Содержание

Введение

Этот документ описывает ситуацию сбоя с широкомасштабной Cisco развертывания IOS® Certificate Server Public Key Infrastructure (PKI) и его потенциальное смягчение путем корректной настройки конфигураций event timer PKI.

Проблема

Пользовательские признаки

Эта проблема может быть замечена в крупномасштабной среде PKI, где Центр регистрации (RA) Cisco IOS настроен для обслуживания сотен и иногда тысяч устройств клиента PKI. Когда этот определенный отказ происходит, хранилище сертификатов от клиентов PKI могло бы отказать или периодически или последовательно.

На клиентах PKI вероятно, что могли бы быть замечены эти сообщения журнала:

После включения этих отладок PKI:

замечено, что запросы клиента сертификат одновременного нажатия клавиш сервера Центра сертификации (CA), но вместо этого получает " HTTP 404 Не Найденное" сообщение об ошибках от сервера CA.

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3
```

```
Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3



Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

> **Примечание:** Когда RA не используется (CA только), эта проблема не является определенным RA и может также произойти.

Устранение неполадок и распознавание ошибки

Один из ключевых признаков, наблюдаемых в сбое, - то, что существует много запросов PKI на RA, который прибывает от клиентов PKI. Это может быть замечено или с NetFlow или с выходными данными захвата пакета. Сумма запросов PKI может сокрушить сервер так, чтобы это не могло ответить достаточно быстро. Один способ проверить это условие к telnet к серверу CA на порте HTTP, который это слушает. Когда сервис слушает на порту и отвечает, необходимо видеть, что открывается соединение. В неисправном состоянии, таймауты попытки telnet, который указывает, что TCP даже не заканчивает трехстороннее квитирование.

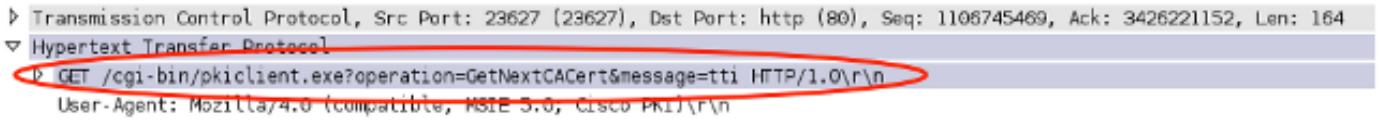
Чтобы лучше понять, почему TCP отказывает, войдите**, транзакции tcp ip отладки обращаются** к команде **<tcp_peer_address>** на сервере для получения понимания обработки сервера потоков TCP к определенному адресу источника TCP (важно задать фильтр адреса при отладке крупномасштабной среды). В неисправном состоянии наблюдаются эти отладки:

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
```

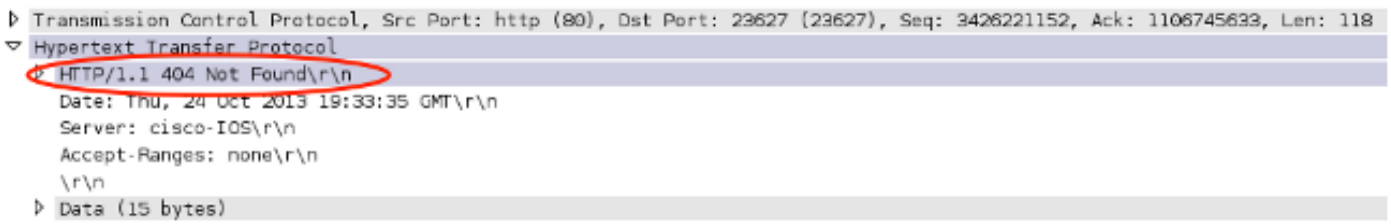
```
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

Совет: В Версиях 15.1 и 15.2 **команда debug ip tcp transactions** не имеет опции адресации на нем. Вместо этой команды введите **пакетный адрес tcp ip отладки <tcp_peer_address**, чтобы также показать, достигнут ли предел очереди подключения.

Захват пакета для запросов PKI может также помочь показывать дополнительные сведения о том, каковы эти запросы PKI. От захвата пакета вы видите большое число запросов, подобных:



Для некоторых из этих запросов, что сервер может фактически ответить на, вы также видите "404 Не Найденный" ответ:



Основная причина

Существует несколько факторов, которые способствуют этой конкретной проблеме. Во-первых, GetNextCACert показывает, что эти запросы PKI являются запросами одновременного нажатия клавиш от клиентов запросить на сертификат CA одновременного нажатия клавиш/тени. Для получения дополнительной информации на операции одновременного нажатия клавиш CA, посмотрите Автоматическую регистрацию PKI IOS, Auto-Rollover и Таймеры. "404 Не Найденный" ответ указывает, что сервер RA/CA не мог бы иметь теневого сертификата во время запроса. Это может быть проверено с **показом крипто-**выходные данные команды **сертификата pki** на серверах RA и CA. Проблема происходит из-за этой конфигурации таймера сертификата, найденной на Сервере pki и клиенте:

Сервер RA/CA

```
CA-Server#show running | section pki server
crypto pki server ca-server
<snip>
lifetime certificate 600
lifetime ca-certificate 1825
auto-rolloverCA-Server#show crypto pki server | include Rollover
Auto-Rollover configured, overlap period 30 days
CA-Server#
```

Клиенты PKI

```
crypto pki trustpoint test enroll url http://enrollment_url.test.com:80
enrollment mode ra subject-name OU = TEST OU, OU = cisco auto-enroll 70
```

Проблема состоит в том, что время законности сертификата CA настроено, чтобы быть 5 годами (1825 дней), но сертификат одновременного нажатия клавиш/тени не становится созданным на сервере CA до 30 дней до текущего истечения сертификата. Сертификаты маршрутизатора имеют 600-дневное время законности, и на основе конфигурации автоматической регистрации, маршрутизатор мог запросить сертификат одновременного нажатия клавиш/тени после 70% 600-дневного срока действия. Это могло быть уже в 180 днях перед текущим временем окончания срока действия сертификата CA. Для подробного вычисления этих времен и пояснения событий PKI, снова обратитесь к Автоматической регистрации PKI IOS, Auto-Rollover и Таймерам. Это объясняет, почему клиенты продолжают запрашивать одновременное нажатие клавиш/тень CA и продолжать получать "404 Не Найденная" ошибка, так как они еще не созданы на сервере. Это условие сохраняется, пока сертификат одновременного нажатия клавиш/тени CA не генерируется.

Тем временем, из-за большого количества запросов, которые входят в сервер RA, Cisco IOS, сервер RA может превысить этот порог соединения HTTP и начать отбрасывать входящие запросы соединения HTTP:

- Максимальный HTTP параллельный предел подключений к серверу. Это может быть изменено максимум на 16 параллельных соединений с **ip http max-connections 16** команд.
- Внутренний предел скорости подключения сервера HTTP 80 соединений в минуту. Когда этот порог достигнут, theCiscoIOS сервер HTTP возвращает к исходному

состоянию и прекращает слушать новые запросы HTTP в течение 15 секунд. В настоящее время этот порог ограничения скорости не конфигурируем пользователем. В результате theTCP "предел очереди подключения, достигнутый" ошибка, замечен с theTCP отладками транзакции.

> **Примечание:** В настоящее время вышеупомянутый порог не может быть проверен с Командой Cisco IOS. Запрос на расширение был открыт для улучшения этого, посмотрите идентификатор ошибки Cisco CSCuj83430.

Решение

Решение этой проблемы состоит в том, чтобы исправить конфигурации event timer PKI на сервере CA, таким образом, что сертификат одновременного нажатия клавиш/тени генерируется до любого запроса одновременного нажатия клавиш клиента PKI. Это может быть сделано с этими шагами:

1. Введите **команду shutdown** под crypto PKI server command.in заказ отключить сервер CA.
2. Увеличьте время наложения одновременного нажатия клавиш на основе срока действия сертификата и конфигурации перерегистрации:

```
CA-Server(config)#crypto pki server ca-server
CA-Server(cs-server)#auto-rollover ?
<0-1825> Overlap time between CA certificates during rollover, in days
<cr>
CA-Server(cs-server)#auto-rollover 365
```

3. Реактивируйте сервер CA.
4. Если существует anRA, вручную одновременное нажатие клавиш там для получения сертификата одновременного нажатия клавиш/тени.

> **Совет:** Для принуждения CA к одновременному нажатию клавиш вручную, не включая auto-rollover, введите **crypto pki server <имя сервера> команда rollover**.

Кроме того, как было указано выше рекомендуется увеличить предел параллельного соединения максимума HTTP 16 для сервера для обработки высокой скорости входящего соединения.