

Peplink Balance Multi-WAN Bonding Routers

Cisco IPsec Configuration Guide

January 2012



Copyright & Trademarks Specifications are subject to change without prior notice. Copyright © 2012 Peplink International Ltd. All Rights Reserved. Peplink and the Peplink logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

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 "3deset" that configured above

```
set transform-set 3deset
```

!--- 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

IPsec VPN Profile ✕

Name	To_Cisco						
Active	☒						
Remote Gateway IP Address	90.99.66.99	Cisco External IP					
Local Networks	☒ 192.168.226.1/24 ☐						
Remote Networks	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Network</th> <th style="width: 50%;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td> 192.168.227.0 </td> <td> 255.255.255.0 (/24) +</td> </tr> </tbody> </table>	Network	Subnet Mask	192.168.227.0	255.255.255.0 (/24) +		
Network	Subnet Mask						
192.168.227.0	255.255.255.0 (/24) +						
Mode	☒ Main Mode (All WANs need to have Static IP) ☐ Aggressive Mode						
Force UDP Encapsulation	☒						
Preshared Key	 ☒ Hide Characters						
	Preshared Key: secret_password						
Local ID							
Remote ID							
Phase 1 (IKE) Proposal	1. 3DES & SHA1 2. -----						
Phase 1 DH Group	☒ Group 2: MODP 1024 ☐ Group 5: MODP 1536						
Phase 1 SA Lifetime	3600	seconds	Default				
Phase 2 (ESP) Proposal	1. 3DES & SHA1 2. -----						
Phase 2 PFS Group	☐ None ☒ Group 2: MODP 1024 ☐ Group 5: MODP 1536						
Phase 2 SA Lifetime	28800	seconds	Default				

WAN Connection Priority

Priority	WAN Selection
1	WAN1
2	WAN2
3	-----

Select the WAN Priority for failover purpose


Save
Cancel

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 3deset
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

IPsec VPN Profile

Name	To_Cisco											
Active	☒											
Remote Gateway IP Address	90.99.66.99	Cisco External IP										
Local Networks	☒ 192.168.226.1/24											
Remote Networks	<table> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> <tr> <td>192.168.227.0</td> <td>255.255.255.0 (/24)</td> <td>☒</td> </tr> <tr> <td></td> <td>255.255.255.0 (/24)</td> <td>☐</td> </tr> </table>	Network	Subnet Mask		192.168.227.0	255.255.255.0 (/24)	☒		255.255.255.0 (/24)	☐		
Network	Subnet Mask											
192.168.227.0	255.255.255.0 (/24)	☒										
	255.255.255.0 (/24)	☐										
Mode	☐ Main Mode (All WANs need to have Static IP) ☒ Aggressive Mode											
Force UDP Encapsulation	☐											
Preshared Key	 ☒ Hide Characters	Preshared key: secret_password										
Local ID	vpn@peplink											
Remote ID	vpn@cisco											
Phase 1 (IKE) Proposal	3DES & SHA1											
Phase 1 DH Group	☒ Group 2: MODP 1024 ☐ Group 5: MODP 1536											
Phase 1 SA Lifetime	3600	seconds	Default									
Phase 2 (ESP) Proposal	3DES & SHA1											
Phase 2 PFS Group	☐ None ☒ Group 2: MODP 1024 ☐ Group 5: MODP 1536											
Phase 2 SA Lifetime	28800	seconds	Default									

WAN Connection Priority

Priority	WAN Selection
1	WAN1
2	WAN2
3	----

Select the WAN Priority for failover purpose

Save Cancel