Cry isa pol
hash
Auth
gr
life
Enc

Psk

Ikev2

1.proposal - Enc,Integrity,Group
2.policy
3.keyring -PsK
4.ikev2-Profile -lifetime,Cert

PSK ----------PSK
Cisco Cisco

Ikev2

local cisco cisco
Remote cisco cisco

local cisco123 cisco456
Remote cisco456 cisco123

Local RSA RSA
Remote RSA RSA

local PSK RSA
Remote RSA PSK

==========

R1:
conf t
int e0/0
Desc conn to internet
ip add 1.1.1.1 255.255.255.0
no sh
int e0/1
Desc LAN1
ip add 10.1.1.1 255.255.255.0
no sh
exit

! Default route to access internet
ip route 0.0.0.0 0.0.0.0 1.1.1.2

R2:
R2:
conf t

int e0/0
Desc conn to Internet
ip add 2.2.2.2 255.255.255.0
no sh
int e0/1
Desc LAN
ip add 10.2.2.2 255.255.255.0
no sh
exit

!Default route to access internet
ip route 0.0.0.0 0.0.0.0 2.2.2.1

Internet:
Conf t
int e0/0
ip add 1.1.1.2 255.255.255.0
no sh
int e0/1
ip add 2.2.2.1 255.255.255.0
no sh
int lo0
Desc CA/NTP server
ip add 3.3.3.3 255.255.255.0
exit

Ntp source lo0
ntp master 1
clock timezone UTC 0
exit

CA config

Cry key generate rsa label CA modulus 2048

ip http server
cry pki server CA
database level complete
issuer-name CN=CA O=CA.com
Lifetime certificate 1095
lifetime ca-certificate 1825
grant auto

==========
R1/R2
ntp server 3.3.3.3

R1
cry key generate rsa label R1 modulus 2048

Cry pki trustpoint CA
enrollment url http://3.3.3.3:80

Subject-name CN=R1.com
rsakeypair R1
exit

Cry pki authenticate CA
yes

Cry pki enroll CA
password
re-enter pass

R2
1.Generate key pair (PUB/PRI)
cry key generate rsa label R2 modulus 2048

2.Define the trustpoint

Cry pki trustpoint CA
enrollment url http://3.3.3.3:80
Subject-name CN=R2.com
rsakeypair R1
exit

3.Verify the CA certificate

Cry pki authenticate CA
yes

4.Send a CSR request

Cry pki enroll CA
password
re-enter pass

==========
R1

```
crypto ikev2 proposal PROP
 encryption aes-cbc-256
 integrity sha512
 group 5
exit

crypto ikev2 policy POL
 proposal PROP
exit

crypto ikev2 keyring KR12
 peer R2
  address 2.2.2.2
  pre-shared-key remote cisco123
```

```
exit

crypto ikev2 profile PROF
 match identity remote address 2.2.2.2 255.255.255.255
 authentication remote pre-share
 authentication local rsa-sig
 keyring local KR12
 pki trustpoint CA
exit

Phase 2:

cry ipsec transform-set tset esp-gcm
exit

Access-list 101 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255

crypto map cmap 10 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set tset
 set ikev2-profile PROF
 match address 101
exit

int e0/0
cry map cmap
exit

=====================================================
R2:
Default proposal/Default policy


crypto ikev2 keyring KR12
 peer R2
  address 1.1.1.1
  pre-shared-key local cisco123
exit

crypto ikev2 profile PROF
 match identity remote address 1.1.1.1 255.255.255.255
 authentication local pre-share
 authentication remote rsa-sig
 keyring local KR12
 pki trustpoint CA
exit

Phase 2:

cry ipsec transform-set tset esp-gcm
exit


Access-list 101 permit ip  10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
```

```
crypto map cmap 10 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set tset
 set ikev2-profile PROF
 match address 101
exit

int e0/0
cry map cmap
exit
```

==========

R1

```
int e0/2
ip add 10.11.11.11 255.255.255.0
no sh
exit

Access-list 101 permit ip 10.11.11.0 0.0.0.255 10.22.22.0 0.0.0.255
```

R2:

```
int e0/2
ip add 10.22.22.22 255.255.255.0
no sh
exit

Access-list 101 permit ip  10.22.22.0 0.0.0.255 10.11.11.0 0.0.0.255

sh cry ikev2 sa
sh cry ikev2 session
sh cry ipsec sa
sh cry engine connections active
```

Flexvpn
SVTI
DVTI