Устаревший SCEP с использованием примера конфигурации интерфейса командой строки

Содержание

Введение

Этот документ описывает использование Устаревшего Протокола SCEP (SCEP) на устройстве адаптивной защиты Cisco (ASA).

> **Внимание. :** С Выпуска 3.0 AnyConnect Cisco не должен использоваться этот метод. Это было ранее необходимо, потому что мобильные устройства не имели 3.x клиент, но и Android и iPhone теперь имеют поддержку прокси SCEP, который должен использоваться вместо этого. Только в случаях, где это не поддерживается из-за ASA, должен вы настраивать Устаревший SCEP. Однако даже в этих случаях, обновление ASA является рекомендуемой опцией.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Устаревшим SCEP.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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.

Общие сведения

SCEP является протоколом, который разработан для создания распределения и аннулирования цифровых сертификатов максимально масштабируемыми. Идея состоит в том, что любой пользователь стандартной сети должен быть в состоянии запросить цифровой сертификат электронно с очень небольшим вмешательством от администраторов сети. Для развертываний VPN, которые требуют проверки подлинности сертификата с предприятием, Центром сертификации (CA), или любой независимый поставщик CA, который поддерживает SCEP, пользователи могут теперь запросить на подписанные сертификаты от клиентских компьютеров без участия администраторов сети.

> **Примечание:** Если вы желаете настроить ASA как сервер CA, то SCEP не является методом соответствующего протокола. См. Локальный раздел CA Документа Cisco **Цифровых сертификатов Настройки** вместо этого.

С Выпуска 8.3 ASA существует два поддерживаемых метода для SCEP:

- Более старый метод, названный Устаревшим SCEP, обсужден в этом документе.
- Метод прокси SCEP является более новыми из этих двух методов, где ASA проксирует запрос хранилища сертификатов от имени клиента. Этот процесс более чист, потому что он не требует дополнительной туннельной группы и также более безопасен. Однако недостаток - то, что SCEP проксирует, только работает с Выпуском 3 AnyConnect Cisco. x. Это означает, что текущая версия клиентской части AnyConnect для мобильных устройств не поддерживает прокси SCEP.

Настройка

Этот раздел предоставляет сведения, который можно использовать для настройки Устаревшего метода Протокола SCEP.

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

Когда Устаревший SCEP используется, вот некоторые важные замечания для учета:

- После того, как клиент получает подписанный сертификат, ASA должен распознать CA, который подписал сертификат, прежде чем это будет в состоянии аутентифицировать клиента. Поэтому необходимо гарантировать, что ASA также регистрируется с сервером

CA. Процесс регистрации для ASA должен быть первым шагом, потому что это гарантирует что:

CA настроен правильно и в состоянии выполнить сертификаты через SCEP при использовании метода регистрации URL.

ASA в состоянии связаться с CA. Поэтому , если клиент не может, то существует проблема между клиентом и ASA.

- Когда первая попытка подключения будет сделана, не будет подписанного сертификата. Должна быть другая опция, которая может использоваться для аутентификации клиента.

- В процессе хранилища сертификатов ASA не служит никакой роли. Это только служит агрегатором VPN так, чтобы клиент мог создать туннель для безопасного получения подписанного сертификата. Когда туннель установлен, клиент должен быть в состоянии достигнуть сервера CA. В противном случае это не быть в состоянии зарегистрироваться.

Зарегистрируйте ASA

Процесс регистрации ASA относительно легок и не запрашивает новой информации. См. Регистрацию Cisco ASA к CA Использование документа SCEP для получения дополнительной информации о том, как зарегистрировать ASA к стороннему CA.

Настройте туннель для использования регистрации

Как упомянуто ранее, для клиента, чтобы быть в состоянии получить сертификат, безопасный туннель должен быть создан с ASA через другой метод аутентификации. Чтобы сделать это, необходимо настроить одну туннельную группу, которая только используется для первой попытки подключения, когда сделан запрос сертификата. Вот снимок конфигурации, которая используется, который определяет эту туннельную группу (важные линии показывают в ***жирных курсивных шрифтах***):

```
rtpvpnoutbound6(config)# show run user
username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0

rtpvpnoutbound6# show run group-policy gp_certenroll
group-policy gp_certenroll internal
group-policy gp_certenroll attributes
wins-server none
dns-server value <dns-server-ip-address>

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value certenroll
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value acl_certenroll
default-domain value cisco.com
webvpn
anyconnect profiles value pro-sceplegacy type user

rtpvpnoutbound6# show run access-l acl_certenroll
access-list acl_certenroll remark to allow access to the CA server
access-list acl_certenroll standard permit host <ca-server-ipaddress>
```

```
rtpvpnoutbound6# show run all tun certenroll
tunnel-group certenroll type remote-access
tunnel-group certenroll general-attributes
address-pool ap_fw-policy
authentication-server-group LOCAL
secondary-authentication-server-group none
default-group-policy gp_certenroll
tunnel-group certenroll webvpn-attributes
authentication aaa
 group-alias certenroll enable
```

Вот клиентский профиль, который может или быть вставлен в файл Блокнота и импортирован в ASA, или это может быть настроено с Менеджером устройств адаптивной безопасности (ASDM) (ASDM) непосредственно:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
   <CertificateEnrollment>
 <AutomaticSCEPHost>rtpvpnoutbound6.cisco.com/certenroll</AutomaticSCEPHost>
 <CAURL PromptForChallengePW="false" >scep_url</CAURL>
 <CertificateImportStore>All</CertificateImportStore>
 <CertificateSCEP>
 <Name_CN>%USER%</Name_CN>
 <KeySize>2048</KeySize>
 <DisplayGetCertButton>true</DisplayGetCertButton>
 </CertificateSCEP>
 </CertificateEnrollment>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
 <ServerList>
 <HostEntry>
```

```
 <HostName>rtpvpnoutbound6.cisco.com</HostName>
 <HostAddress>rtpvpnoutbound6.cisco.com</HostAddress>
 </HostEntry>
 </ServerList>
</AnyConnectProfile>
```

> **Примечание:** URL группы не настроен для этой туннельной группы. Это важно, потому что Устаревший SCEP не работает с URL. Необходимо выбрать туннельную группу ее псевдонимом. Это вызвано тем, что идентификатора ошибки Cisco CSCtq74054. При испытании проблем из-за URL группы вы, возможно, должны были бы развить этот дефект.

Настройте туннель для аутентификации сертификата пользователя

Когда сертификат ID со знаком получен, соединение с проверкой подлинности сертификата возможно. Однако фактическая туннельная группа, которая используется для соединения еще не была настроена. Эта конфигурация подобна конфигурации для любого другого профиля подключения. Это условие синонимично с туннельной группой а не быть перепутанным с клиентским профилем, который использует проверку подлинности сертификата.

Вот снимок конфигурации, которая используется для этого туннеля:

```
rtpvpnoutbound6(config)# show run access-l acl_fw-policy

access-list acl_fw-policy standard permit 192.168.1.0 255.255.255.0

rtpvpnoutbound6(config)# show run group-p gp_legacyscep
group-policy gp_legacyscep internal
group-policy gp_legacyscep attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_fw-policy
default-domain value cisco.com
webvpn
anyconnect modules value dart

rtpvpnoutbound6(config)# show run tunnel tg_legacyscep
tunnel-group tg_legacyscep type remote-access
tunnel-group tg_legacyscep general-attributes
address-pool ap_fw-policy
 default-group-policy gp_legacyscep
tunnel-group tg_legacyscep webvpn-attributes
 authentication certificate
group-alias legacyscep enable
group-url https://rtpvpnoutbound6.cisco.com/legacyscep enable
```

Возобновите сертификат пользователя

Когда сертификат пользователя истекает или отозван, AnyConnect Cisco отказывает проверку подлинности сертификата. Единственная опция должна повторно соединиться с туннельной группой хранилища сертификатов для инициирования регистрации SCEP снова.

Проверка

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

> **Примечание:** Так как Устаревший метод SCEP должен только быть внедрен с использованием мобильных устройств, этот раздел только имеет дело с мобильными клиентами.

Выполните эти шаги для проверки конфигурации:

1. Когда вы попытаетесь соединиться впервые, введите имя хоста ASA или IP-адрес.
2. Выберите **certenroll** или псевдоним группы, который вы настроили в Настраивании Туннеля для раздела Использования Регистрации этого документа. Вам тогда предлагают для имени пользователя и пароля, и **получить** кнопка **сертификата** отображена.
3. Нажмите **получить** кнопку **сертификата**.

При проверке клиентских журналов эти выходные данные должны отобразиться:

```
[06-22-12 11:23:45:121] <Information> - Contacting https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:45:324] <Warning> - No valid certificates available for authentication.
[06-22-12 11:23:51:767] <Information> - Establishing VPN session...
[06-22-12 11:23:51:879] <Information> - Establishing VPN session...
[06-22-12 11:23:51:884] <Information> - Establishing VPN - Initiating connection...
[06-22-12 11:23:52:066] <Information> - Establishing VPN - Examining system...
[06-22-12 11:23:52:069] <Information> - Establishing VPN - Activating VPN adapter...
[06-22-12 11:23:52:594] <Information> - Establishing VPN - Configuring system...
[06-22-12 11:23:52:627] <Information> - Establishing VPN...
[06-22-12 11:23:52:734] <Information> - VPN session established to
https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:52:764] <Information> - Certificate Enrollment - Initiating, Please Wait.
[06-22-12 11:23:52:771] <Information> - Certificate Enrollment - Request forwarded.
[06-22-12 11:23:55:642] <Information> - Certificate Enrollment - Storing Certificate
[06-22-12 11:24:02:756] <Error> - Certificate Enrollment - Certificate successfully
imported. Please manually associate the certificate with your profile and reconnect.
```

Даже при том, что последнее сообщение показывает **ошибку**, это только, чтобы сообщить пользователю, что этот шаг необходим для того клиента использоваться для следующей попытки подключения, которая находится во втором профиле подключения, который настроен в Настраивании Туннеля для раздела Аутентификации Сертификата пользователя этого документа.

Дополнительные сведения

- CSCtq74054 SCEP не инициируется при использовании URL (псевдоним asa-IP/tunnel-group)
- Техническая поддержка и документация