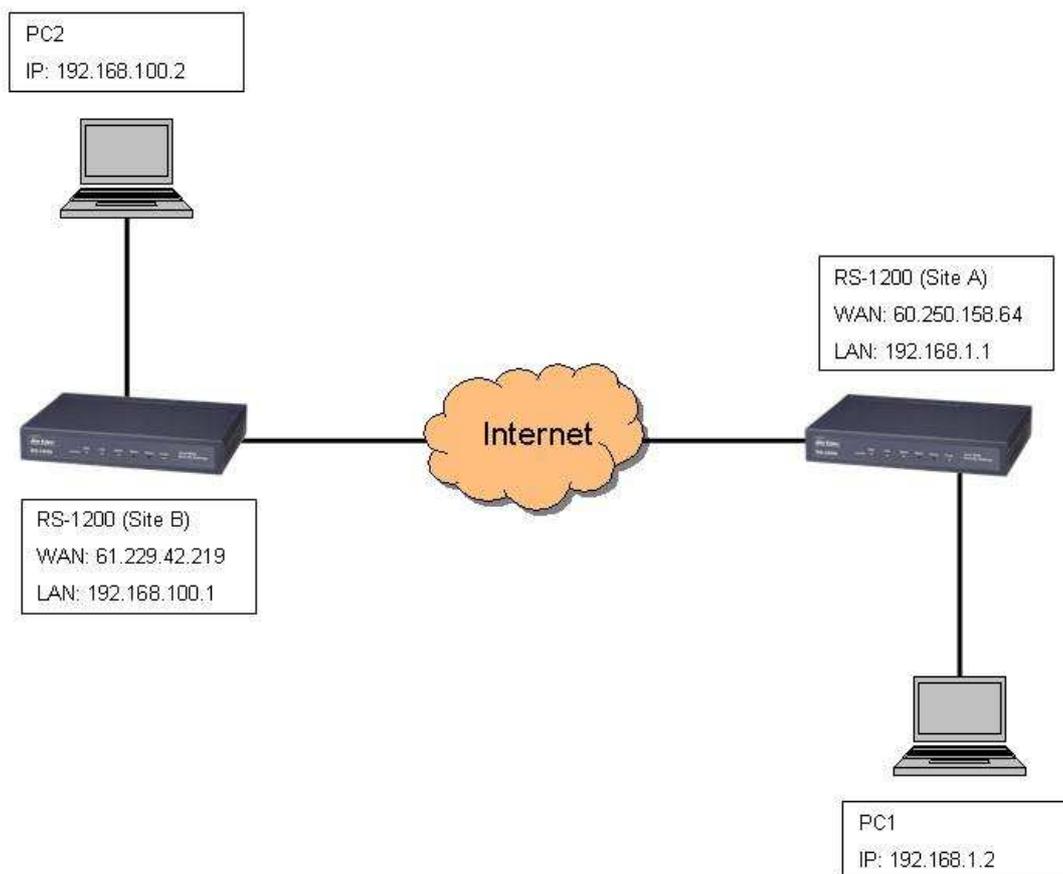


How to establish the VPN between two RS Series



Note: Here, we use the RS-1200 for the example, it can also be used on the RS-2500 and RS-3000.

Site A RS-1200 Configuration:

1. Configure **VPN** → **IPSec Autokey** as following example:
 - **Remote Gateway:** indicate the other side VPN router's IP address or domain name
 - **Preshared Key:** user can define the key by himself, the key uses to identify the exchanged data for VPN
 - **Encryption:** support DES, 3DES, AES-128, AES-192, and AES-256, AES-256 provides more secure encrypted type but less performance.
 - **Authentication:** support MD5 and SHA-1
 - Both sides **Preshared Key**, **Encryption** and **Authentication** setting must be the same, or VPN tunnel cannot be built up.

How to establish the VPN between two RS Series

- **ISAKMP Life Time, IPSec Life Time:** both settings are related to the life time of VPN tunnel, if you do not know how to configure it, just leave the setting as default.

Necessary Item	
Name	RS_01
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name:	61.229.42.219 (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 2
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 2
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 Connect	
Dead Peer Detection	delay: 5 Second Timeout: 60 Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

2. Configure **Tunnel** to define further IPSec rule. (In RS-1200, the item name is **Trunk**)

- **Source Subnet / Mask:** indicate Site A LAN IP subnet
- **Destination Subnet / Mask:** indicate Site B LAN IP subnet

How to establish the VPN between two RS Series

- **Keep alive IP:** it uses to trigger the connection of VPN tunnel in order to keep VPN tunnel working. It is usually to configure the Keep alive IP with the other VPN side router's LAN IP address.
- **Show remote Network Neighborhood:** allow NetBIOS protocol to pass through VPN tunnel

Modify RS_01_Tunnel Tunnel	
Name	RS_01_Tunnel
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.1.0 / 255.255.255.0
To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.100.0 / 255.255.255.0
<input type="radio"/> Remote Client	
IPSec / PPTP Setting	RS_01
Keep alive IP	192.168.100.1
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

3. Enable IPSec VPN in Outgoing and Incoming Policy

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	RS_01_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)

How to establish the VPN between two RS Series

Modify Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	RS_01_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
NAT	<input type="checkbox"/> Enable

Site B RS-1200 Configuration:

1. Configure **VPN** → **IPSec Autokey** as following example:

How to establish the VPN between two RS Series

Necessary Item	
Name	RS_100
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Destination	<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name: <input type="text" value="60.250.158.64"/> (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 2
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 2
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"/> (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)

- Configure **Tunnel** to define further IPSec rule. (In RS-1200, the item name is **Trunk**)

How to establish the VPN between two RS Series

Modify RS_100_Tunnel Tunnel	
Name	RS_100_Tunnel
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.100.0 255.255.255.0
To Destination	
<input checked="" type="radio"/> To Destination Subnet / Mask	192.168.1.0 255.255.255.0
<input type="radio"/> Remote Client	
IPSec / PPTP Setting	RS_100
Keep alive IP :	192.168.1.1
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

3. Enable IPSec VPN in Outgoing and Incoming Policy

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	RS_100_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)

How to establish the VPN between two RS Series

Modify Policy	
Source Address:	Outside_Any ▾
Destination Address:	Inside_Any ▾
Service:	ANY ▾
Schedule:	None ▾
Tunnel:	RS_100_Tunnel ▾
Action:	PERMIT ▾
Traffic Log:	<input type="checkbox"/> Enable
Statistics:	<input type="checkbox"/> Enable
CoS:	None ▾
MAX. Bandwidth Per Source IP:	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP:	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions:	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
NAT:	<input type="checkbox"/> Enable

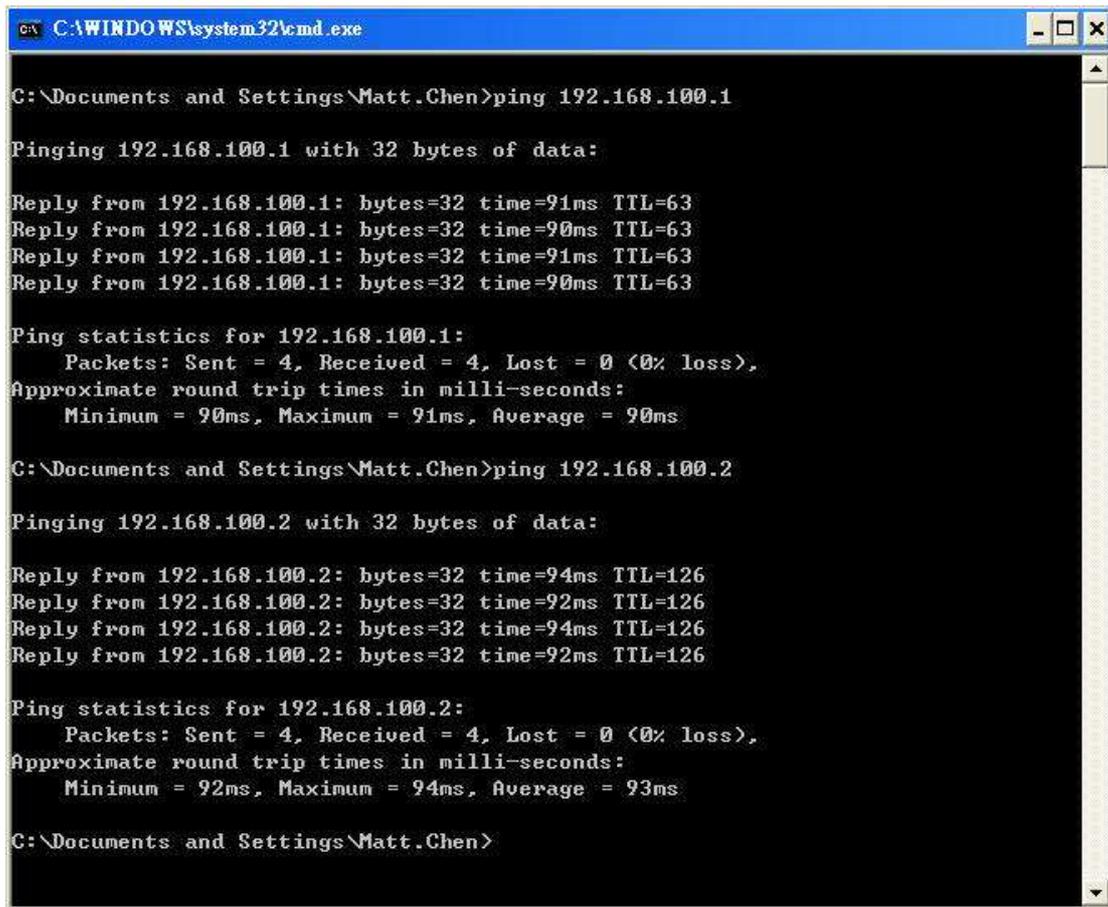
4. Finish both site of VPN setting.

Verify the VPN connection

From Site A PC 192.168.1.2

1. Try to ping Site B LAN IP 192.168.100.1 and the IP address 192.168.100.2 of PC2, both ping results are fine.

How to establish the VPN between two RS Series



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

C:\Documents and Settings\Matt.Chen>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time=91ms TTL=63
Reply from 192.168.100.1: bytes=32 time=90ms TTL=63
Reply from 192.168.100.1: bytes=32 time=91ms TTL=63
Reply from 192.168.100.1: bytes=32 time=90ms TTL=63

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 90ms, Maximum = 91ms, Average = 90ms

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

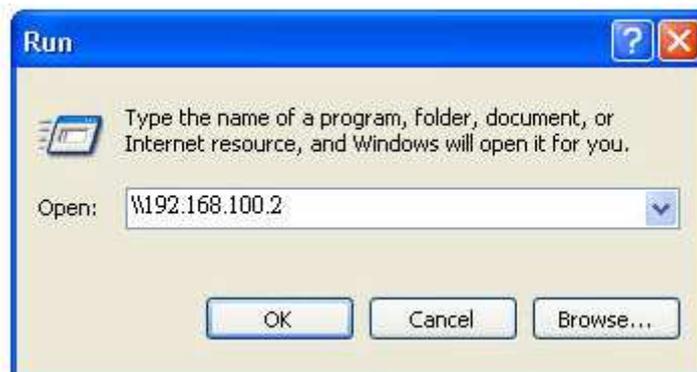
Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=94ms TTL=126
Reply from 192.168.100.2: bytes=32 time=92ms TTL=126
Reply from 192.168.100.2: bytes=32 time=94ms TTL=126
Reply from 192.168.100.2: bytes=32 time=92ms TTL=126

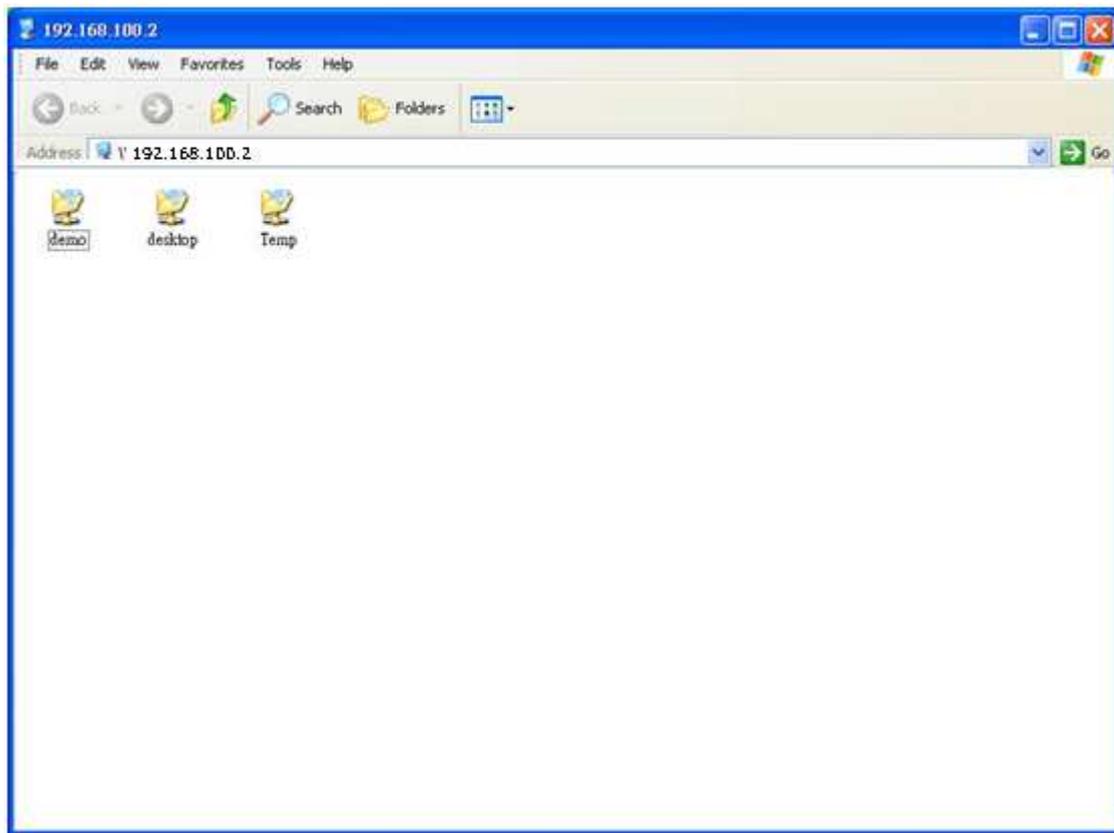
Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 92ms, Maximum = 94ms, Average = 93ms

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

2. PC1 also can connect to PC2 directly using IP 192.168.100.2, and send file to PC2.



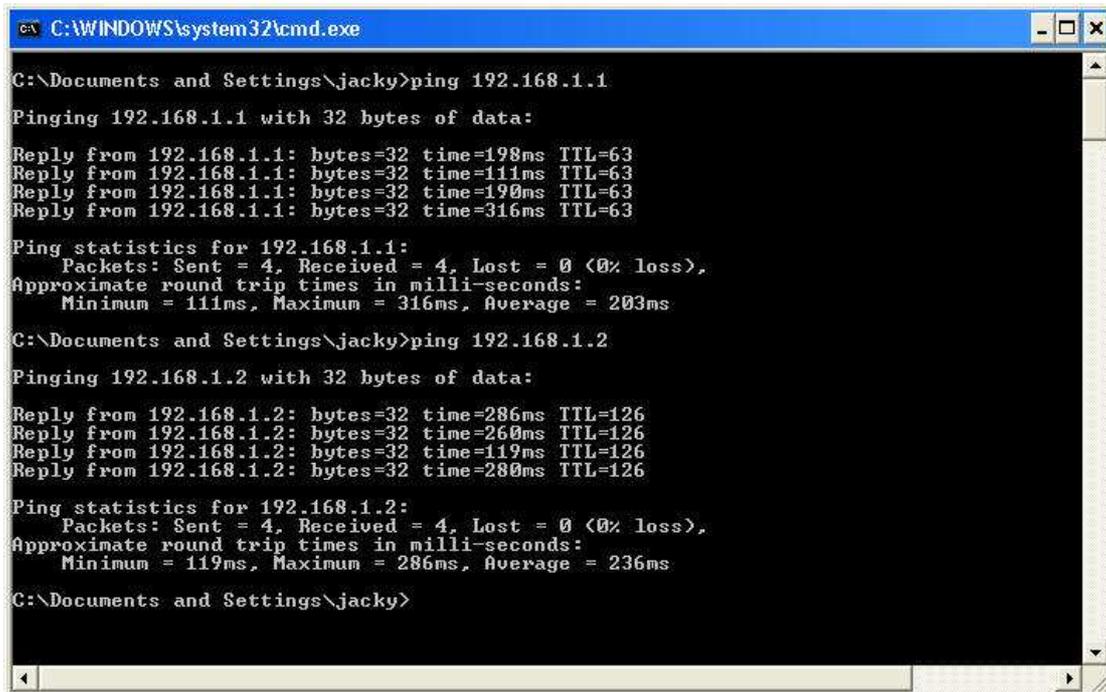
How to establish the VPN between two RS Series



From Site B PC 192.168.100.2

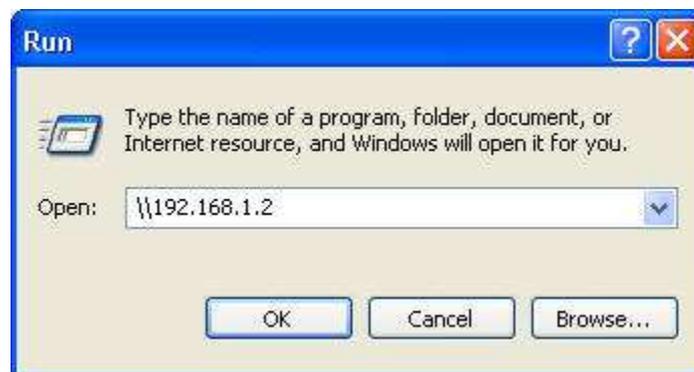
1. Try to ping Site A LAN IP 192.168.1.1 and the IP address 192.168.1.2 of PC1, both ping results are fine.

How to establish the VPN between two RS Series

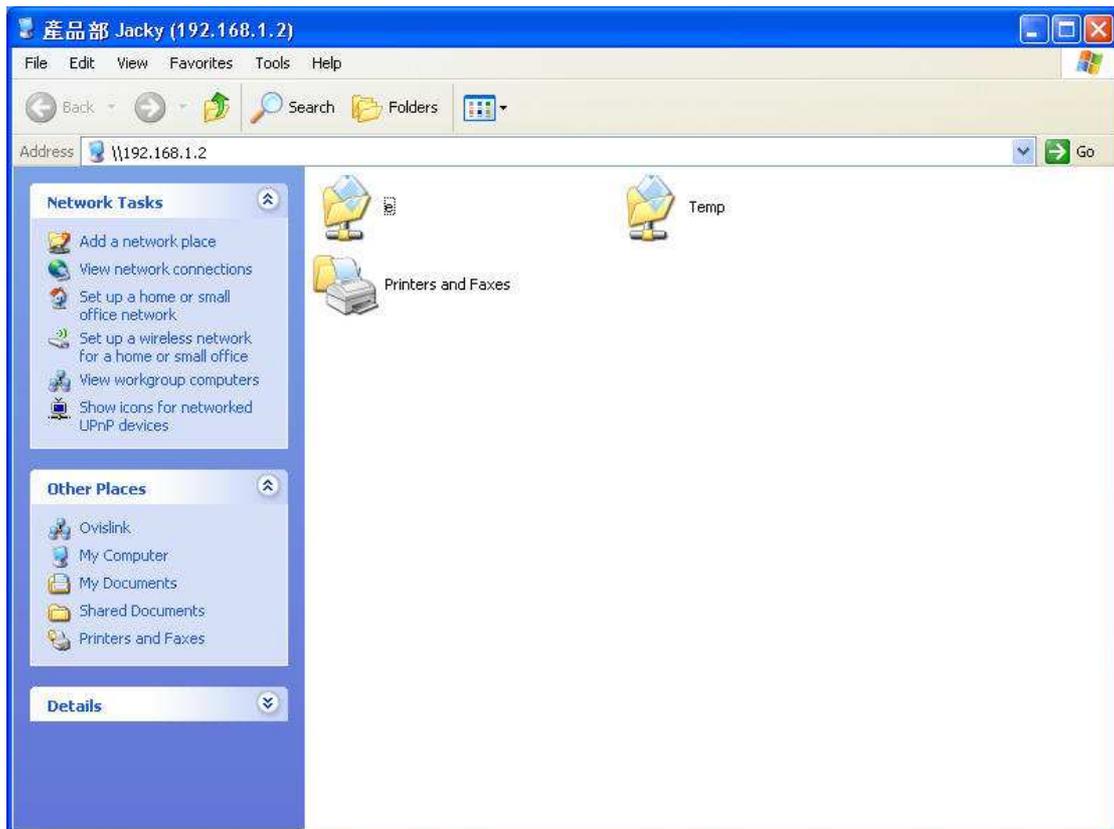


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\jacky>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=198ms TTL=63
Reply from 192.168.1.1: bytes=32 time=111ms TTL=63
Reply from 192.168.1.1: bytes=32 time=190ms TTL=63
Reply from 192.168.1.1: bytes=32 time=316ms TTL=63
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 111ms, Maximum = 316ms, Average = 203ms
C:\Documents and Settings\jacky>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=286ms TTL=126
Reply from 192.168.1.2: bytes=32 time=260ms TTL=126
Reply from 192.168.1.2: bytes=32 time=119ms TTL=126
Reply from 192.168.1.2: bytes=32 time=280ms TTL=126
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 119ms, Maximum = 286ms, Average = 236ms
C:\Documents and Settings\jacky>
```

2. PC2 also can connect to PC1 directly using IP 192.168.1.2, and send file to PC1



How to establish the VPN between two RS Series



3. So, we know the IPsec connection is working well.