

Create IPSec VPN tunnel with IP-8000VPN and WN-300ARM-VPN

Topology:



Environment:

IP-8000VPN - WAN IP: 60.250.158.66, LAN IP: 192.168.2.254

WN-300ARM-VPN - WAN IP: PPPoE, DDNS: airlive15.dyndns.org, LAN IP: 192.168.0.1

IP-8000VPN Setting:

1. Enable VPN and NetBIOS broadcast, type in first tunnel name and click More to configure IPSec VPN setting.

VPN Settings		
Item	Setting	
▶ VPN	<input checked="" type="checkbox"/> Enable	
▶ NetBIOS broadcast	<input checked="" type="checkbox"/> Enable	
▶ Max. number of tunnels	<input type="text" value="1"/>	

ID	Tunnel Name	Method
1	<input type="text" value="To-WAN300"/>	IKE <input type="button" value="More"/>
2	<input type="text"/>	IKE <input type="button" value="More"/>
3	<input type="text"/>	IKE <input type="button" value="More"/>
4	<input type="text"/>	IKE <input type="button" value="More"/>
5	<input type="text"/>	IKE <input type="button" value="More"/>

2. Enter following information at IKE setting:

- Tunnel Name: To-WAN300 (user can define any name)
- Local Subnet: 192.168.2.0
- Local Netmask: 255.255.255.0
- Remote Subnet: 192.168.0.0
- Remote Netmask: 255.255.255.0
- Remote Gateway: airlive15.dyndns.org
- Preshare Key: 123456789
- Press "Select IKE Proposal..." button to define IKE authentication and encryption.
- Press "Select IPSec Proposal..." button to define IPSec authentication and encryption.
- Press Save button to save the setting, and reboot the router to activate the setting.

VPN Settings - Tunnel 1 - IKE	
Item	Setting
▶ Tunnel Name	<input type="text" value="To-WAN300"/>
▶ Local Subnet	<input type="text" value="192.168.2.0"/>
▶ Local Netmask	<input type="text" value="255.255.255.0"/>
▶ Remote Subnet	<input type="text" value="192.168.0.0"/>
▶ Remote Netmask	<input type="text" value="255.255.255.0"/>
▶ Remote Gateway	<input type="text" value="airlive15.dyndns.org"/>
▶ Preshare Key	<input type="text" value="123456789"/>
▶ Auto-reconnect	<input checked="" type="checkbox"/> Enable
▶ IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
▶ IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/> <input type="button" value="Help"/>	

VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
▶ IKE Proposal index	<div>IKE_1</div> <div>Remove</div>

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	IKE_1	Group 1 ▼	3DES ▼	MD5 ▼	3600	Sec. ▼
2		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
3		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
4		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
5		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
6		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
7		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
8		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
9		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼
10		Group 1 ▼	3DES ▼	SHA1 ▼	0	Sec. ▼

Proposal ID -- select one -- ▼

Add to

 Proposal index

Save
 Undo
 Back
 Help

VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
▶ IPSec Proposal index	<div>IPSec_1</div> <div>Remove</div>

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	IPSec_1	None ▼	ESP ▼	3DES ▼	None ▼	28800	Sec. ▼
2		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
3		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
4		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
5		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
6		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
7		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
8		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
9		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼
10		None ▼	ESP ▼	3DES ▼	None ▼	0	Sec. ▼

Proposal ID -- select one -- ▼

Add to

 Proposal index

Save
 Undo
 Back
 Help

WN-300ARM-VPN Setting:

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint

Address Type:

Address Data:

☒ NetBIOS Enable

Local LAN

IP Address

IP address: . . .

Subnet Mask: . . .

Remote LAN

IP Address

IP address: . . .

Subnet Mask: . . .

IKE

Direction

Exchange Mode

Diffie-Hellman (DH) Group

Local Identity Type

Data

Remote Identity Type

Data

SA Parameters

Encryption:

Authentication:

Pre-shared Key:

SA Life Time: (Seconds)

☐ Enable PFS (Perfect Forward Security)