



How to Configure PnVPN

Hillstone Networks Inc.



Submitter	Auditor		Version	Date
Name	Name		V1	2018/x/xY

Content

1. Preface.....	3
2. Topology	3
3. Step by Step.....	4
4. Troubleshooting	16

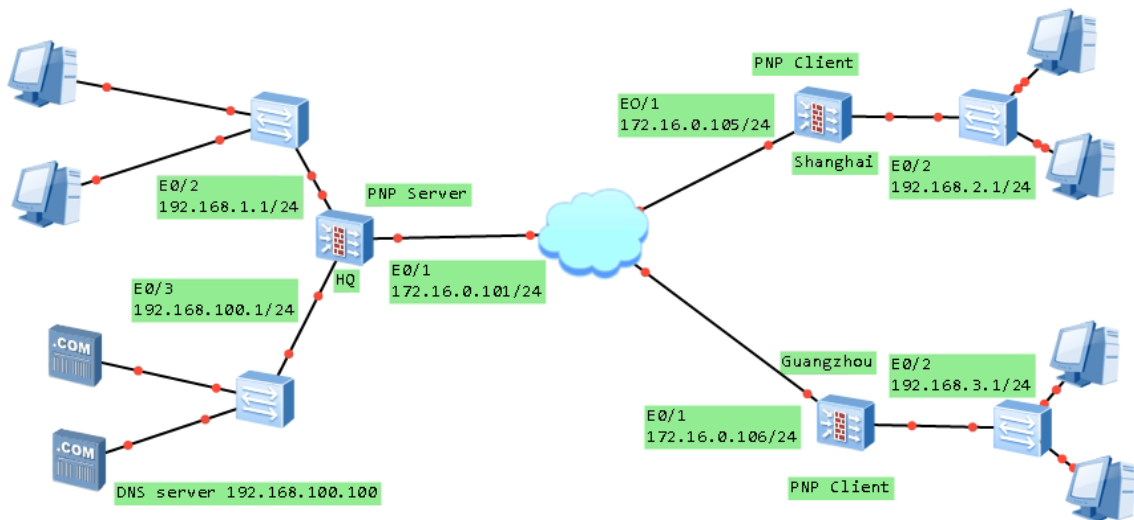
1. Preface

This setting guide is for PnP IPsec vpn, for further support please contact TAC

The workflow for PnPVPN is as follows:

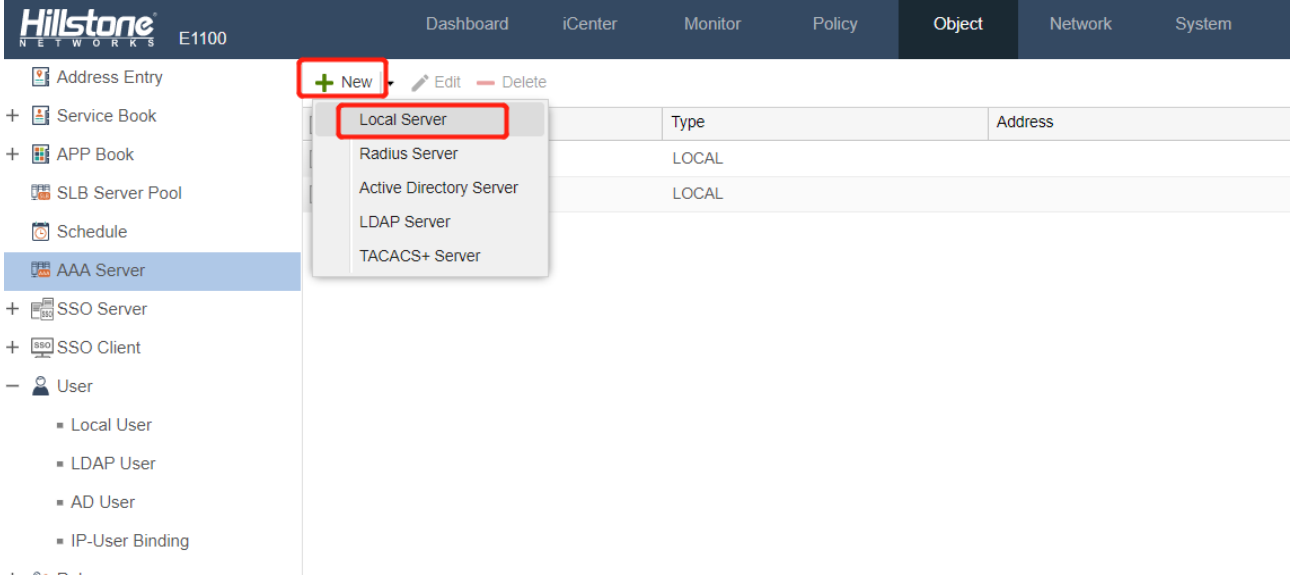
1. The client initiates a connection request and sends its own ID and password to the server.
2. The server validates the ID and password when it receives the client request. If the client passes the authentication, the server issues configuration information including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc. to the client.
3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

2. Topology

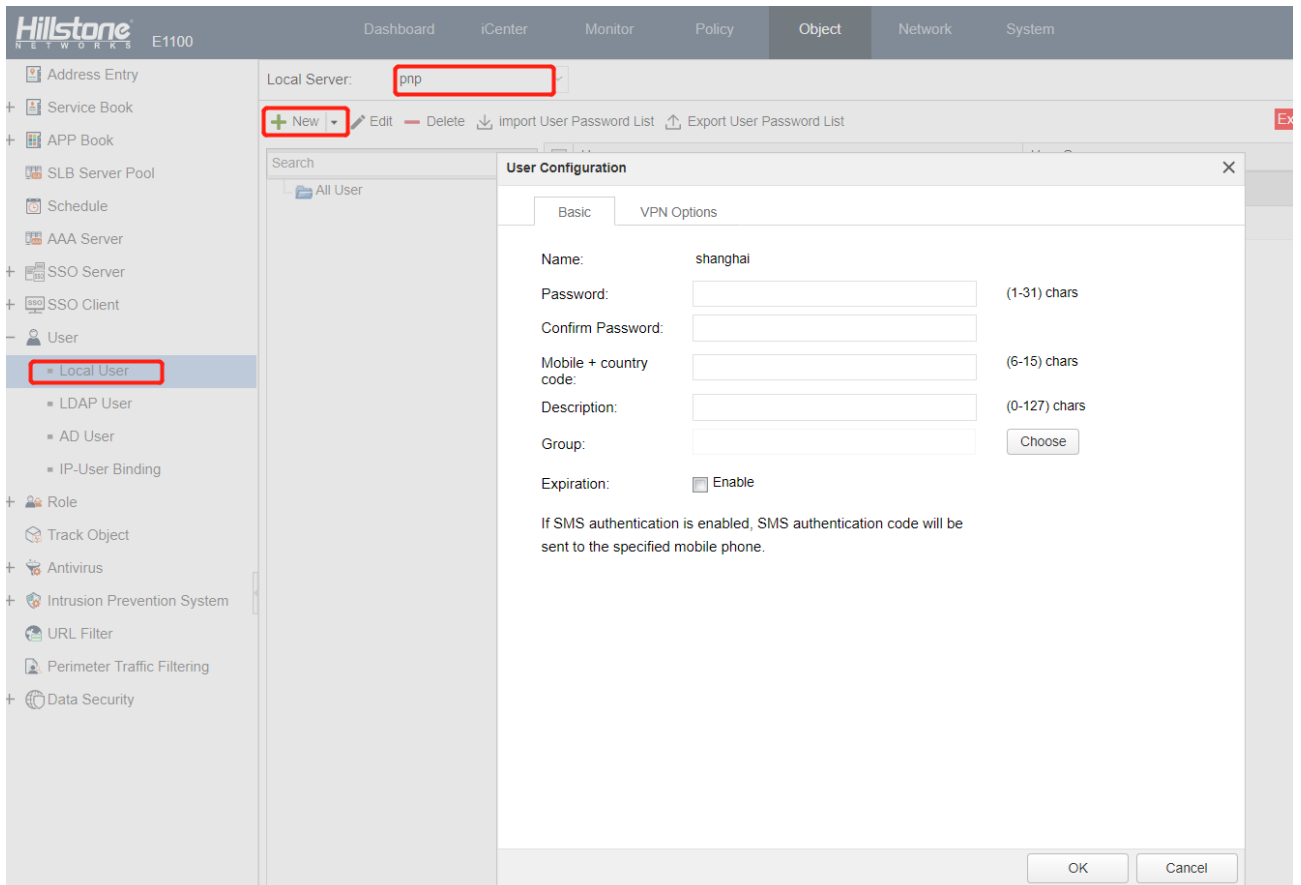


3. Step by Step

Configure AAA server and user, choose Local Server

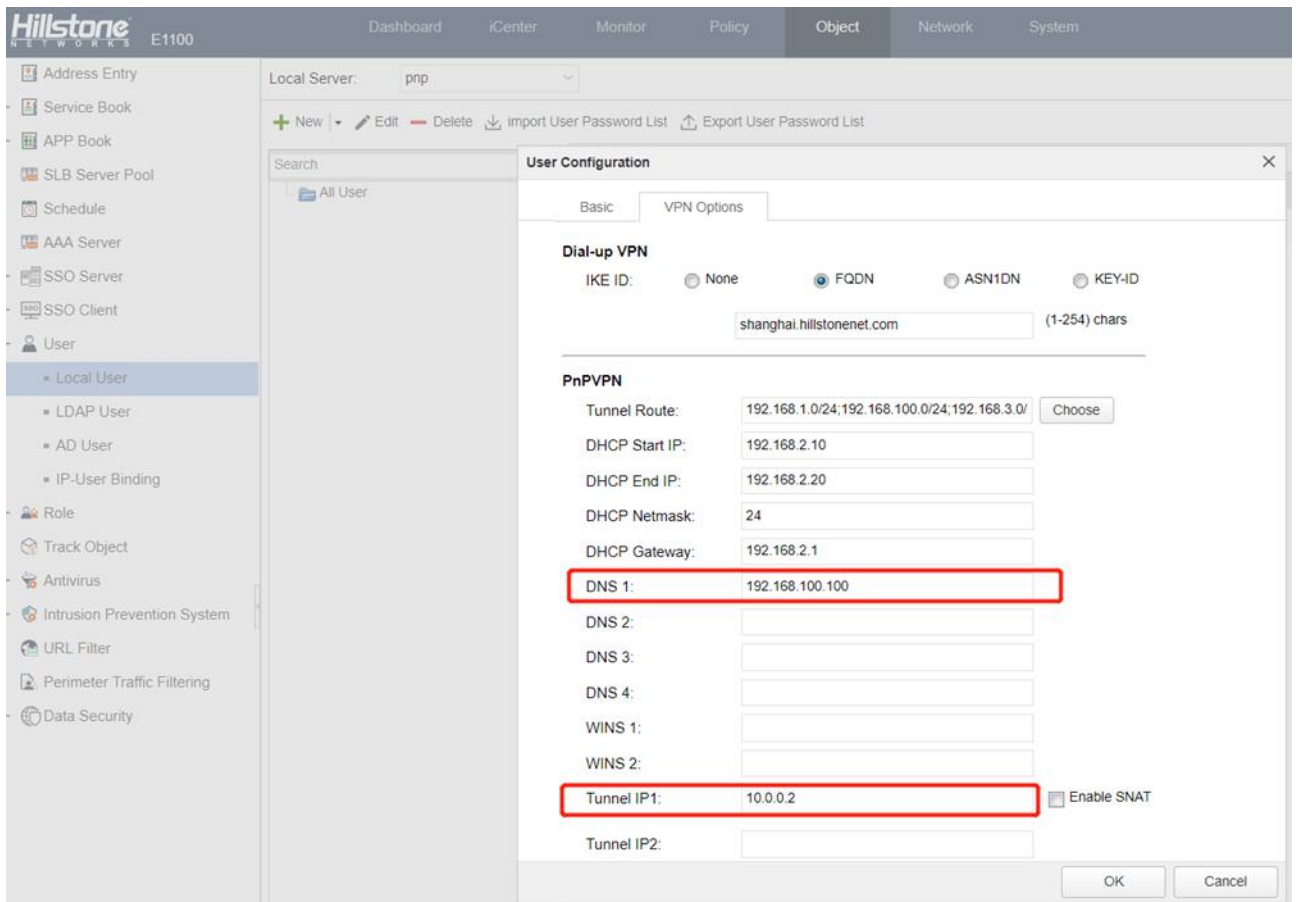


Add user in the AAA server you have created



Configure user's network

Caution: If there is an internal DNS server in server side which would be used by client side, you need to configure Tunnel IP for this user, because PnPVPN enabled DNS proxy on the VPN incoming interface, client firewall works as a DNS proxy for client PC or client server, if there is no Tunnel IP configured, the DNS proxy would fail



Configure IKE VPN

Start with p1 proposal, here we use default setting

The dialog box is titled "Phase1 Proposal Configuration" and contains the following settings:

- Proposal Name: p1
- Authentication: Pre-share, RSA-Signature, DSA-Signature
- Hash: MD5, SHA, SHA-256, SHA-384, SHA-512
- Encryption: 3DES, DES, AES, AES-192, AES-256
- DH Group: Group1, Group2, Group5, Group14, Group15, Group16
- Lifetime: 86400 (300-86400)seconds, default: 86400

Buttons: OK, Cancel

Then comes p2 proposal, pay attention here that PFS Group should choose Group2

The dialog box is titled "Phase2 Proposal Configuration" and contains the following settings:

- Proposal Name: p2
- Protocol: ESP, AH
- Hash: MD5, SHA, SHA-256, SHA-384, SHA-512, NULL (Up to 3 can be selected.)
- Encryption: 3DES, DES, AES, AES-192, AES-256, NULL (Up to 4 can be selected.)
- Compression: None, Deflate
- PFS Group: Group1, Group2, Group5, Group14, Group15, Group16, No PFS
- Lifetime: 28800 (180-86400) seconds, default: 28800
- Lifsize: Enable

Buttons: OK, Cancel

Now configure VPN peer, it is a little different from site-to-site IPSec, after fill in the parameter, click Generate button to generate PnP client user password

The image shows the 'VPN Peer Configuration' dialog box with the 'Basic' tab selected. The following fields are highlighted with red boxes:

- Name: pnp
- Interface: ethernet0/1
- Mode: Aggressive
- Type: User Group
- AAAServer: pnp
- Local ID: None
- Peer ID: None
- Proposal1: p1
- Per-shared Key: (5-127) chars
- User Key:

The image shows the 'VPN Peer Configuration' dialog box with the 'Basic' tab selected. The 'Generate the User Key' sub-dialog is open, showing the following fields:

- IKE ID: shanghai.hillstonenet.com (1-255) chars
- Per-shared Key: (5-127) chars
- Generate Result: zIRoryEutAU81dCZLEH4K+LN/z8=

Red annotations are present:

- A red box around the 'Per-shared Key' field in the sub-dialog with the text "auto fill in" and an arrow pointing to it.
- A red box around the 'Generate Result' field with the text "this is for client user to use" and an arrow pointing to it.
- A red box around the 'Per-shared Key' field in the main dialog.
- A red box around the 'Generate' button in the main dialog.

Then go to advanced page of VPN peer, choose Generate Route option to generate route towards client subnet automatically

VPN Peer Configuration

Basic | **Advanced**

Connection Type: Bidirectional Initiator Responder

NAT Traversal: Enable

Any Peer ID: Enable

Generate Route: Enable

DPD: Enable

Description: (1-255) chars

XAUTH Server: Enable

OK Cancel

Configure IKE VPN options

IKE VPN Configuration

Basic | **Advanced**

Peer

Peer Name:

Information:

Name	Mode	Type	Local ID	Peer ID
pnp	Aggressive	User Group		

Tunnel

Name:

Mode: tunnel transport

P2 Proposal:

Proxy ID: Auto Manual

OK Cancel

On the advanced option page, here are some parameters overlapped with user configuration page, they are designed for distributing uniform parameter to save troubles, when there is a conflict between the two settings, configuration in the user configuration mode has higher priority over settings in the IKE tunnel configuration mode

The screenshot shows the 'IKE VPN Configuration' dialog box with the 'Advanced' tab selected. The 'Basic' tab is also visible. The following parameters are listed:

- DNS1:
- DNS2:
- DNS3:
- DNS4:
- WINS1:
- WINS2:
- Enable Idle Time: Enable
- DF-Bit: Copy Clear Set
- Anti-Replay: Disable 32 64 128 256 512
- Commit Bit: Enable
- Accept-all-proxy-ID: Enable
- Auto connect: Enable
- Tunnel Route:
- Description: (0-255) chars
- VPN Track: Enable

Buttons: OK, Cancel

User Configuration

Basic | **VPN Options**

Dial-up VPN

IKE ID: None FQDN ASN1DN KEY-ID

(1-254) chars

PnVPN

Tunnel Route:

DHCP Start IP:

DHCP End IP:

DHCP Netmask:

DHCP Gateway:

DNS 1:

DNS 2:

DNS 3:

DNS 4:

WINS 1:

WINS 2:

Tunnel IP1: Enable SNAT

Tunnel IP2:

Configure tunnel interface, of course ip address is needed if there configured Tunnel IP for client user

Tunnel Interface [X]

Basic Properties Advanced RIP

Basic

Interface Name: tunnel1

Description: [] (0-63) chars

Binding Zone: Layer 2 Zone Layer 3 Zone TAP No Binding

Zone: VPN [v]

HA sync: Enable

IP Configuration

Type: Static IP DHCP PPPoE

IP Address: 10.0.0.1

Net mask: 255.255.255.0

Set as Local IP

Enable DNS Proxy Proxy Proxy-Trans

Enable DNS Bypass

Advanced DHCP... [v]

Management

Telnet SSH Ping HTTP HTTPS SNMP

Routing

Reverse Route: Enable Close Auto

OK Cancel

Tunnel Interface

Basic Properties Advanced RIP

Advanced DHCP...

Management
 Telnet SSH Ping HTTP HTTPS SNMP

Routing
 Reverse Route: Enable Close Auto

Tunnel Binding
 Tunnel Type: IPsec VPN SSL VPN L2TP VPN
 VPN Name: pnp
 Gateway:

<input type="checkbox"/>	VPN Name	Type	Gateway
<input type="checkbox"/>	pnp	IPSec VPN	

Add Delete

Bandwidth
 Up Bandwidth: 1,000,000,000 (512,000 ~ 1000,000,000,000)bps
 Down Bandwidth: 1,000,000,000 (512,000 ~ 1000,000,000,000)bps

Proactive Webauth
 Enable local

OK Cancel

Since we have choose Generate Route option in VPN peer setting, here we don't bother to add routes manually, or we need to add it manually

Then comes to the policy making, make sure PnP client devices could access what they need to access through the tunnel

ID	Name	Source			Destination		Service	Applica
		Zone	Address	User	Zone	Address		
2		trust	any		untrust	any	any	
3		trust	any		VPN	any	any	
4		VPN	any		trust	any	any	
5		VPN	any		VPN	any	any	
6		VPN	any		dmz	any	any	
7		dmz	any		VPN	any	any	

The configure on server side is done here

Now go to the client site to set up the PnP VPN

Server address is the PnP egress interface ip on server's side

ID is the fqdn string in user configuration

Password is generated in VPN peer page

Outgoing IF is the interface connecting to the Internet on client firewall

Incoming IF is the interface connecting internal PC or Server on client firewall

The screenshot shows the Hillstone E1100 Network Management Console. The 'Network' tab is selected, and the 'IKE VPN Configuration' page is active. A red box highlights the 'VPN' option in the left sidebar. A red arrow points from the 'VPN' option to the 'PnPVPN Client' configuration dialog box. The dialog box contains the following fields:

- Server Address1: 172.16.1.101 (A.B.C.D)/(1-255)chars
- Server Address2: (A.B.C.D)/(1-255)chars
- ID: shanghai.hillstonenet.com (1-254) chars
- Password: (6-31)chars
- Confirm Password: (6-31)chars
- Auto Save: Enable
- Outgoing IF1: ethernet0/1
- Outgoing IF2: (empty)
- Incoming IF: ethernet0/2

After clicking OK, we can see that the PnP vpn is established

ID	VPN Name	Direction	Peer	Port	Algorithm	SPI	CPI	Lifetime (s)	Lifesize (KB)	Status
2	PnP-vpn	outbound	172.16.1.101	500	esp.3des/sha1-	2df7d3a3	0	28694	0	Active
2	PnP-vpn	inbound	172.16.1.101	500	esp.3des/sha1-	3a8a124a	0	28694	0	Active

Route is genetated on server side

St...	Virtual R...	IP/Netmask	Next-hop ...	Gateway/...	Interface	Protocol	Schedule	Precede...	Metric	Weight	Track Sta...
	trust-vr	0.0.0.0/0	Interface	172.16.1.1	ethernet0/1	DHCP		1	0	1	
	trust-vr	10.0.0.0/24	Interface		tunnel1	Connected		0	0	1	
	trust-vr	10.0.0.1/32	Interface		tunnel1	HOST		0	0	1	
	trust-vr	10.0.0.2/32	Interface	10.0.0.2	tunnel1	VPN		1	0	1	
	trust-vr	172.16.1.0/24	Interface		ethernet0/1	Connected		0	0	1	
	trust-vr	172.16.1.101/32	Interface		ethernet0/1	HOST		0	0	1	
	trust-vr	192.168.1.0/24	Interface		ethernet0/2	Connected		0	0	1	
	trust-vr	192.168.1.1/32	Interface		ethernet0/2	HOST		0	0	1	
	trust-vr	192.168.2.0/24	Interface	10.0.0.2	tunnel1	VPN		1	0	1	
	trust-vr	192.168.100.0/24	Interface		ethernet0/3	Connected		0	0	1	
	trust-vr	192.168.100.1/32	Interface		ethernet0/3	HOST		0	0	1	

Incoming interface on client side has acquired relevant configuration, tunnel interface has been created accordingly, and also route, policy, DNS server

Interface	Interface Name	Status	Type	IP/Netmask	MAC	Zone	Vsys	Users/IPs	Speed Out	Speed In	Description
	cellular0/0		Static	0.0.0.0/0	001c.545f.94d6	untrust	root	0	0 bps	0 bps	
	ethernet0/0		Static	0.0.0.0/0	001c.545f.9498	NULL	root	0	0 bps	0 bps	
	ethernet0/1		DHCP	172.16.1.105/24	001c.545f.9499	untrust	root	0	1.92 Kbps	1.13 Kbps	
	ethernet0/2		Static	192.168.2.1/24	001c.545f.949a	trust	root	1	0 bps	1.66 Kbps	
	ethernet0/3		Static	0.0.0.0/0	001c.545f.949b	NULL	root	0	0 bps	0 bps	
	ethernet0/4		Static	0.0.0.0/0	001c.545f.949c	NULL	root	0	0 bps	0 bps	
	ethernet0/5		Static	0.0.0.0/0	001c.545f.949d	NULL	root	0	0 bps	0 bps	
	ethernet0/6		Static	0.0.0.0/0	001c.545f.949e	NULL	root	0	0 bps	0 bps	
	ethernet0/7		Static	0.0.0.0/0	001c.545f.949f	NULL	root	0	0 bps	0 bps	
	ethernet0/8		Static	0.0.0.0/0	001c.545f.94a0	NULL	root	0	0 bps	0 bps	
	tunnel1		Static	10.0.0.2/32	0000.0000.0000	VPN	root	0	464 bps	0 bps	
	vswitchif1		Static	0.0.0.0/0	001c.545f.949a	NULL	root	0	0 bps	0 bps	

St...	Virtual...	IP/Netmask	Next-hop Type	Gateway/Next-ho...	Interface	Protocol	Sched...	Prece...	Metric	Weight	Track ...	Descri..
	trust-vr	0.0.0.0/0	Interface	172.16.1.1	ethern...	DHCP		1	0	1		
	trust-vr	172.16.1.0/24	Interface		ethern...	Conne...		0	0	1		
	trust-vr	172.16.1.105/32	Interface		ethern...	HOST		0	0	1		
	trust-vr	192.168.1.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		
	trust-vr	192.168.2.0/24	Interface		ethern...	Conne...		0	0	1		
	trust-vr	192.168.2.1/32	Interface		ethern...	HOST		0	0	1		
	trust-vr	192.168.3.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		
	trust-vr	192.168.100.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		

ID	Name	Zone	Source Address	User	Zone	Destination Address	Service	Applica
1		trust	any		untrust	any	any	
4		VPN	any		trust	any	any	
5		trust	any		VPN	any	any	

Server IP	Virtual Router	Egress Interface	Type
192.168.100.100	trust-vr	ethernet0/2	VPN
58.240.57.33	trust-vr	ethernet0/1	DHCP
221.6.4.66	trust-vr	ethernet0/1	DHCP

4. Troubleshooting

We can debug the whole process of vpn negotiation and parameter distribution via enable `debug vpn ike basic/packet`, here I cited the part of parameter distributing on server side, we can easily see the way how it works here

```
2019-06-09 03:41:46, DEBUG@VPN: IPC start (SA_BIND_INT)
2019-06-09 03:41:46, DEBUG@VPN: Sa index: 7
2019-06-09 03:41:46, DEBUG@VPN: SA 7 tunnel interface(48) is binded,nh_addr:ac10
0165
2019-06-09 03:41:46, DEBUG@VPN: dns notify: ifid:33, vrid:1, dns1:00000000, doma
inname:(null), action:0
2019-06-09 03:41:46, DEBUG@VPN: dns notify: ifid:33, vrid:1, dns1:c0a86464, doma
inname:(null), action:1
2019-06-09 03:41:46, DEBUG@VPN: pnpvpn gen config
2019-06-09 03:41:46, DEBUG@VPN: Generate conf:
interface ethernet0/2
no dns-proxy
no dhcp-server enable
no ip address
exit
no dhcp-server pool pnpauto
dhcp-server pool pnpauto
address 192.168.2.10 192.168.2.20
gateway 192.168.2.1
netmask 255.255.255.0
exit
ip dns-proxy domain any name-server use-system
interface ethernet0/2
ip address 192.168.2.1 255.255.255.0
dhcp-server enable pool pnpauto
dns-proxy
exit
interface tunnell
no ip address
no ip address unnumber
ip address 10.0.0.2/32
exit
```