VPN Встроенное Положение с помощью iPEP ISE и ASA

Содержание

Введение

Этот документ предоставляет сведения о том, как установить встроенное положение с Устройством адаптивной защиты (ASA) и платформой Identity Services Engine (ISE).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 8.2 (4) для ASA и версии 1.1.0.665 для ISE.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании

условных обозначений, используемых в технической документации Cisco.

Общие сведения

ISE предоставляет много AAA Services (Положение, Профилирование, Аутентификация, и т.д.). Некоторые Сетевые устройства (NAD) поддерживают изменение авторизации (CoA) Радиуса, которое позволяет динамично изменять профиль авторизации конечного устройства на основе его Положения или Представляющий результат. Другие NADs, такие как ASA еще не поддерживают эту функцию. Это означает, что ISE, работающий во Встроенном режиме Осуществления Положения (iPEP), необходим для динамичного изменения политики доступа к сети конечного устройства.

Базовое понятие - то, что весь трафик пользователя пройдет iPEP с узлом, также действующим как RADIUS прокси.

Основной поток

1. Пользователь VPN входит.
2. ASA отправляет запрос к iPEP узлу (ISE).
3. iPEP переписывает запрос (путем добавления атрибутов AV-ПАРЫ CISCO, чтобы указать, что это - iPEP аутентификация), и отправляет запрос к Узлу Политики ISE (PDP).
4. PDP отвечает назад на iPEP, который передаст NAD.
5. Если пользователь аутентифицируется, MUST NAD передает учет - запускают запрос (см. CSCtz84826). Это инициирует инициирование сеанса на iPEP. На данном этапе пользователь перенаправлен для положения. Кроме того, необходимо включить промежуточное бухгалтерское обновление для туннеля, установленного от Портала WEBVPN, поскольку ISE ожидает иметь обрамленный IP-адрес атрибута в учете радиуса. Однако при соединении с порталом, IP-адрес VPN клиента еще не известен, потому что не установлен туннель. Это гарантирует, что ASA передаст промежуточные обновления, такой как тогда, когда будет установлен туннель.
6. Пользователь проходит оценку положения, и на основе результатов PDP обновит использование сеанса CoA на iPEP.

Этот снимок экрана иллюстрирует этот процесс:

Пример топологии

Конфигурация ASA

Конфигурация ASA является простой IPSec Удаленной VPN:

```
!
interface Ethernet0/0
nameif ISE
security-level 50
ip address 192.168.102.253 255.255.255.0
!
interface Ethernet0/1
```

```
nameif outside
security-level 0
ip address 10.48.39.236 255.255.255.0
!
access-list split extended permit ip 192.168.0.0 255.255.0.0 any
!
aaa-server ISE protocol radius
interim-accounting-update
!--- Mandatory if tunnel established from WEBVPN Portal aaa-server ISE (ISE) host
192.168.102.254 !--- this is the iPEP IP key cisco crypto ipsec transform-set TS1 esp-aes esp-
sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-
association lifetime kilobytes 4608000 crypto dynamic-map DMAP1 10 set transform-set TS1 crypto
dynamic-map DMAP1 10 set reverse-route crypto map CM1 10 ipsec-isakmp dynamic DMAP1 crypto map
CM1 interface outside crypto isakmp enable outside crypto isakmp policy 1 authentication pre-
share encryption aes hash sha group 2 lifetime 86400 ! ip local pool VPN 192.168.5.1-
192.168.5.100 ! group-policy DfltGrpPolicy attributes dns-server value 192.168.101.3 !--- The
VPN User needs to be able to resolve the CN from the !--- ISE HTTPS Certificate (which is sent
in the radius response) vpn-tunnel-protocol IPSec svc webvpn split-tunnel-policy tunnelspecified
split-tunnel-network-list value split address-pools value VPN ! tunnel-group cisco general-
attributes address-pool VPN authentication-server-group ISE accounting-server-group ISE !---
Does not work without this (see introduction) ! tunnel-group cisco ipsec-attributes pre-shared-
key cisco ! route outside 0.0.0.0 0.0.0.0 10.48.39.5 1 route ISE 192.168.0.0 255.255.0.0
192.168.102.254 1 !--- You need to make sure the traffic to the local subnets !--- are going
through the inline ISE !
```

Конфигурация ISE

Конфигурация iPEP

Первое, что нужно сделать состоит в том, чтобы добавить ISE как iPEP Узел. Можно найти дополнительные сведения о процессе здесь:

http://www. cisco . com/en/US/docs/security/ise/1.1/user_guide/ise_ipep_deploy.html#wp1110248.

Это в основном, что необходимо настроить в различных вкладках (снимки экрана, предоставленные в этом разделе, иллюстрируют это):

- Настройте недоверяемого IP и параметры настройки Глобального IP - адреса (в этом случае, недоверяемый IP 192.168.102.254).
- Развертывания являются режимом маршрутизации.
- Поместите статический фильтр для ASA, которому позволят пройти iPEP коробку (иначе, к/от подключения, ISE через iPEP коробку отброшен).
- Настройте ISE Политики как сервер RADIUS и ASA как Клиент RADIUS.
- Добавьте маршрут к Подсети VPN, которая указывает к ASA.
- Установите Контролирующий ISE как Главный компьютер регистрации (порт 20514 по умолчанию; в этом случае ISE политики контролирует также).

Важные конфигурационные требования сертификата:

Прежде, чем попытаться зарегистрировать iPEP узел, гарантируйте, что встречен следующий сертификат Расширенные Ключевые Требования к использованию. Если сертификаты не будут должным образом настроены на iPEP и узлах Admin, то процесс регистрации завершит. Однако вы потеряете доступ администратора к iPEP узлу. Следующие детали экстраполировались от ISE 1.1.x iPEP Руководство по развертыванию:

Присутствие определенных комбинаций атрибутов в локальных сертификатах Узлов

администрирования и Промежуточных узлов может препятствовать тому, чтобы работала обоюдная проверка подлинности.

Атрибуты:

- Расширенное использование ключа (EKU) — проверка подлинности сервера
- Расширенное использование ключа (EKU) — аутентификация клиента
- Тип свидетельства netscape — аутентификация SSL - сервера
- Тип свидетельства netscape — аутентификация клиента SSL

Любая из следующих комбинаций требуется для сертификата администрирования:

- Оба атрибута EKU должны быть отключены, если оба атрибута EKU отключены во Встроенном сертификате Положения, или оба атрибута EKU должны быть включены, если атрибут сервера включен во Встроенном сертификате Положения.
- Должны быть отключены оба Атрибута типа Свидетельства Netscape, или обоим нужно включить.

Любая из следующих комбинаций требуется для Встроенного сертификата Положения:

- Должны быть отключены оба атрибута EKU, или обоим нужно включить, или один только атрибут сервера должен быть включен.
- Должны быть отключены оба Атрибута типа Свидетельства Netscape, или обоим нужно включить, или один только атрибут сервера должен быть включен.
- Где самоподписано локальные сертификаты используются на Узлах администрирования и Промежуточных узлах, необходимо установить подписанный сертификат Узла администрирования в трастовом списке Промежуточного узла. Кроме того, если у вас есть и основные и вторичные Узлы администрирования в ваших развертываниях, необходимо установить подписанный сертификат обоих Узлов администрирования в трастовом списке Промежуточного узла.
- Где подписано CA локальные сертификаты используются на Узлах администрирования и Промежуточных узлах, обоюдная проверка подлинности должна работать правильно. В этом случае сертификат подписания CA установлен на Узле администрирования до регистрации, и этот сертификат реплицирован в Промежуточный узел.
- Если выполненные CA ключи используются для обеспечения связи между Узлами администрирования и Промежуточными узлами перед регистрацией Промежуточного узла необходимо добавить открытый ключ (сертификат CA) от Узла администрирования до списка сертификата CA Промежуточного узла.

Основная конфигурация:

Конфигурация режима развертываний:

Конфигурация фильтров:

Конфигурация RADIUS:

Статические маршруты:

Регистрация:

Аутентификация и конфигурация положения

Существует три состояния положения:

- Неизвестный: Положение еще не сделано
- Совместимый: Положение сделано, и система Совместима
- Не соответствующий стандарту: Положение сделано, но система отказала по крайней мере одну проверку

Теперь профили авторизации должны быть созданы (который будет Встроенными Профилями Авторизации: Это добавит ipep-authz=true атрибут в AV-паре Cisco), который будет использоваться для differents случая.

Обычно, Неизвестный профиль возвращает URL перенаправления (обнаружение положения), который передаст трафик пользователя к ISE и попросит устанавливать Агента NAC. Если Агент NAC будет уже установлен, то это позволит его Запросу на обнаружение HTTP быть переданным ISE.

В этом профиле по крайней мере используется ACL, который позволяет Трафик HTTP ISE и DNS.

Совместимые и Не соответствующие стандарту профили обычно возвращают загружаемый список ACL для предоставления доступа к сети на основе профиля пользователя. Не соответствующий стандарту профиль может позволить пользователям обращаться к Web-серверу для загрузки Антивируса, например, или предоставление ограничило доступ к сети.

В данном примере Неизвестные и Совместимые профили созданы, и присутствие notepad.exe, поскольку проверены требования.

Положение представляет конфигурацию

Первое, что нужно сделать состоит в том, чтобы создать Загружаемые списки ACL (DACL) и профили:

Примечание: Это не является обязательным для имения названия DACL, совпадающего с именем профиля.

- СовместимыйACL: ipep-неизвестныйПрофиль авторизации: ipep-неизвестный
- Не соответствующий стандартуACL: ipep-не-соответствующий-стандартуПрофиль авторизации: ipep-не-соответствующий-стандарту

Неизвестный DACL:

Неизвестный профиль:

Совместимый DACL:

Совместимый профиль:

Конфигурация авторизации

Теперь, когда профиль создан, необходимо совпасть с Запросом RADIUS, прибывающим из iPEP, и примениться к ним правильные профили. iPEP ISEs определен с типом специального устройства, который будет использоваться в Правилах авторизации:

NADs:

Авторизация:

Примечание: Если агент не установлен на машине, можно определить Клиента, Настраивающего правила.

Результат

Вам предлагают установить агента (в данном примере, клиентская инициализация уже установлена):

Некоторые выходные данные на данном этапе:

```
ciscoasa# show vpn-sessiondb remote

Session Type: IPsec
Username     : cisco                  Index        : 26
Assigned IP  : 192.168.5.2            Public IP    : 10.48.39.134
Protocol     : IKE IPsec
License      : IPsec
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 143862                 Bytes Rx     : 30628
Group Policy : DfltGrpPolicy          Tunnel Group : cisco
Login Time   : 13:43:55 UTC Mon May 14 2012
Duration     : 0h:09m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

И от iPEP:

```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 2 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
```

Как только агент загружен и установлен:

Агент должен автоматически обнаружить ISE и выполняет оценку положения (предполагающий, что вам уже определили правила положения, который является другим предметом). В данном примере положение успешно, и это появляется:

Примечание: Существует две аутентификации в снимке экрана выше. Однако, потому что iPEP коробка кэширует ACL, она не загружена каждый раз.

На iPEP:

```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 3 0
w-ise-ipep-1/admin# show pep table accesslist normal
```

```
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406:
permit ip any any

#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
w-ise-ipep-1/admin#
```

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация