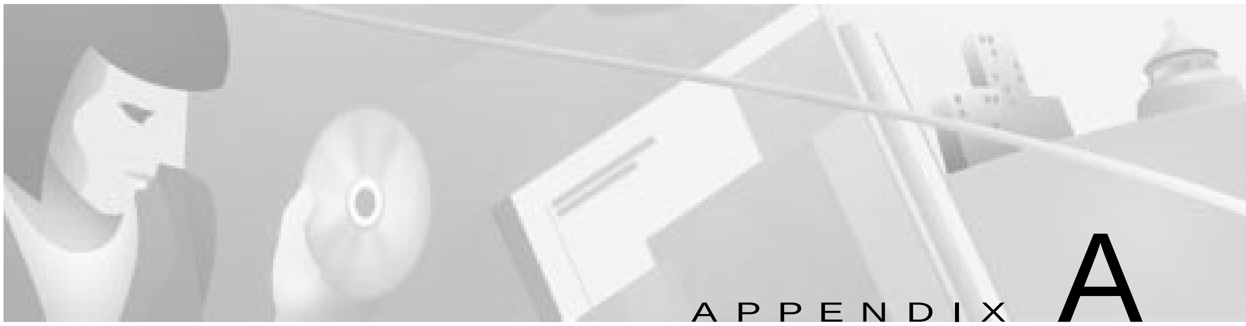


Configuring Entrust Digital Certificates

This appendix provides additional information on requesting digital certification from the Entrust CA server and configuring ca-identity configuration commands on your gateway. Use this appendix with Chapter 6, “Configuring Digital Certification,” and the enrollment procedures on the Entrust web site.

Entrust Certificate Authority

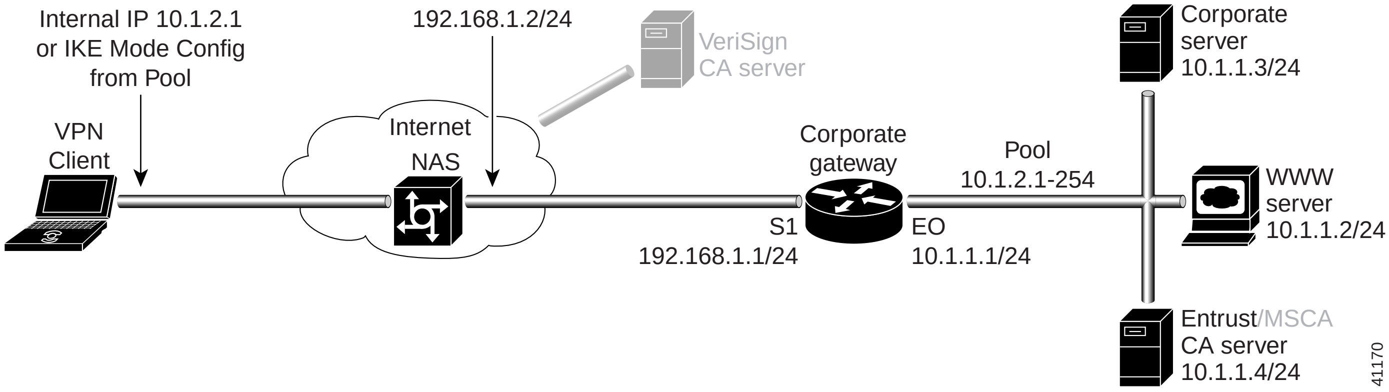
This CA requires that both IPSec peers transact with a Registration Authority (RA), which then forwards the requests through to the CA. Both the remote IPSec peer and the local IPSec peer must be configured with the both the CA and RA public keys. The CA and RA public keys are signature and encryption key pairs, which must be generated and enrolled for authentication to occur.

For information on configuring Entrust CA, see the following URLs:

- On configuring Entrust/VPN Connector:
  http://www.entrust.com/entrust/vpnconnect/
- On configuring Certificate Enrollment Protocol and Entrust:
  http://freecerts.entrust.com/vpncerts/cep.htm
- On Configuring a Networking Device with Entrust/VPN Connector:
  http://freecerts.entrust.com/vpncerts/cep_config.htm

Note While Cisco Secure VPN Client supports Entrust, the Entrust enrollment method is subject to change over time. Please see the Entrust web site at http://www.entrust.com for the current enrollment method.

Figure A-1 Entrust CA Server Topology



Configuring Entrust CA Identity on the Gateway

This step corresponds to the “Declaring the CA” section in Chapter 6, “Configuring Digital Certification.”

To enroll your certificate with a CA, perform the following tasks, as described in Table A-1:

- Specify the CA
- Specify Compatibility with CA’s RA
- Specify CA’s Enrollment URL
- Specify LDAP Support
- Specify CRL Option

Table A-1 Declare the CA

Command	Purpose
`hq_sanjose(config)# crypto ca identity example.com`	To declare the CA your router should use, enter the **crypto ca identity** global configuration command. This command invokes the ca-identity (cfg-ca-id) configuration mode. In this example, *example.com* is defined as the domain name for which this certificate is requested.
`hq_sanjose(cfg-ca-id)# enrollment mode ra`	To indicate compatibility with the CA’s Registration Authority (RA) system, enter the **enrollment mode ra** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)# enrollment url http://entrust-ca`	To specify the CA’s location where your router should send certificate requests by indicating the CA’s enrollment URL, enter the **enrollment url** ca-identity configuration command. In this example, *http://entrust-ca* is specified as the CA server.

Table A-1 Declare the CA (continued)

Command	Purpose
`hq_sanjose(cfg-ca-id)#` **`query url http://entrust-ca`**	To specify Lightweight Directory Access Protocol (LDAP) support, enter the **query url** ca-identity configuration command. This command is required if your CA supports both RA and LDAP. LDAP is a query protocol used when the router retrieves certificates and CRLs. The default query protocol is Certificate Enrollment Protocol (CEP). In this example, *http://entrust-ca* is specified as the LDAP server.
`hq_sanjose(cfg-ca-id)#` **`crl optional`**	To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the **crl optional** ca-identity configuration command.
`hq_sanjose(cfg-ca-id)#` **`exit`**	To exit ca-identity (cfg-ca-id) configuration mode, enter the **exit** ca-identity configuration command.