Configuring IPSec with PKI on Cisco IOS — Digital Certificates

Step 1.
Configure the CA Server (Cisco IOS)

```
Router(config)#hostname CA-Server
CA-Server(config)#ip http server
CA-Server(config)#crypto pki server EXAMPLE-CA
CA-Server(cs-server)#issuer-name CN=EXAMPLE-CA
CA-Server(cs-server)#grant auto
CA-Server(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: EXAMPLE-PASSWORD

Re-enter password: EXAMPLE-PASSWORD
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.
```

The Certificate Authority (CA) server has HTTP enabled because authentication and certificate enrollment in Step 2 will use the Simple Certificate Enrollment Protocol (SCEP) which communicates over HTTP port 80. In this configuration, the CA automatically grants certificates to incoming enrollment requests. The CA creates its own Digital Certificate key-pair (public/private) which has the private key password protected.

Step 2.
Configure the Client (Cisco IOS)

```
Router(config)#hostname R1
R1(config)#ip domain name EXAMPLE-DOMAIN
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.EXAMPLE-DOMAIN

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R1(config)#crypto pki trustpoint CA-SERVER
R1(ca-trustpoint)#enrollment url http://10.100.0.1
R1(ca-trustpoint)#revocation-check none
R1(ca-trustpoint)#exit
R1(config)#crypto pki authenticate CA-SERVER
Certificate has the following attributes:
       Fingerprint MD5: BA65AFA6 D004E420 BF79C4EF BE9B6801
      Fingerprint SHA1: 56CC07AC A94CF64E D88B3C20 CDC687A2 4B035ED7

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
R1(config)#
R1(config)#crypto pki enroll CA-SERVER
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: EXAMPLE-PASSWORD
Re-enter password: EXAMPLE-PASSWORD

% The subject name in the certificate will include: R1.EXAMPLE-DOMAIN
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA-SERVER' commandwill show the fingerprint.
```

The Client creates a public/private key-pair. Next, the Client creates a trustpoint which is used to configure the trusted CA Server's IP address (enrollment url). Optionally, a trustpoint may also instruct a Client to review a certificate revocation list (CRL), or to use a specific RSA key-pair (or Elliptic Curve/EC key-pair) with the particular trustpoint CA Server. After configuring a trustpoint, the Client authenticates the CA Server. During authentication, the Client receives the Root Certificate from the CA Server using SCEP (HTTP GET request). Finally, the Client enrolls with the CA, this is when the Client receives its identity certificate. Client enrollment is also called the Certificate Signing Request (CSR) and uses the format PKCS#10.

Step 3.
Configure IPSec on the Client for secure tunnel

PKI Digital Certificates authenticate the IKEv1 Phase 1 or IKEv2 Phase 1 of the IPSec tunnel setup. Basic configurations for IKEv1 Crypto Map, IKEv1 Static VTI, and IKEv2 Static VTI are shown below.

Crypto Map Configuration

```
R1(config)#ip access-list extended ACL-CRYPTO
R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config-ext-nacl)#exit
R1(config)#
R1(config)#crypto isakmp policy 100
R1(config-isakmp)#authentication rsa-sig
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto ipsec transform-set CRYPTO-TRANSFORM esp-aes
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#crypto map CRYPTO-MAP 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.2.0.1
R1(config-crypto-map)#set transform-set CRYPTO-TRANSFORM
R1(config-crypto-map)#match address ACL-CRYPTO
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface Gi0/1
R1(config-if)#crypto map CRYPTO-MAP
R1(config-if)#exit
R1(config)#
```

Static VTI Tunnel IKEv1

```
R1(config)#crypto isakmp policy 100
R1(config-isakmp)#authentication rsa-sig
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto ipsec transform-set CRYPTO-TRANSFORM esp-aes
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#crypto ipsec profile CRYPTO-PROFILE
R1(ipsec-profile)#set transform-set CRYPTO-TRANSFORM
R1(ipsec-profile)#exit
R1(config)#
R1(config)#interface Tunnel10
R1(config-if)#tunnel protection ipsec profile CRYPTO-PROFILE
R1(config-if)#exit
R1(config)#
```

In an ISAKMP policy, the default authentication is RSA signatures. Therefore, the line `authentication rsa-sig` could be omitted in the above configurations. Furthermore, both the crypto map and the static VTI tunnel configuration above use IKEv1 which is a deprecated security standard as of April 2023. IKEv2 is now the preferred standard. The RFC 9395 provides details on this topics.

Step 3. (continued)
Configure IPSec on the Client for secure tunnel

Static VTI Tunnel IKEv2

```
R1(config)#crypto ikev2 proposal CRYPTO-PROPOSAL
IKEv2 proposal MUST either have a set of an encryption algorithm other than aes-gcm, an
integrity algorithm and a DH group configured or
 encryption algorithm aes-gcm, a prf algorithm and a DH group configured
R1(config-ikev2-proposal)#encryption aes-cbc-256
R1(config-ikev2-proposal)#integrity sha256
R1(config-ikev2-proposal)#group 21
R1(config-ikev2-proposal)#exit
R1(config)#
R1(config)#crypto ikev2 policy CRYPTO-POLICY
IKEv2 policy MUST have atleast one complete proposal attached
R1(config-ikev2-policy)#match address local 10.1.0.1
R1(config-ikev2-policy)#proposal CRYPTO-PROPOSAL
R1(config-ikev2-policy)#exit
R1(config)#
R1(config)#crypto pki certificate map EXAMPLE-MAP 10
R1(ca-certificate-map)#issuer-name eq cn=EXAMPLE-CA
R1(ca-certificate-map)#exit
R1(config)#
R1(config)#crypto ikev2 profile CRYPTO-IKEV2-PROFILE
IKEv2 profile MUST have:
   1. A local and a remote authentication method.
   2. A match identity or a match certificate or match any statement.
R1(config-ikev2-profile)#match identity remote address 10.2.0.1 255.255.255.255
R1(config-ikev2-profile)#authentication remote rsa-sig
R1(config-ikev2-profile)#authentication local rsa-sig
R1(config-ikev2-profile)#pki trustpoint CA-SERVER
R1(config-ikev2-profile)#exit
R1(config)#
R1(config)#crypto ipsec transform-set CRYPTO-TRANSFORM esp-aes
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#crypto ipsec profile CRYPTO-IPSEC-PROFILE
R1(ipsec-profile)#set transform-set CRYPTO-TRANSFORM
R1(ipsec-profile)#set ikev2-profile CRYPTO-IKEV2-PROFILE
R1(ipsec-profile)#exit
R1(config)#
R1(config)#interface Tunnel10
R1(config-if)#tunnel protection ipsec profile CRYPTO-IPSEC-PROFILE
R1(config-if)#exit
R1(config)#
```

networkstudysite.com