how to create vpn connection between cisco router and DFL unit.doc

Before the scenario hands-on, we assume that the readers already along with following abilities:

- 1. The simple routing concept
- 2. The basic concept for LAN-to-LAN IPSEC.

Scenario summary:

DFL-210/800/1600/2500 f/w:v2.12.00



Object:

Establish the IPSEC tunnels between HQ and branch office.

HQ

Step1. Set the IP address for Lan and Wan respectively



Step2. Create an address object to represent the Branch office.



Step4. Create a pre-share key object. In this case, we use "test" ASCII string.

F- 6 System	
Dijects	🛃 General
ALG ALG Services Services Services Authentication Objects Authentication Objects VPN Objects Services	PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the p Name: sharekey Shared Secret
Contraction Contraction Contraction Contraction Contraction Contraction Contraction	Passphrase Shared Secret: ******* Confirm Secret: *******
	C Hexadecimal Key
	Passphrase Generate Random Key
	() Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared
	2 Comments
	Comments: test

Step5. Create a IPsec interface for branch office with the **sharekey** object created in previous step. Please refer the following list for detail configuration parameter:

Property	Valus			
Index	1			
Name	ipsec_if			
LocalNetwork	lannet			

RemoteNetwork	remote-office-net				
RemoteEndpoint	1.1.1.1				
IKEAlgorithms	Medium				
IPSecAlgorithms	Medium				
IKELifeTimeSeconds	28800				
IPSecLifeTimeSeconds	3600				
IPSecLifeTimeKilobytes	0				
EncapsulationMode	Tunnel				
AuthMethod	PSK (Pre-shared keying)				
PSK	sharekey				
XAuth	Off				
DHCPOverIPSec	No				
AddRouteToRemoteNet	No				
PlaintextMTU	1424				
OriginatorIPType	LocalInterface (Local interface)				
IKEMode	Main (Mainmode)				
DHGroup	2				
PFS	None				
SetupSAPer	Net (Per network)				
DeadPeerDetection	Yes				
NATTraversal	OnIfNeeded (Only if needed)				
KeepAlive	Disabled				
Metric	90				
AutoInterfaceNetworkRoute	Yes				
MTU	1500				
Comments	(none)				



Step7. Create an interface group for IP rule setting. This group includes lan, ipsec_if interface object.

SHome 🛛 🗙 Configuration 🚽 🎢	Tools 🗸 💁 Status 🗸 🔧 Maintenance 🚽
Address Book	InterfaceGroup
ALG	🔊 General
Schedules	Use an interface group to combine several interfacek for a simplified security policy.
VPN Objects	Name: ipsec-lan-if
E List	Security/Transport Equivalent
	Available Selected
interfaces	any ipsec-if lan
WI AN	dmz wan
- 🥳 IPsec	**
PPPoE	
PPTP/L2TP Servers	*
Interface Groups	Comments
Routing	Comments:
DP / PS	

Step8. Create an IP rule to allow both office users accessing computers each other.

🖨 🙀 Address Book	👖 💈 🔋 😵	💲 IP Rule				
hterfaceAddresses	General G	og Settings NAT	SAT			
Authentibation Objects	8 An I	Prule specifies what	it action to) perform on network	traffic that match	es the specified filter criteria.
	Name:	ipsec-traffic				
- (D List	Action:	Allow	~			
	Service:	all_services	~			
- Carlorithms	Schedule:	(None)	~			
E- \$ IP Rules	Address	Filter				
star_o_wan san_to_dmz san_to_lan	Spe.	cify source interface	and sour	ce network, together	with destination i	nterface and destination net
- 🙀 dmz_to_wan		Source		Destination		
🔀 wan_to_lan	Interface:	ipsec-lan-if	~	ipsec-lan-if	~	
wan_to_dmz -	Network:	all-nets	~	all-nets	~	
l- 🚰 Interfaces	🔊 Commen	ts				
- UR VLAN	Comments:					

Branch Office

Step1. Set the IP address for Fa 0/0 and Fa 0/1 interface respectively

```
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 duple* auto
 speed auto
Step2. Setup IKE phase 1 parameter
crypto isakmp policy 1
 encr 3des
                             Ι
 authentication pre-share
 group 2
 lifetime 28800
Step3. Setup pre-share key and remote endpoint
crypto isakmp key test address 3.3.3.3
•
•
Step4. Setup IKE phase 2 parameter
```

```
crypto ipsec transform-set 3des-sha1 esp-3des esp∑sha-hmac
!
```

```
Step5. Create add access list to tell router which traffic need to use IPSec encryption

access-list 111 permīt ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255

! ______

! _____
```

Step6. Group pre-share key, phase2 setting and access list object to a one crypto map object.

```
crypto map test1 1 ipsec-isakmp
set peer 3.3.3.3
set transform-set 3des-sha1
match address 111
?
?
Setp7. Put the crypto map object on the out going interface
interface FastEthernet0/0
+ crypto map test1
?
End of document.
```