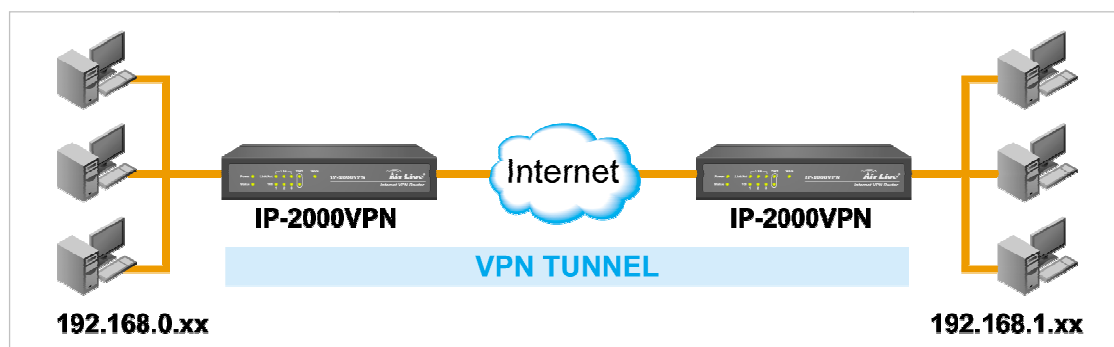


## How to create IPSec VPN tunnel with using DDNS

Based on ISP's policy, the WAN IP will be changed per every specific time. In that case, if user wants to create IPSec VPN tunnel, he has to apply DDNS service and use it as the remote endpoint.

Following are the steps to configure both IP-2000VPN devices with DDNS:



### Environment:

	IPSec Site A	IPSec Site B
<b>WAN IP address</b>	Dynamic real IP	Dynamic real IP
<b>DDNS name</b>	airlive15.dyndns.org	airlive16.dyndns.org
<b>LAN IP Subnet</b>	192.168.1.x	192.168.0.x
<b>Pre-shared Key</b>	12345678	12345678
<b>IKE Encryption</b>	3DES	3DES
<b>IKE Authentication</b>	MD5	MD5
<b>DH Group</b>	Group 2	Group 2
<b>Local Identity Type</b>	Fully Qualified Domain Name	Fully Qualified Domain Name
<b>Local Identity Data</b>	airlive15.dyndns.org	airlive16.dyndns.org
<b>Remote Identity Type</b>	Fully Qualified Domain Name	Fully Qualified Domain Name
<b>Remote Identity Data</b>	airlive16.dyndns.org	airlive15.dyndns.org
<b>Exchange Mode</b>	Aggressive Mode	Aggressive Mode

## How to create IPSec VPN tunnel with using DDNS

<b>ESP Encryption</b>	3DES	3DES
<b>ESP Authentication</b>	MD5	MD5

## How to create IPSec VPN tunnel with using DDNS

**VPN Policy Definition**

**Name:** SiteA

☒ Enable Policy  
☐ Allow NetBIOS traffic

**Remote VPN endpoint**

☐ Dynamic IP  
☐ Fixed IP: 0 . 0 . 0 . 0  
☒ Domain Name: airlive16.dyndns.org

**Local IP addresses**

Type: Subnet address IP address: 192 . 168 . 1 . 0 ~ 0  
Subnet Mask: 255 . 255 . 255 . 0

**Remote IP addresses**

Type: Subnet address IP address: 192 . 168 . 0 . 0 ~ 0  
Subnet Mask: 255 . 255 . 255 . 0

**Authentication & Encryption**

☐ AH Authentication MD5  
☒ ESP Encryption 3DES Key Size: n/a (AES only)  
☒ ESP Authentication MD5  
☐ Manual Key Exchange  
☒ IKE (Internet Key Exchange)

DirectionBoth Directions  
Local Identity TypeFully Qualified Domain Name  
Local Identity Dataairlive15.dyndns.org  
Remote Identity TypeFully Qualified Domain Name  
Remote Identity Dataairlive16.dyndns.org  
Authentication☐ RSA Signature (requires certificate)  
☒ Pre-shared Key  
Authentication Algorithm: MD5  
Encryption: 3DES Key Size: n/a (AES only)  
Exchange ModeAggressive Mode  
IKE SA Life Time: 180 (secs)  
☒ IKE Keep Alive Ping IP Address: 192 . 168 . 0 . 1  
IPSec SA Life Time: 300 (secs)  
DH GroupGroup 2 (1024 Bit)  
IKE PFSDisabled  
IPSec PFSNone

## How to create IPSec VPN tunnel with using DDNS

### VPN Policy Definition

**Name:** SiteB
 ☒ Enable Policy
 ☐ Allow NetBIOS traffic

**Remote VPN endpoint**
☐ Dynamic IP
 ☐ Fixed IP: 0 . 0 . 0 . 0
 ☒ Domain Name: airlive15.dyndns.org

**Local IP addresses**
 Type: Subnet address
 IP address: 192 . 168 . 0 . 0 ~ 0
 Subnet Mask: 255 . 255 . 255 . 0

**Remote IP addresses**
 Type: Subnet address
 IP address: 192 . 168 . 1 . 0 ~ 0
 Subnet Mask: 255 . 255 . 255 . 0

**Authentication & Encryption**
☐ AH Authentication MD5
 ☒ ESP Encryption 3DES Key Size: n/a (AES only)
 ☒ ESP Authentication MD5
 ☐ Manual Key Exchange
 ☒ IKE (Internet Key Exchange)

Direction: Both Directions
 Local Identity Type: Fully Qualified Domain Name
 Local Identity Data: airlive16.dyndns.org
 Remote Identity Type: Fully Qualified Domain Name
 Remote Identity Data: airlive15.dyndns.org
 Authentication:
 ☐ RSA Signature (requires certificate)
 ☒ Pre-shared Key
 Authentication Algorithm: MD5
 Encryption: 3DES Key Size: n/a (AES only)
 Exchange Mode: Aggressive Mode
 IKE SA Life Time: 180 (secs)
 ☒ IKE Keep Alive
 Ping IP Address: 192 . 168 . 1 . 1
 IPsec SA Life Time: 300 (secs)
 DH Group: Group 2 (1024 Bit)
 IKE PFS: Disabled
 IPsec PFS: None