IPSec Authentication using x509 certificates

Srividya Anantapatnaikuni - 2021-06-25 - 0 Comments - in IPSec

Introduction:

In this article, we will establish the IPsec VPN connection using certificate-based authentication.

The Self-signed CA, server and client certificates can be generated using either EASY-RSA utility or openssl commands.

Generate certs using openssl commands:

$Generate CA

```
openssl genrsa 2048 > cakey.pem
openssl req -x509 -new -nodes -days 1095 -sha256 -key cakey.pem -subj
/CN=IPsec\ Root\ CA -out cacert.pem
```

$Generate Server Certificate and Key

```
openssl req -newkey rsa:2048 -days 365 -nodes -sha256 -subj
/CN=IPsec\ Server -keyout serverkey.pem -out serverreq.pem
openssl x509 -req -in serverreq.pem -days 365 -extensions v3_req -CA
cacert.pem -CAkey cakey.pem -set_serial 01 -out servercert.pem
```

$Generate Client Certificate

```
openssl req -newkey rsa:2048 -days 365 -nodes -sha256 -subj
/CN=IPsec\ Client -keyout clientkey.pem -out clientreq.pem
openssl x509 -req -in clientreq.pem -days 365 -extensions v3_req -CA
cacert.pem -CAkey cakey.pem -set_serial 02 -out clientcert.pem
```

Server:

```
set vpn ipsec esp-group MyESPGroup proposal 1 encryption 'aes128'
set vpn ipsec esp-group MyESPGroup proposal 1 hash 'sha1'

set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group '2'
```

```
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption 'aes128'
set vpn ipsec ike-group MyIKEGroup proposal 1 hash 'sha1'

set vpn ipsec ipsec-interfaces interface 'eth0'

set vpn ipsec site-to-site peer 203.0.113.45 authentication id
'CN=IPSec Server'
set vpn ipsec site-to-site peer 203.0.113.45 authentication mode
'x509'
set vpn ipsec site-to-site peer 203.0.113.45 authentication remote-id
'CN=IPsec Client'
set vpn ipsec site-to-site peer 203.0.113.45 authentication x509 ca-
cert-file '/config/auth/ipsec/cacert.pem'
set vpn ipsec site-to-site peer 203.0.113.45 authentication x509
cert-file '/config/auth/ipsec/servercert.pem'
set vpn ipsec site-to-site peer 203.0.113.45 authentication x509 key
file '/config/auth/ipsec/serverkey.pem'
set vpn ipsec site-to-site peer 203.0.113.45 connection-type
'respond'
set vpn ipsec site-to-site peer 203.0.113.45 ike-group 'MyIKEGroup'
set vpn ipsec site-to-site peer 203.0.113.45 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 203.0.113.45 local-address
'192.0.2.10'
set vpn ipsec site-to-site peer 203.0.113.45 vti bind 'vti0'
set vpn ipsec site-to-site peer 203.0.113.45 vti esp-group
'MyESPGroup'
```

Client:

```
set vpn ipsec esp-group MyESPGroup proposal 1 encryption 'aes128'
set vpn ipsec esp-group MyESPGroup proposal 1 hash 'sha1'

set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group '2'
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption 'aes128'
set vpn ipsec ike-group MyIKEGroup proposal 1 hash 'sha1'

set vpn ipsec ipsec-interfaces interface 'eth0'

set vpn ipsec site-to-site peer 192.0.2.10 authentication id
'CN=IPsec Client'
set vpn ipsec site-to-site peer 192.0.2.10 authentication mode 'x509'
```

```
set vpn ipsec site-to-site peer 192.0.2.10 authentication remote-id
'CN=IPSec Server'
set vpn ipsec site-to-site peer 192.0.2.10 authentication x509 ca-
cert-file '/config/auth/ipsec/cacert.pem'
set vpn ipsec site-to-site peer 192.0.2.10 authentication x509 cert-
file '/config/auth/ipsec/clientcert.pem'
set vpn ipsec site-to-site peer 192.0.2.10 authentication x509 key
file '/config/auth/ipsec/clientkey.pem'
set vpn ipsec site-to-site peer 192.0.2.10 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.0.2.10 ike-group 'MyIKEGroup'
set vpn ipsec site-to-site peer 192.0.2.10 local-address
'203.0.113.45'
set vpn ipsec site-to-site peer 192.0.2.10 vti bind 'vti0'
set vpn ipsec site-to-site peer 192.0.2.10 vti esp-group 'MyESPGroup'
```

Note: authentication id/remote-id is required for the x509 authentication. Here, the "**common name** " provided while generating the server/client certificates is used. For example, CN=IPSec Server.

Refer this link for EASY-RSA utility.

In this case, the configuration is same as mentioned above but the id/remote-id has to be the entire string specifying the distinguished name of the certificates. For example, `'C=US, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationalUnit, CN=IPSec Server, N=EasyRSA, E=me@myhost.mydomain'` or you can just specify the common name, i.e.

```
set vpn ipsec site-to-site peer 203.0.113.45 authentication id 'IPSec
Server'
```