Revoking OpenVPN® Certificates

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses revocation of OpenVPN® certificates.[1]

See the following:

6.1 OpenVPN® Certificate Revocation

Perform the steps in the following procedure to revoke certificates for your OpenVPN® connections. (The steps are written for use on a Windows system.)

1. In the management computer's directory system, navigate to the directory for certificate authorization and generation. (In the Windows directory, that is the \easy-rsa subdirectory.)

   Note: For details, see Section 2.1, *Navigating to the OpenVPN Directories*, on page 2 of the document *Navigating to OpenVPN Directories*.

2. In the \easy-rsa directory, type **vars** and press the **Enter** key.

   ❖ The vars.bat file runs.

3. Identify the client or server whose certificate will be revoked—in this example, *client4name*.

4. Type **revoke-full *client4name*** and press the **Enter** key.

   ❖ The certificate authority revokes the certificate and key for the stated entity (*client4name*, Figure 6-1).

1. OpenVPN® uses transport layer security (TLS, successor to secure socket layers, SSL). For information about VPNs that use IP security (IPsec), see one of the following documents:
   - *Configuring IPsec VPNs in the EN-1000™*
   - *Configuring IPsec VPNs in the EN-2000™*
   - *The EN-4000™ in IPsec Virtual Private Networks*

For information on trademarks, safety, limitations of liability, and similar topics, see http://www.encorenetworks.com/disclaimer/.

© 2020 Encore Networks, Inc.
All rights reserved.

Note: Error 23, near the end of the listing, indicates that a verification test was conducted. The connection failed because the former certificate had been revoked.

Figure 6-1. Revoking a Certificate

The **revoke-full** command also generates a certificate revocation list (CRL). That file (named crl.pem) is generated in the \keys directory (a subdirectory of \easy-rsa).

5 In the \easy-rsa directory, type **cd keys** and press the **Enter** key.

❖ The command window moves to the \keys directory.

6 In the \keys directory, type **copy crl.pem ..\easy-rsa** and press the **Enter** key.

❖ The file crl.pem is copied to the directory \easy-rsa.

Note: This allows the OpenVPN server to see the certificate revocation list.

7 Then, in the \keys directory, type **cd ..\easy-rsa** and press the **Enter** key.

❖ The command window moves up to the \easy-rsa directory.

8 In the \easy-rsa directory, type **crl-verify crl.pem** to direct the server to use CRL verification.

❖ The server will verify each client against the CRL upon client connection to OpenVPN. A client whose certificate has been revoked will be disconnected.

Note: If a certificate for a *server* is revoked, the CRL file should be distributed to all clients.

Distribution of the CRL file is unnecessary for revocation of a *client* certificate, because a client will not connect to another client.

6.2 More Information

For a list of documents for OpenVPN® connections over EN routers, see the *Reference Manual for OpenVPN® on EN™ Routers*.