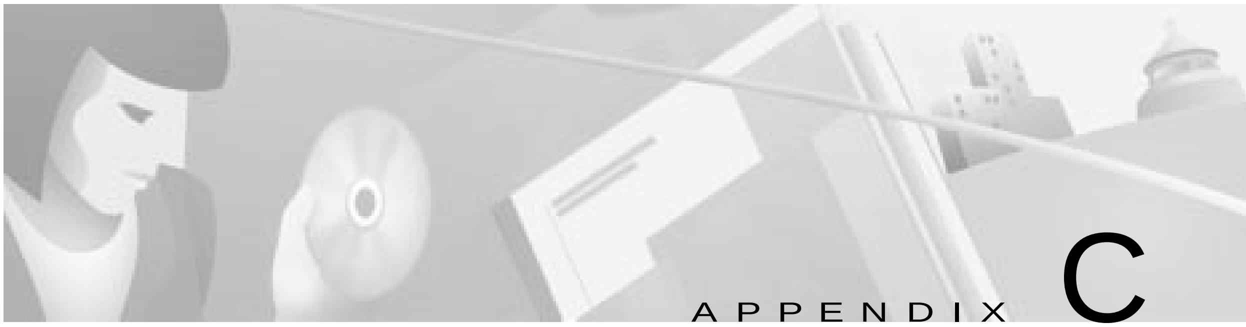


APPENDIX C

Configuring VeriSign Digital Certificates

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

VeriSign Certificate Authority

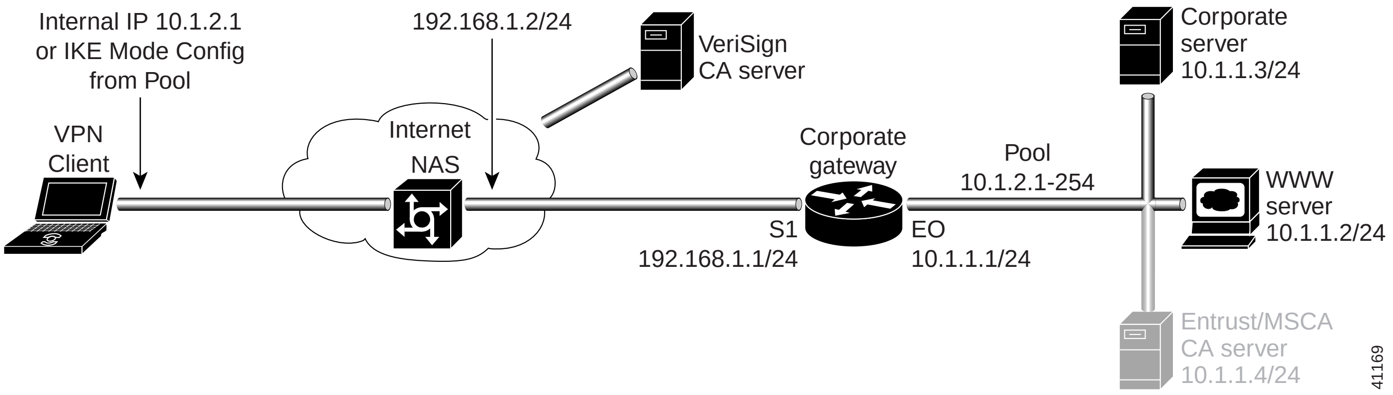
This CA provides certificate processing, backup, key recovery, and customer support. The gateway administrator handles approval, enrollment, validation, issuance, and renewal of digital certificates.

This section includes the following topics:

- Sending Certification Request to VeriSign CA Server
- Configuring VeriSign CA Identity on Gateway

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

Figure C-1 VeriSign CA Server Topology



Sending Certification Request to VeriSign CA Server

This step corresponds to "Sending the Certification Request to the CA Server" in Chapter 6, "Configuring Digital Certification." For details on submitting a VeriSign certificate request to the Verisign CA, see the following URL: http://www.verisign.com/onsite/ipsec/ciscoIntro.html

Configuring VeriSign CA Identity on Gateway

This step corresponds to "Declaring the CA" in Chapter 6, "Configuring Digital Certification."

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

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

Table C-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://onsiteipsec.VeriSign.com`**	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://onsiteipsec.VeriSign.com* is specified as the CA server.
`hq_sanjose(cfg-ca-id)#` **`query url http://onsiteipsec.VeriSign.com`**	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://onsiteipsec.VeriSign.com* is specified as the LDAP server.

Table C-1 Declare the CA (continued)

Command	Purpose
`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.