到目标服务器的连接。如果成功，就向客户端发送一条 200 Connection Established 响应。

```
HTTP/1.0 200 Connection established
Proxy-agent: Netscape-Proxy/1.1
```

更多有关安全隧道和安全代理的信息，请回顾 8.5 节。

14.10 更多信息

安全和密码问题是非常重要，也非常复杂的问题。如果想学习更多有关 HTTP 安全性、数字加密技术、数字证书以及公开密钥基础设施方面的内容，可以从下面这几个地方开始。

14.10.1 HTTP安全性

- *Web security, Privacy & Commerce*[13]（《Web 安全与电子商务》）
  Simson Garfinkel 著，O'Reilly & Associates 公司。这是 Web 安全以及 SSL/TLS 和数字证书方面最好、最可读的入门型书籍之一。

- http://www.ietf.org/rfc/rfc2818.txt
  RFC 2818，“HTTP Over TLS”（“TLS 上的 HTTP”），说明了如何在 SSL 的后继协议——TLS 协议之上实现安全 HTTP。 336

- http://www.ietf.org/rfc/rfc2817.txt
  RFC 2817，“Upgrading to TLS Within HTTP/1.1”（“在 HTTP/1.1 中升级到 TLS”），说明了如何使用 HTTP/1.1 中的升级机制在现存的 TCP 连接上启动 TLS。这样非安全和安全 HTTP 流量就可以共享相同的知名端口了（在这种情况下，使用的是 http: 的 80 端口，而不是 https: 的 443 端口）。还可以使用虚拟主机技术。这样，使用一台 HTTP+TLS 服务器就可以区分出发往同一个 IP 地址上不同主机名的流量了。

14.10.2 SSL与TLS

- http://www.ietf.org/rfc/rfc2246.txt
  RFC 2246，“The TLS Protocol Version 1.0”（“TLS 协议版本 1.0”），对（SSL 的后继协议）TLS 协议的版本 1.0 进行了规范。TLS 提供了因特网上通信的私密性。协议允许客户端 / 服务器应用程序以防止窃听、篡改以及伪造报文的方式进行通信。

- http://developer.netscape.com/docs/manuals/security/sslin/contents.htm
  “Introduction to SSL”（“SSL 简介”）介绍了 SSL 协议。SSL 最初是由网景公司

注 13：本书中文版由中国电力出版社出版。（编者注）