

DSR3 information:

LAN1 IP: 192.168.30.1/24

WAN IP: 3.3.3.3/24

WAN Gateway: 3.3.3.2

[Setup procedure]

VPN Hub settings:

DSR1

1. Set the WAN IP address to 1.1.1.1 and Gateway IP address to 1.1.1.2.

ISP Connection Type	
ISP Connection Type:	Static IP
IP Address:	1.1.1.1
IP Subnet Mask:	255.255.255.0
Gateway IP Address:	1.1.1.2
Domain Name System (DNS) Servers	
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	168.95.2.1
MAC Address	
MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

2. Set the LAN IP address to 192.168.10.1, and enable the function of DHCP server on the LAN interface, the DHCP client starts IP address is 192.168.10.100, the ending IP address is 192.168.10.200.

3. In the setting page of IPSEC Policy, create an IPsec policy and fill the necessary value in following columns: (Blue part)

Policy Name:	Vpn1
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	FQDN
[FQDN column]	0.0.0.0
Enable Mode Config:	Uncheck
Enable NetBIOS:	Uncheck
Enable Rollover:	Uncheck
Protocol:	ESP
Enable DHCP:	Uncheck
Local IP:	Any

Local Start IP Address:	[blank]
Local End IP address:	[blank]
Local Subnet Mask:	[blank]
Remote IP:	Any
Remote Start IP Address:	[blank]
Remote End IP Address	[blank]
Remote Subnet Mask:	[blank]
Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	On
NAT Keep Alive Frequency(In seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	[blank]
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	[blank]
Encryption Algorithm:	AES-128
Key Length:	[blank]
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group2 (1024bit)
SA-Lifetime(sec):	28800
Enable Dead Peer Detection:	Uncheck
Detection Period:	[Keep default]
Reconnect after failure count:	[Keep default]
Extended Authentication:	None
Authentication Type:	[Keep default]
Username:	[blank]
Password:	[blank]
Phase2-(Manual Policy Parameters)	
SPI-Incoming:	[Keep default]
SPI-Outgoing:	[Keep default]
Encryption Algorithm:	[Keep default]
Key Length:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Integrity Algorithm:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 seconds
Encryption Algorithm:	DES
Key Length:	[Keep default]
Integrity Algorithm:	SHA-1
PFS Key Group	Uncheck

VPN Spoke1 settings

DSR2

1. Set the WAN1 IP address to 5.5.5.5 and Gateway IP address to 5.5.5.2.

ISP Connection Type	
ISP Connection Type:	Static IP
IP Address:	5.5.5.5
IP Subnet Mask:	255.255.255.0
Gateway IP Address:	5.5.5.2

Domain Name System (DNS) Servers	
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	168.95.2.1

MAC Address	
MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

2. Set the LAN IP address to 192.168.50.1, and enable the function of DHCP server on the LAN interface, the DHCP client starts IP address is 192.168.50.100, the ending IP address is 192.168.50.200.

3. In the setting page of IPSEC Policy, create two IPsec policies as below figure shown, one to the local net of **DSR1**, another to the local net of **DSR3**.

IPSEC POLICIES								LOGOUT
This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable and disable IPsec VPN policies from this page.								
List of VPN Policies								
Auto Policy								
<input type="checkbox"/>	Status	Name	Type	IPsec Mode	Local	Remote	Auth	Encr
<input type="checkbox"/>	Enabled	vpn1	Auto Policy	Tunnel Mode	192.168.50.0 / 255.255.255.0	192.168.10.0 / 255.255.255.0	SHA-1	DES
<input type="checkbox"/>	Enabled	vpn2	Auto Policy	Tunnel Mode	192.168.50.0 / 255.255.255.0	192.168.30.0 / 255.255.255.0	SHA-1	DES
Manual Policy								
Edit		Enable		Disable		Delete		Add

The detail parameters of IPSec policy of VPN1: (Blue part)

Policy Name:	Vpn1
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address
[FQDN column]	1.1.1.1
Enable Mode Config:	Uncheck
Enable NetBIOS:	Uncheck
Enable Rollover:	Uncheck
Protocol:	ESP
Enable DHCP:	Uncheck
Local IP:	Subnet
Local Start IP Address:	192.168.50.0
Local End IP address:	[blank]
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.10.0
Remote End IP Address	[blank]
Remote Subnet Mask:	255.255.255.0
Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	On
NAT Keep Alive Frequency(In seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	[blank]
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	[blank]
Encryption Algorithm:	AES-128
Key Length:	[blank]
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group2 (1024bit)
SA-Lifetime(sec):	28800
Enable Dead Peer Detection:	Uncheck
Detection Period:	[Keep default]
Reconnect after failure count:	[Keep default]
Extended Authentication:	None
Authentication Type:	[Keep default]
Username:	[blank]
Password:	[blank]
Phase2-(Manual Policy Parameters)	
SPI-Incoming:	[Keep default]
SPI-Outgoing:	[Keep default]
Encryption Algorithm:	[Keep default]

Key Length:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Integrity Algorithm:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 seconds
Encryption Algorithm:	DES
Key Length:	[Keep default]
Integrity Algorithm:	SHA-1
PFS Key Group	Uncheck

The detail parameters of IPSec policy of VPN2: (Blue part)

Policy Name:	Vpn2
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address
[FQDN column]	1.1.1.1
Enable Mode Config:	Uncheck
Enable NetBIOS:	Uncheck
Enable Rollover:	Uncheck
Protocol:	ESP
Enable DHCP:	Uncheck
Local IP:	Subnet
Local Start IP Address:	192.168.50.0
Local End IP address:	[blank]
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.30.0
Remote End IP Address	[blank]
Remote Subnet Mask:	255.255.255.0
Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	On
NAT Keep Alive Frequency(In seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	[blank]
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	[blank]
Encryption Algorithm:	AES-128
Key Length:	[blank]
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key

Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group2 (1024bit)
SA-Lifetime(sec):	28800
Enable Dead Peer Detection:	Uncheck
Detection Period:	[Keep default]
Reconnect after failure count:	[Keep default]
Extended Authentication:	None
Authentication Type:	[Keep default]
Username:	[blank]
Password:	[blank]
Phase2-(Manual Policy Parameters)	
SPI-Incoming:	[Keep default]
SPI-Outgoing:	[Keep default]
Encryption Algorithm:	[Keep default]
Key Length:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Integrity Algorithm:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 seconds
Encryption Algorithm:	DES
Key Length:	[Keep default]
Integrity Algorithm:	SHA-1
PFS Key Group	Uncheck

VPN Spoke2 settings

DSR3

1. Set the WAN1 IP address to 3.3.3.3 and Gateway IP address to 3.3.3.2.

ISP Connection Type	
ISP Connection Type:	Static IP
IP Address:	3.3.3.3
IP Subnet Mask:	255.255.255.0
Gateway IP Address:	3.3.3.2

Domain Name System (DNS) Servers	
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	168.95.2.1

MAC Address	
MAC Address Source:	Use Default Address
MAC Address:	00:00:00:00:00:00

2. Set the LAN IP address to 192.168.30.1, and enable the function of DHCP server on the LAN interface, the DHCP client starts IP address is 192.168.30.100, the ending IP address is 192.168.30.200.

3. In the setting page of IPSEC Policy, create two IPsec policies as below figure shown, one to the local net of **DSR1**, another to the local net of **DSR2**.

IPSEC POLICIES									LOGOUT
This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable and disable IPsec VPN policies from this page.									
List of VPN Policies									
Auto Policy									
<input type="checkbox"/>	Status	Name	Type	IPsec Mode	Local	Remote	Auth	Encr	
<input type="checkbox"/>	Enabled	vpn1	Auto Policy	Tunnel Mode	192.168.30.0 / 255.255.255.0	192.168.10.0 / 255.255.255.0	SHA-1	DES	
<input type="checkbox"/>	Enabled	vpn2	Auto Policy	Tunnel Mode	192.168.30.0 / 255.255.255.0	192.168.50.0 / 255.255.255.0	SHA-1	DES	
Manual Policy									
Edit		Enable		Disable		Delete		Add	

The detail parameters of IPSec policy of VPN1: (Blue part)

Policy Name:	Vpn1
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address
[FQDN column]	1.1.1.1
Enable Mode Config:	Uncheck
Enable NetBIOS:	Uncheck
Enable Rollover:	Uncheck
Protocol:	ESP
Enable DHCP:	Uncheck
Local IP:	Subnet
Local Start IP Address:	192.168.30.0
Local End IP address:	[blank]
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.10.0
Remote End IP Address	[blank]
Remote Subnet Mask:	255.255.255.0
Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	On
NAT Keep Alive Frequency(In seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	[blank]
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	[blank]
Encryption Algorithm:	AES-128
Key Length:	[blank]
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group2 (1024bit)
SA-Lifetime(sec):	28800
Enable Dead Peer Detection:	Uncheck
Detection Period:	[Keep default]
Reconnect after failure count:	[Keep default]
Extended Authentication:	None
Authentication Type:	[Keep default]
Username:	[blank]
Password:	[blank]
Phase2-(Manual Policy Parameters)	
SPI-Incoming:	[Keep default]
SPI-Outgoing:	[Keep default]
Encryption Algorithm:	[Keep default]

Key Length:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Integrity Algorithm:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 seconds
Encryption Algorithm:	DES
Key Length:	[Keep default]
Integrity Algorithm:	SHA-1
PFS Key Group	Uncheck

The detail parameters of IPSec policy of VPN2: (Blue part)

Policy Name:	Vpn2
Policy Type:	Auto Policy
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address
[FQDN column]	1.1.1.1
Enable Mode Config:	Uncheck
Enable NetBIOS:	Uncheck
Enable Rollover:	Uncheck
Protocol:	ESP
Enable DHCP:	Uncheck
Local IP:	Subnet
Local Start IP Address:	192.168.30.0
Local End IP address:	[blank]
Local Subnet Mask:	255.255.255.0
Remote IP:	Subnet
Remote Start IP Address:	192.168.50.0
Remote End IP Address	[blank]
Remote Subnet Mask:	255.255.255.0
Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	On
NAT Keep Alive Frequency(In seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	[blank]
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	[blank]
Encryption Algorithm:	AES-128
Key Length:	[blank]
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key

Pre-shared key:	testtest
Diffie-Hellman (DH) Group:	Group2 (1024bit)
SA-Lifetime(sec):	28800
Enable Dead Peer Detection:	Uncheck
Detection Period:	[Keep default]
Reconnect after failure count:	[Keep default]
Extended Authentication:	None
Authentication Type:	[Keep default]
Username:	[blank]
Password:	[blank]
Phase2-(Manual Policy Parameters)	
SPI-Incoming:	[Keep default]
SPI-Outgoing:	[Keep default]
Encryption Algorithm:	[Keep default]
Key Length:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Integrity Algorithm:	[Keep default]
Key-In:	[Keep default]
Key-Out:	[Keep default]
Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 seconds
Encryption Algorithm:	DES
Key Length:	[Keep default]
Integrity Algorithm:	SHA-1
PFS Key Group	Uncheck

[Expected result]

PC1, PC2, and PC3 are able to reach each other by private IP address.