How to set up an overlapping network with IPSec tunnel in DFL unit

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 IPSEC interface

3. The concept of overlapping network issue. If you need mode information, please refer the following

Scenario summary:

DFL-210/800/1600/2500/860/260 must use f/w:v2.26.00 or later



PC2 IP address: 192.168.30.20/24

Object:

PC1 and PC2 can access each other with IPSec tunnel.

DFL-2560

Step1. Set the IP address for LAN, Wan and other network objects respectively.

Remote	network = t	he opposi	ite virtual	network
Remote	metwork - t	ne opposi	ite viituai	network

	4	1	💡 wan1_dns1	0.0.0.0	Primary DNS server for interface wan1.
🗟 DFL-2560	5	1	wan1_dns2	0.0.0.0	Secondary DNS server for interface wan1.
🗄 🌀 System	6	1	wan2_ip	192.168.120.254	IPAddress of interface wan2
🖻 🤪 Objects	7	1	wan2net	192.168.120.0/24	The network on interface wan2
E Address Book	8	1	an1_ip	192.168.10.1	IPAddress of interface lan1
- InterfaceAddresses	9	1	an1net	192.168.10.0/24	The network on interface lan1
ALG with AV/WCF	10	1	lan2_ip	1.1.1.1	IPAddress of interface lan2
Services	11	1	lan2net	1.1.1.0/24	The network on interface lan2
Pools	12	1	lan3_ip	192.168.30.1	IPAddress of interface lan3
NAT Pools	13	1	an3net	192.168.30.0/24	The network on interface lan3
Schedules	14	1	an4_ip	192.168.40.1	IPAddress of interface lan4
Authentication Objects	15	1	an4net	192.168.40.0/24	The network on interface lan4
UTTO Deserve Files	16	1	dmz1_ip	172.17.100.254	IPAddress of interface dmz1
HIP Banner Files	17	1	dmz1net	172.17.100.0/24	The network on interface dmz1
- S ID Duloc	18	1	dmz2_ip	172.17.110.254	IPAddress of interface dmz2
an1 to wan1	19	1	dmz2net	172.17.110.0/24	The network on interface dmz2
Access	20	1	dmz3_ip	172.17.120.254	IPAddress of interface dmz3
E R Interfaces	21	1	dmz3net	172.17.120.0/24	The network on interface dmz3
Ethernet	22	1	dmz4_ip	172.17.130.254	IPAddress of interface dmz4
TIM VLAN	23	1	dmz4net	172.17.130.0/24	The network on interface dmz4
	24	1	remote_network	192.168.2.0/24	
	25	1	ipsec-local-net	192.168.1.1-192.168.1.254	
PPTP/L2TP Servers					Right-click on a row for additional optic
	•			ш	
ADD					

Step2. Create a pre-shared key for IPSEC interface.

DFL-2560	Authent	ication Objects nd modify Pre-Shared Keys and Certificates.			
E Gystern Dijects E Address Book	Add 🗸				
	# 🕶	Name 🐨	Туре 🤝	Туре 🔍	Comments 🐨
ALG with AV/WCF	1	HTTPSAdminCert	Certificate	Local	
🏠 Services	2	🔊 dlink	Pre-Shared Key	ASCII	
					Right-dick on a row for additional options.
	E (•
E 📴 VPN Objects					

Step3. Create a NAT POOL object as the screenshot below.

😽 Home 🛛 📉 Configuration 🗸 🛛 👖	📔 Tools 🗸 📔 🧟 Status 🗸 🛛 🗞 Maintenance 🗸
DFL-2560 B System Dojects D	A NAT Pool is used for NATing multiple concurrent connections to using different source IP addresses. General Proxy ARP Advanced General
Ald with AV/WCF Services IP Pools NAT Pools Schedules VPN Objects HTTP Banner Files Stleues IP Rules IP Rul	Name: ipsec-local-net Pool Type: Fixed Image: Ipsec-local-net Image: Ipsec-local-net Image: Ipsec-local-net Image: Ipsec-local-net Image: Ipsec-local-net Image: Image: Image:
Ellernet - Sellernet - Seller	Comments

Step4. Create an IPSEC interface as the following screenshots.

한 Local ID

Local ID Type:

Local ID Value

Auto

~

Selects the type of Local ID to use.

Specify the local identity of the tunnel ID.

🗄 📕 IGMP

🗈 👔 IDP / IPS

🗄 🛃 Route Load Balancing



Step5. Add a routing entry for the virtual LAN net and add default gateway for the LAN2.

# -	Name 🔻	IP address 🔻	Network 💌	Default Gateway 🔻	Enable DHCP Client 🔍 Comments 🔍
	🔝 dmz1	🗟 dmz1_ip	🗟 dmz1net		No
2	🔝 dmz2	🗟 dmz2_ip	💡 dmz2net		No
1	🔝 dmz3	🗟 dmz3_ip	🗟 dmz3net		No
	🔝 dmz4	🗟 dmz4_ip	🗟 dmz4net		No
1	🔝 wan1	🗟 wan1_ip	🗟 wan1net		No
	wan2	😽 wan2_ip	🗟 wan2net		No
	🔝 lan1	🗟 lan1_ip	🗟 lan1net		No
	🔝 lan2	😽 lan2_ip	😽 lan2net	5 1.1.1.2	No
	🔝 lan3	🤘 lan3_ip	🚽 lan3net		No
0	Ian4	😼 lan4_ip	🗟 lan4net		No

		# 🔻	Туре 🔻	Interface 🔻	Network 📼	Gateway 👻 🛛 Loc	al IP address 🤜	Metric 💌	Monitor this route	Comments 🔻
🖳 🖳 DFL-2560	<u>^</u>	1	्री Route	🔝 lan3	9 192.168.1.0/24			0	No	
System Objects Bules		2	्ही Route	😚 ipsec	💡 remote_network			90	No	Direct route for network remote_network over inter
E \$ IP Rules		3	्ही Route	🔝 dmz1	💡 dmz1net			100	No	Direct route for network dmz1net over interface dm
Access		4	्ही Route	🔝 dmz2	💡 dmz2net			100	No	Direct route for network dmz2net over interface dm
		5	्री Route	🔝 dmz3	💡 dmz3net			100	No	Direct route for network dmz3net over interface dm
PPoE	Е	6	्ही Route	🔝 dmz4	💡 dmz4net			100	No	Direct route for network dmz4net over interface dm
PPTP/L2TP Clients		7	्री Route	🔝 wan1	🖳 waninet			100	No	Direct route for network wan1net over interface wa
Routing		8	्ही Route	wan2	💡 wan2net			100	No	Direct route for network wan2net over interface wa
s Routing Rules		9	्री Route	🔝 lan1	🖳 laninet			100	No	Direct route for network lan1net over interface la
OSPF GMP		10	्ही Route	🔝 lan2	💡 lan2net			100	No	Direct route for network lan2net over interface la
 Route Load Balancing Kouting Settings 		11	्री Route	🔝 lan2	🖓 all-nets	Q 1.1.1.2		100	No	Default route over interface lan2.

Step6. Create one SAT and one Allow rule as the following screenshots for the IPSEC in bound traffic.

Add 🛨							
•	Name 💌	Action 💌	Src If 💌	Src Net 💌	Dest If 🔻	Dest Net 💌	Service 💌
	💲 vpn-in	兰 SAT	😚 ipsec	🗟 all-nets	🔝 lan3	9 192.168.1.0/24	🗑 all_services
	\$ vpn-in	👬 Allow	😚 ipsec	🗟 all-nets	🔝 lan3	9 192.168.1.0/24	🔯 all_services
	\$ vpn-out	T NAT	🔝 lan3	🗟 lan3net	😚 ipsec	🖁 all-nets	all_services
	<pre>\$ ping_fw</pre>	🟦 Allow	🔝 lan1	🗟 lan1net	🔝 core	🗟 lan1_ip	🔯 ping-inbound
	💈 lan3-to-lan2	T Allow	🔝 lan3	🗟 lan3net	🔝 lan2	🗟 lan2net	🔯 all_services
	🤰 lan1_to_wan1						

SAT rule:

🂈 vp	😫 vpn-in											
An IP	rule specifies what action	to perform on network traffic that matches the specified filter criteria.										
Genera	al Log Settings	NAT SAT Multiplex SAT SLB SAT SLB Monitors										
躗 Gene	eral											
Name:	vpn-in											
Action:	SAT	×										
Service:	all_services	×										
Schedule:	(None)	×										
_												
刘 Addr	ess Filter											
Specify sou	roe interface and source n	etwork, together with destination interface and destination network. All parameters have to match for the rule to match.										
	Interface	Network										
Source:	ipsec	all-nets										
Destination:	lan3	192.168.1.0/24										

\$	Vpn-in An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.	
G	ieneral Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors	
ۍ 🛃	General	
Tran	slate the	
	Source IP	
	Destination IP	
to:	New IP Address: 192.168.30.0	
	New Port:	
	Al-to-One Mapping: rewrite all destination IPs to a single IP	
		ок

Allow rule:

	An IP rule specifies what action to perform on network traffic that matches the specified filter oriteria.										
Genera	al Log Settings	NAT SAT I	Multiplex SAT SLB SAT SLB Monitors								
射 Gene	🛃 General										
Name:	vpn-in										
Action:	Allow	*									
Service:	all_services	*									
Schedule:	(None)	*									
🛃 Addr	ess Filter										
Specify sou	roe interface and source netwo	ork, together with destinatio	on interface and destination network. All parameters have to match for the rule to match.								
	Interface	Network									
Source:	ipsec 🗸	all-nets	✓								
Destination:	lan3 🗸	192.168.1.0/24	v								
谢 Com	ments										

Step7. Create a NAT rule as the following screenshots for the IPSEC out bound traffic.

	al Log Setting	gs NA	AT SAT	Multiplex S	AT SLB SAT	SLB Monitor	s	
Con.								
gene	erai							
Name:	vpn-out							
Action:	NAT	~						
Service:	all_services	*						
Schedule:	(None)	*						
🔰 Addr	ess Fliter							
Addr	ress Filter	oe network, t	together with de	stination interface a	nd destination network	. All parameters have t	o match for the rule to r	natch.
Specify sou	ess Filter	oe network, t Ne	together with de etwork	stination interface a	nd destination network	. All parameters have t	o match for the rule to r	natch.
Specify sou	ess Filter urce interface and sour Interface Ian3	oe network, t Ne	together with de etwork an3net	stination interface a	nd destination network	. All parameters have t	o match for the rule to r	natch.

DFL-2560G

Step1. Set the IP address for LAN, Wan and other network objects respectively.

Remote network = the opposite virtual network

		# 🕶	Name 🔻	Address 🔻	User Auth Groups 🔻	Comments 🔻
		1	🤤 wan1_ip	8.8.8.8		IPAddress of interface wan1
GPL-2560G	n.	2	😽 wan1net	8.8.8.0/24		The network on interface wan1
E Objects		з	🗟 wan1_gw	0.0.0.0		Default gateway for interface wan1.
Address Book		4	🗟 wan1_dns1	0.0.0.0		Primary DNS server for interface wan1.
InterfaceAddresses		5	🗟 wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1.
ALG with AV/WCF		6	🦁 wan2_ip	192.168.120.254		IPAddress of interface wan2
Services		7	🦁 wan2net	192.168.120.0/24		The network on interface wan2
IP Pools		8	😌 lan1_ip	192.168.10.1		IPAddress of interface lan1
Cabadalas		9	🖯 lan1net	192.168.10.0/24		The network on interface lan1
Authentiasticn Objects	Е	10	🖁 lan2_ip	2.2.2.1		IPAddress of interface lan2
THE VPN Objects		11	🗟 lan2net	2.2.2.0/24		The network on interface lan2
HTTP Banner Files		12	😌 lan3_ip	192.168.30.1		IPAddress of interface lan3
Rules		13	😌 lan3net	192.168.30.0/24		The network on interface lan3
E Interfaces		14	🤤 lan4_ip	192.168.40.1		IPAddress of interface lan4
		15	🗟 lan4net	192.168.40.0/24		The network on interface lan4
🔤 VLAN		16	😽 dmz1_ip	172.17.100.254		IPAddress of interface dmz1
😚 IPsec		17	G dmz1net	172.17.100.0/24		The network on interface dmz1
		18	😽 dmz2_ip	172.17.110.254		IPAddress of interface dmz2
		19	G dmz2net	172.17.110.0/24		The network on interface dmz2
PPTP/L2TP Servers		20	🦁 dmz3_ip	172.17.120.254		IPAddress of interface dmz3
PPTP/L2TP Clients		21	🖁 dmz3net	172.17.120.0/24		The network on interface dmz3
Interface Groups		22	🦁 dmz4_ip	172.17.130.254		IPAddress of interface dmz4
ARP		23	G dmz4net	172.17.130.0/24		The network on interface dmz4
E-100 Routing		24	🤤 ipsec-local-net	192.168.2.1-192.168.2.254		
E Routing Tables		25	🖁 remote_network	192.168.1.0/24		
main						

Step2. Create a pre-shared key for IPSEC interface.

Authenticatio	Pre-Shared Keys and Certificates.		
Add 🛩			
# 🔻	Name 💌	Туре 🔻	Туре 💌
1	😡 HTTPSAdminCert	Certificate	Local
2	🔊 dlink	Pre-Shared Key	ASCII
•		III	

Step3. Create a NAT POOL object as the screenshot below.

DEL 25500	≨ ipsec-local-net
Curtan	A NATE Pool is used for NATIng multiple concurrent connections to using different source in addresses.
E System	General Proxy ARP Advanced
Dijects	
Address Book	彭 General
ALG with AV/WCF	Name: ipsec-local-net
	Post T and Street
	Pool Type: These
MAT Pools	Use IP Ranne
	IR Research and the state
	ir naige. Ipset local liet
🗉 🙀 VPN Objects	
HTTP Banner Files	IP Pool: (None)
🛨 🕞 Rules	Number of IPs:
🖻 😭 Interfaces	
	A Commonto
📖 VLAN	
🚱 IPsec	Comments:
PPPoE	
PPTP/L2TP Servers	
PPTP/L2TP Clients	
Interface Groups	

Step4. Add a routing entry for the virtual LAN net and add default gateway for the LAN2.

≢ ▼	Name 🔻	IP address 🔻	Network 🔻	Default Gateway 🔻	Enable DHCP Client Comments
L	🔝 dmz1	🗟 dmz1_ip	🗟 dmz1net		No
2	🔝 dmz2	🗟 dmz2_ip	🗟 dmz2net		No
3	🔝 dmz3	🗟 dmz3_ip	🗟 dmz3net		No
1	🔝 dmz4	😼 dmz4_ip	🗟 dmz4net		No
5	🔝 wan1	😽 wan1_ip	🗟 wan1net		No
5	🔝 wan2	😽 wan2_ip	😽 wan2net		No
7	🔝 lan1	🖁 lan1_ip	🖁 lan1net		No
3	🔝 lan2	😼 lan2_ip	😼 lan2net	2.2.2.2	No
9	🔝 lan3	😽 lan3_ip	😽 lan3net		No
0	Ian4	😼 lan4 ip	lan4net		No

		# 🔻	Туре 🔻	Interface 🔻	Network 👻 🛛 Gateway 👻	Local IP address 🔍 Metric 👻
NAI Pools	^	1	्री Route	🔝 lan3	9 192.168.2.0/24	0
Schedules Schedules		2	्री Route	😚 ipsec	Fremote_network	90
HTTP Banner Files		3	्री Route	🔝 dmz1	🐺 dmz1net	100
- WEthernet		4	्री Route	🔝 dmz2	💡 dmz2net	100
		5	्री Route	🔝 dmz3	💡 dmz3net	100
PPTP/L2TP Servers		6	्री Route	🔝 dmz4	🐺 dmz4net	100
ARP	E	7	्री Route	🔝 wan1	🐺 waninet	100
e Routing Tables		8	्रौ Route	🔝 wan2	🦞 wan2net	100
		9	्री Route	🔝 lan1	🐺 lan1net	100
■- IGMP ■- B Route Load Balancing		10	्री Route	🔝 lan2	💡 lan2net	100
Routing Settings		11	्री Route	lan2	🐺 all-nets 🛛 🐺 2.2.2.2	100

Step5. Create an IPSEC interface as the following screenshots.



General Authen	tication XAuth Routing IKE Settings Keep-alive Advanced
Authentication	
X.509 Certificate	
Root Certificate(s)	
Available	Selected
Gateway certificate:	(None)
Identification list:	(None)
Pre-shared Key	

Step6. Create one SAT and one Allow rule as the following screenshots for the IPSEC in bound traffic.

1100							
: -	Name 🐨	Action 🔻	Src If 🔻	Src Net 🔻	Dest If 🔻	Dest Net 💌	Service 💌
	💈 vpn-in	SAT	😚 ipsec	😽 all-nets	🔝 lan3	9 192.168.2.0/24	all_services
	💈 vpn-in	Allow	😚 ipsec	🗟 all-nets	🔝 lan3	9 192.168.2.0/24	all_services
	\$ vpn-out	T NAT	Ian3	🗟 lan3net	😚 ipsec	🗟 all-nets	all_services
	💈 ping_fw	n Allow	🔝 lan1	💡 lan1net	🔝 core	💡 lan1_ip	👩 ping-inboun
	•		Records.		Reverse a		0



Genera	al Log Settings	NA	r sat	Multiple	x SAT	SLB SA	TS	LB Monitors			
🔰 Gene	eral										
Name:	vpn-in		7								
Action:	SAT Name	e 🗸									
Service:	all_services	~									
Schedule:	(None)	~									
			-								
🔰 Addr	ess Filter										
Specify sou	urce interface and source n	etwork, to	gether with destinat	ion interfa	ce and des	tination networ	rk. All para	meters have to	match for	r the rule to match.	
	Interface	Net	work								
	ipsec	🗸 al	-nets	~							
Source:											

G	An IP rule specifie eneral Log	as what action to perform	on network tr	mathic that matches the s Multiplex SAT	SLB SAT	a. SLB Monitors		
ه 🛃	General							
Trans to:	Iate the Source IP O Destination	IP						
	New IP Address:	192.168.30.0	~	_				
	New Port:			🚺 This value may only	be applied on TCP	/UDP services with port	set to either a single	oort number or a port range wi
	All-to-One I	/lapping: rewrite all des	ination IPs to	a single IP				

Allow rule:

Genera	al Log Sett	ings I	NAT SAT	Multiplex S	SAT SLB SAT	SLB Monitors	
	J						1
🔰 Gene	eral						
Name:	vpn-in						
Action:	Allow	~					
Service:	all_services	*					
Schedule:	(None)	~					
🔰 Addr	ess Filter						
Addro	ess Filter	urce network	k, together with destin	ation interface a	and destination network	k. All parameters have to	match for the rule to r
Specify sou	ess Filter	ource network	k, together with destin Network	ation interface a	and destination network	k. All parameters have to	match for the rule to r
Addro Specify sou	ess Filter	surce network	k, together with destin	ation interface a	and destination network	k. All parameters have to	match for the

Step7. Create a NAT rule as the following screenshots for the IPSEC out bound traffic.

	1-OUT rule specifies what ac	tion to perform on network t	raffic that matches the specified filter criteria.
Genera	I Log Setting	gs NAT SAT	Multiplex SAT SLB SAT SLB Monitors
躗 Gene	eral		
Name:	vpn-out		
Action:	NAT	*	
Service:	all_services	*	
Schedule:	(None)	~	
한 Addro	ess Filter		
Specify sou	rce interface and sour	œ network, together with de	stination interface and destination network. All parameters have to match for the rule to match.
	Interface	Network	
Source:	lan3	✓ lan3net	✓
Destination:	ipsec	✓ all-nets	✓

Result:

PC1 can access PC2 with 192.168.2.20. PC2 can access PC1 with 192.168.1.10 Note that the log page below is captured on DFL-2560G

2011-06-08 04:27:10	Info	CONN 600001	vpn-in	ICMP	ipsec lan3	192.168.1.1 192.168.2.20	conn_open
satdestrule=vpr	i-in conn=open co	onnsrcid=11221 o	conndestid=11221				
2011-06-08 04:27:10	Info	CONN 600001	IPsecBeforeRules	ESP	lan2 core	1.1.1.1 2.2.2.1	conn_open
conn=open conr	nsrcid=0 conndes	tid=0					
2011-06-08 04:27:10	Info	IPSEC 1803021					ipsec_sa_statistics
done=1 success	=1 failed=0						
2011-06-08 04:27:10	Info	IPSEC 1802046					ipsec_sa_lifetime
sec=3600							
2011-06-08 04:27:10	Info	IPSEC 1802043					ipsec_sa_informal
spiin="9b205d9	6 " spiout="16f4c	d03 " alg=aes-cb	c keysize=128 mac=h	mac-md5-96			
2011-06-08 04:27:10	Info	IPSEC 1802058					ipsec_sa_informal
local_id="192.1	58.2.0/24 any" re	mote_id="192.16	8.1.0/24 any"				
2011-06-08 04:27:10	Info	IPSEC 1802703					ike_sa_negotiation_completed ike_sa_completed
local_peer="2.2	.2.1 ID 2.2.2.1" r	emote_peer="1.:	1.1.1 ID 1.1.1.1" initia	tor_spi="20db8ea	a8 a83dbc39" res	ponder_spi="4746592c ea8aeea3" int	_severity=6
2011-06-08 04:27:10	Info	IPSEC 1802040					ipsec_sa_negotiation_completed ipsec_sa_enabled
sa=Responder i	nfo="tunnel" loca	_peer="2.2.2.1]	D 2.2.2.1" remote_pe	er="1.1.1.1 ID 1	.1.1.1" spi_in="E	SP 9b205d96" spi_out="ESP 16f4cd03	"
2011-06-08 04:27:10	Info	IPSEC 1802703					ike_sa_negotiation_completed ike_sa_completed
local peer="2.2	.2.1 ID 2.2.2.1" n	emote peer="1.;	L.1.1 ID 1.1.1.1" initia	tor spi="20db8ea	a8 a83dbc39" res	ponder spi="4746592c ea8aeea3" int	severity=6

END