[Foreword]

1) Use IKE Config Mode to create VPN tunnel.

[Topology]



[Setup]

1. Create Interface Addresses Objects

Objects > Address Book > InterfaceAddresses

An address folder	Addresses r can be used to group related address object	s for better overview.		
Add 👻 🚮 Edit t	his object			
# 👻	Name 👻	Address -	User Auth Groups -	Comments -
1	😽 wan_ip	61.218.67.126		IPAddress of interface wan
2	😽 wannet	61.218.67.120/29		The network on interface wan
3	💡 wan_gw	61.218.67.121		Default gateway for interface wan.
4	🤤 wan_dns1	0.0.0		Primary DNS server for interface wan.
5	🤤 wan_dns2	0.0.0		Secondary DNS server for interface wan.
6	📴 lan_ip	192.168.1.1		IPAddress of interface lan
7	😔 lannet	192.168.1.0/24		The network on interface lan
8	😼 dmz_ip	172.17.100.254		IPAddress of interface dmz
9	😡 dmznet	172.17.100.0/24		The network on interface dmz
10	IPSec_Pool	192.168.1.200-192.168.	1.220	
11	G LAN_Mask	255.255.255.0		
12	Google_DNS	8.8.8		
13	HiNet_DNS	168.95.1.1		

2. Create Authentication Objects

Objects > Authentication Objects

	ation Objects modify Pre-Shared Keys and Certificates.				
Add 🗸					
# 👻	Name 🛩	Туре	Туре –	Comments -	
1	6 HTTPSAdminCert	Certificate	Local		
2	🔏 Key	Pre-Shared Key	ASCII		

Create VPN Objects for IKE Config Mode Pool
 Objects > VPN Objects > IKE Config Mode Pool

# 🔻			IP Pool Type -	
0			Static	
General				
General				
) Genera	i l			
Use a pre	defined IPPool Ob	ject		
0				
IP Pool:	(None)	~		
 Use a Str 	atic IP Pool			
IP Pool	IPSec_Pool	~		
Netmas	- LAN Mask			
Wether				
J Optiona	d.			
ONS:	Google_DNS	~		
BNSWINS	HiNet DNS	v		
DHCP:	(None)	*		

4. Create IPsec Interfaces

Interfaces > IPsec

IPsec	c tunnel interfaces used for est	ablishing IPsec VPN co	nnections to and from this system	n.		
🐴 Add 🚽 🚿 Advar	noed Settings	•				
#~	Name 👻	Local Net -	Remote Net -	Remote Endpoint	Auth -	Comments -
1	<u> IPSec Tunnel</u>	🗟 lannet	🗟 all-nets		PSK	
General Aut	hentication XAuth	Routing IKE	Settings Keep-alive	Advanced		
Name:	IPSec_Tunnel					
Local Network:	lannet 🗸					
Remote Network:	all-nets 🗸					
Remote Endpoint:	(None)					
Encapsulation mode:	Tunnel 🗸					
IKE Config Mode Pool	ConfigModePool 🗸					
Algorithms						
IKE Algorithms:	Medium 🗸					
IKE Lifetime:	28800		seconds			
IPsec Algorithms:	Medium					
IPsec Lifetime:	3600		seconds			
IPsec Lifetime:	0		kilobytes			
General	thentication XAuth	Routing IKE	Settings Keep-alive	Advanced		
Pre-shared Key						
Pre-shared key:	Key	Selec	s the Pre-shared key to use with	this IPsec Tunnel.		
General Aut	hentication XAuth	Routing	Settings Keep-alive	Advanced		
1 Routing						
Allow DHCP over	IPsec from single-host clients					
Dynamically add	route to the remote network wh	en a tunnel is establish	ed			
General Aut	thentication XAuth	Routing IKE	Settings Keep-alive	Advanced		
Automatic Rou	ute Creation					
Automatically add rout	e for remote network.					14
Add route for rem	ote network					
Route metric: 90						

5. Create IP Rules

8 IKE	Config_Mod	ed to group IP Ru	les into logical groups for be	tter overview and simplifie	d management.		
Add -	- Edit this object						
	•						
# -	Name -	Action	Source interface	Source network	Destination interface	Destination network	Service
# • 1	Name -	Action -	Source interface	Source network	Destination interface	Destination network	Service

[Test & Confirm]

If PC1 connection success to firewall. You can follow those notices to check VPN tunnel.

- 1. PC1 ping PC2
- 2. Use ipconfig command on PC1. Check PC1 isn't it use IP-Pool range IP.

Command Prompt	- 🗆 🕽
C:\>ipconfig	
Windows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix : IP Address	
Ethernet adapter {FF6E9A3A-85A1-41B4-9CE9-46A4E8F71A6C}:	
Connection-specific DNS Suffix : IP Address	
C:\>ping 192.168.1.20	
Pinging 192.168.1.20 with 32 bytes of data:	
Reply from 192.168.1.20: bytes=32 time=66ms TTL=127	
Ping statistics for 192.168.1.20: Packets: Sent = 1, Received = 1, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 66ms, Maximum = 66ms, Average = 66ms Control-C Cc C:>>_	

3. Check Firewall route states.

Routing	Table Contents				
outing Table:	<main></main>				
how all routes:	(Including routes to i	nterface addresses and Layer 3 Cac	he entries)		
o not show sing	e host routes:				
- Inventes to dis	100				
ax routes to dis	100				
	Apply				
Routing ta	Apply ble contents (max 100 entrie:	s)		_	_
Routing ta	Apply ble contents (max 100 entries Network	s) Interface	Gateway	Local IP	Metric
Routing ta Flags D	Apply ble contents (max 100 entries Network 192.168.1.208	s) Interface IPSec_Tunnel	Gateway	Local IP	Metric 0
Routing ta Flags D	Apply. ble contents (max 100 entries Network 192.168.1.208 61.218.67.120/29	s) Interface IPSec_Tunnel wan	Gateway	Local IP	Metric 0 100
Routing ta Flags D	Apply. ble contents (max 100 entries Network 192.168.1.208 61.218.67.120/29 172.17.100.0/24	s) Interface IPSec_Tunnel wan dmz	Gateway	Local IP	Metric 0 100 100
Routing ta Flags D	Apply. ble contents (max 100 entrie: Network 192.168.1.208 61.218.67.120/29 172.17.100.0/24 192.168.1.0/24	s) Interface IPSec_Tunnel wan dmz lan	Gateway	Local IP	Metric 0 100 100 100

4. Firewall command line

Firewall command line
DFL-260:/> ikesnoop
Ike snooping is not active DFL-260:/> ikesnoop -on -verbose
Ike snooping is active - verbose mode; snooping address * DFL-260:/>
When PC1 connection VPN. Use same command in firewall. (ikesnoop –on –verbose) (ikesnoop -off)
Notification : DPD R-U-THERE-ACK
2011-08-10 09:37:07: IkeSnoop: Received IKE packet from 218.210.16.29:500 Exchange type : Informational ISAKMP Version : 1.0 Flags : E (encryption) Cookies : 0xd48162bc1b55e46f -> 0x5a61d8726081a629 Message ID : 0x23e51c1a Packet length : 80 bytes # payloads : 2 Payloads : HASH (Hash) Payload data length : 16 bytes N (Notification) Payload data length : 28 bytes Protocol ID : ISAKMP Notification : DPD R-U-THERE

Use routes command

routes	S				
Flags	Network	Iface	Gateway	Local IP	Metric
D	192.168.1.207	IPSec_Tunnel			0
	61.218.67.120/29	wan			100
	172.17.100.0/24	dmz			100
	192.168.1.0/24	lan			100
	0.0.0.0/0	wan	61.218.67.121		100

END