Configuring IPSEC VPN Using New CLI

HOW TO GUIDE

Global configuration parameters

**crypto ikev1 dpd-keepalive <seconds>** # seconds between keepalives, in absence of traffic
**crypto ikev1 nat-keepalive <seconds>** # seconds between NAT keepalives
**crypto ikev2 dpd-keepalive <seconds>** # seconds between keepalives, in absence of traffic
**crypto ikev2 nat-keepalive <seconds>** # seconds between NAT keepalives
**crypto ikev2 cookie-challenge <limit>** # start cookie-challenge on half-open SA ‘limit’
**crypto ikev2 max-in-negotiation-sa <value>** # max half-open IKE SAs allowed
**crypto ipsec security-association <lifetime seconds|kilobytes <value>**

IKEv1 Site-2-site

1) Configure IKEv1 Policy

```
crypto ikev1 policy <name>
dpd-keepalive <seconds>  # seconds between keepalives, in absence of traffic
lifetime <seconds>       # IKE lifetime in seconds
mode (main|aggressive)  # IKEv1 mode of operation
proposal encr <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>
```

2) Configure IKEv1 Peer

```
crypto ikev1 peer <name>
  authentication { psk <pre-shared-key> | rsa } # common for local and remote
  ip (address <A.B.C.D> | fqdn host.domain.com) # remote peer IP/FQDN
  remote-identity {address <ip>| fqdn <value>| email <value>| string <value> | dn <value>}
  local-identity {address <ip>| fqdn <value>| email <value>| string <value> | dn <value>}
  use ikev1-policy <Policy Name>
```

3) Configure Transform set

4) Configure ACL, rules

5) Configure Crypto Map

```
crypto map <name> <seq> ipsec-isakmp
  peer (1|2|3) (ikev1|ikev2) <name>  # peer priority is the key
  pfs <1|2|5>
  security-association <lifetime seconds|kilobytes <value>/level perhost>
  transform-set <name>
  use ip-access-list <name>
```

6) Attach crypto map to interface

IKEv1 Remote VPN

1) Configure IKEv1 Policy

```
crypto ikev1-policy <name>
dpd-keepalive <seconds>  # seconds between keepalives, in absence of traffic
lifetime <seconds>       # IKE lifetime in seconds
mode (main|aggressive)  # IKEv1 mode of operation
proposal encr <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>
```
2) Configure IKEv1 Peer
   crypto peer-ikev1 <name>
      authentication { psk <pre-shared-key> | rsa } # common for local and remote
      ip address 0.0.0.0 # remote peer (any)
      remote-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <val>}
      local-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <val>}
      use ikev1-policy <Policy Name>

3) Configure Transform set
4) Configure ACL, rules
5) Configure Crypto Map
   crypto map <name> <seq> ipsec-isakmp dynamic
   peer (1|2|3)(ikev1|ikev2) <name> # peer priority is the key
   pfs <1|2|5>
   remote-type xauth|ipsec-l2tp|none # default is xauth
   security-association <lifetime seconds|kilobytes <value>/level perhost>
   transform-set <name>
   use ip-access-list <name>

6) Configure IKEv1 remote-vpn parameters
   crypto ikev1 remote-vpn
      authentication-method (local | radius )
      ip-local-pool <A.B.C.D/M> # static pool of virtual IPs
      local user <username> password <pwd> # mandatory for xauth local
      nameserver (primary | secondary) <A.B.C.D>
      use aaa-policy <name> # to configure radius server IPs
      wins (primary | secondary) <A.B.C.D>

7) Attach crypto map to interface

IKEv2 Site-2-site

1) Configure IKEv2 Policy
   dpd-keepalive <seconds> # interval between keepalives, in absence of traffic
   lifetime <seconds>
   sa-per-acl # setup single SA for all rules in the access list
   proposal encr <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>

2) Configure IKEv2 Peer
   crypto peer-ikev2 <name>
      authentication { {psk <pre-shared-key> | rsa} {local|remote} }
      ip (address <A.B.C.D> | fqdn <host.domain.com>) # remote peer IP /FQDN
      remote-identity {address <ip>|fqdn <value>|email <value>| string <value> |dn <val>}
      local-identity {address <ip>|fqdn <value>|email <value>|string <value> |dn <val>}
      use ikev2-policy <Policy Name>

3) Configure Transform set
   crypto ipsec transform-set <name> <encryption-method> <authentication-method>
   mode <tunnel/transport>

4) Configure ACL, rules
5) Configure Crypto Map
   crypto map <name> <seq> ipsec-isakmp
      peer (1|2|3)(ikev1|ikev2) <name> # peer priority is the key
      pfs <1|2|5>
      security-association <lifetime seconds|kilobytes <value>/level perhost>
      transform-set <name>
      use ip-access-list <name>
6) Attach crypto map to interface

**IKEv2 remote VPN**

1) Configure IKEv2 Policy
   crypto ikev2-policy <name>
   cookie-challenge <number>  # start cookie challenge at half-open SA crosses <number>
   dpd-keepalive <seconds>    # interval between keepalives, in absence of traffic
   ike-lifetime <seconds>
   max-in-negotiation-sa <limit>  # max half-open IKE SAs allowed
   proposal encr <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>

2) Configure IKEv2 Peer
   Crypto ikev2 peer <name>
   authentication {(psk <pre-shared-key> | rsa) (local|remote|)}
   ip address 0.0.0.0           # remote peer (any)
   remote-identity {address <ip>| fqdn <value>| email <value>| string <value> | dn <val} |
   local-identity {address <ip>| fqdn <value>| email <value>| string <value> | dn <val} |
   use ikev2-policy <Policy Name>

3) Configure Transform set
   crypto ipsec transform-set <name> <encryption-method> <authentication-method>
   mode <tunnel/transport>

4) Configure ACL, rules

5) Configure Crypto Map
   crypto map <name> <seq> ipsec-isakmp dynamic
   peer (1|2|3) (ikev1|ikev2) <name>  # peer priority is the key
   pfs <1|2|5>
   remote-type (xauth|ipsec-l2tp | none)  # default is xauth
   security-association <lifetime seconds|kilobytes <value> perhost>
   transform-set <name>
   use ip-access-list <name>

6) Configure IKEv2 remote-vpn parameters
   Crypto ikev2 remote-vpn
   authentication-method (local | radius)
   dhcp-server (address|hostname) <val> (giaddr A.B.C.D |)
   ip-local-pool <A.B.C.D/M>  # static pool of virtual IPs
   local user <username> password <pwd>
   nameserver (primary | secondary) <A.B.C.D>
   netmask <A.B.C.D/M>
   use aaa-policy <name>  # to configure radius servers
   wins (primary | secondary) <A.B.C.D>

7) Attach crypto map to interface
LEGENDS:
1) Fields in **RED** are mandatory
2) Fields in **BOLD** are defaults

Example:

Follow the below example configuration for site to site VPN, between RFS4000 and a RFS6000.

**Router 1:**

```
ip access-list site-site-router1
permit ip 192.168.30.0/24 192.168.50.0/24 rule-precedence 10
!
rfs4000 00-23-68-22-A1-B8
...
crypto ikev1 policy rtr1
dpd-keepalive 30
dpd-retries 5
lifetime 86400
isakmp-proposal default encryption aes-256 group 2 hash sha
mode main
crypto ikev1 peer rtr1
ip address 192.168.20.61
no remoteid
no localid
authentication psk 0 symbol123
use ikev1-policy rtr1
crypto ipsec transform-set rtr1 esp-null esp-sha-hmac
mode tunnel
crypto map rtr1 1 ipsec-isakmp
use ip-access-list site-site-router1
security-association level perhost
peer 1 ikev1 rtr1
```
no local-endpoint-ip
no pfs
no security-association lifetime seconds
no security-association lifetime kilobytes
security-association inactivity-timeout 900
transform-set rtr1

...interface vlan1
  ip address 192.168.10.41/24
  crypto map rtr1

**Router 2:**

ip access-list site-site-router2
  permit ip 192.168.50.0/24 192.168.30.0/24 rule-precedence 10
!

rfs6000 00-15-70-81-7B-35
...
crypto ikev1 policy rtr2
  dpd-keepalive 30
dpd-retries 5
lifetime 86400
isakmp-proposal default encryption aes-256 group 2 hash sha
mode main
crypto ikev1 peer rtr2
  ip address 192.168.10.41
  no remoteid
  no localid
  authentication psk 0 symbol123
  use ikev1-policy rtr2
crypto ipsec transform-set rtr2 esp-null esp-sha-hmac
mode tunnel
crypto map rtr2 1 ipsec-isakmp
  use ip-access-list site-site-router2
  security-association level perhost
peer 1 ikev1 rtr2
  no local-endpoint-ip
  no pfs
  no security-association lifetime seconds
  no security-association lifetime kilobytes
  security-association inactivity-timeout 900
  transform-set rtr2
...
interface vlan2
  ip address 192.168.20.61/24
  crypto map rtr2