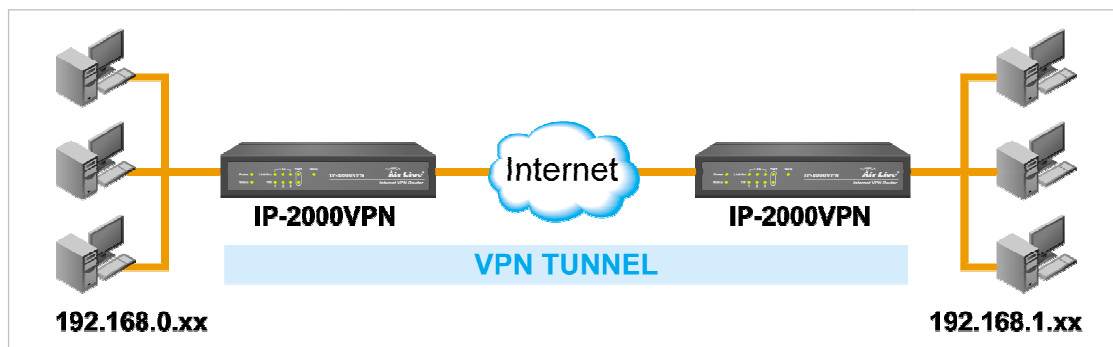


## How to create IPsec VPN tunnel with using DDNS

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:**   Enable Policy  
 Allow NetBIOS traffic

**Remote VPN endpoint**  
 Dynamic IP  
 Fixed IP:      
 Domain Name:

**Local IP addresses**  
Type:  IP address:     ~   
Subnet Mask:

**Remote IP addresses**  
Type:  IP address:     ~   
Subnet Mask:

**Authentication & Encryption**  
 AH Authentication   
 ESP Encryption  Key Size:  (AES only)  
 ESP Authentication   
 Manual Key Exchange  
 IKE (Internet Key Exchange)  
Direction:   
Local Identity Type:   
Local Identity Data:   
Remote Identity Type:   
Remote Identity Data:   
Authentication:  RSA Signature (requires certificate)  
 Pre-shared Key  
  
Authentication Algorithm:   
Encryption:  Key Size:  (AES only)  
Exchange Mode:   
IKE SA Life Time:  (secs)  
 IKE Keep Alive Ping IP Address:      
IPSec SA Life Time:  (secs)  
DH Group:   
IKE PFS:   
IPSec PFS:

# How to create IPSec VPN tunnel with using DDNS

## VPN Policy Definition

Name:

Enable Policy  
 Allow NetBIOS traffic

**Remote VPN endpoint**

Dynamic IP  
 Fixed IP:      
 Domain Name:

**Local IP addresses**

Type:  IP address:     ~   
Subnet Mask:

**Remote IP addresses**

Type:  IP address:     ~   
Subnet Mask:

**Authentication & Encryption**

AH Authentication

ESP Encryption  Key Size:  (AES only)

ESP Authentication

Manual Key Exchange

IKE (Internet Key Exchange)

Direction:

Local Identity Type:

Local Identity Data:

Remote Identity Type:

Remote Identity Data:

Authentication:  RSA Signature (requires certificate)  
 Pre-shared Key

Authentication Algorithm:

Encryption:  Key Size:  (AES only)

Exchange Mode:

IKE SA Life Time:  (secs)

IKE Keep Alive Ping IP Address:

IPSec SA Life Time:  (secs)

DH Group:

IKE PFS:

IPSec PFS: