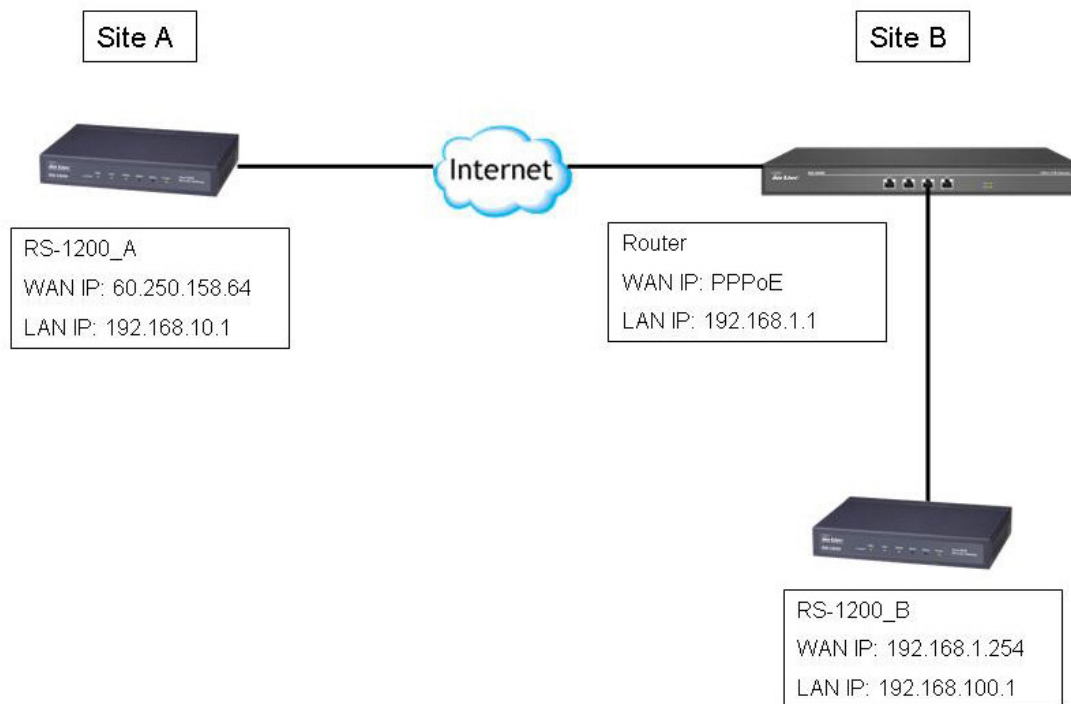


## How to create IPSec VPN via NAT

### Topology:



### Environment:

#### RS-1200\_A:

WAN IP address: 60.250.158.64

LAN IP address: 192.168.10.1

#### Router at Site B:

WAN IP address: PPPoE

DDNS: enable, DDNS name is [airlive15.dyndns.org](http://airlive15.dyndns.org)

LAN IP address: 192.168.1.1

#### RS-1200\_B:

WAN IP address: 192.168.1.254

LAN IP address: 192.168.100.1

## Configuration of RS-1200 at Site A

### 1. Policy Object → VPN → IPsec Autokey: Configure IPsec setting

**Air Live®** Policy Object > VPN > IPsec Autokey

**System**  
**Interface**  
**Policy Object**  
Address  
Service  
Schedule  
QoS  
Authentication  
Content Blocking  
IM / P2P Blocking  
Virtual Server  
**VPN**  
One-Step IPsec  
IPsec Autokey  
PPTP Server  
PPTP Client  
Tunnel  
**Policy**  
Anomaly Flow IP  
Monitor

**Necessary Item**

Name	Site_A
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Remote	<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name: <input type="text" value="airlive15.dyndns.org"/> (Max. 99 characters)
	<input type="radio"/> Remote Gateway or Client -- Dynamic IP
Authentication Method	Preshare
Preshared Key	<input type="text" value="12345678"/> (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1
IPsec Algorithm	<input checked="" type="radio"/> Data Encryption + Authentication
	<input type="radio"/> Authentication Only
ENC Algorithm	3DES
AUTH Algorithm	MD5

**Optional Item**

Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	<input type="text" value="3600"/> Seconds (Range: 1200 - 86400)
IPsec Lifetime	<input type="text" value="28800"/> Seconds (Range: 1200 - 86400)
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
My ID	<input type="text"/> (Max. 39 characters)
Peer ID	<input type="text" value="192.168.1.254"/> (Max. 39 characters)
GRE/IPsec	
GRE Local IP	<input type="text"/>
GRE Remote IP	<input type="text"/>
<input type="checkbox"/> Manual Connect	
Dead Peer Detection	delay: <input type="text" value="5"/> Second Timeout: <input type="text" value="60"/> Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

Note: In order to identify the WAN IP address of RS-1200 at Site B, user needs to specify the Peer ID on Site A RS-1200 IPsec setting, the Peer ID must be the WAN IP address of Site B RS-1200, in this example, the Peer ID is 192.168.1.254.

### 2. Policy Object → VPN → Tunnel: Define the further IPsec information

**Air Live®** Policy Object > VPN > Tunnel

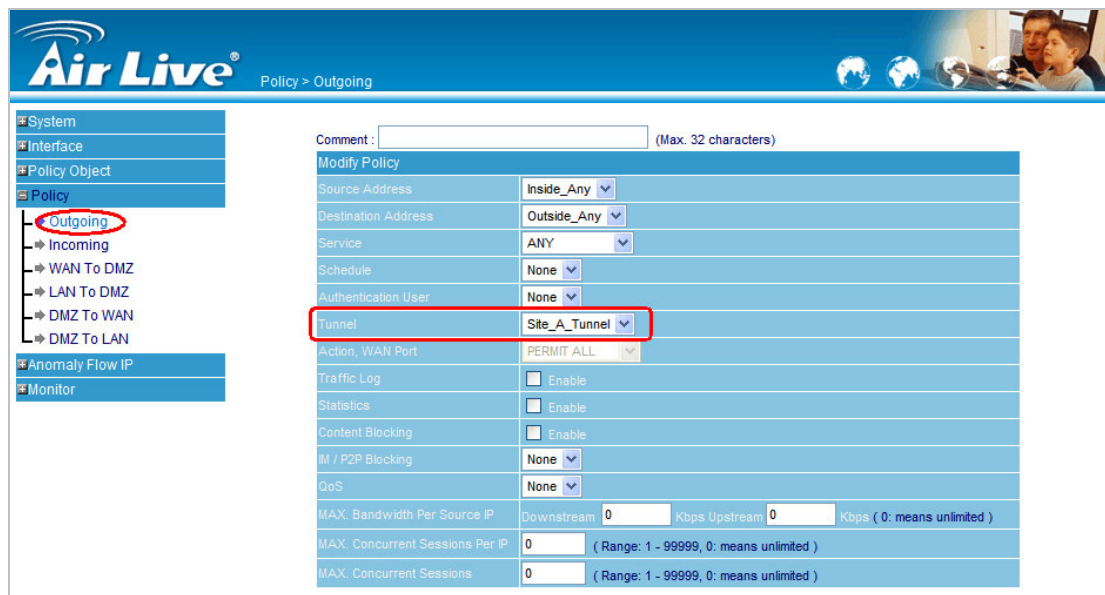
**System**  
**Interface**  
**Policy Object**  
Address  
Service  
Schedule  
QoS  
Authentication  
Content Blocking  
IM / P2P Blocking  
Virtual Server  
**VPN**  
One-Step IPsec  
IPsec Autokey  
PPTP Server  
PPTP Client  
**Tunnel**  
**Policy**  
Anomaly Flow IP  
Monitor

**Modify Site\_A\_Tunnel Tunnel**

Name	Site_A_Tunnel
From Local	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Local Subnet / Mask	<input type="text" value="192.168.10.0"/> / <input type="text" value="255.255.255.0"/>
To Remote	<input checked="" type="radio"/> To Remote Subnet / Mask: <input type="text" value="192.168.100.0"/> / <input type="text" value="255.255.255.0"/>
	<input type="radio"/> Remote Client
IPsec / PPTP Setting	Site_A
Keep alive IP:	<input type="text" value="192.168.100.1"/>
<input type="checkbox"/> Show remote Network Neighborhood	

**Cancel**

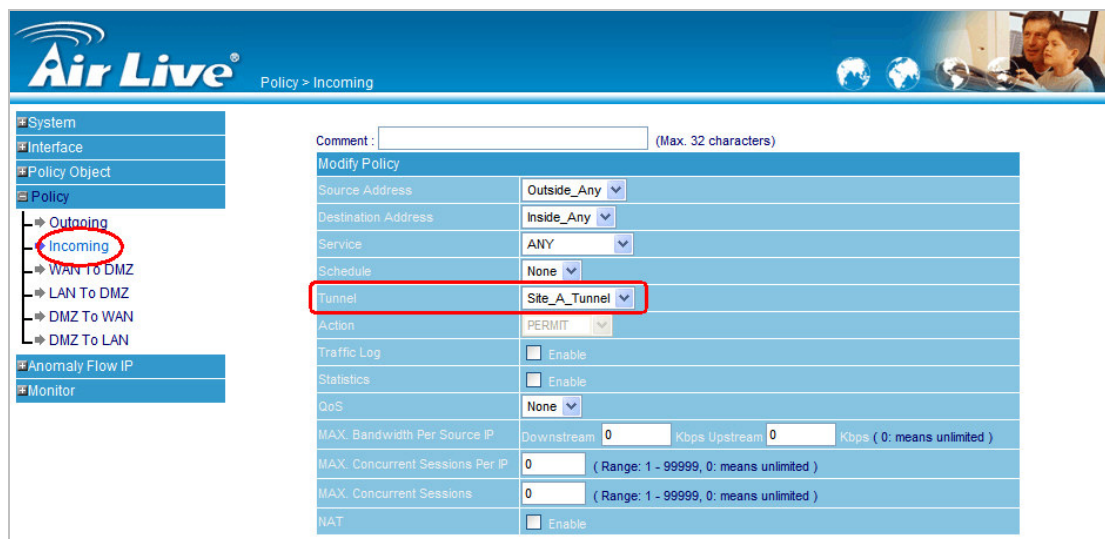
### 3. Policy → Outgoing: enable IPSec VPN



The screenshot shows the 'Air Live' web interface for configuring an outgoing policy. The left sidebar has a tree view with 'Policy' expanded and 'Outgoing' selected. The main area is titled 'Policy > Outgoing' and contains a 'Modify Policy' form. The form fields are: Source Address (Inside\_Any), Destination Address (Outside\_Any), Service (ANY), Schedule (None), Authentication User (None), Tunnel (Site\_A\_Tunnel), Action, WAN Port (PERMIT ALL), Traffic Log (Enable), Statistics (Enable), Content Blocking (Enable), M / P2P Blocking (None), QoS (None), MAX. Bandwidth Per Source IP (Downstream 0 Kbps Upstream 0 Kbps), MAX. Concurrent Sessions Per IP (0), and MAX. Concurrent Sessions (0). The 'Tunnel' field is highlighted with a red box.

Field	Value
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	Site_A_Tunnel
Action, WAN Port	PERMIT ALL
Traffic Log	Enable
Statistics	Enable
Content Blocking	Enable
M / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps
MAX. Concurrent Sessions Per IP	0
MAX. Concurrent Sessions	0

### 4. Policy → Incoming: enable IPSec VPN



The screenshot shows the 'Air Live' web interface for configuring an incoming policy. The left sidebar has a tree view with 'Policy' expanded and 'Incoming' selected. The main area is titled 'Policy > Incoming' and contains a 'Modify Policy' form. The form fields are: Source Address (Outside\_Any), Destination Address (Inside\_Any), Service (ANY), Schedule (None), Tunnel (Site\_A\_Tunnel), Action (PERMIT), Traffic Log (Enable), Statistics (Enable), QoS (None), MAX. Bandwidth Per Source IP (Downstream 0 Kbps Upstream 0 Kbps), MAX. Concurrent Sessions Per IP (0), MAX. Concurrent Sessions (0), and NAT (Enable). The 'Tunnel' field is highlighted with a red box.

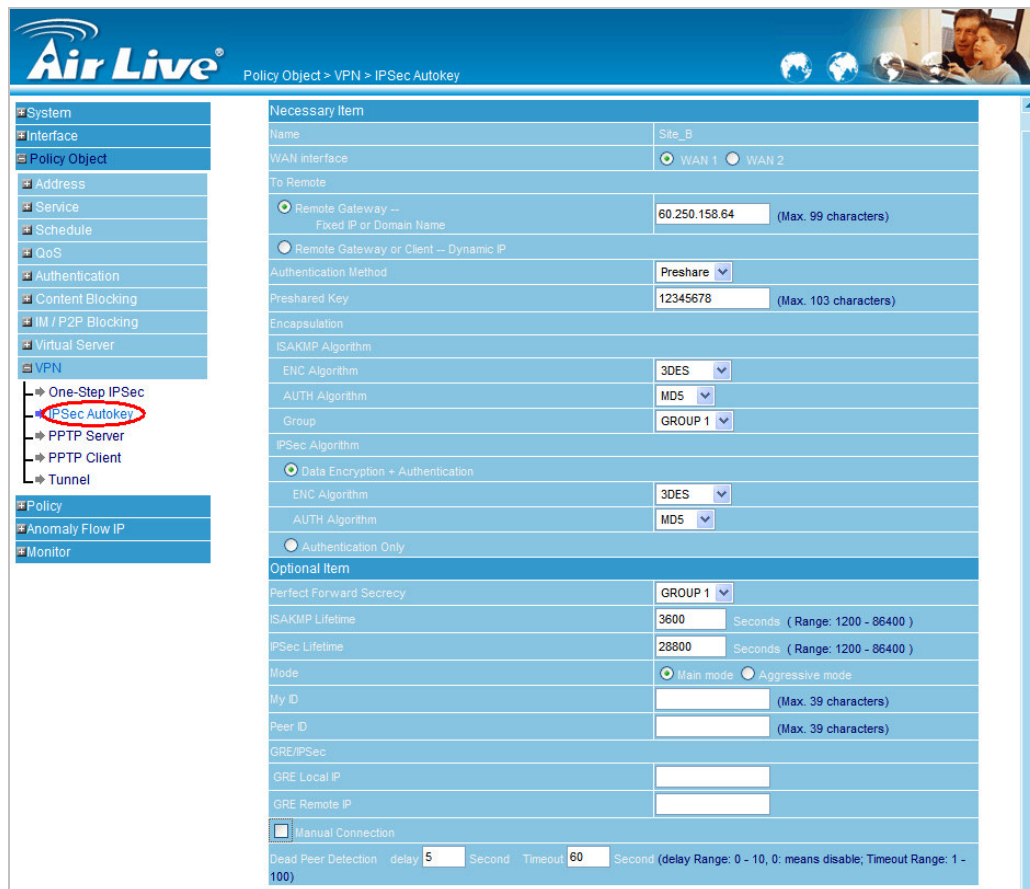
Field	Value
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	Site_A_Tunnel
Action	PERMIT
Traffic Log	Enable
Statistics	Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps
MAX. Concurrent Sessions Per IP	0
MAX. Concurrent Sessions	0
NAT	Enable

## Configuration of NAT Router at Site B

1. If the router connects to ISP with PPPoE, user can enable DDNS service to resolve the changeable WAN IP address, in order to keep IPSec VPN connecting.
2. Define **Virtual Server** or **Port Forwarding** to redirect **IP 50, IP 51, UDP 500, UDP 4500** to RS-1200 in Router's LAN site.

## Configuration of RS-1200 at Site B

### 1. Policy Object → VPN → IPSec Autokey: Configure IPSec setting



The screenshot shows the 'Air Live' web interface for configuring a VPN Policy Object. The breadcrumb trail is 'Policy Object > VPN > IPSec Autokey'. The left sidebar contains a tree view with 'VPN' expanded and 'IPSec Autokey' selected. The main area is divided into 'Necessary Item' and 'Optional Item' sections.

Necessary Item	
Name	Site_B
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	60.250.158.64 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare
Preshared Key	12345678 (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1
IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
My ID	(Max. 39 characters)
Peer ID	(Max. 39 characters)
GRE/IPSec	
GRE Local IP	
GRE Remote IP	
<input type="checkbox"/> Manual Connection	
Dead Peer Detection	delay: 5 Second Timeout: 60 Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

Note: User does not need to specify Peer ID on RS-1200 of Site B.

### 2. Policy Object → VPN → Tunnel: Define the further IPSec information

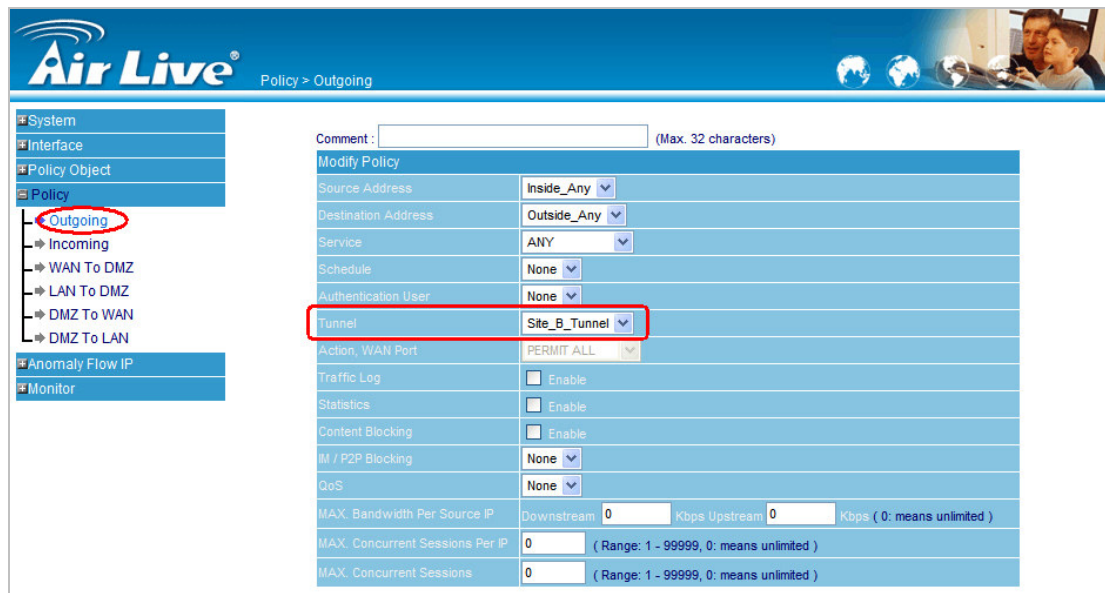


The screenshot shows the 'Air Live' web interface for configuring a VPN Policy Object. The breadcrumb trail is 'Policy Object > VPN > Tunnel'. The left sidebar contains a tree view with 'VPN' expanded and 'Tunnel' selected. The main area is titled 'Modify Site\_B\_Tunnel Tunnel'.

Modify Site_B_Tunnel Tunnel	
Name	Site_B_Tunnel
From Local	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Local Subnet / Mask	192.168.100.0 255.255.255.0
To Remote	
<input checked="" type="radio"/> To Remote Subnet / Mask	192.168.10.0 255.255.255.0
<input type="radio"/> Remote Client	
IPSec / PPTP Setting	Site_B
Keep alive IP:	192.168.10.1
<input type="checkbox"/> Show remote Network Neighborhood	

Cancel

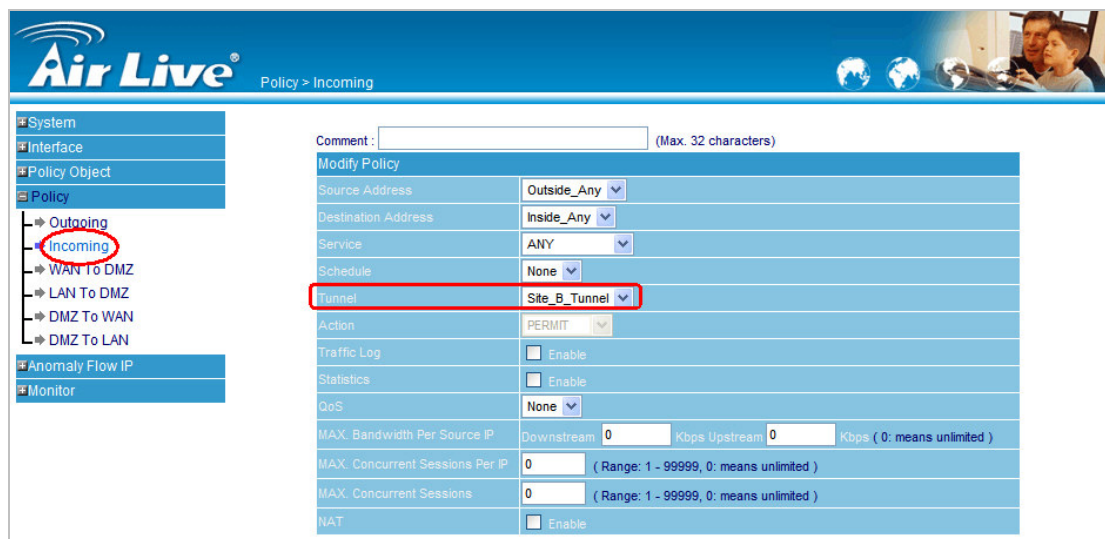
### 3. Policy → Outgoing: enable IPSec VPN



The screenshot shows the 'Air Live' web interface for configuring an outgoing policy. The left sidebar contains a tree view with 'Policy' expanded and 'Outgoing' selected. The main area is titled 'Policy > Outgoing' and contains a 'Modify Policy' form. The form fields are as follows:

Field	Value
Comment	(Max. 32 characters)
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	Site_B_Tunnel
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)

### 4. Policy → Incoming: enable IPSec VPN



The screenshot shows the 'Air Live' web interface for configuring an incoming policy. The left sidebar contains a tree view with 'Policy' expanded and 'Incoming' selected. The main area is titled 'Policy > Incoming' and contains a 'Modify Policy' form. The form fields are as follows:

Field	Value
Comment	(Max. 32 characters)
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	Site_B_Tunnel
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
NAT	<input type="checkbox"/> Enable

5. Then the user in Site A or Site B can connect to the other side of server or PC to access data.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Matt.Chen>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : Jacky
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 區域連線 3:

    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8169/8110 Family Gigabit Ethernet NIC
    Physical Address. . . . . : 00-4F-63-01-37-EA
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
    DHCP Server . . . . . : 192.168.100.1
    DNS Servers . . . . . : 168.95.1.1
    Lease Obtained. . . . . : 2008年11月17日 下午 01:49:51
    Lease Expires . . . . . : 2008年11月18日 下午 01:49:51

C:\Documents and Settings\Matt.Chen>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=112ms TTL=126
Reply from 192.168.100.2: bytes=32 time=95ms TTL=126
Reply from 192.168.100.2: bytes=32 time=293ms TTL=126
Reply from 192.168.100.2: bytes=32 time=95ms TTL=126

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 95ms, Maximum = 293ms, Average = 148ms

C:\Documents and Settings\Matt.Chen>
```

**Attention:** There are two key points for the configuration:

1. The router of Site B must support to forward IP protocol, and it is not available if the router only supports to forward TCP and UDP protocol.
2. The RS-1200 of Site A must be specified an IP address at Peer ID, otherwise the VPN tunnel can not be created.