Проверка CRL по HTTP на концентраторе Cisco VPN 3000

Содержание

Введение

Этот документ описывает, как включить проверку списка отозванных сертификатов (CRL) сертификаты центра сертификации (CA), установленные в Cisco VPN 3000 Concentrator с помощью режима HTTP.

Сертификат, как обычно ожидают, будет допустим для его всего периода достоверности. Однако, если сертификат становится недопустимом вследствие к таким вещам как изменение имени, изменение ассоциации между предметом и CA и компромиссом безопасности, CA отзывает сертификат. Под X.509 CAs отзывают сертификаты путем периодического запуска CRL со знаком, где каждый отозванный сертификат определен его серийным номером. Включение Проверки CRL означает, что каждый раз Концентратор VPN использует сертификат для аутентификации, это также проверяет CRL, чтобы гарантировать, что не был отозван проверяемый сертификат.

CAs используют Протокол LDAP / базы данных HTTP, чтобы сохранить и распределить CRL. Они могли бы также использовать другие средства, но Концентратор VPN полагается на доступ LDAP/HTTP.

Проверка CRL HTTP представлена в версии 3.6 Концентратора VPN или позже. Однако основанная на LDAP Проверка CRL была представлена в более раннем 3.x версии. Этот документ только обсуждает Проверку CRL с помощью HTTP.

Примечание: Размер кэша CRL Концентраторов серии VPN 3000 зависит от платформы, и это не может быть настроено согласно желанию администратора.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Вы успешно установили Туннель IPSec от VPN 3.x Аппаратные клиенты с помощью сертификатов для аутентификации Протокола IKE (без включенной Проверки CRL).
- Ваш Концентратор VPN имеет подключение к серверу CA в любом случае.
- Если ваш сервер CA связан с открытым интерфейсом, то вы открыли необходимые правила в общем фильтре (по умолчанию).

Используемые компоненты

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

- Версия 4.0.1 C VPN 3000 Concentrator
- VPN 3.x аппаратный клиент
- Microsoft CA server для генерации сертификата и Проверки CRL, работающей на Сервере Windows 2000.

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Схема сети

В настоящем документе используется следующая схема сети:

Настройка концентратора VPN 3000

Пошаговые инструкции

Для настройки концентратора VPN 3000 выполните следующие шаги:

1. Выберите **Administration> Certificate Management** для запроса сертификата, если у вас нет сертификата.Выберите **Click here для установки сертификата** для установки

корневого сертификата на Концентраторе VPN.
2. Выберите **Install CA certificate**.
3. Выберите **SCEP (Simple Certificate Enrollment Protocol)** для получения сертификатов CA.
4. От окна SCEP введите завершенный URL сервера CA в диалоговом окне URL.В данном примере IP-адрес сервера CA 172.18.124.96. Так как данный пример использует сервер CA Microsoft, завершенный URL является http://172.18.124.96/certsrv/mscep/mscep.dll. Затем, введите однословный дескриптор в диалоговое окно CA Descriptor. Данный пример использует CA.
5. Нажмите **Retrieve**.Ваш сертификат CA должен появиться под окном Administration> Certificate Management. Если вы не видите сертификат, вернитесь к Шагу 1 и выполните процедуру снова.
6. Как только у вас есть сертификат CA, выберите **Administration> Certificate Management> Enroll** и нажмите **Сертификат идентификации**.
7. Нажмите **Enroll via SCEP в...** для просьбы сертификата идентификации.
8. Выполните эти шаги для заполнения Регистрационной формы:Введите общее имя для Концентратора VPN, который будет использоваться в инфраструктуре открытого ключа (PKI) в поле Common Name (CN).Введите свой отдел в поле Organizational Unit (OU). OU должен совпасть с настроенным именем группы IPSec.Введите свою организацию или компанию в поле Organization (O).Введите свой город или город в поле Locality (L).Введите свое состояние или область в поле (SP) Состояния/Области.Введите свою страну в поле Country (C).Введите Полное доменное имя (FQDN) для Концентратора VPN, который будет использоваться в PKI в поле Fully Qualified Domain Name (FQDN).Введите адрес электронной почты для Концентратора VPN, который будет использоваться в PKI в Альтернативном имени субъекта (адрес электронной почты) поле.Введите пароль вызова для запроса сертификата в поле Challenge Password.Повторно введите пароль вызова в поле Verify Challenge Password.Выберите размер ключа для генерируемых Открытых и секретных ключей криптосистемы RSA от выпадающего списка Размера ключа.
9. Выберите **Enroll** и просмотрите Статус SCEP в состоянии последовательного опроса.
10. Перейдите к своему серверу CA для утверждения сертификата идентификации. Как только это утверждено на сервере CA, ваш Статус SCEP должен быть Установлен.
11. Под Управлением сертификатами необходимо видеть Сертификат идентификации.Если вы не делаете, проверьте вход в систему вашего сервера CA для большего количества устранения проблем.
12. Выберите **View** на своем полученном сертификате, чтобы видеть, имеет ли ваш сертификат CRL Distribution Point (CDP).CDP перечисляет все CRL Distribution Point от отправителя этого сертификата. Если у вас есть CDP на вашем сертификате, и вы используете имя DNS для передачи запроса к серверу CA, удостоверьтесь, что вам определили серверы DNS в вашем Концентраторе VPN для решения имени хоста с IP-адресом. В этом случае пример CA имя хоста сервера является jazib-pc, который решает к IP-адресу 172.18.124.96 на сервере DNS.
13. Нажмите **Configure** на своем сертификате CA для включения Проверки CRL на полученных сертификатах.Если бы у вас есть CDP на вашем полученном сертификате, и требуется использовать его, затем выбрать **Use CRL distribution points от проверяемого сертификата**.Так как система должна получить и исследовать CRL от сетевой точки распространения, разрешение Проверки CRL могло бы замедлить времена отклика системы. Кроме того, если сеть является медленной или

переполненной, Проверка CRL могла бы отказать. Позвольте CRL, кэширующемуся смягчить эти потенциальные проблемы. Это хранит полученные CRL в локальной временной памяти и поэтому позволяет Концентратору VPN проверять статус аннулирования сертификатов более быстро.С включенным кэшированием CRL, первые проверки Концентратора VPN, существует ли требуемый CRL в кэше и проверяет серийный номер сертификата против списка серийных номеров в CRL, когда это должно проверить статус аннулирования сертификата. Если его серийный номер найден, сертификат считают отозванным. Концентратор VPN получает CRL из внешнего сервера или когда он не находит требуемый CRL в кэше, когда период достоверности кэшируемого CRL истек, или когда истекло настроенное время обновления. Когда Концентратор VPN получает новый CRL от внешнего сервера, он обновляет кэш с новым CRL. Кэш может содержать до 64 CRL.**Примечание:** Кэш CRL существует в памяти. Поэтому перезагрузка Концентратора VPN очищает кэш CRL. Концентратор VPN повторно размещает кэш CRL с обновленными CRL, поскольку это обрабатывает новые запросы на проверку подлинности одноранговых узлов.Если вы выбираете **Use статические CRL Distribution Point**, то можно использовать до пяти статических CRL Distribution Point, как задано на этом окне. При выборе этой опции необходимо ввести по крайней мере один URL.Можно также выбрать **Use CRL distribution points от сертификата, проверяемого**, или выбрать **Use статические CRL Distribution Point**. Если Концентратор VPN не может найти пять CRL Distribution Point в сертификате, он добавляет статические CRL Distribution Point до предела пять. Если вы выбираете эту опцию, включаете по крайней мере один Протокол CRL Distribution Point. Также необходимо ввести по крайней мере один (и не больше, чем пять) статические CRL Distribution Point.Выберите **No CRL Checking**, если вы хотите отключить Проверку CRL.При Кэшировании CRL выберите **Включенную** коробку, чтобы позволить Концентратору VPN кэшировать полученные CRL. По умолчанию не должен включать кэширование CRL. При отключении кэширования CRL (отменяйте коробку), кэш CRL очищен.Если вы настроили политику извлечения CRL, которая использует CRL Distribution Point от проверяемого сертификата, выберите протокол точки распространения для использования для получения CRL. Выберите **HTTP** в этом случае для получения CRL. Назначьте правила HTTP на фильтр открытого интерфейса, если ваш сервер CA находится к открытому интерфейсу.

Мониторинг

Выберите **Administration> Certificate Management** и нажмите **выставленный для обозрения Все кэши CRL**, чтобы видеть, кэшировал ли ваш Концентратор VPN какие-либо CRL от сервера CA.

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Журналы от концентратора

Включите эти события на Концентраторе VPN, чтобы удостовериться, что работает Проверка CRL.

1. Выберите **Configuration> System> Events> Classes** для установки уровней регистрации.
2. Под Именем класса выбирают **IKE**, **IKEDBG**, **IPSEC**, **IPSECDBG** или **CERT**.
3. Нажмите **Add** или **Modify**, и выберите **Степени серьезности ошибки к опции 1-13 Log**.
4. Нажмите **Apply**, если вы хотите модифицировать или **Добавить**, хотите ли вы добавить новую запись.

Журнал успешных событий концентратора

Если ваша Проверка CRL успешна, эти сообщения замечены в Журналах событий с фильтрацией.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1 Certificate has not been revoked: session = 2
1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1 CERT_Callback(62f56e8, 0, 0) 1320 08/15/2002
13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53 Group [ipsecgroup] Validation of certificate
successful (CN=client_cert, SN=61521511000000000086)
```

См. Успешные Журналы Концентратора для завершения вывода успешного журнала концентратора.

Отказавшие журналы

Если ваша Проверка CRL в не успешный, эти сообщения замечены в Журналах событий с фильтрацией.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2 Failed to retrieve revocation list: session = 5
1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2 CRL retrieval over HTTP has failed. Please
make sure that proper filter rules have been configured. 1335 08/15/2002 18:00:36.730 SEV=7
CERT/8 RPT=2 Error processing revocation list: session = 5, reason = Failed to retrieve CRL from
the server.
```

См. Журналы отозванных концентраторов для завершения вывода отказавшего журнала концентратора.

См. Успешные Клиентские Журналы для завершения вывода успешного клиентского журнала.

См. Журналы отозванных клиентов для завершения вывода отказавшего клиентского журнала.

Устранение неполадок

См. Устранение проблем Проблем с подключением на VPN 3000 Concentrator для большего количества сведений об устранении проблем.

Дополнительные сведения

- Страница поддержки концентраторов Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Client
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация