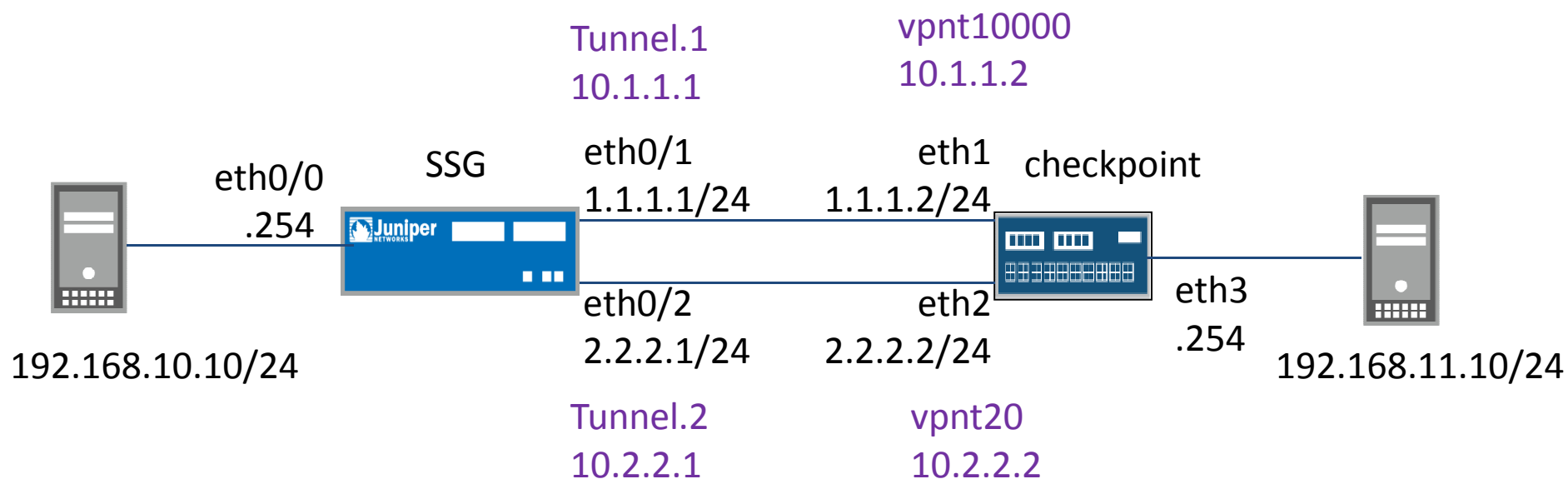


# Checkpoint v.s SSG route base IPSec VPN 架構圖



1. 在 Security Gateway Web 介面上新增 VTI (Tunnel Interface)

The screenshot shows the Check Point Gaia Portal Network Management interface. The left sidebar contains a navigation menu with 'Network Management' and 'Network Interfaces' highlighted. The main area displays a table of interfaces. The 'Add' button is highlighted with a red box. The table lists various interfaces, with three VPN-Tunnel entries (vpnt20, vpnt30, and vpnt10000) highlighted with red boxes. The status of these interfaces is 'Up'.

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth1	Ethernet	1.1.1.2	255.255.255.0	-	-	No Link	
eth2	Ethernet	2.2.2.2	255.255.255.0	-	-	Up	
eth3	Ethernet	192.168.11.254	255.255.255.0	-	-	Up	
eth4	Ethernet	-	-	-	-	Down	
eth5	Ethernet	-	-	-	-	Down	
eth6	Ethernet	4.4.4.2	255.255.255.0	-	-	No Link	
eth7	Ethernet	3.3.3.2	255.255.255.0	-	-	No Link	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	
vpnt20	VPN-Tunnel	-	-	-	-	Up	
vpnt30	VPN-Tunnel	-	-	-	-	Up	
vpnt40	VPN-Tunnel	-	-	-	-	Up	
vpnt10000	VPN-Tunnel	-	-	-	-	Up	

Check Point 4800 R77.10-GW

Network Management > Network Interfaces

View mode: Advanced

Network Management

- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- NetFlow Export

System Management

- Time
- Cloning Group
- SNMP
- Job Scheduler

Interfaces

Name	Type
eth1	Eth
eth2	Eth
eth3	Eth
eth4	Eth
eth5	Eth
eth6	Eth
eth7	Eth
lo	Lo

**Edit vpnt10000**

Link Status: Up  
Type: VPN-Tunnel  
**Enable:**   
Comment:

**VPN Tunnel**

VPN Tunnel ID: 10000  
Peer: ssg-wan1

**VPN Tunnel Type**

Numbered  Unnumbered  
Local Address: 10 . 1 . 1 . 2  
Remote Address: 10 . 1 . 1 . 1  
Physical device: Select...

OK Cancel

Configuration

Link Status	Comment
No Link	
Up	
Down	
Down	
No Link	
No Link	
Up	
Up	
Up	
Up	
Up	

Displaying 1 - 13 of 13

2. 隨便選擇一個 ID 編號, 並輸入 Peer 名稱 (此名稱需與 Smart Dashboard 裡的 Interoperable Devices 名稱一樣)

3. 輸入自己的 Tunnel interface IP 及 remote tunnel interface ip

View mode: Advanced

- PIM
- RIP
- OSPF
- Route Aggregation
- Inbound Route Filters
- Route Redistribution
- Routing Options
- Router Discovery
- Policy Based Routing
- Routing Monitor

User Management

- Change My Password
- Users
- Roles
- Password Policy
- Authentication Servers
- System Groups

High Availability

- VRRP
- Advanced VRRP

Maintenance

Routing Options

Apply Reload

Equal Cost Multipath

Maximum Paths: 8

Kernel Options

Kernel Routes:

Protocol Rank

OSPF Routes: Default: 10

RIP Routes: Default: 100

BGP Routes: Default: 170

OSPF ASE Routes: Default: 150

Advanced Routing Options

Wait For Clustering:

Wait For Clustering is intended for ClusterXL systems only.

Auto Restore Iface Routes:

Auto Restore Iface Routes is to avoid loss of interface routes.

ECMP, 預設已經是8條, 不用改

Check Point 4800 R77.10-GW admin Sign Out

Advanced Routing > OSPF

View mode: Advanced

- PIM
- PDP
- OSPF**
- Route Aggregation
- Inbound Route Filters
- Route Redistribution
- Routing Options
- Router Discovery
- Policy Based Routing
- Routing Monitor

User Management

- Change My Password
- Users
- Roles
- Password Policy
- Authentication Servers
- System Groups

High Availability

- VRRP
- Advanced VRRP

Open Shortest Path First (OSPF) is an interior gateway protocol (IGP) used to exchange routing information between routers within a single autonomous system (AS). OSPF is suitable for core networks with a large number of routers.

**Global Settings**

Router ID: 3 . 3 . 3 . 3      RFC 1583 Compatibility:

SPF Delay: Default: 2 seconds      SPF Hold Time: Default: 5 seconds

Default ASE Route Cost: Default: 1      Default ASE Route Type: Type 1

Graceful Restart Helper:

Apply

**Interfaces**

Add Edit Delete

Interface	Area	Hello Interval	Dead Interval	Retransmit Interval	Election Priority	OSPF Cost	Use Virtual Address	Authentication
eth3	backbone	10 seconds	40 seconds	5 seconds	1	1	No	None
vpnt20	backbone	3 seconds	10 seconds	1 second	1	1	No	None
vpnt10000	backbone	3 seconds	10 seconds	5 seconds	1	1	No	None

4. 設定 Tunnel interface 及 LAN port 啟用 OSPF, area, timer (注意 timer 值需跟 SSG 一樣)

172.17.99.179 - Check Point SmartDashboard R77.10 - Standard

Check Point SmartDashboard

5. 到 Smart Dashboard 新增一個空的 Group object

Group Properties - Null\_Group

Name: Null\_Group

Comment:

Color: Black

Group Convention

Suggest to add objects to this group

Not in Group:

Type to Search

Name	IP Address
All_Internet	0.0.0.0 - 2...
AuxiliaryNet	
CP4800	172.17.99...
CP_default_Office_Mod...	172.16.10...
CPDShield	
DMZNet	
InternalNet	

Add >

< Remove

View...

In Group:

Type to Search

Name	IP Address	Co
------	------------	----

New

New Expanded Group

OK

Cancel

Network Objects

- Check Point
- Nodes
- Interoperable Devices
- Networks
- Groups**
  - Null\_Group**
- Address Ranges
- Dynamic Objects

Objects List Identity Awareness SmartWorkflow

172.17.99.179 Read Only Mode Policy Installation Status



172.17.99.160 - Check Point SmartDashboard R77.10 - Standard

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention

Overview Policy NAT Track Logs Analyze & Report

### Policy

No.	Hits	Name	Source
Accept VPN traffic rule (configured from the c...			
-	-	-	Any
1	5K	-	lab
2	24K	-	Any

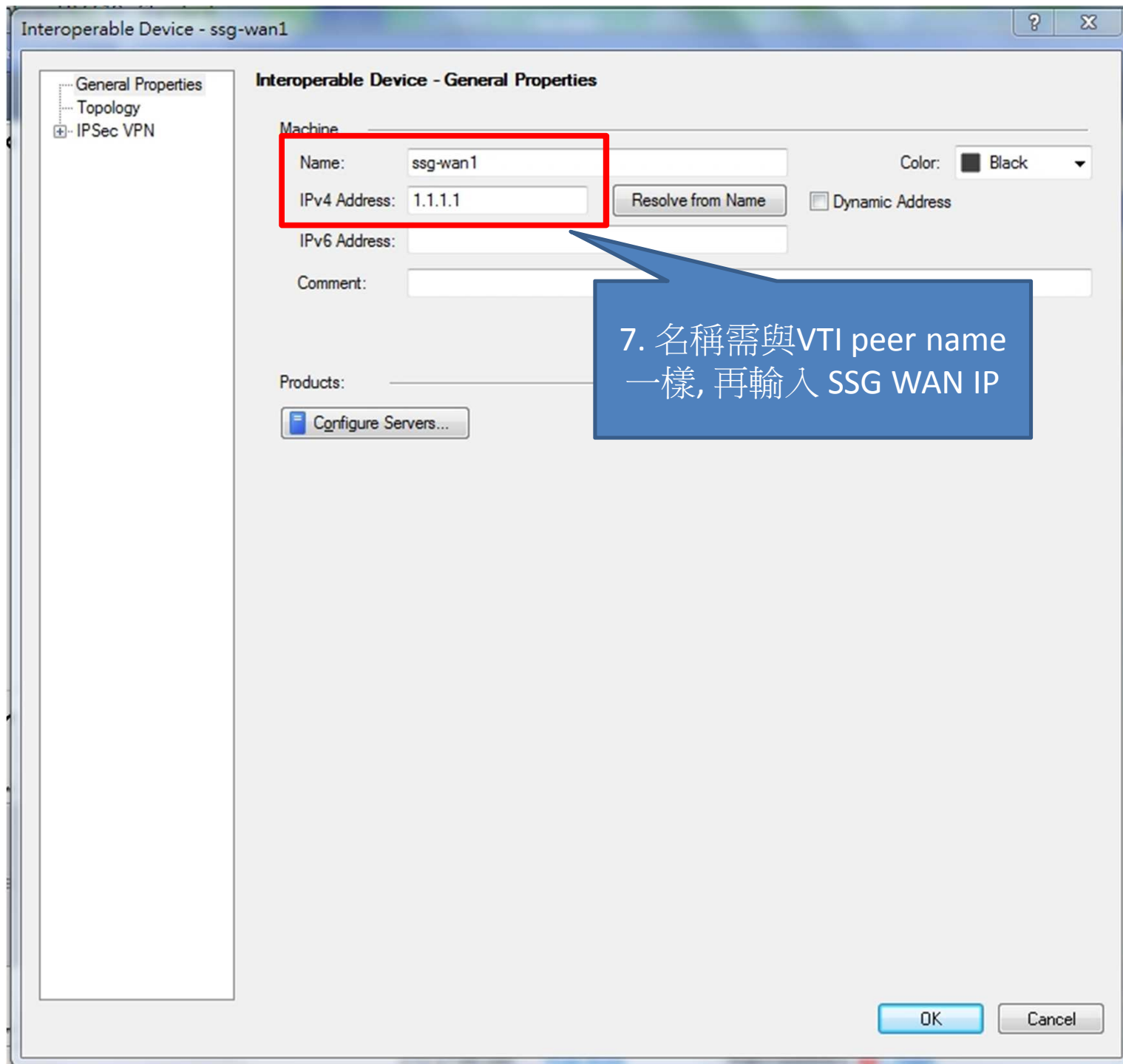
Network Objects

- Check Point
  - CP-SMS-R77
  - CP\_GW
- Nodes
- Interoperable Devices
  - ns204-wan3
  - ns204-wan4
  - ssg-wan1
  - ssg-wan2
- Networks

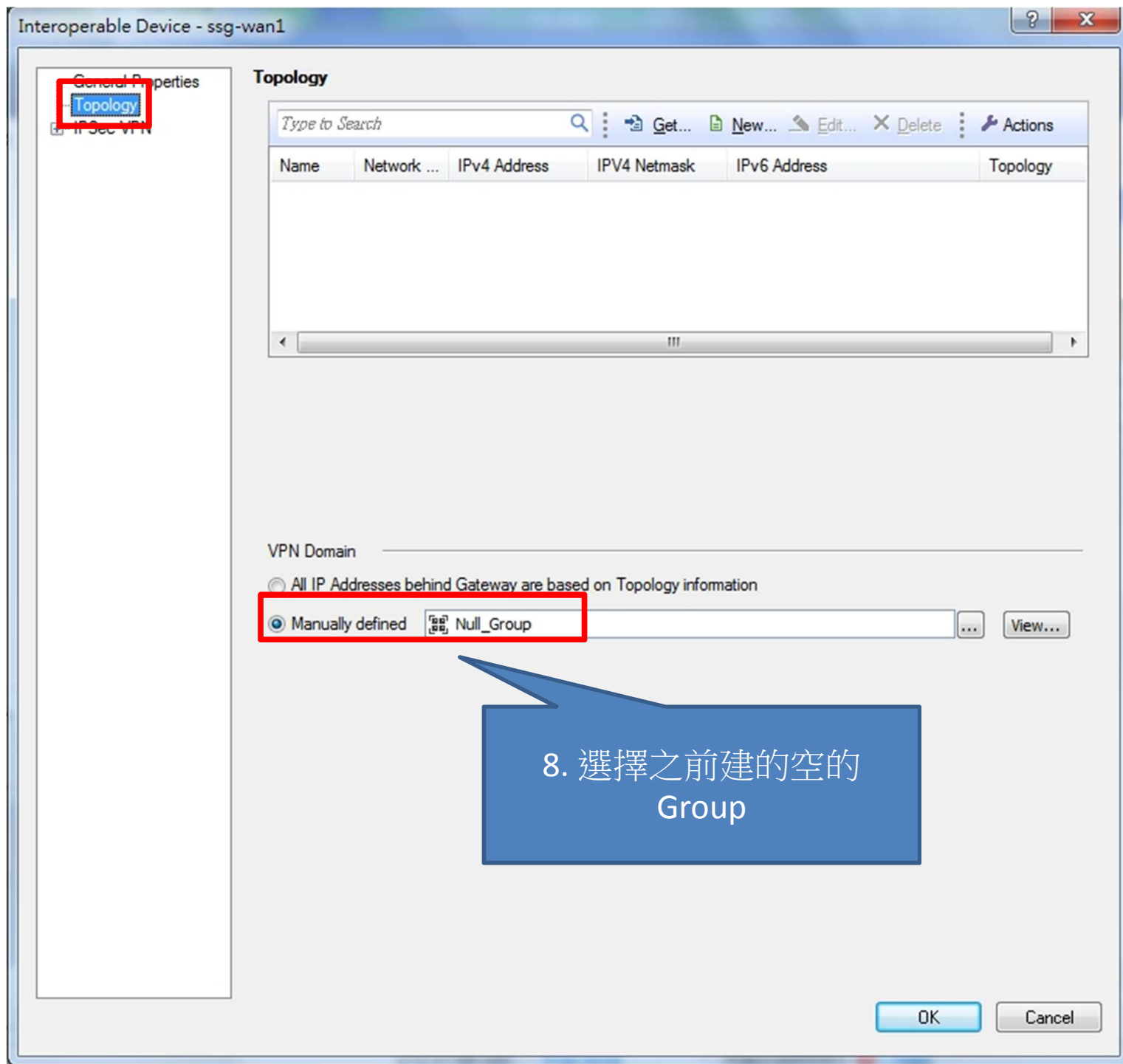
6. 新增 Interoperable device (名稱需與VTI peer name 一樣)

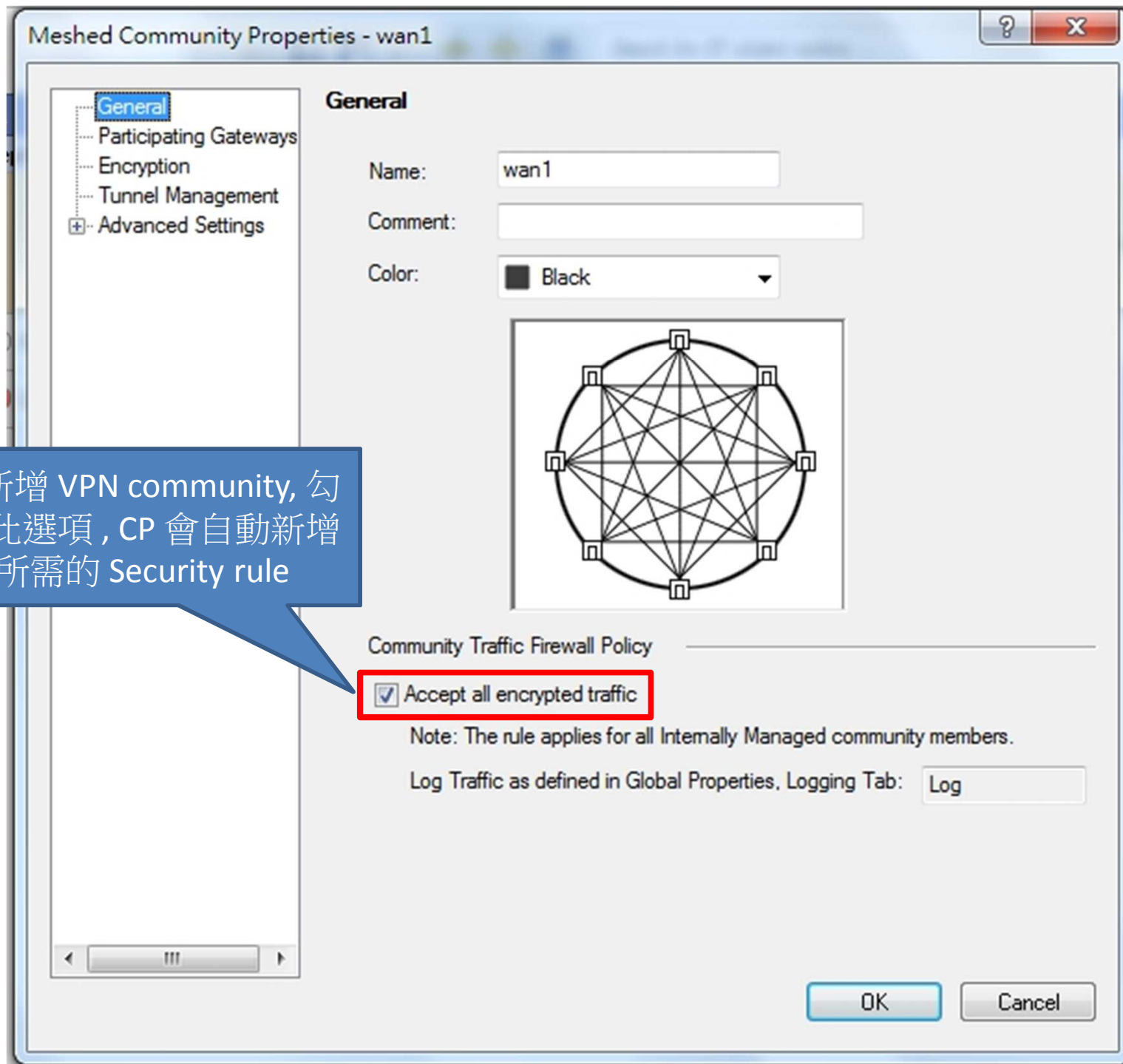
Objects List Identity Awareness SmartV

For Help, press F1 172.1

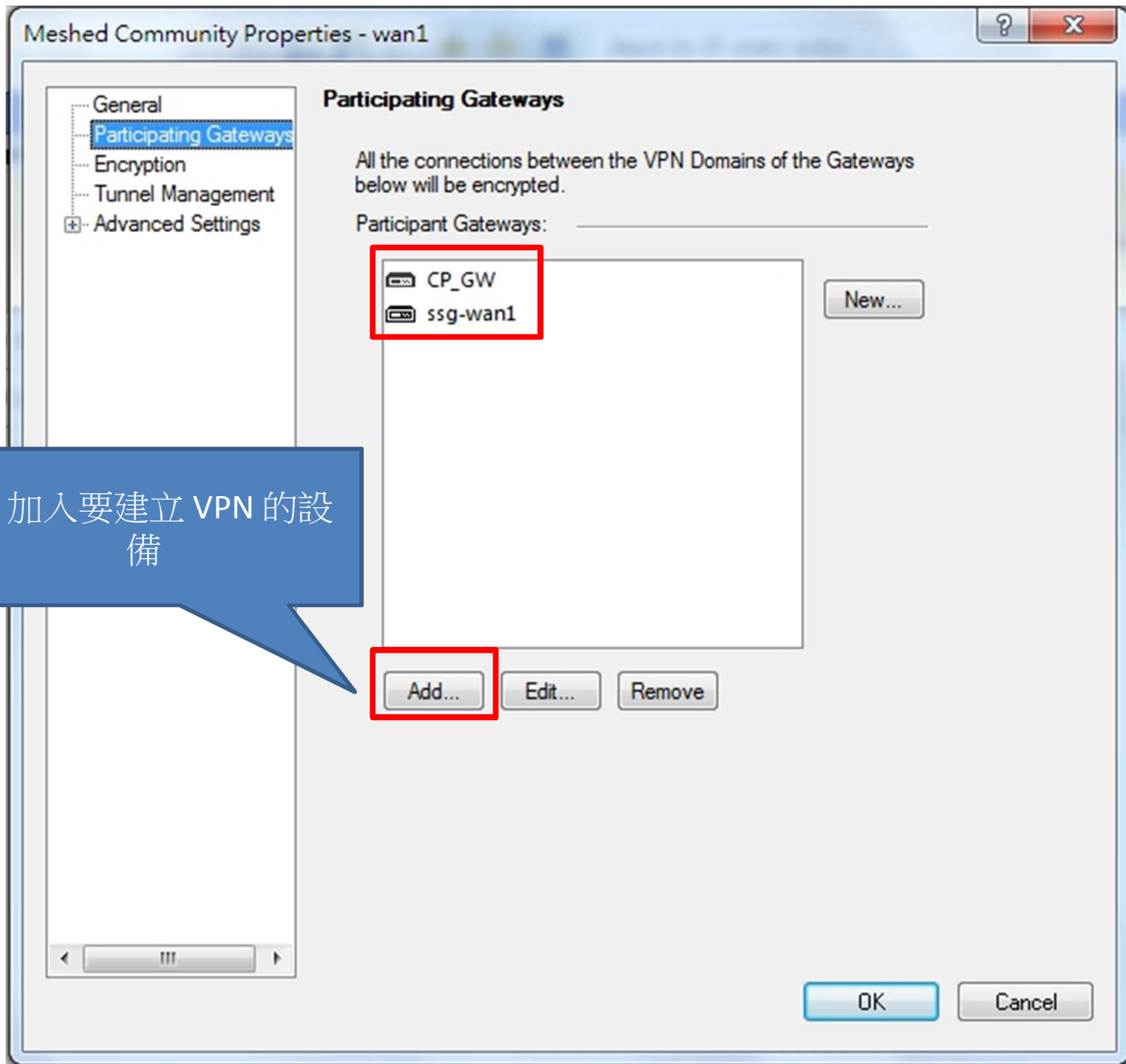


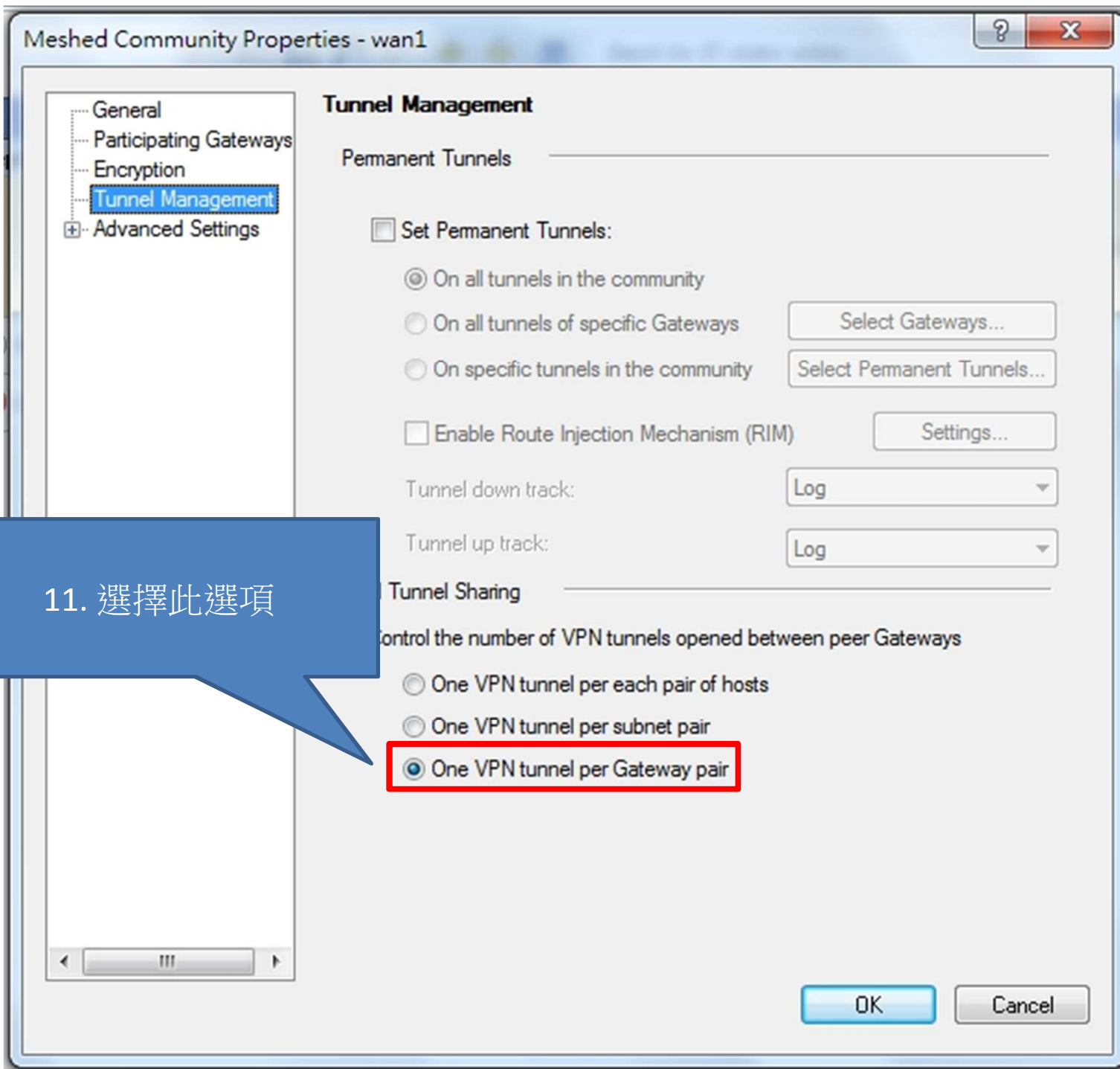


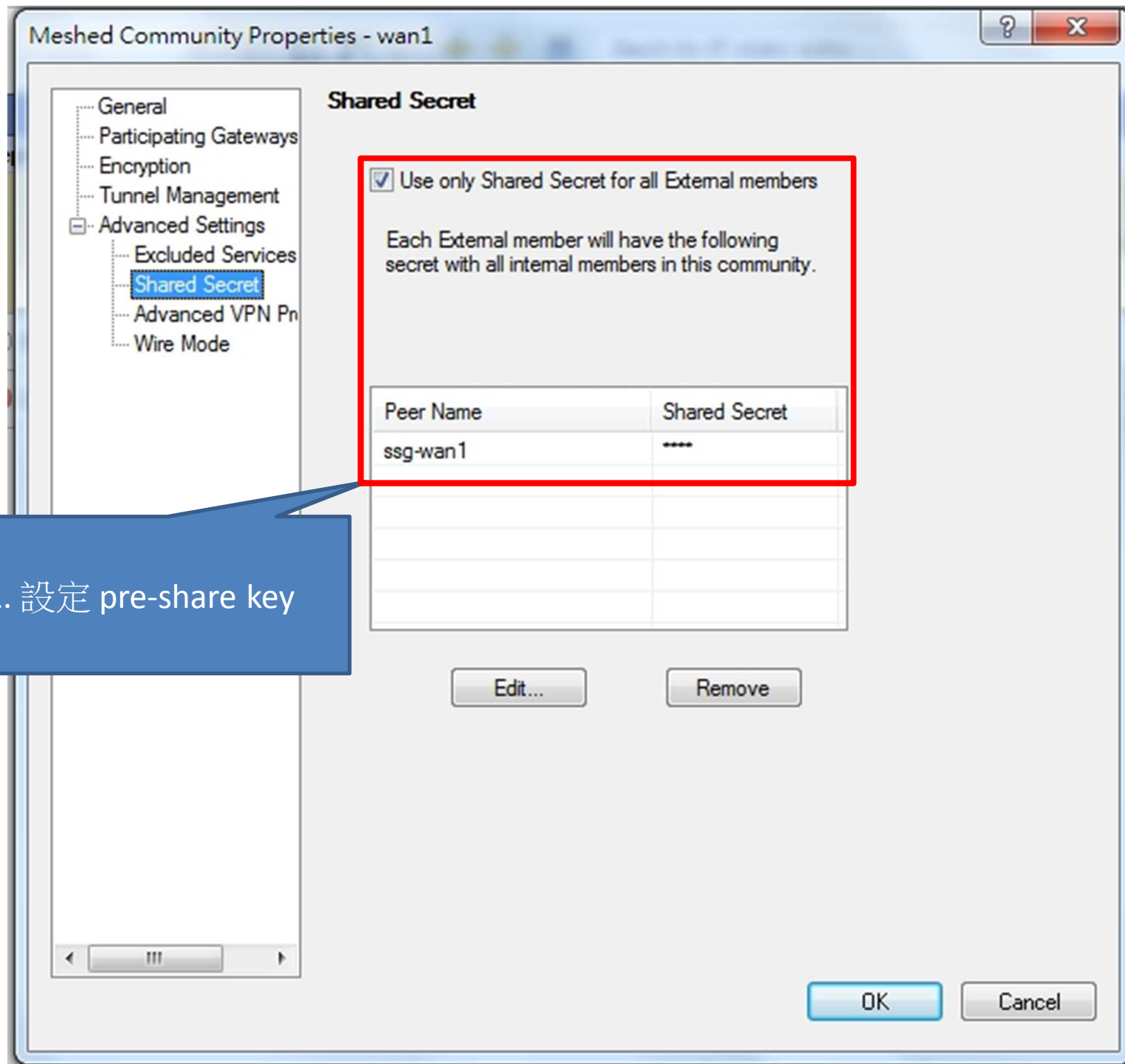


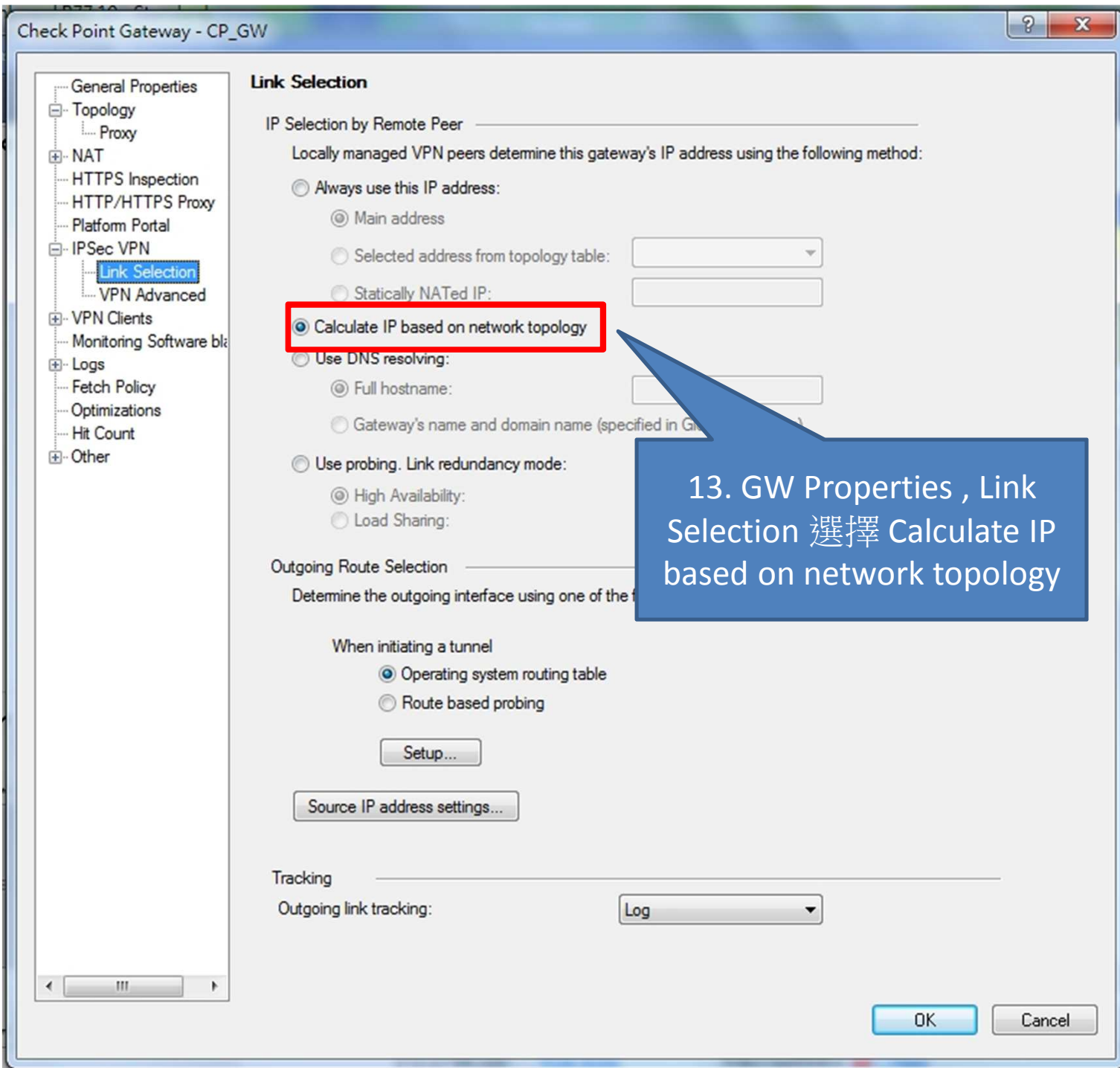


9. 新增 VPN community, 勾選此選項, CP 會自動新增所需的 Security rule

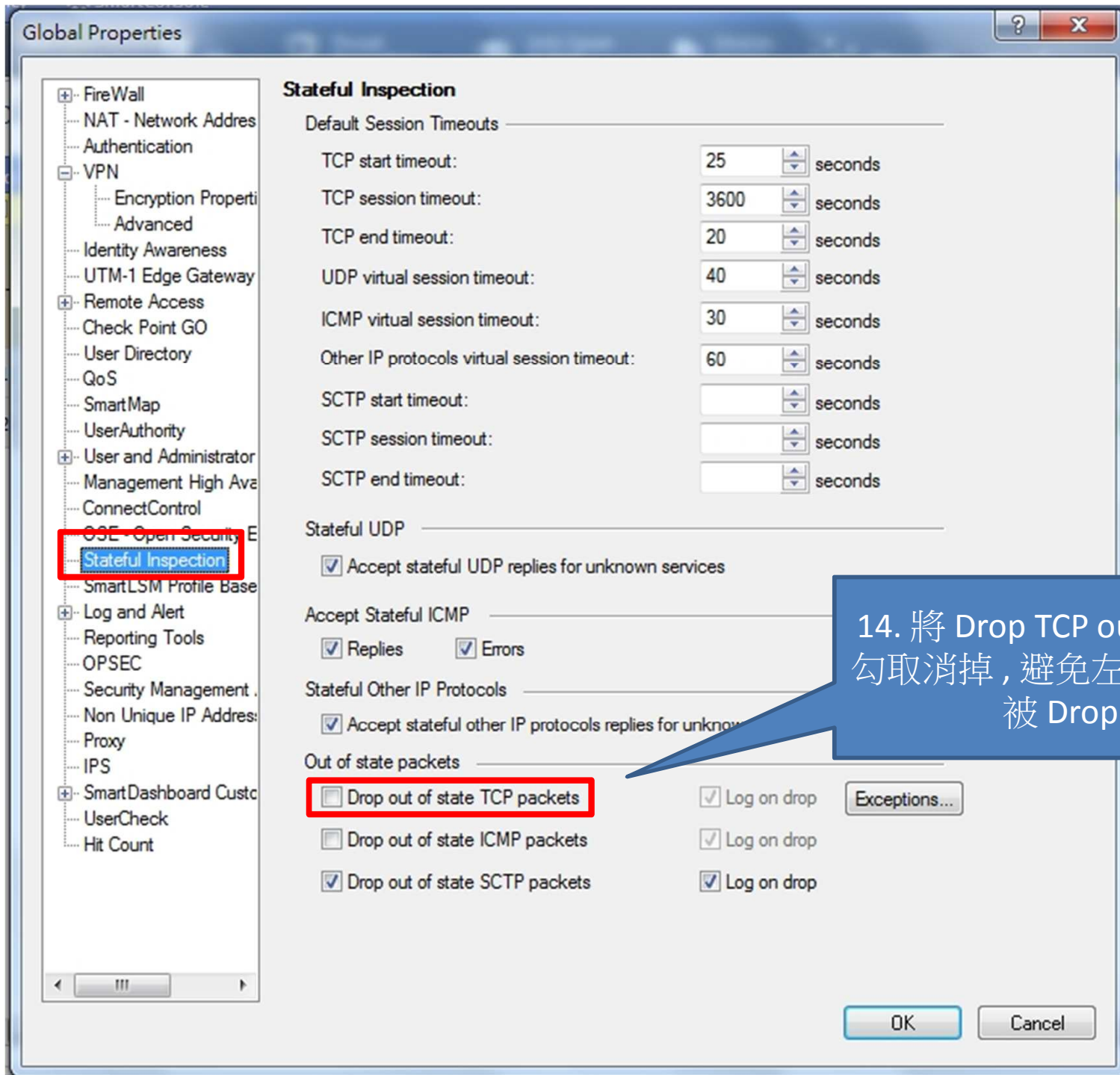












# 功能驗證

# Checkpoint OSPF interfaces

```
R77.10-GW> show ospf interfaces
```

Name	IP Address	Area ID	State	NC	DR Interface	BDR Interface
vpnt10000	10.1.1.1	0.0.0.0	P2P	1	0.0.0.0	0.0.0.0
vpnt20	10.2.2.1	0.0.0.0	P2P	1	0.0.0.0	0.0.0.0
eth3	192.168.11.254	0.0.0.0	DR	0	192.168.11.254	0.0.0.0

```
R77.10-GW> █
```

# Checkpoint OSPF neighbors

```
R77.10-GW> show ospf neighbors

Neighbor state flag: G - graceful restart

Neighbor ID      Pri   State   Dead    Address      Interface     Err
-----
192.168.10.254   1     FULL    104     10.1.1.1     10.1.1.1     1
192.168.10.254   1     FULL    92      10.2.2.1     10.2.2.1     0

R77.10-GW> █
```



# SSG OSPF interfaces

```
SSG350M-> get vr trust-vr protocol ospf interface
VR: trust-vr RouterId: 192.168.10.254
-----
D - Down, L - Loopback, W - Wait, PTP - Point-to-Point
DR - Designated Router, BDR - Backup Designated Router
O - Other
Int      IpAddr      NetMask      AreaId      Status      St
-----
eth0/0   192.168.10.254 255.255.255.0 0.0.0.0     enabled     DR
tun.1    10.1.1.1      255.255.255.0 0.0.0.0     enabled     PTP
tun.2    10.2.2.1      255.255.255.0 0.0.0.0     enabled     PTP
SSG350M->
```



# SSG OSPF neighbors

```
SSG350M-> get vr trust-vr protocol ospf neighbor  
VR: trust-vr RouterId: 192.168.10.254
```

```
-----  
Neighbor(s) on interface tunnel.2 (Area 0.0.0.0)  
-----  
IpAddr/IfIndex RouterId Pri State Opt Up StateChg  
-----  
10.2.2.2 3.3.3.3 0 Full E 3d;16:54:30 (+6 -0)
```

```
-----  
Neighbor(s) on interface tunnel.1 (Area 0.0.0.0)  
-----  
IpAddr/IfIndex RouterId Pri State Opt Up StateChg  
-----  
10.1.1.2 3.3.3.3 0 Full E 3d;16:49:20 (+6 -0)
```

```
Neighbor(s) on interface ethernet0/0 (Area 0.0.0.0)
```

```
SSG350M->
```

# SSG routing table

```
SSG350M-> get route
```

```
IPv4 Dest-Routes for <untrust-vr> (0 entries)
```

```
H: Host C: Connected S: Static A: Auto-Exported  
I: Imported R: RIP/RIPng P: Permanent D: Auto-Discovered  
N: NHRP  
iB: IBGP eB: EBGP O: OSPF/OSPFv3 E1: OSPF external type 1  
E2: OSPF/OSPFv3 external type 2 trailing B: backup route
```

```
IPv4 Dest-Routes for <trust-vr> (18 entries)
```

ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
* 4	1.1.1.1/32	eth0/1	0.0.0.0	H	0	0	Root
* 6	2.2.2.1/32	eth0/2	0.0.0.0	H	0	0	Root
* 10	10.1.1.1/32	tun.1	0.0.0.0	H	0	0	Root
58	10.1.1.1/32	tun.2	10.2.2.2	O	60	11	Root
82	10.1.1.1/32	tun.1	10.1.1.2	O	60	11	Root
* 12	10.2.2.1/32	tun.2	0.0.0.0	H	0	0	Root
91	10.2.2.1/32	tun.2	10.2.2.2	O	60	11	Root
92	10.2.2.1/32	tun.1	10.1.1.2	O	60	11	Root
* 7	172.17.99.0/24	eth0/3	0.0.0.0	C	0	0	Root
* 2	192.168.10.254/32	eth0/0	0.0.0.0	H	0	0	Root
* 87	192.168.11.0/24	tun.2	10.2.2.2	O	60	11	Root
* 88	192.168.11.0/24	tun.1	10.1.1.2	O	60	11	Root
* 1	192.168.10.0/24	eth0/0	0.0.0.0	C	0	0	Root
* 8	172.17.99.125/32	eth0/3	0.0.0.0	H	0	0	Root
* 9	10.1.1.0/24	tun.1	0.0.0.0	C	0	0	Root
* 11	10.2.2.0/24	tun.2	0.0.0.0	C	0	0	Root
* 5	2.2.2.0/24	eth0/2	0.0.0.0	C	0	0	Root
* 3	1.1.1.0/24	eth0/1	0.0.0.0	C	0	0	Root