IOS PKI 자동 등록, 자동 롤오버 및 타이머

목차

소개

이 문서에서는 자동 등록 및 자동 롤오버 작업의 Cisco IOS® PKI(Public Key Infrastructure) 작업 및 이러한 작업에 대해 각 PKI 타이머가 계산되는 방법에 대해 설명합니다.

인증서는 일정한 수명을 가지며 특정 시점에 만료됩니다.인증서가 VPN 솔루션에 대한 인증 목적으로 사용되는 경우(예:) 이러한 인증서가 만료되면 엔드포인트 간의 VPN 연결이 끊어질 수 있는 인증 오류가 발생합니다.이 문제를 방지하기 위해 다음 두 가지 메커니즘을 자동 인증서 갱신에 사용할 수 있습니다.

- 클라이언트/스포크 라우터의 자동 등록
- CA(인증 기관) 서버 라우터의 자동 롤오버

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PKI와 신뢰의 개념
- 라우터에서 CA의 기본 컨피그레이션

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

용어

자동 등록

엔드 디바이스의 인증서가 곧 만료될 예정이면 자동 등록은 중단 없이 새 인증서를 가져옵니다.자동 등록이 구성된 경우 클라이언트/스포크 라우터는 자체 인증서(ID 또는 ID 인증서라고도 함)가 만료되기 전에 언제든지 새 인증서를 요청할 수 있습니다.

자동 롤오버

이 매개변수는 CS(Certificate Server)가 롤오버(섀도우) 인증서를 생성하는 시기를 결정합니다.인수 없이 CS 구성 아래에 명령을 입력하면 기본 시간은 30일입니다.

> **참고:**이 문서의 예에서 이 매개 변수의 값은 *10분입니다*.

CA 서버의 인증서가 곧 만료될 경우 자동 롤오버를 통해 CA는 중단 없이 새 인증서를 얻을 수 있습니다.자동 롤오버가 구성된 경우 CA 라우터는 자체 인증서가 만료되기 전에 언제든지 새 인증서를 생성할 수 있습니다.*섀도* 또는 *롤오버* 인증서라고 하는 새 인증서는 현재 CA 인증서가 만료되는 정확한 시점에 활성화됩니다.

이 문서의 Introduction(소개) 섹션에 언급된 두 가지 기능을 사용하면 PKI 구축이 자동화되고 스포크 또는 클라이언트 디바이스에서 현재 CA 인증서 만료 전에 섀도/롤오버 ID 인증서 및 섀도우/롤오버 CA 인증서를 얻을 수 있습니다.이렇게 하면 현재 ID 및 CA 인증서가 만료될 때 새 ID 및 CA 인증서로 중단 없이 전환할 수 있습니다.

수명 ca 인증서

이 매개변수는 CA 인증서의 수명을 지정합니다.이 매개변수의 값은 일/시/분 단위로 지정할 수 있습니다.

> **참고**: 이 문서의 예에서 이 매개변수의 값은 *30분입니다*.

수명 인증서

이 매개변수는 CA 라우터에서 발급되는 ID 인증서의 수명을 지정합니다.이 매개변수의 값은 일/시/분 단위로 지정할 수 있습니다.

> **참고**: 이 문서의 예에서 이 매개변수의 값은 *20분입니다.*

구성

> **참고**: *수명*, *자동 롤오버* 및 *자동 등록*에 대한 더 작은 PKI 타이머 값은 이 문서에서 주요 자동 등록 및 자동 롤오버 개념을 설명하기 위해 사용됩니다.라이브 네트워크 환경에서는 이러한

매개변수에 기본 수명을 사용하는 것이 좋습니다.

팁: *롤오버* 및 재등록과 같은 모든 PKI 타이머 기반 이벤트는 권한 있는 시간 소스가 없는 경우 영향을 받을 수 있습니다.따라서 PKI를 수행하는 모든 라우터에서 NTP(Network Time Protocol)를 구성하는 것이 좋습니다.

Cisco IOS CA 서버 컨피그레이션

이 섹션에서는 Cisco IOS CA 서버의 컨피그레이션 예를 제공합니다.

```
RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up

crypto pki server ios-ca
issuer-name CN=Root-CA,OU=TAC,C=IN
grant auto
hash sha512
lifetime certificate 0 0 20
lifetime ca-certificate 0 0 30
cdp-url http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
auto-rollover 0 0 10
database url flash:
```

참고: 자동 **롤오버** 명령으로 지정된 값은 *현재 CA 인증서*의 종료 날짜*가* 롤오버 인증서가 생성되기 *전의 일*/시간/분 수입니다.따라서 CA 인증서가 12:00부터 12:30까지 유효한 경우 **자동 롤오버 0 0 10은 롤오버** CA 인증서가 약 12:20에 생성됨을 의미합니다.

Cisco IOS CA 서버에서 컨피그레이션**을** 확인하려면 show crypto pki certificate 명령을 입력합니다.

```
RootCA#show crypto pki certificate
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

이 출력에 따라 라우터는 2012년 11월 25일 9:16~9:46 IST에 유효한 CA 인증서를 포함합니다.자동 롤오버가 10분 동안 구성되므로 섀도우/롤오버 인증서는 2012년 11월 25일 *9.36 IST*에 의해 생성될 것으로 예상됩니다.

확인하려면 show crypto pki **timer** 명령**을** 입력합니다.

```
RootCA#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:22.283 IST Sun Nov 25 2012
PKI Timers
| 12:50.930
| 12:50.930 SESSION CLEANUP
CS Timers
| 16:43.558
| 16:43.558  CS SHADOW CERT GENERATION
| 26:43.532 CS CERT EXPIRE
| 26:43.558 CS CRL UPDATE
```

이 출력에 따라 **show crypto pki timer** 명령이 9.19 IST에서 실행되었으며 shadow/rollover 인증서가 16.43분 내에 생성될 것으로 예상됩니다.

[09:19:22 + 00:16:43] = **09:36:05**, 즉 [end-date_of_current_CA_cert - auto_rollover_timer];즉, [09:46:05 - 00:10:00] = **09:36:05**.

클라이언트/스포크 라우터 컨피그레이션

이 섹션에서는 클라이언트/스포크 라우터의 컨피그레이션 예를 제공합니다.

```
Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up

crypto pki trustpoint client1
enrollment url http://10.1.1.1:80
subject-name CN=Client-1,OU=TAC,c=IN
revocation-check crl
auto-enroll 70 regenerate
```

> **참고**: **auto-enroll** 명령은 라우터에서 자동 등록 기능을 활성화합니다. 명령 구문은 **auto-enroll** [*val%*] [regenerate*]입니다*.

이전 출력에서 자동 등록 기능은 70%로 지정됩니다.즉, **[**lifetime of current_**ID_cert]의** 70%에 라우터가 CA와 함께 자동으로 등록됩니다.

> **팁**: PKI 타이머가 제대로 작동하도록 자동 등록 값을 60% 이상으로 설정하는 것이 좋습니다.

재생성 옵션은 인증서 재등록/갱신 목적으로 새로운 RSA(Rivest-Shamir-Addleman) 키를 생성하는 것입니다.이 옵션을 지정하지 않으면 현재 RSA 키가 사용됩니다.

실제 자동 등록

자동 등록 기능을 확인하려면 다음 단계를 완료하십시오.

1. 클라이언트 라우터에서 **신뢰 지점을** 수동으로 인증하려면 crypto pki authenticate 명령을 입력합니다.

```
Client-1(config)#crypto pki authenticate client1
```

참고:이 명령에 대한 자세한 내용은 Cisco IOS Security 명령 참조를 참조하십시오.
명령을 입력하면 다음과 유사한 출력이 표시됩니다.

```
Certificate has the following attributes:
Fingerprint MD5: 006B2E44 37FBC3F1 AA14F32B CDC4462E
Fingerprint SHA1: 2999CC53 8BF65247 C0D704E9 FDC73002 A33910D4

% Do you accept this certificate? [yes/no]:
```

2. 클라이언트 라우터에서 CA 인증서를 수락하려면 **yes**를 입력합니다.그런 다음 **RENEW** 타이머가 라우터에서 시작됩니다.

```
Client-1#show crypto pki timer
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. RENEW 타이머가 0에 도달하면 클라이언트 라우터는 ID 인증서를 얻기 위해 자동으로 CA에 등록됩니다.인증서가 수신되면 **show crypto pki certificate** 명령을 입력하여 확인합니다.

```
Client-1#show crypto pki certificate
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:16:57 IST Nov 25 2012
end date: 09:36:57 IST Nov 25 2012
renew date: 09:30:08 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

```
Associated Trustpoints: client1
```

갱신 **날짜**는 **09:30:08**이며 다음과 같이 계산됩니다.

시작 시간 + (%renewal of ID_cert_lifetime)

또는

09:16:57 + (70% * 20분) = **09:30:08**

PKI 타이머는 다음을 반영합니다.

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:01.714 IST Sun Nov 25 2012
PKI Timers
| 1:21.790
| 1:21.790 SESSION CLEANUP
| 11:06.894  RENEW client1
```

4. RENEW 타이머가 만료되면 라우터는 새 ID 인증서를 얻기 위해 CA와 함께 다시 등록합니다.인증서 갱신이 발생한 후 새 ID 인증서를 보려면 **show crypto pki cert** 명령을 입력합니다.

```
Client-1#show crypto pki cert
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:55.063 IST Sun Nov 25 2012
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
```

```
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

더 이상 *갱신 날짜*가 없습니다.대신 **SHADOW** 타이머가 시작됩니다.

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

프로세스 로직은 다음과 같습니다.

- **ID** 인증서의 종료 날짜가 **CA 인증서**의 종료 날짜와 같지 **않은** 경우 **자동 등록 백분율을 기준으로 갱신 날짜를 계산하고 RENEW 타이머를 시작합니다.**
- **ID** 인증서의 종료 날짜가 **CA** 인증서의 종료 날짜와 같으면 현재 CA 인증서가 유효한 경우에만 현재 ID 인증서가 유효하기 때문에 갱신 프로세스가 필요하지 않습니다.대신 **SHADOW** 타이머가 시작됩니다.

이 타이머는 **auto-enroll** 명령에 언급된 백분율을 기반으로 계산됩니다.예를 들어, 이전 예에 표시된 갱신된 ID 인증서의 유효 일자를 고려하십시오.

```
Validity Date of current ID cert:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

이 인증서의 수명은 16분입니다.따라서 롤오버 타이머(즉, SHADOW 타이머)는 16분의 70%이며, 이는 약 11분에 해당합니다.이 계산은 라우터가 이전에 이 문서에 표시된 PKI 섀도우 타이머에 해당하는 [09:30:09 + 00:11:00] = 09:41:09에 섀도/롤오버 인증서에 대한 요청을 시작함을 의미합니다.

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922 IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618  SHADOW client1
```

자동 롤오버 실행

이 섹션에서는 작동 중인 자동 롤오버 기능에 대해 설명합니다.

Cisco IOS CA 서버에서

SHADOW 타이머가 만료되면 롤오버 인증서가 CA 라우터에 나타납니다.

```
RootCA#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:36:28.184 IST Sun Nov 25 2012
CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
 start date: 09:46:05 IST Nov 25 2012
end   date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

클라이언트 라우터에서

이 문서에서 앞서 설명한 대로 자동 등록 기능은 클라이언트 라우터에서 섀도우 타이머를 시작했습니다.SHADOW 타이머가 만료되면 자동 등록 기능을 사용하면 라우터가 *롤오버/섀도우 CA* 인증서에 대해 CA 서버를 요청할 수 있습니다.수신되면 롤오버/*섀도우 ID* 인증서도 쿼리합니다.결과적으로 라우터에는 두 쌍의 인증서가 있습니다.현재 쌍 및 롤오버/섀도우 인증서가 포함된 다른 쌍:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
```

```
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1
```

CA Certificate (Rollover)

```
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Certificate

```
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

CA Certificate

```
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

롤오버 ID 인증서의 유효성을 확인합니다.

```
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

인증서 수명은 단 4분(Cisco IOS CA 서버에 구성된 예상 20분 대신). Cisco IOS CA 서버당 *절대* ID 인증서 수명은 20분(즉, 지정된 클라이언트 라우터의 경우 발급된 ID 인증서(현재 + 섀도)의 수명 합계는 20분 이하여야 함)이어야 합니다.

이 프로세스는 여기에서 자세히 설명합니다.

- 다음은 라우터에 있는 현재 ID 인증서의 유효성입니다.

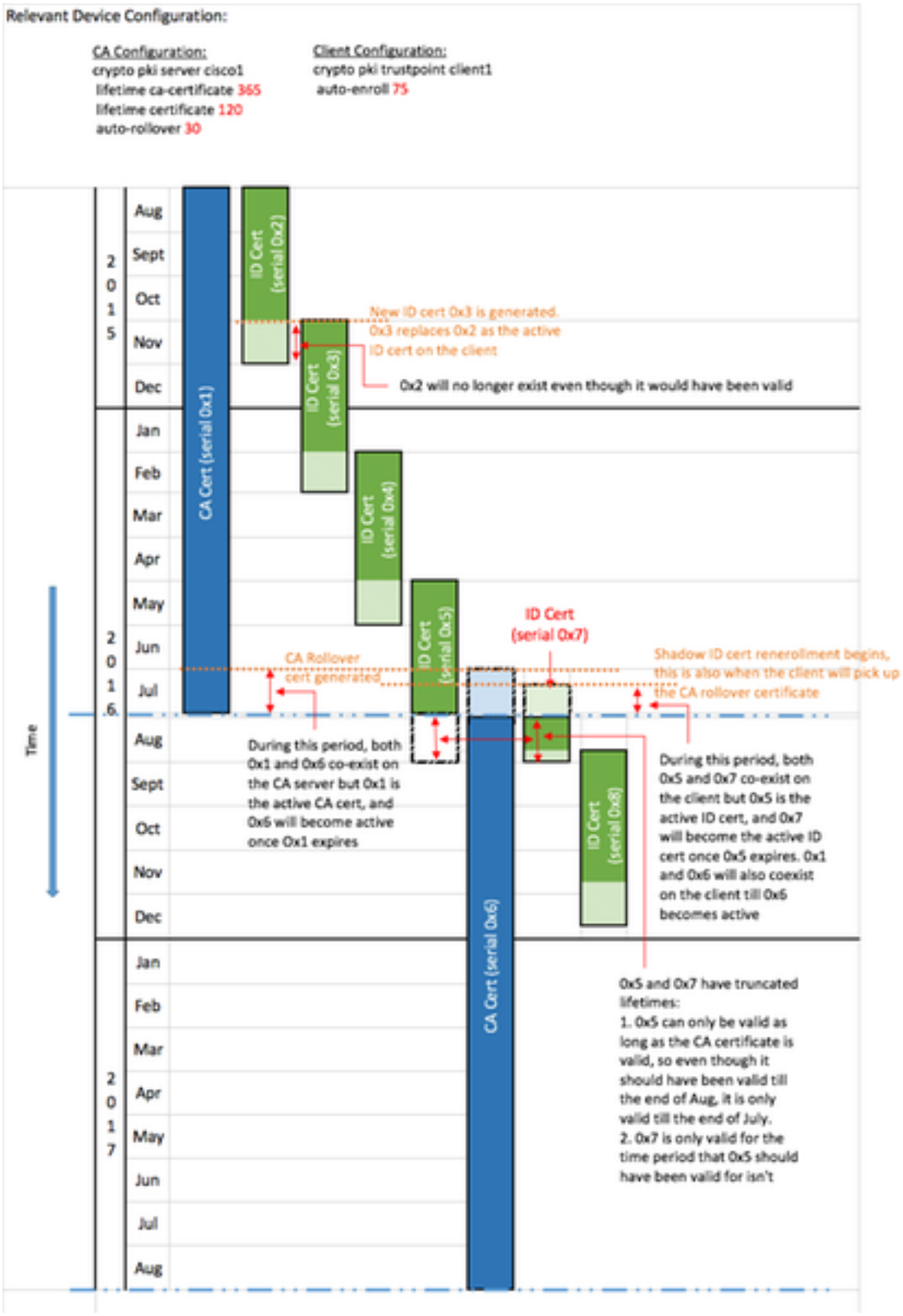
  ```
  start date: 09:30:09 IST Nov 25 2012
  end date: 09:46:05 IST Nov 25 2012
  ```

  따라서 *current_id_cert_lifetime*은 16분입니다.
- 다음은 롤오버 ID 인증서의 유효 기간입니다.

  ```
  start date: 09:46:05 IST Nov 25 2012
  end date: 09:50:09 IST Nov 25 2012
  ```

  따라서 *롤오버_id_cert_lifetime*은 4분입니다.
- Cisco IOS에 따라 [current_id_cert_lifetime]이(가) [rollover_id_cert_lifetime]에 추가될 때 [total_id_cert_lifetime]과(와) 같아야 합니다.이것은 이 경우에 사실이다.

롤오버 및 등록이 포함된 샘플 PKI 타임라인



중요 고려 사항

- PKI 타이머가 제대로 작동하려면 신뢰할 수 있는 시계가 필요합니다.클라이언트 라우터와 Cisco IOS CA 라우터 간에 클럭을 동기화하려면 NTP를 사용하는 것이 좋습니다.NTP가 없는 경우 라우터의 시스템/하드웨어 시계를 사용할 수 있습니다.하드웨어 시계를 구성하고 이를 신뢰할 수 있게 만드는 방법에 대한 자세한 내용은 Basic System Management Configuration Guide, Cisco IOS Release 12.4T를 참조하십시오.

- 라우터가 다시 로드되면 NTP를 동기화하는 데 몇 분 정도 걸립니다.그러나 PKI 타이머는 거의

즉시 설정됩니다.버전 15.2(3.8)T 및 15.2(4)S부터 PKI 타이머는 NTP가 동기화된 후 자동으로 재평가됩니다.

- PKI 타이머는 절대 상태가 아닙니다.*남은 시간*을 기반으로 하므로 재부팅 후 다시 계산됩니다.예를 들어, 클라이언트 라우터에 100일 동안 유효한 ID 인증서가 있고 자동 등록 기능이 80%로 설정되어 있다고 가정합니다.그런 다음 재등록이 80일 이후에 이루어질 것으로 예상됩니다.라우터가 60일에 다시 로드되면 다음과 같이 부팅되고 PKI 타이머를 다시 계산합니다. (*남은 시간*) * (*%auto-enroll*) = (100-60) * 80% = 32일

  따라서 재등록은 [60 + 32] = 92일에 발생합니다.

- 자동 등록 및 자동 롤오버타이머를 구성할 때 PKI 클라이언트가 요청을 할 때 PKI 서버에서 SHADOW CA 인증서 가용성을 허용하는 값으로 구성하는 것이 중요합니다.이를 통해 대규모 환경에서 잠재적인 PKI 서비스 장애를 줄일 수 있습니다.

관련 정보

- 공개 키 인프라로 Cisco IOS 보안 구축 백서
- 공개 키 인프라:구축 혜택 및 기능 백서
- 공개 키 인프라 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems