Проверка действительности сертификата веб-сервера

Веб-браузер может отказаться устанавливать HTTPS-соединение с веб-сервером, если проверка сертификата сервера показала его недействительность, а именно:

- выдавший его сертификационный центр не является доверенным, то есть не входит в иерархию ни одного из доверенных корневых центров;
- срок действия сертификата истек;
- имя сервера, набранного пользователем, не совпадает ни с одним из доменным именем сервера, фигурирующим в сертификате.

Браузер обычно уведомляет пользователя о том, что сертификат сервера по какой-то причине является недействительным, оставляя на усмотрение пользователя окончательное решение – отказаться от соединения или все же установить его. Иногда сложный механизм проверки аутентичности сервера работает вхолостую, потому что пользователи недооценивают угрозы со стороны «невыясненных» веб-серверов и предпочитают действовать на свой страх и риск.

Ситуацию с недействительным сертификатом веб-сервера легко промоделировать в учебных целях, чтобы посмотреть на поведение своего браузера в таких ситуациях. Вы можете проделать это, задав имя какого-нибудь веб-сервера, поддерживающего HTTPS соединения, в усеченном виде, то есть без имени самого сайта, а только его старшую часть, относящуюся к имени домена. Например, мы сделали это с сайтом компании Cisco, обратившись к нему так: https://cisco.com.

Результат такого запроса показан на рис. 8.6. Браузер Safari предупреждает, что сайт претендует на то, чтобы быть сайтом «cisco.com», хотя и имеет другой имя, www.cisco.com. Действительно, видно, что компания Cisco получила сертификат на имя www.cisco.com, которое фигурирует в параметре Common Name. Дальнейший просмотр сертификата показывает, что вообще-то специалисты Cisco понимали, что пользователи могут интересоваться различными сайтами Cisco, имеющими имена, отличные от www.cisco.com, и поэтому поместили их в расширение сертификата, описывающее альтернативные имена сайта (рис. 8.7). В этот список попали: www1.cisco.com, www2.cisco.com, www3.cisco.com, www.static-cisco.com, www-rtp.cisco.com и cisco-images.cisco.com, однако имени cisco.com среди них нет, поэтому браузер и не признал сертификат за действительный.

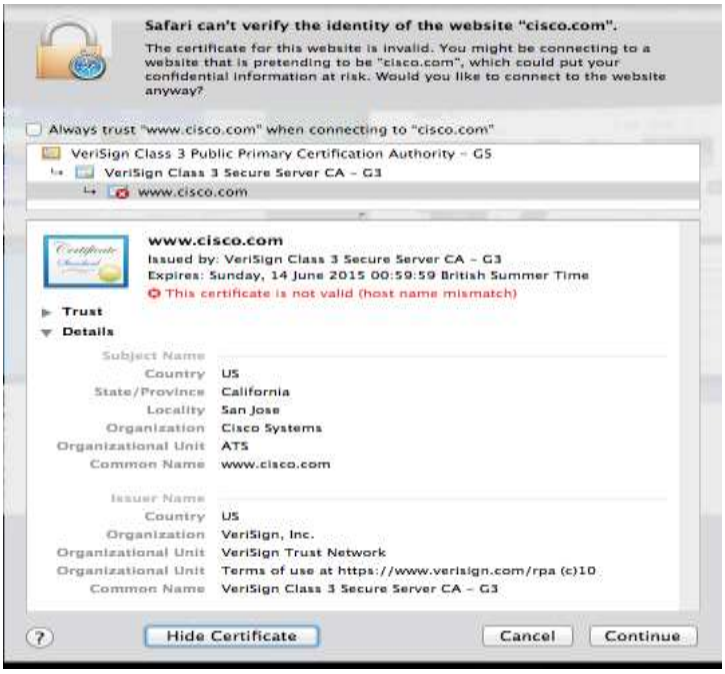

Рис. 8.6. «Недействительный» сертификат сайта cisco.com

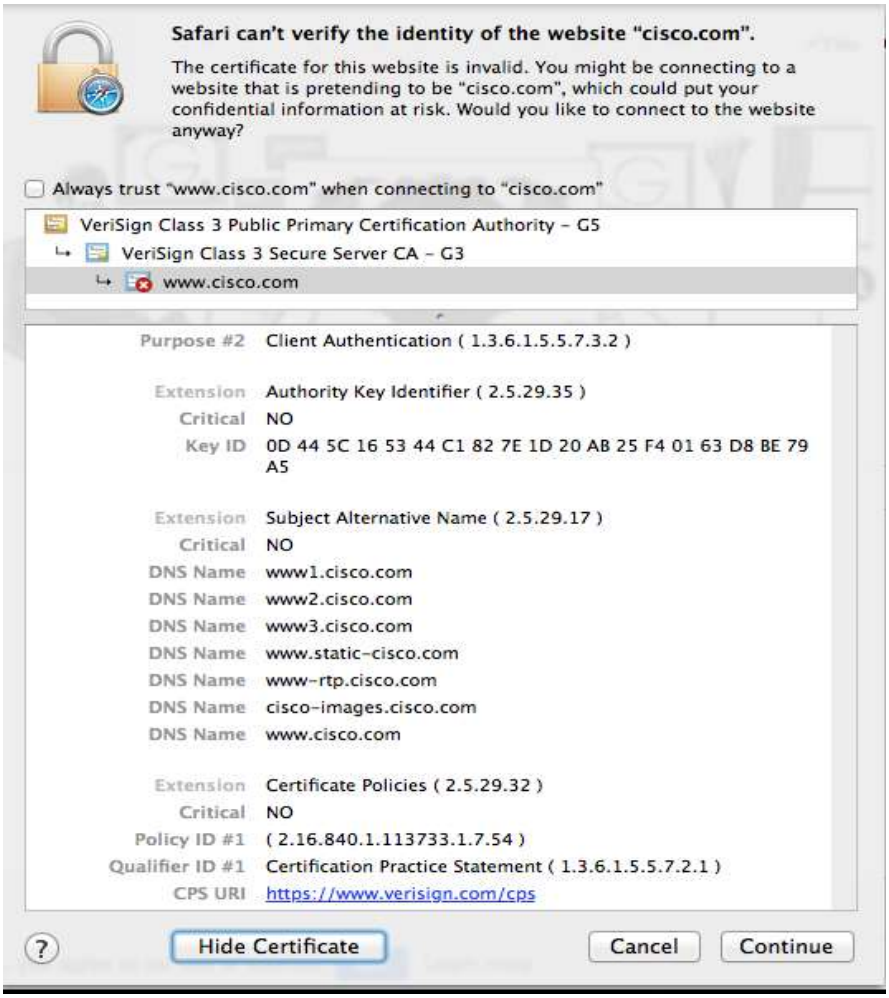

Рис. 8.7. Альтернативные имена сайта www.cisco.com