Introduction

This document describes a failure situation with a large scale Cisco IOS® Certificate Server Public Key Infrastructure (PKI) deployment and its potential mitigation by correctly tuning the PKI event timer configurations.

Problem

User Symptoms

This problem can be seen in a large-scale PKI environment where a Cisco IOS Registration Authority (RA) is configured to service hundreds and sometimes thousands of PKI client devices. When this particular failure occurs, certificate enrollment from PKI clients might fail either intermittently or consistently.

On the PKI clients it is likely that these log messages might be seen:

*Dec 30 15:37:46.996: CRYPTO_PKI: Socket timeout
*Dec 30 15:40:47.929: %PKI-3-SOCKETSEND: Failed to send out message to CA server.

After you enable these PKI debugs:

d debug crypto pki message
d debug crypto pki validation

it is seen that the client requests the Certificate Authority (CA) server rollover certificate, but instead receives an "HTTP 404 Not Found" error message from the CA server.
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: 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

Note: This issue is not RA specific and can also happen when an RA is not used (CA only).

Troubleshoot and Problem Identification

One of the key symptoms observed in the failure is that there are a lot of PKI requests on the RA that come from the PKI clients. This can be seen with either NetFlow or packet capture outputs. The amount of PKI requests can overwhelm the server so that it cannot respond quickly enough. One way to verify this condition is to telnet to the CA server on the HTTP port that it is listening to. When the service listens on the port and responds, you should see the connection open. In the failed state, the telnet attempt times out which indicates that TCP does not even finish the 3-way handshake.

In order to better understand why TCP fails, enter the `debug ip tcp transactions address <tcp_peer_address>` command on the server in order to gain insights into the server's handling of TCP flows to a particular TCP source address (it is important to specify the address filter when you debug a large-scale environment). In the failed state, these debugs are observed:

TCP0: bad seg from x.x.x.x -- connection queue limit reached:
port 80 seq 1276472961 ack 0 rcvnx 0 rcvwnd 4128 len 0
TCP0: bad seg from x.x.x.x -- connection queue limit reached:
port 80 seq 1276472961 ack 0 rcvnx 0 rcvwnd 4128 len 0
TCP0: bad seg from x.x.x.x -- connection queue limit reached:
Tip: In Versions 15.1 and 15.2 the **debug ip tcp transactions** command does not have an address option on it. In place of this command, enter the **debug ip tcp packet address <tcp_peer_address>** in order to also show if the connection queue limit is reached.

A packet capture for the PKI requests can also help reveal additional information about what these PKI requests are. From the packet capture, you can see an large number of requests similar to:

```

Hypertext Transfer Protocol
GET /cgi-bin/pkclient.exe?operation=GetNextCACert&message=tftp://T01.0/0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
```

For some of these requests that the server can actually respond to, you also see a "404 Not Found" response:

```

Hypertext Transfer Protocol
404 Not Found
```

**Root Cause**

There are a few factors that contribute to this particular problem. First, the GetNextCACert shows that these PKI requests are rollover requests from the clients to request for a rollover/shadow CA certificate. For more details on the CA rollover operation, see **IOS PKI Auto-Enroll, Auto-Rollover, and Timers**. The "404 Not Found" response indicates that the RA/CA server might not have the shadow certificate at the time of the request. This can be verified with the **show crypto pki certificate** command output on the CA and RA servers. The problem is due to this certificate timer configuration found on the PKI server and client:

**RA/CA Server**

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

**PKI Clients**

```
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
```
The problem is that the CA certificate validity time is configured to be 5 years (1825 days), but the rollover/shadow certificate does not get created on the CA server until 30 days prior to the current certificate expiry. The router certificates have a 600 day validity time, and based on the auto-enroll configuration, the router could request a rollover/shadow certificate after 70% of the 600 day lifetime. This could be as early as 180 days before the current CA certificate expiration time. For a detailed calculation of these times and explanation of the PKI events, again refer to IOS PKI Auto-Enroll, Auto-Rollover, and Timers. This explains why the clients continue to request the CA rollover/shadow, and continue to receive the "404 Not Found" error since they are not created on the server yet. This condition persists until the CA rollover/shadow certificate is generated.

In the meantime, due to the large amount of requests that come into the RA server, the Cisco IOS RA server can exceed this HTTP connection threshold and start to drop incoming HTTP connection requests:

- The maximum HTTP concurrent server connections limit. This can be changed to a maximum of 16 concurrent connections with the `ip http max-connections 16` command.
- The internal HTTP server connection rate limit of 80 connections per minute. When this threshold is reached, the Cisco IOS HTTP server throttles back and stops listening to new HTTP requests for 15 seconds. Currently, this rate limit threshold is not user configurable. As a result, the TCP "connection queue limit reached" error is seen with the TCP transaction debugs.

  **Note:** Currently the above threshold cannot be monitored with a Cisco IOS command. An enhancement request has been opened to improve this, see Cisco bug ID CSCuj83430.

**Solution**

The solution to this problem is to correct the PKI event timer configurations on the CA server such that a rollover/shadow certificate is generated prior to any PKI client rollover request. This can be done with these steps:

1. Enter the **shutdown** command under the crypto PKI server command in order to disable the CA server.
2. Increase the rollover overlap time based on the certificate lifetime and reenrollment configuration:

   ```
   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. Reenable the CA server.
4. If there is an RA, manually rollover the RA to retrieve the rollover/shadow certificate.

  **Tip:** In order to force the CA to rollover manually without enabling auto-rollover, enter the `crypto pki server <server-name> rollover` command.
Also, as discussed previously, it is recommended to increase the HTTP maximum concurrent connection limit to 16 in order for the server to handle a high incoming connection rate.