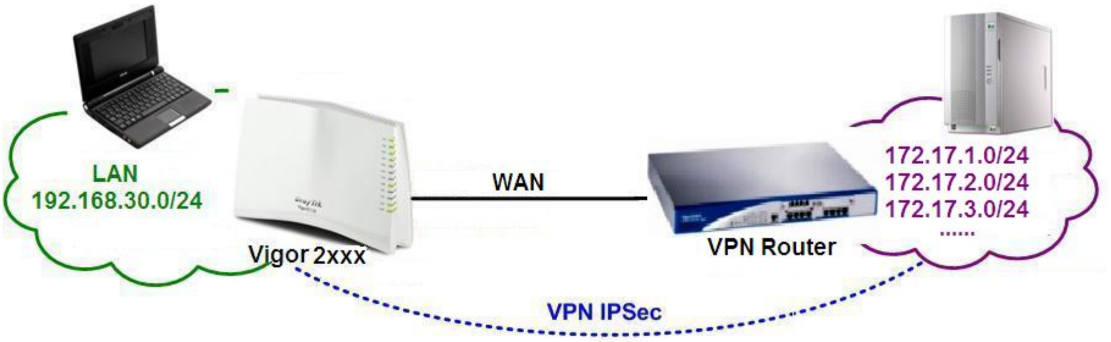
Multiple SA Application Note

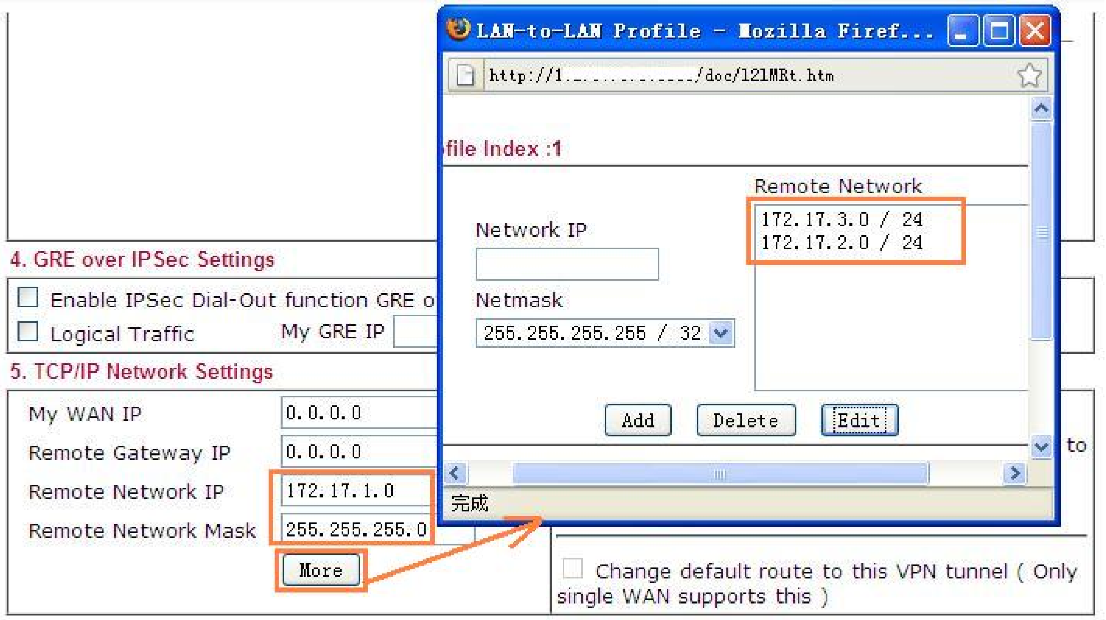
Background

Suppose we have the following scenario. On the left side is a Vigor 2xxx router, for example a Vigor 2950. Behind the VPN Router are multiple subnets. To access all these subnets via the IPSec tunnel from 192.168.30.0/24 we have two methods: **static routes** or **multiple SA's**.



Static Route over IPSec tunnel

If the VPN Router is also a Vigor 2xxx router, we can use the **static routes over IPSec tunnel** feature which is supported by all Vigor 2xxx series routers. In this case, you add the multiple subnets in Vigor 2xxx on the left side. See figure shown below.


LAN-to-LAN Profile - Mozilla Firef...
http://1._............/doc/121MRt.htm
Add
Delete
Edit
More
完成
to

file Index :1

Remote Network
172.17.3.0 / 24
172.17.2.0 / 24

Network IP:

Netmask: 255.255.255.255 / 32

4. GRE over IPSec Settings

☐ Enable IPSec Dial-Out function GRE o

☐ Logical Traffic My GRE IP

5. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

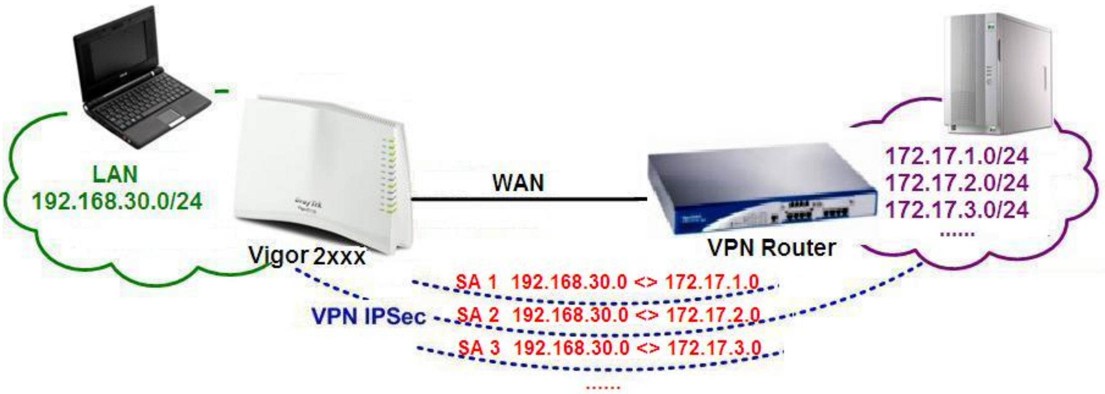
Remote Network IP: 172.17.1.0

Remote Network Mask: 255.255.255.0

☐ Change default route to this VPN tunnel (Only single WAN supports this)

Multiple SA's (Security Associations)

If the VPN Router is a Vigor 3300/V or any other 3rd party router which doesn't support **static routes over IPSec tunnel** feature, you have to use IPSec multiple SA's feature.



Introduction

This topic explains how to use multiple SA on Vigor router. And this application note is divided into the following two sections.

Section I tells you how to use Multiple SA feature between two routers.

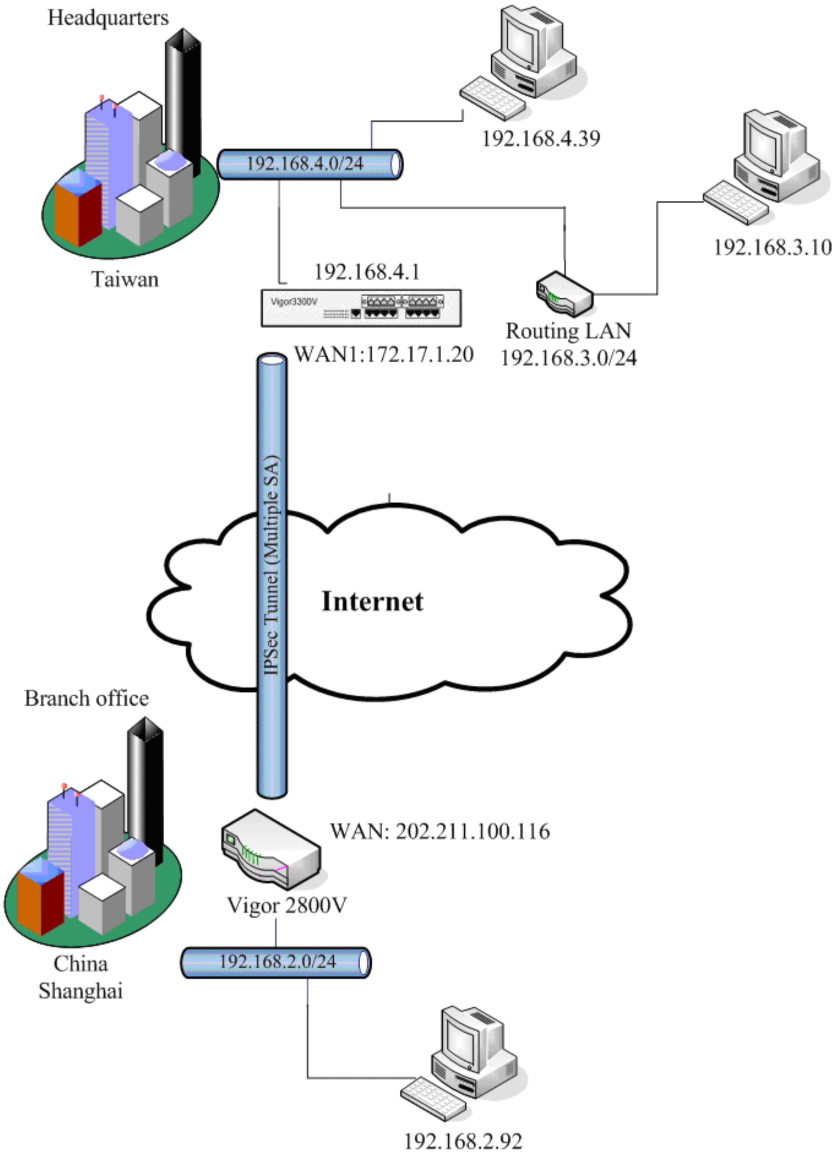
Section II tells you how to use Multiple SA feature to achieve VPN three parts communication.

Section I

In this example, the Branch office has a Vigor 2800V router. And the headquarters office has a Vigor 3300V router.

Both 2800V and 3300V support multiple SA.

This feature is enabled by default, you don't need to manually 'enable' it.



	Headquarters 3300V	Branch Office 2800V
WAN IP	172.17.1.20	202.211.100.116
LAN IP	192.168.4.1	192.168.2.1
Internal network	192.168.3.0/24 192.168.4.0/24	192.168.2.0/24
Encryption Method	DES－SHA1	DES－SHA1

In order to access both two subnets on 3300V sites from 2800V site through VPN tunnel, we should build two IPSec tunnels from 2800V to 3300V.

The first tunnel is between these two subnets:

192.168.2.0/24 and 192.168.4.0/24

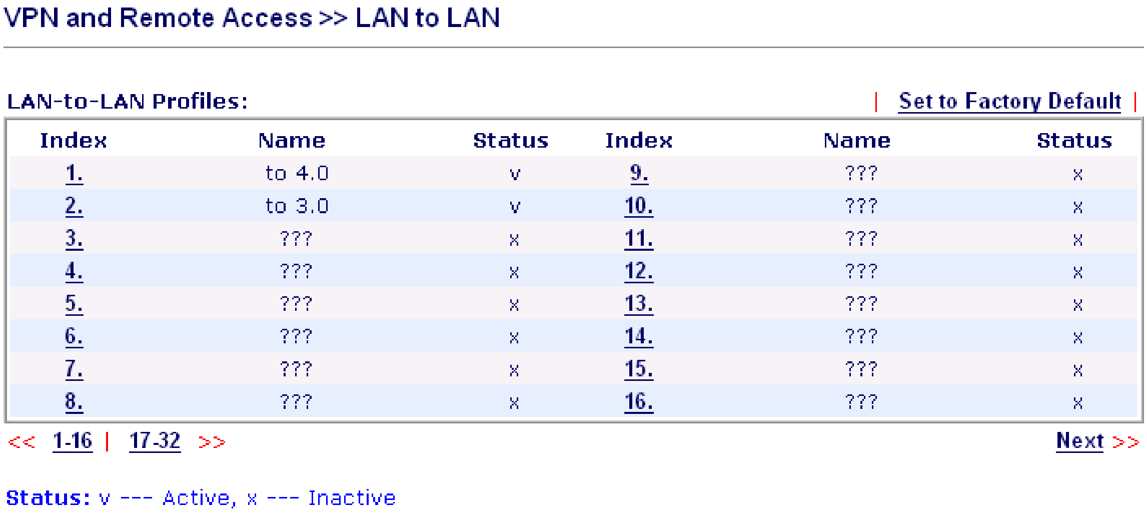
The second tunnel is between these two subnets:

192.168.2.0/24 and 192.168.3.0/24

Please note: You must set the same pre-shared key for both of two tunnels!

On 2800V's **VPN and Remote Access >> LAN to LAN** setup page,

Please create two VPN profiles and configure as follows:



VPN and Remote Access >> LAN to LAN

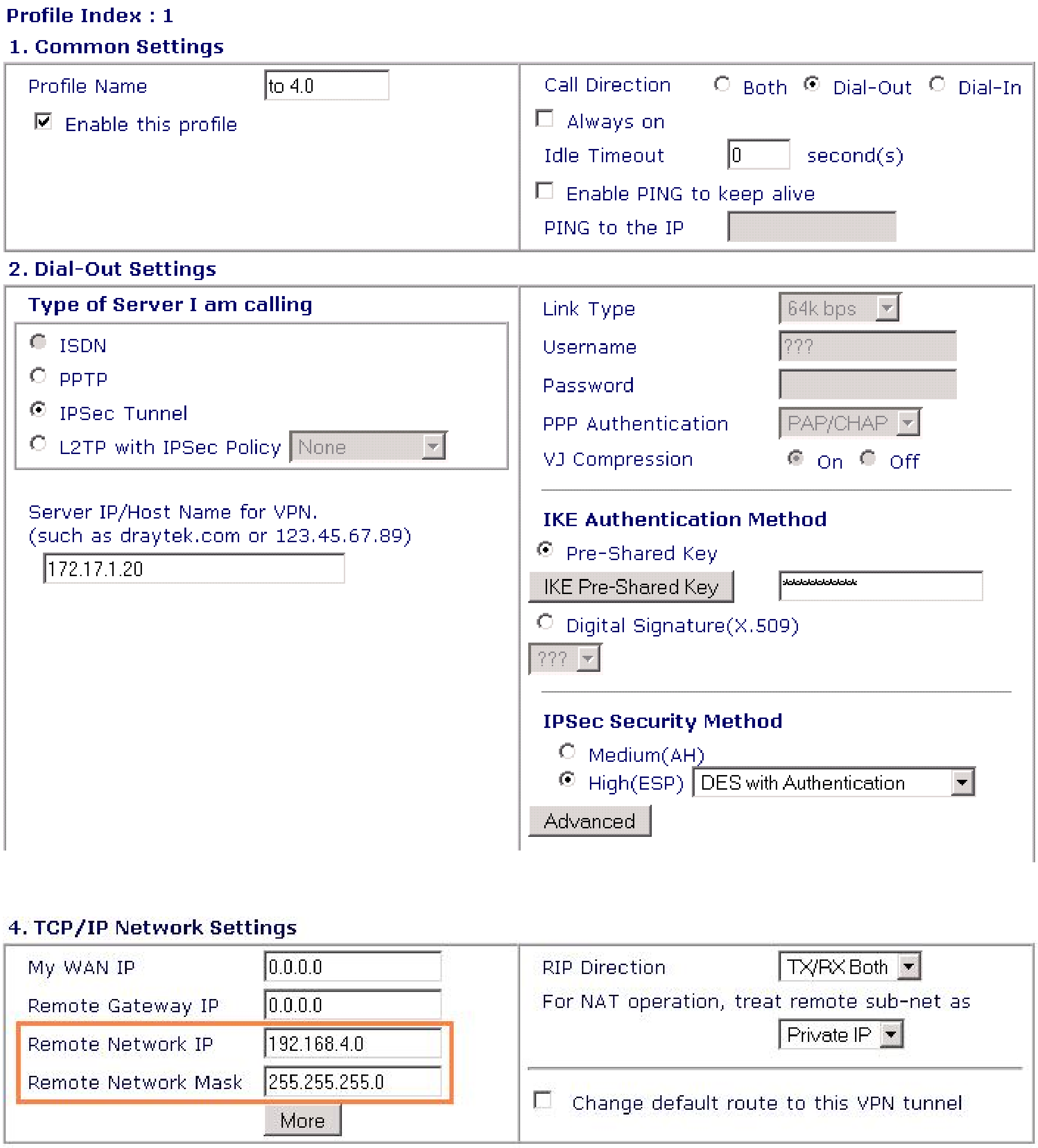
LAN-to-LAN Profiles: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	to 4.0	v	9.	???	x
2.	to 3.0	v	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< 1-16 | 17-32 >> Next >>

Status: v --- Active, x --- Inactive

Profile 1



Profile Index : 1

1. Common Settings

Profile Name: to 4.0

☑ Enable this profile

Call Direction ○ Both ● Dial-Out ○ Dial-In

□ Always on

Idle Timeout: 0 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
172.17.1.20

Link Type: 64k bps

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: **********

○ Digital Signature(X.509)

???

IPSec Security Method

○ Medium(AH)

● High(ESP): DES with Authentication

Advanced

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.4.0

Remote Network Mask: 255.255.255.0

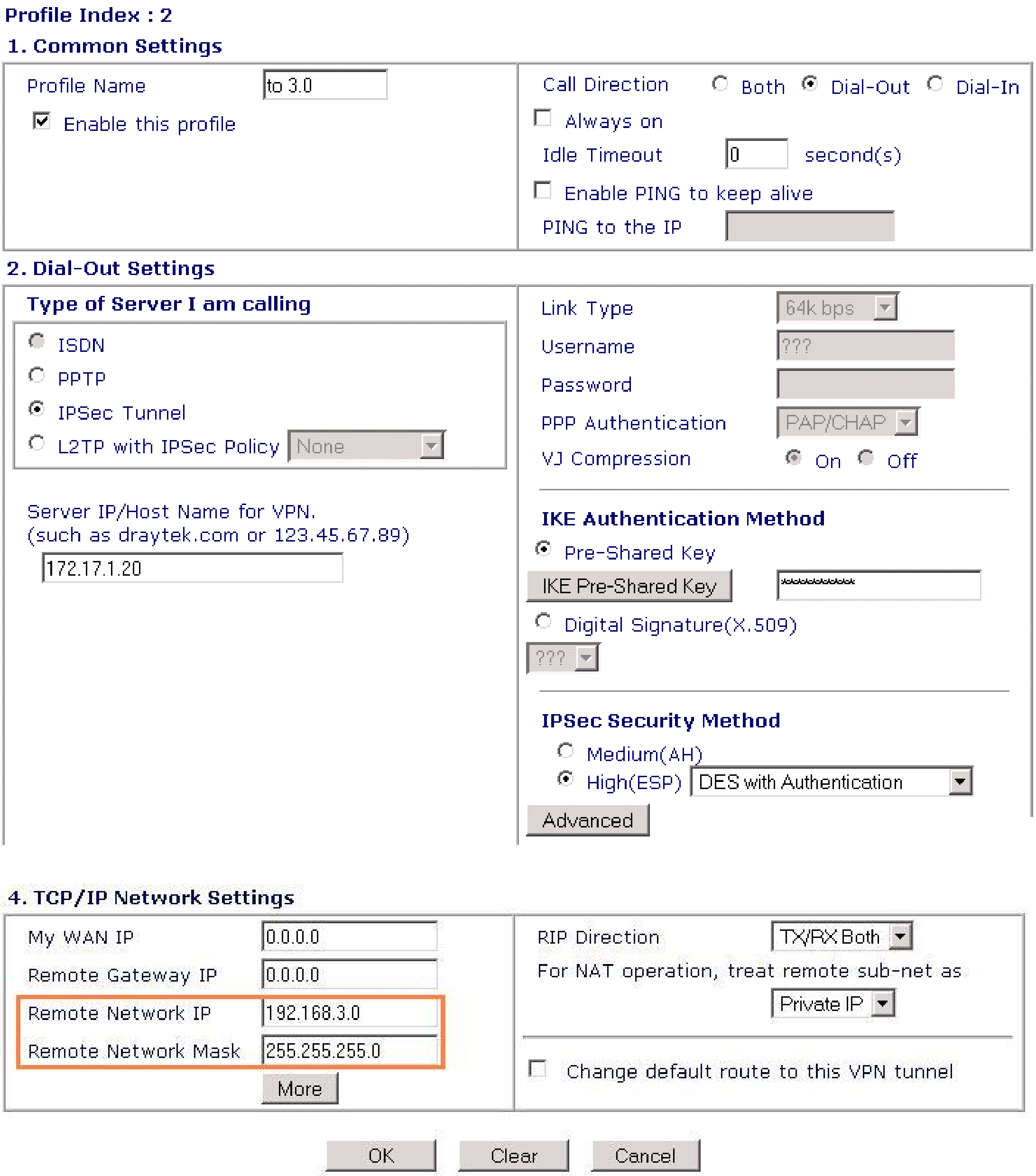
More

RIP Direction: TX/RX Both

For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

Profile 2



Profile Index : 2

1. Common Settings

Profile Name: to 3.0

☑ Enable this profile

Call Direction ○ Both ● Dial-Out ○ Dial-In

□ Always on

Idle Timeout: 0 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

172.17.1.20

Link Type: 64k bps

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: **********

○ Digital Signature(X.509)

???

IPSec Security Method

○ Medium(AH)

● High(ESP): DES with Authentication

Advanced

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.3.0

Remote Network Mask: 255.255.255.0

More

RIP Direction: TX/RX Both

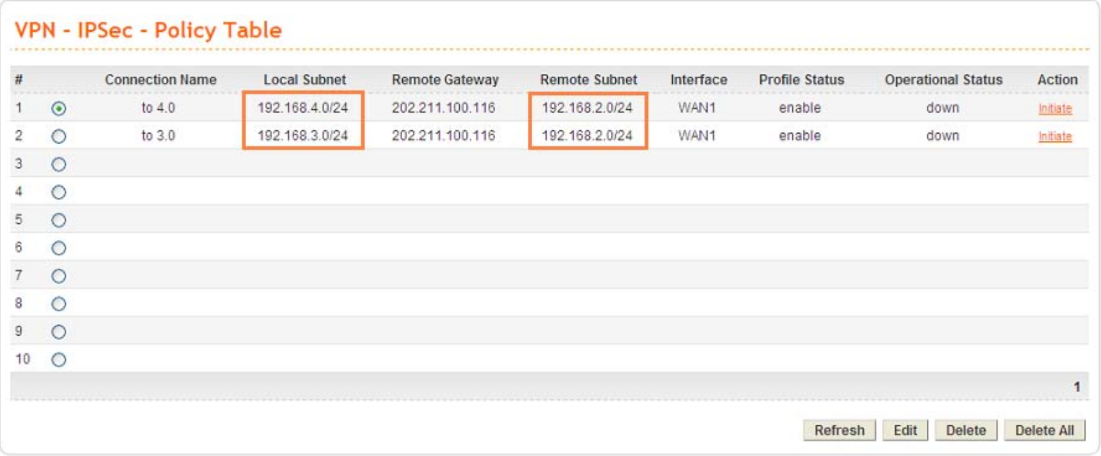
For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

OK Clear Cancel

On 3300V site, please also create two IPSec policies on

VPN - IPSec - Policy Table setup page:

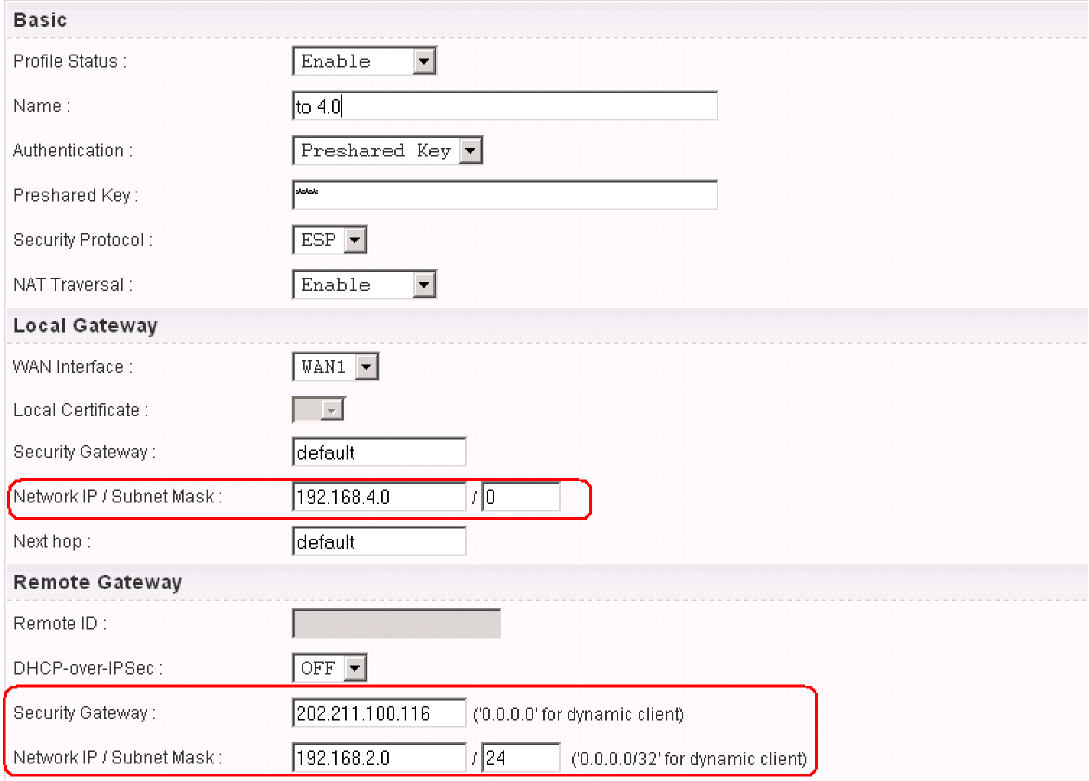


VPN - IPSec - Policy Table

#		Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Interface	Profile Status	Operational Status	Action
1	●	to 4.0	192.168.4.0/24	202.211.100.116	192.168.2.0/24	WAN1	enable	down	Initiate
2	○	to 3.0	192.168.3.0/24	202.211.100.116	192.168.2.0/24	WAN1	enable	down	Initiate
3	○								
4	○								
5	○								
6	○								
7	○								
8	○								
9	○								
10	○								

1

Profile 1



Basic

Profile Status : Enable

Name : to 4.0

Authentication : Preshared Key

Preshared Key : ***

Security Protocol : ESP

NAT Traversal : Enable

Local Gateway

WAN Interface : WAN1

Local Certificate :

Security Gateway : default

Network IP / Subnet Mask : 192.168.4.0 / 0

Next hop : default

Remote Gateway

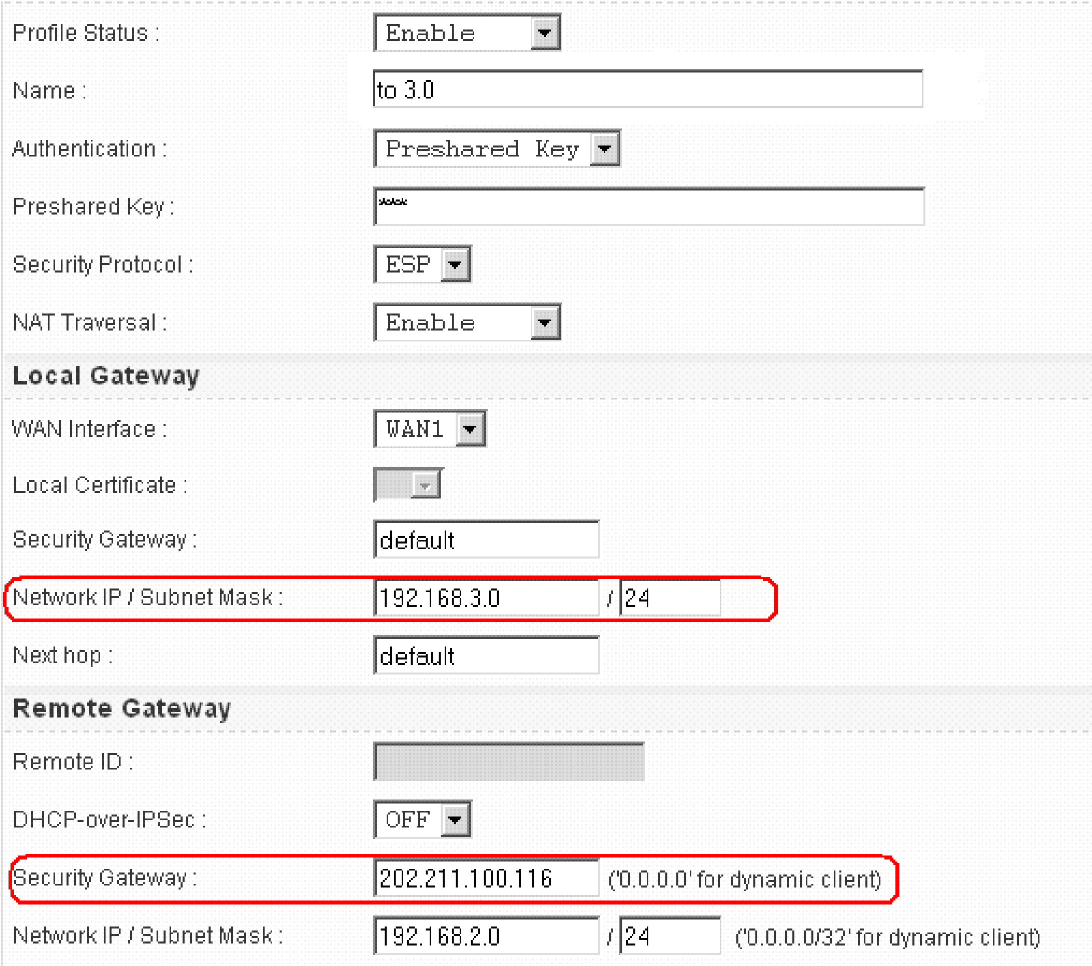
Remote ID :

DHCP-over-IPSec : OFF

Security Gateway : 202.211.100.116 ('0.0.0.0' for dynamic client)

Network IP / Subnet Mask : 192.168.2.0 / 24 ('0.0.0.0/32' for dynamic client)

Profile 2



Profile Status :	Enable
Name :	to 3.0
Authentication :	Preshared Key
Preshared Key :	***
Security Protocol :	ESP
NAT Traversal :	Enable

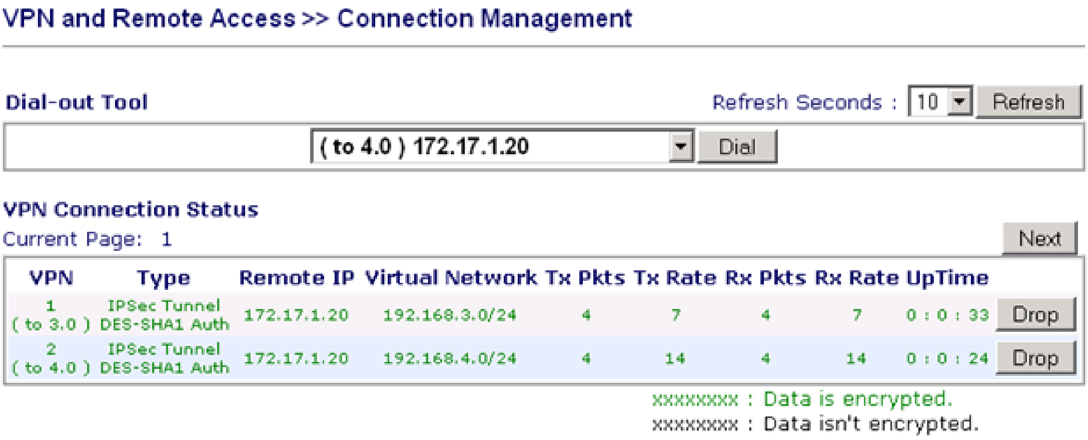
Local Gateway

WAN Interface :	WAN1
Local Certificate :	
Security Gateway :	default
Network IP / Subnet Mask :	192.168.3.0 / 24
Next hop :	default

Remote Gateway

Remote ID :	
DHCP-over-IPSec :	OFF
Security Gateway :	202.211.100.116 ('0.0.0.0' for dynamic client)
Network IP / Subnet Mask :	192.168.2.0 / 24 ('0.0.0.0/32' for dynamic client)

After the tunnels are up, we can access both two subnets behind 3300V from 2800 site through VPN tunnel and vice versa.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

(to 4.0) 172.17.1.20 Dial

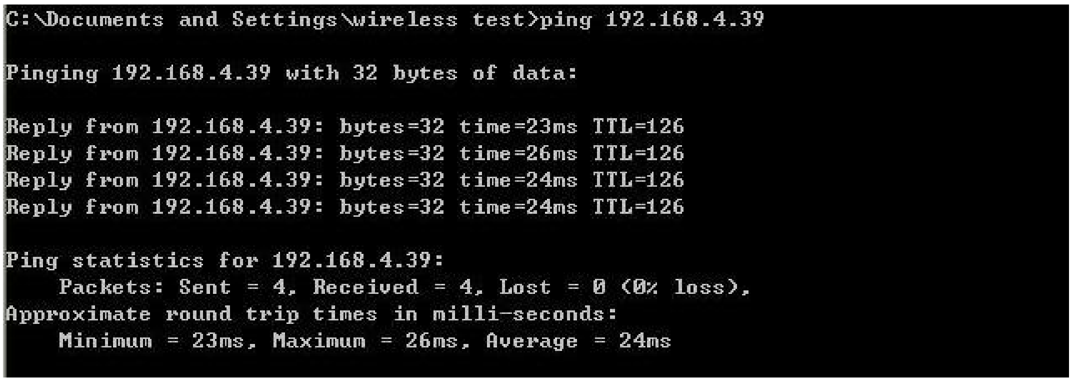
VPN Connection Status

Current Page: 1

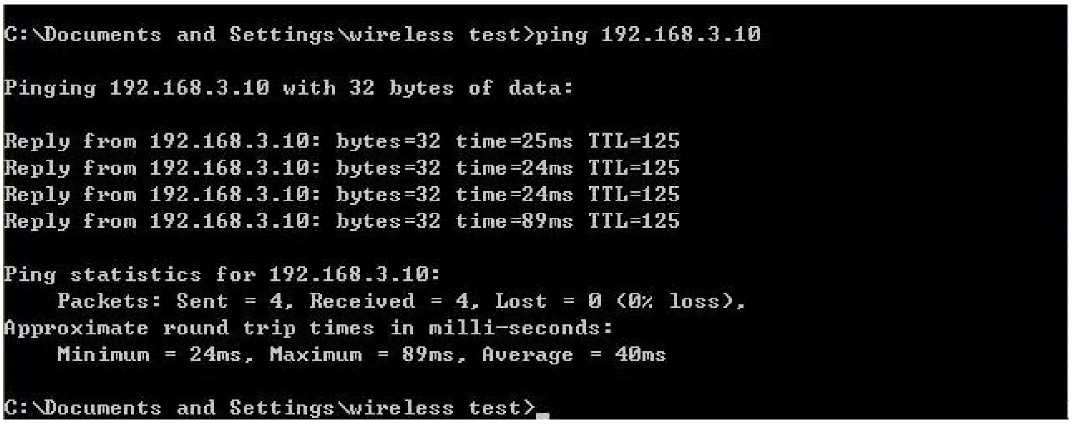
Next

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
1 (to 3.0)	IPSec Tunnel DES-SHA1 Auth	172.17.1.20	192.168.3.0/24	4	7	4	7	0 : 0 : 33	Drop
2 (to 4.0)	IPSec Tunnel DES-SHA1 Auth	172.17.1.20	192.168.4.0/24	4	14	4	14	0 : 0 : 24	Drop

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.



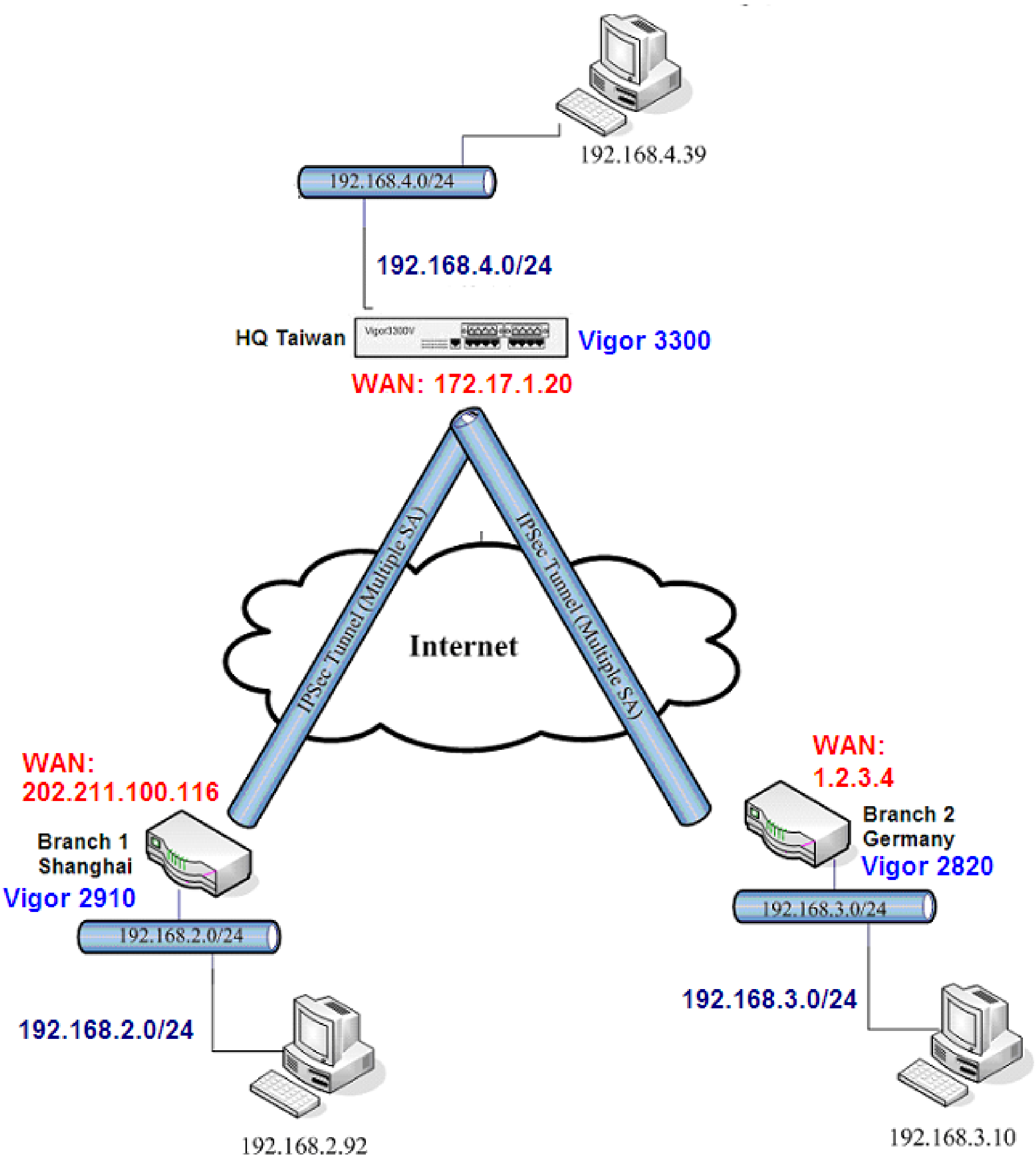
```
C:\Documents and Settings\wireless test>ping 192.168.4.39

Pinging 192.168.4.39 with 32 bytes of data:

Reply from 192.168.4.39: bytes=32 time=23ms TTL=126
Reply from 192.168.4.39: bytes=32 time=26ms TTL=126
Reply from 192.168.4.39: bytes=32 time=24ms TTL=126
Reply from 192.168.4.39: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.4.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 26ms, Average = 24ms
```



```
C:\Documents and Settings\wireless test>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time=25ms TTL=125
Reply from 192.168.3.10: bytes=32 time=24ms TTL=125
Reply from 192.168.3.10: bytes=32 time=24ms TTL=125
Reply from 192.168.3.10: bytes=32 time=89ms TTL=125

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 89ms, Average = 40ms

C:\Documents and Settings\wireless test>
```

Section II

In this example, there are two branch offices Shanghai (2800V) and Hongkong (2800V’). Both of two branch offices’ routers connect to headquarters office’s 3300V through VPN tunnel. There is no VPN tunnel between the two branch offices. We should use Multiple SA function to achieve VPN three parts communication.



	Headquarters 3300V	Branch 1 Shanghai 2910	Branch 2 Hongkong 2820
WAN IP	172.17.1.20	202.211.100.116	1.2.3.4
LAN IP	192.168.4.1	192.168.2.1	192.168.3.1
Internal network	192.168.4.0/24	192.168.2.0/24	192.168.3.0/24

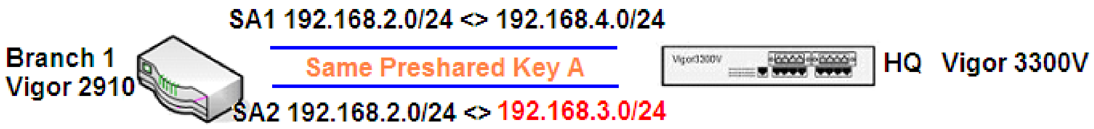
We should create two VPN profiles on each 2800V routers.

We must use the same pre-shared key on each 2800's two profiles.

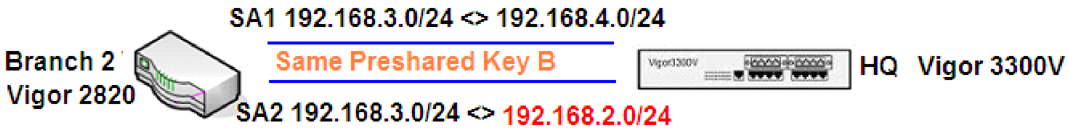
Also, we should create four IPsec policies on 3300V.

About VPN network settings, please refer to the below Table:

For the other VPN basic settings, please refer to the example in Section I.



Branch 1
Vigor 2910
SA1 192.168.2.0/24 <> 192.168.4.0/24
Same Preshared Key A
SA2 192.168.2.0/24 <> 192.168.3.0/24
HQ Vigor 3300V



Branch 2
Vigor 2820
SA1 192.168.3.0/24 <> 192.168.4.0/24
Same Preshared Key B
SA2 192.168.3.0/24 <> 192.168.2.0/24
HQ Vigor 3300V

Profile Index	Router	Preshared Key	Remote gateway	Local subnet	Remote subnet
1	**Vigor2910**	**A**	172.17.1.20	default	192.168.4.0/24
2	**Vigor2910**	**A**	172.17.1.20	default	192.168.3.0/24
1	**Vigor2820**	**B**	172.17.1.20	default	192.168.4.0/24
2	**Vigor2820**	**B**	172.17.1.20	default	192.168.2.0/24
1	**Vigor3300V**	**A**	202.211.100.116	192.168.4.0	192.168.2.0/24
2	**Vigor3300V**	**A**	202.211.100.116	192.168.3.0	192.168.2.0/24
3	**Vigor3300V**	**B**	1.2.3.4	192.168.4.0	192.168.3.0/24
4	**Vigor3300V**	**B**	1.2.3.4	192.168.2.0	192.168.3.0/24