс утверждения может извлечь выгоду из предназначения узла клиента:

Повторно передайте отчёт с *wuauclt* в случае необходимости.

Проверьте статус ПК на WSUS

Этот образ показывает, как проверить статус ПК на WSUS:

Одно обновление должно быть установлено для следующего обновления с WSUS.

Установленный сеанс VPN

После того, как сеанс VPN установлен, правило авторизации ISE *ASA-VPN_quarantine* используется, который возвращает профиль авторизации *Положения*. В результате трафик HTTP от оконечной точки перенаправлен для обновления AnyConnect 4 и инициализации модуля положения:

На этом этапе статус сеанса на ASA указывает на ограниченный доступ с перенаправлением трафика HTTP к ISE:

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username    : cisco                 Index       : 69
Assigned IP : 172.16.50.50          Public IP   : 192.168.10.21

<...some output omitted for clarity...>

ISE Posture:
 Redirect URL : https://ise14.example.com:8443/portal/gateway?sessionId=ac101f64000
45000556b6a3b&portal=283258a0-e96e-...
 Redirect ACL : Posture-redirec
```

Модуль положения получает политику от ISE и выполняет исправление

Модуль положения получает политику от ISE. Отладки **ise-psc.log** показывают требование, которое передается модулю положения:

```
2015-06-05 07:33:40,493 DEBUG [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
 <package>
   <id>10</id>
   <name>WSUS</name>
   <version/>
   <description>This endpoint has failed check for any AS installation</description>
   <type>10</type>
   <optional>0</optional>
   <path>42#1</path>
```

```
   <remediation_type>1</remediation_type>
   <remediation_retry>0</remediation_retry>
   <remediation_delay>0</remediation_delay>
   <action>10</action>
   <check>
     <id>pr_WSUSCheck</id>
   </check>
   <criteria/>
 </package>
</cleanmachines>
```

Модуль положения автоматически инициирует Агента Обновления Microsoft Windows для соединения с WSUS и обновлениями загрузки согласно конфигурации в политике WSUS (все автоматически без любого вмешательства пользователя):

Примечание: Некоторые обновления могли бы потребовать перезапуска системы.

Полный доступ к сети

Вы будете видеть это после того, как о станции сообщит как совместимой модуль положения AnyConnect:

Отчёт передается ISE, который переоценивает политику и поражает правило авторизации *ASA-VPN_compliant*. Это предоставляет полный доступ к сети (через Радиус CoA). Перейдите к **Операциям> Аутентификации** для подтверждения этого:

Отладки **(ise-psc.log)** также подтверждают Состояние совместимости, триггер CoA и последние настройки для положения:

```
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureManager -:cisco:
ac101f6400039000556b4200:::- Posture report token for endpoint mac
08-00-27-DA-EF-AD is Healthy
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:
ac101f6400039000556b4200:::- entering triggerPostureCoA for session
ac101f6400039000556b4200
DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:ac
101f6400039000556b4200:::- Posture CoA is scheduled for session id
[ac101f6400039000556b4200]

DEBUG [portal-http-service17][] cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:
ac101f6400039000556b4200:::- DM_PKG report non-AUP:html = <!--X-Perfigo-DM-Error=0-->
<!--error=0--><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0-->
<!--X-Perfigo-Auto-Close-Login-Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0-->
<!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-UserKey=dummykey-->
<!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-Perfigo-Session=-->
<!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter-->
<!--X-Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4-->
<!--X-Perfigo-DHCP-Renew-Delay=1--><!--X-Perfigo-Client-MAC=08:00:27:DA:EF:AD-->

DEBUG [pool-183-thread-1][]cisco.cpm.posture.runtime.PostureCoA -:cisco:
ac101f6400036000556b3f52:::- Posture CoA is triggered for endpoint [08-00-27-da-ef-ad]
with session [ac101f6400039000556b4200]
```

Кроме того, ISE, Подробный Отчет об оценке Положения подтверждает, что станция совместима:

Примечание: Точный Адрес для управления доступом к среде (MAC) физического

сетевого интерфейса на Microsoft Windows PC известен из-за расширений ACIDEX.

Устранение неполадок

В настоящее время нет никаких сведений об устранении проблем, доступных для этой конфигурации.

Важные примечания

Этот раздел предоставляет немного важной информации о конфигурации, которая описана в этом документе.

Подробные данные опции для исправления WSUS

Важно дифференцировать условие требования от исправления. AnyConnect инициирует Агента Обновления Microsoft Windows для проверения соответствия, зависящего от *Проверить обновлений Windows с помощью* значения исправления.

Для данного примера используется *Уровень важности*. С *Важной* установкой Агент Microsoft Windows проверяет, существует ли какое-либо ожидание (не установленным) важные обновления. Если существует, то исправление начинается.

Процесс исправления мог бы тогда установить все важные и менее важные обновления на основе конфигурации WSUS (обновления, утвержденные для определенной машины).

С *Проверить* набором *использования обновлений Windows* как **Правила Cisco** решают условия, которые детализированы в требовании, совместима ли станция.

Сервис Windows Update

Для развертываний без сервера WSUS существует другой тип исправления, который может использоваться, вызвал *Исправление Windows Update*:

Этот тип исправления позволяет, что контроль над Microsoft Windows Обновляет настройки, и позволяет вам выполнить незамедлительные обновления. Типичное условие, которое используется с этим типом исправления, является *pc_AutoUpdateCheck*. Это позволяет вам проверять, включено ли значение Обновления Microsoft Windows на оконечной точке. В противном случае можно включить его и выполнить обновление.

Интеграция SCCM

Новая характеристика для Версии 1.4 ISE звонила*, управление исправлениями* обеспечивает интеграцию со многими сторонними поставщиками. Зависящий от поставщика, составные опции доступны и для условий и для исправлений.

Для Microsoft поддерживаются и Сервер управления системой (SMS) и Системный менеджер конфигурации центра (SCCM).

Дополнительные сведения

- Сервисы положения на руководстве по конфигурации Cisco ISE
- Руководство администратора платформы Cisco Identity Services Engine, выпуск 1.4
- Руководство администратора платформы Cisco Identity Services Engine, выпуск 1.3
- Разверните Windows Server Update Services в своей организации
- Cisco Systems – техническая поддержка и документация