Peplink Balance Multi-WAN Bonding Routers

Cisco IPsec Configuration Guide

January 2012

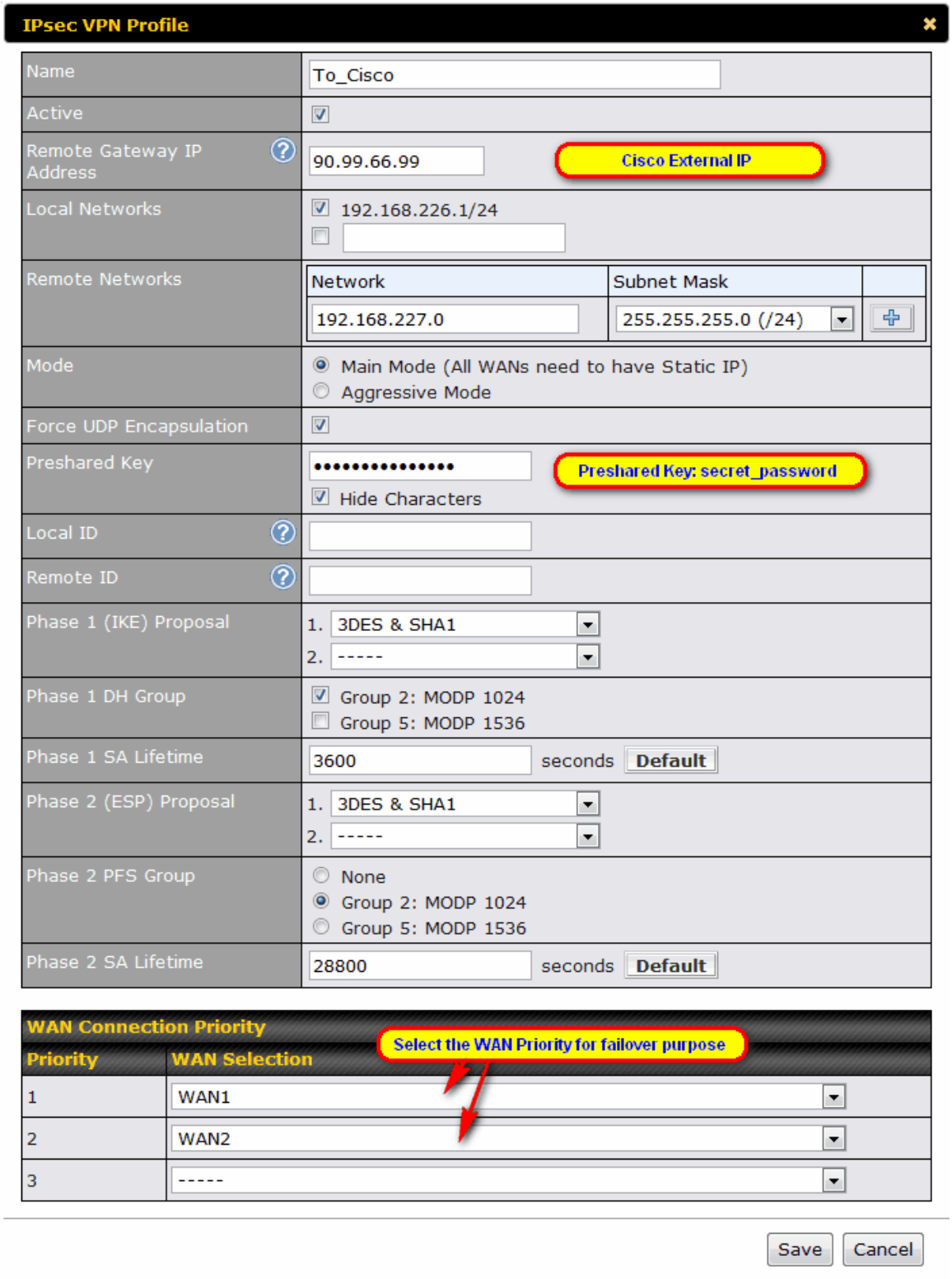
1 Configure IPsec (Main Mode) between Peplink and Cisco

IPsec configuration on Cisco

```
!--- Configure an ISAKMP policy
!--- It is belongs to Phase 1 negotiations

crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2


!--- Specifies the preshared key "abc123" for Peplink's WAN1 and WAN2

crypto isakmp key abc123 address 210.9.66.68
crypto isakmp key abc123 address 60.2.2.2


!--- Configure IPsec policies and specify the transform sets
!--- It is belongs to Phase 2 negotiations

crypto ipsec transform-set 3desset esp-3des esp-sha-hmac


!--- Creates crypto map for IKE establish the IPsec SA
!--- It is belongs to Phase 2 negotiations

crypto map peplink_map 10 ipsec-isakmp


!--- Sets the IP addresses of the remote Peplink
!--- You have to enter the outgoing public IP if Peplink is behind NAT

 set peer 210.9.66.68
 set peer 60.2.2.2
```

```
!--- Specifies IPsec to use the transform-set “3desset” that
configured above

 set transform-set 3desset

!--- Specifies the traffic to be encrypted.

 match address 100



!--- External Side

interface FastEthernet0/0
 ip address 90.99.66.99 255.255.255.0
 duplex auto
 speed auto
 crypto map peplink_map


!--- Internal Side

interface FastEthernet0/1
 ip address 192.168.227.1 255.255.255.0
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 90.99.66.1
!
!

!--- Define access list for IPsec traffic from subnet
!--- 192.168.227.0/24 to 192.168.226.0/24

access-list 100 permit ip 192.168.227.0 0.0.0.255 192.168.226.0
0.0.0.255
```

IPsec Configuration on Peplink



2 Configure IPsec (Aggressive Mode) between Peplink and Cisco

IPsec configuration on Cisco

```
!--- Define Keyring, pre-shared key with hostname

crypto keyring dynkey
 pre-shared-key hostname vpn@peplink key secret_password


!--- Create an ISAKMP policy for Phase 1 negotiation
!--- with 3DES, SHA1, DH Group 2

crypto isakmp policy 10
encr 3des
authentication pre-share
group 2

!--- Define ISAKMP Profile and include Keyring “dynkey” to this
profile
!--- Cisco U-FQDN is vpn@cisco
!--- Peplink U-FQDN is vpn@peplink

crypto isakmp profile dynprofile
  keyring dynkey
  self-identity user-fqdn vpn@cisco
  match identity user vpn@peplink
  initiate mode aggressive


!--- Part of IPsec phase 2 negotiation
!--- Define IPsec transform-set with ESP, 3DES, HMAC_SHA

crypto ipsec transform-set 3desset esp-3des esp-sha-hmac


!--- Part of IPsec phase 2 negotiation
```

```
!--- Add the Transform-set and ISAKMP profile which defined above to
this
!--- crypto dyanmaic map.
!--- Set the PFS Group 2 and include the access list.

crypto dynamic-map dynmap 10
set transform-set 3desset
set pfs group2
set isakmp-profile dynprofile
match address 100


!--- Add the dynamic map into crypto map

crypto map crymap 10 ipsec-isakmp dynamic dynmap

!--- External side.

interface FastEthernet0/0
ip address 90.99.66.99 255.255.255.0
duplex auto
speed auto


!--- Apply crypto map to the interface

crypto map crymap


!--- Internal side.

interface FastEthernet0/1
ip address 192.168.227.1 255.255.255.0
duplex auto
speed auto

ip route 0.0.0.0 0.0.0.0 90.99.66.1


!--- Define access list for IPsec traffic from subnet
!--- 192.168.227.0/24 to 192.168.226.0/24

access-list 100 permit ip 192.168.227.0 0.0.0.255 192.168.226.0
0.0.0.255
```

IPsec Configuration on Peplink