



# How to Configure PnPVPN

Hillstone Networks Inc.



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

# Content

1.	Preface	3
2.	Тороlоду	3
3.	Step by Step	1
4.	Troubleshooting	3



## 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

Hillstone E1100	Dashboard	iCenter Mon	tor Policy	Object	Network	System
Address Entry	🕂 New 🔽 🖍 Edit 🗕 Delete					
+ 🛃 Service Book	Local Server	Туре		ŀ	Address	
+ 🔝 APP Book	Radius Server	LOCA	-			
🖫 SLB Server Pool	Active Directory Server	LOCA	-			
Schedule	LDAP Server					
🛗 AAA Server	TACACS+ Server					
+ 📲 SSO Server						
+ 🔤 SSO Client						
— 🙎 User						
Local User						
LDAP User						
= AD User						
IP-User Binding						

#### Configure AAA server and user, choose Local Server

#### Add user in the AAA server you have created

				Object	Network		
Address Entry	Local Server: pnp						
+ 🕌 Service Book		J import Liser Password List	Evport Liser E	Daceword Liet			
+ 🏢 APP Book			J Export Osci i	dooword List			
🖫 SLB Server Pool	Search	User Configuration					×
o Schedule	🔤 🚰 All User	Basic VPN 0	Options				
🖼 AAA Server							
+ Esso Server		Name:	shanghai				
+ 🔤 SSO Client		Password:				(1-31) chars	
– 🙎 User		Confirm Password:					
= Local User		Mobile + country code:				(6-15) chars	
= LDAP User		Description:				(0-127) chars	
= AD User		Group:				Choose	
= IP-User Binding		E se la fina	Enable				
+ 🔐 Role		Expiration:	Enable				
😪 Track Object		If SMS authentication	i is enabled, Sl	MS authenticati	on code will be		
+ 😽 Antivirus		sent to the specified	nobile priorie.				
+ 🍪 Intrusion Prevention System							
🔁 URL Filter							
Perimeter Traffic Filtering							
+ 🛞 Data Security							
						ОК	Cancel



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

Hillstone E1100	Dashboard id	Center Monitor Po	licy Object Network	System
<ul> <li>Address Entry</li> <li>Service Book</li> <li>APP Book</li> </ul>	Local Server: pnp + New ► ✓ Edit — Delete	, import User Password List 🛧 Exp	ort User Password List	
<ul> <li>SLB Server Pool</li> <li>Schedule</li> <li>AAA Server</li> <li>SSO Server</li> <li>SSO Client</li> <li>Liner</li> </ul>	All User	Basic VPN Optio Dial-up VPN IKE ID: ON	ns e	KEY-ID (1-254) chars
Local User     LDAP User     AD User     IP-User Binding     Role     Track Object     Anthrings		PnPVPN Tunnel Route: DHCP Start IP: DHCP End IP: DHCP Netmask: DHCP Gateway:	192.168.1.0/24;192.168.100.0/24;192.168.3.0/ 192.168.2.10 192.168.2.20 24 192.168.2.1	Choose
<ul> <li>Intrusion Prevention System</li> <li>URL Filter</li> <li>Perimeter Traffic Filtering</li> <li>Data Security</li> </ul>		DNS 1: DNS 2: DNS 3: DNS 4: WINS 1: WINS 2: Tunnel IP1:	192.166.100.100	Enable SNAT
		Tunnel IP2:		OK Cancel



#### Configure IKE VPN

Ph	ase1 Proposal Configu	ration	154	-sig		dts		ے ۲
<b></b>	Proposal Name:	р1						
	Authentication:	Pre-share	0	RSA-Signature	O DSA-S	Signature		
	Hash:	MD5	SHA	SHA-256	SHA-384	SHA-512		
	Encryption:	3DES	O DES	O AES	AES-192	AES-256		
Įt	DH Group:	Group1	Group2	Group5	Group14	Group15		
C	Lifetime :		(300-86400	)seconds,defau				
Ŀ								
							ОК	Cancel

Start with p1 proposal, here we use default setting

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

Pha	se2 Proposal Configura	tion						×
	Proposal Name:	p2						
	Protocol:	ESP	O AH					
	Hash:	MD5	V SHA	SHA-256	SHA-384	SHA-512	(Up to 3 can be selected.)	
	Encryption:	3DES	DES	AES	AES-192	AES-256	(Up to 4 can be selected.)	
	Compression:	None	Deflate					
-   -	PFS Group:	Group1	Group2	Group	5 🔵 Grou	ip14 🔘 Gro	pup15	
E	Lifetime :	28800		(180-86400) seconds, default: 28800				
-	Lifesize:	Enable						
							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

VPN Peer Configuration			×
Basic Advan	iced		
Name:	pnp		
Interface: Mode:	ethernet0/1 Main  Aggressive		
Туре:	Static IP Dynamic IP OUSer Group		
AAAServer:	pnp ~		
Local ID:	None  FQDN U-FQDN ASN1-DN KEY_ID IPV4		
Peer ID:	None		
Proposal1:	p1 ~		
Proposal2:	~		
Proposal3:	×		
Proposal4:	~		
Per-shared Key:	(5-127) chars		
User Key:	Generate		
		ок	Cancel

VPN Peer Configuration					×
Basic Advan	ced				
Name:	pnp				
Interface:	ethernet0/1	Generate the Liser Key		×	
Mode:	Main	Generate the Oser Ney		^	
Туре:	Static IP	IKE ID:	shanghai.hillstonenet.com	(1-255) chars	
AAAServer:	pnp	Per-shared Key:		(5-127) chars	
Local ID:	None	auto fill in	Generate Disable		
Peer ID:	None				
Proposal1:	p1	Generate Result:	zIRoryEutAU81dCZLEH4K +LN/z8=		
Proposal2:					<b>_</b>
Proposal3:				this is for o	client user to use
Proposal4:	/	~			
Per-shared Key:		(5	5-127) chars		
User Key:	Genera	te			
					OK Cancel



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

VPN Peer Co	nfiguration					×
Basi	Advanced					
Conne NAT Tr Any Pe Genera DPD: Descri	ction Type:  Bidirect aversal: Enable er ID: Enable te Route: Enable Enable Enable	tional 💿 Initiator	Responder (1-255) chars			
XAUT	I Server: 📄 Enable		(1200) (1140)			
					ОК	Cancel

#### Configure IKE VPN options

Per   Per   Per Name:   pnp   Advanced     Information:   Name   Mode   Type   Local ID   Peer ID   pnp   Aggressive   User Group     Tunnel   Name:   pnp   Mode:   Information:   Proposal:   Proxy ID:   Image:	Peer   Peer Name:   ppp   Edit     Information:   Name   Mode   Type   Local ID   Peer ID     pnp   Aggressive   User Group     Tunnel   Name:   pnp   Mode:   Image:   Image:   Pip:   Mode:   Image:   Pip:   Pip:   Pip:   Image:   Pip:   Image:   Image:   Pip:   Image:   Pip:   Image:   Image:  <	Per   Per   Per Name:   Name   Mode   Type   Local ID   Peer ID   pnp   Aggressive   User Group     Turnel   Name:   pnp   Mode:   Information:   Proposal:   P2   Proxy ID:   Image:   Image:   Image:   Participation:   Image:   Image: <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
Basic Advanced     Peer Peer Name:   pnp Edit   Information: Name   pnp Aggressive   User Group     Turnel   Name: pnp   Mode: • tunnel   • tunnel   P2 Proposal:   P2   Proxy ID:   • Auto	Basic Advanced     Peer Peer Name:   pnp Edit   Information: Name   Mode Type   Local ID   pnp   Aggressive   User Group     Tunnel   Name:   pnp   Mode:   Innel   tansport   P2 Proposal:   p2   Proxy ID:   Image:     Auto     Manual	Basic Advanced     Peer Name: pnp   Information: Name   Mame Mode   Type Local ID   Peer ID   pnp   Aggressive   User Group     Tunnel   Name:   pnp   Mode:   Image:   P2 Proposal:   P2 Proposal:   P2 Proposal:   P2 Proposal:   Patto   Manual	PN Configuration						
Peer Name: pnp   Information: Name   Mode Type   Local ID Peer ID   pnp Aggressive   User Group	Peer Name: pnp   Information: Name   Mode Type   Local ID Peer ID   pnp Aggressive   User Group	Peer Name: pnp   Information: Name   Mode Type   Local ID Peer ID   pnp Aggressive   User Group     Turnel   Name: pnp   Mode: • tunnel   • tunnel • transport   P2 Proposal: • Auto   • Auto • Manual	Basic Adva	inced					
Peer Name:pnpEditInformation:NameModeTypeLocal IDPeer IDpnpAggressiveUser Group	Peer Name: pnp Edit   Information: Name Mode Type Local ID Peer ID   pnp Aggressive User Group     Tunnel   Name: pnp   Mode: © tunnel © transport   P2 Proposal: p2   Proxy ID: © Auto © Manual	Peer Name:pnpEditInformation:NameModeTypeLocal IDPeer IDpnpAggressiveUser Group	Peer						
Information:NameModeTypeLocal IDPeer IDpnpAggressiveUser GroupTunnelName:pnpMode:© transportP2 Proposal:p2Proxy ID:@ AutoManual	Information:NameModeTypeLocal IDPeer IDpnpAggressiveUser GroupTunnelName:pnpMode:ImpImpMode:ImpImpP2 Proposal:P2Proxy ID:Imp <td>Information:NameModeTypeLocal IDPeer IDpnpAggressiveUser GroupTunnelName:pnpMode:© transportFransportP2 Proposal:p2Proxy ID:@ Auto@ Manual</td> <td>Peer Name:</td> <td>pnp</td> <td>~</td> <td>Edit</td> <td></td> <td></td> <td></td>	Information:NameModeTypeLocal IDPeer IDpnpAggressiveUser GroupTunnelName:pnpMode:© transportFransportP2 Proposal:p2Proxy ID:@ Auto@ Manual	Peer Name:	pnp	~	Edit			
pnp     Aggressive     User Group       Tunnel         Name:     pnp        Mode:     Image:     Image:       P2 Proposal:     p2        Proxy ID:     Image:     Image:	pnpAggressiveUser GroupTunnelName:pnpMode:ImpMode:ImpP2 Proposal:p2Proxy ID:ImpImpManual	pnpAggressiveUser GroupTunnelName:pnpMode:Image: Image: I	Information:	Name	Mode	Туре	Local ID	Peer ID	
Tunnel         Name:       pnp         Mode:       Image: Imag	Tunnel       Name:       pnp         Mode:       Image: Im	Tunnel       Name:       pnp         Mode:       Image: Im		pnp	Aggressive	User Group			
Name:     pnp       Mode:     Image:	Tunnel       pnp         Name:       on tunnel       transport         P2 Proposal:       p2          Proxy ID:       Image: Auto       Manual	Tunnel       pnp         Mode:       Image: Im							
Name:pnpMode:Image: Image:	Name:pnpMode:Image: Image:	Name:pnpMode:Image: Image:	Tunnel						
Mode:     Image: I	Mode:       Image:	Mode:	Name:	pnp					
P2 Proposal:     p2     ~       Proxy ID:     Image: Auto Im	P2 Proposal: p2 ~ Proxy ID: O Auto Manual	P2 Proposal: p2 ~ Proxy ID: O Auto Manual	Mode:	tunnel	transport				
Proxy ID: <ul> <li>Auto</li> <li>Manual</li> </ul>	Proxy ID: <ul> <li>Auto</li> <li>Manual</li> </ul>	Proxy ID: <ul> <li>Auto</li> <li>Manual</li> </ul>	P2 Proposal:	p2	$\checkmark$				
			Proxy ID:	Auto	Manual				



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

IKE	VPN Configuration							,	×
	Basic Advand	ced							
	DNS1:								
	DNS2:								
	DNS3:								
	DNS4:								
	WINS1:								
	WINS2:								
	Enable Idle Time	Enable							
	DF-Bit:	Copy		Clear		Set			
	Anti-Replay	Disable	32	64	128	256	6 512		
	Commit Bit:	Enable	0	0	0	0	0		
	Accept-all-proxy-ID:	Enable							
	Auto connect:	Enable							
				Cho	lose				
	Tunnel Route:			one					
	Description:			(0-28	55) chars				
	VPN Track:	Enable							
								ОК	Cancel



All User	Shanghai	
User Configuration		>
Basic VPN Option	S	
Dial-up VPN		
IKE ID: ONONE	FQDN	KEY-ID
	shanghai.hillstonenet.com	(1-254) chars
PnPVPN		
Tunnel Route:	192.168.1.0/24;192.168.100.0/24;192.168.3.0/	Choose
DHCP Start IP:	192.168.2.10	
DHCP End IP:	192.168.2.20	
DHCP Netmask:	24	
DHCP Gateway:	192.168.2.1	
DNS 1:	192.168.100.100	7
DNS 2:		
DNS 3:		
DNS 4:		
WINS 1:		
WINS 2:		
Tunnel IP1:	10.0.0.2	Enable SNAT
Tunnel IP2:		
		OK Cancel

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



Tunnel Interface		×
Basic Prope	rties Advanced RIP	
Basic		
Interface Name:	tunnel1	
Description:	(0-63) chars	
Binding Zone:	Layer 2 Zone   Layer 3 Zone   TAP   No Binding	
Zone:	VPN ~	
HA sync:	Enable	
IP Configuration		
Туре:	Static IP     DHCP     PPPoE	
IP Address:	10.0.0.1	
Net mask:	255.255.255.0	
Set as Local IP		
Enable DNS Pro	xy 💿 Proxy 💿 Proxy-Trans	
Enable DNS Byp	ass	
Advanced DHC	P   •	
Management		
Telnet	SSH 📝 Ping 🦳 HTTP 🦳 HTTPS 📄 SNMP	
Routing		
Reverse Route:	Enable Close  Auto	
	OK Cance	ł



nel Interface				×
Basic Propert	ies Advanced F	RIP		
Advanced DHCP	🖛			
Management	SH 🔽 Ping 📄	HTTP HTTPS	SNMP	
Routing				
Reverse Route:	Enable Close	Auto		
Tunnel Binding				
Tunnel Type:	IPsec VPN	SSL VPN	L2TP VPN	
VPN Name:	pnp ~			
Gateway:				
VPN Name	Туре	Gateway	Add	
pnp	IPSec VPN		Delete	
Bandwidth				
Bandwidth Up Bandwidth:	1,000,000,000	(512,000 ~ 1000	0,000,000,000)bps	
Bandwidth Up Bandwidth: Down Bandwidth:	1,000,000,000	(512,000 ~ 1000 (512,000 ~ 1000	0,000,000,000)bps 0,000,000,000)bps	
Bandwidth Up Bandwidth: Down Bandwidth: Proactive Webauth	1,000,000,000	(512,000 ~ 1000 (512,000 ~ 1000	0,000,000,000)bps 0,000,000,000)bps	
Bandwidth Up Bandwidth: Down Bandwidth: Proactive Webauth	1,000,000,000 1,000,000,000	(512,000 ~ 1000 (512,000 ~ 1000	0,000,000,000)bps 0,000,000,000)bps	
Bandwidth Up Bandwidth: Down Bandwidth: Proactive Webauth Enable	1,000,000,000 1,000,000,000	(512,000 ~ 1000 (512,000 ~ 1000	0,000,000,000)bps 0,000,000,000)bps	

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	Namo		Source		De	stination	Sonrico	Applica
	Name	Zone	Address	User	Zone	Address	Service	Applica
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

Hillstone E1100	Dashboard	iCenter	Monitor	Policy Obj	ect Network	System	SG-6000	L hillstone@root
🔒 Zone	IKE VPN Configuration	n				PnPVPN Client	IPSec-XAUTH Add	ress Pool   IPSec Vi
1 Interface	IKE VDN List	VDN Deer List	P1 Proposal	P2 Proposal				
I DNS				T 2 T TOPOGUI				
DHCP	+ New / Edit -	- Delete						
DDNS	Name	Protocol	riash	Faryption	Compression	PFS Group	Lifetime	Lifesize
PPPoE	esp-sha256-aes12	2 esp	sha-256	aes		group2	28800	
P. Virtual Wire	esp-sha256-aes1	2 esp	sha of	aes	-	no pfs	28800	
♦ Intual Router	esp-sna256-aes2	5 esp	sha 256	aes-206		group2	28800	
11 VSwitch	esp-sila256-3des	esp	sha-256	3des	-	aroun2	28800	
Port Mirroring	esp-sha250-3( Pi	nPVPN Configuration	0110-200			×	28800	
🚡 3G/4G	esp-md5-aes1						28800	
* Routing	esp-md5-aes1	Server Address1:	172.16.1.101	(	A.B.C.D)/(1-255)chars		28800	
C Outbound	esp-md5-aes2	Server Address2:		(	A.B.C.D)/(1-255)chars		28800	
	esp-md5-aes2	ID:	shanghai.hills	stonenet.com (	1-254) chars		28800	
VPN	esp-md5-3des	Password:	•••••		6-31)chars		28800	
= IPSec VPN	Die la dar	Confirm Password:			6-31)chars		00000	
= SSL VPN	Displaying 1 - 12 (	Auto Save:	Enable			< P	age 1 /1 >	>1 G 50 ~
= 12TP VPN	Manual Key VPN	Outgoing IF1:	ethernet0/1	~				
○ 002 1Y	🕂 New 🥒 Edit	Outgoing IF2:		~				
@ WebAuth	Name	Incoming IF:	ethernet0/2	~			R	emote SPI
Application Lawar Cateway								
Global Network Parameters		Delete			ок	Cancel		



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



#### 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	Interface	172.16.1.1	ethernet0/1	DHCP		1	0	1	
	trust-vr	10.0.0/24	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	
<b>.</b>	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	
<u>.</u>	trust-vr	192.168.2.0/24	Interface	10.0.0.2	tunnel1	VPN		1	0	1	
۰	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



-											
[1] Interface	Interface Name	Status	Туре	IP/Netmask	MAC	Zone	Vsys	Users/IPs	Speed Out	Speed In	Description
+ 🔤 DNS	cellular0/0	Q Q Q G	Static	0.0.0/0	001c.545f.94d6	untrust	root	0	0 bps	0 bps	
DHCP	ethernet0/0	Q Q Q G	Static	0.0.0/0	001c.545f.9498	NULL	root	0	0 bps	0 bps	
DDNS	ethernet0/1	•	DHCP	172.16.1.105/24	001c.545f.9499	untrust	root	0	1.92 Kbps	1.13 Kbps	
m PPPoE	ethernet0/2	•	Static	192.168.2.1/24	001c.545f.949a	trust	root	1	0 bps	1.66 Kbps	1
₽ Virtual Wire	ethernet0/3	Q Q Q G	Static	0.0.0/0	001c.545f.949b	NULL	root	0	0 bps	0 bps	
+ Nirtual Router	ethernet0/4	Q Q Q G	Static	0.0.0/0	001c.545f.949c	NULL	root	0	0 bps	0 bps	
Not Missing	ethernet0/5	Q Q Q G	Static	0.0.0/0	001c.545f.949d	NULL	root	0	0 bps	0 bps	
3G/4G	ethernet0/6	Q Q Q G	Static	0.0.0/0	001c.545f.949e	NULL	root	0	0 bps	0 bps	
+ - Routing	ethernet0/7	Q Q Q G	Static	0.0.0/0	001c.545f.949f	NULL	root	0	0 bps	0 bps	
+ 🕣 Outbound	ethernet0/8	Q Q Q	Static	0.0.0/0	001c.545f.94a0	NULL	root	0	0 bps	0 bps	
🛃 Inbound	tunnel1	•	Static	10.0.0.2/32	0000.0000.0000	VPN	root	0	464 bps	0 bps	
- WN VPN	vswitchif1	Q Q Q G	Static	0.0.0/0	001c.545f.94a9	NULL	root	0	0 bps	0 bps	_
= IPSec VPN											

-												-	
	St	Virtual	IP/Netmask	Next-hop Type	Gateway/Next-ho	Interface	Protocol	Sched	Prece	Metric	Weight	Track	Descri.
	<b>.</b>	trust-vr	0.0.0/0	Interface	172.16.1.1	ethern	DHCP		1	0	1		
	<b></b>	trust-vr	172.16.1.0/24	Interface		ethern	Conne		0	0	1		
	<b>.</b>	trust-vr	172.16.1.105/32	Interface		ethern	HOST		0	0	1		
	<b>.</b>	trust-vr	192.168.1.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		
	<b>.</b>	trust-vr	192.168.2.0/24	Interface		ethern	Conne		0	0	1		
	<b>.</b>	trust-vr	192.168.2.1/32	Interface		ethern	HOST		0	0	1		
	<b>.</b>	trust-vr	192.168.3.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		
	<b></b>	trust-vr	192.168.100.0/24	Interface	172.16.1.101	tunnel1	VPN		1	0	1		

E Security Policy	+	New	🎤 Edit 🗕 Delete 🛛 Copy	🗂 Paste 🗸 🍴	Move 🗸 🚥					🖓 Fi
+ t] NAT			News		Source		De	stination		
+ 🙀 iQoS		ID	Name	Zone	Address	User	Zone	Address	Service	Applica
😡 Session Limit		1		trust	any		untrust	any	any	
+ 🤤 ARP Defense		4		VPN	any		trust	any	any	
SSL Proxy		5		trust	any		VPN	any	any	
+ 🏖 Global Blacklist										

📇 Zone	+ New - Delete	+ New - Delete									
🖺 Interface	Server IP	Virtual Router	Egress Interface	Туре							
- 🔤 DNS	192.168.100.100	trust-vr	ethernet0/2	VPN							
<ul> <li>DNS Server</li> </ul>	58.240.57.33	trust-vr	ethernet0/1	DHCP							
<ul> <li>DNS Proxy</li> </ul>	221.6.4.66	trust-vr	ethernet0/1	DHCP							
<ul> <li>Analysis</li> </ul>											
- Cache											
<ul> <li>NBT Cache</li> </ul>											
DHCP											
DDNS											
PPPoE											
Po Virtual Wire											



### 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 tunnel1
no ip address
no ip address unnumber
ip address 10.0.0.2/32
exit
```