

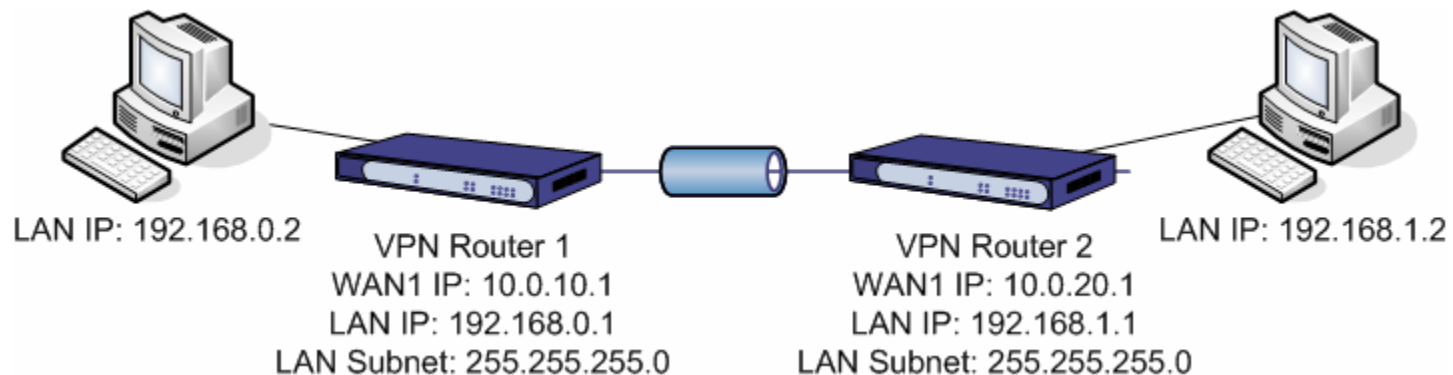
XiNCOM VPN Guide - Example VPN Configurations

Provided by XiNCOM's Client Care Team.

Gateway to Gateway

This section instructs you how to create a VPN tunnel between two XiNCOM VPN gateways. The following example is based on two XiNCOM DPG503 VPN gateways with firmware version 3.2 Rel 27 Built Date: Oct 26 2004. The example also applies to the XiNCOM DPG603 VPN gateway. We will be using only WAN1 for this example.

NOTE: The local WAN IP addresses in this configuration are used only as an example. This example was performed over a LAN. Real IP addresses are required to make this connection over the Internet.



Indicated in the example above, both routers must reside on different IP subnets. A VPN tunnel works very similar to a static route. If you use the same IP subnet for both sides, the computers that reside behind the VPN devices will not use the default route in order to go to the remote side. This will cause the computers to search for a destination IP address locally rather than using the VPN tunnel.

Configuration of VPN Router 1:

This configuration guide assumes that the Primary Configuration of your Twin WAN Gateway is complete and you are successfully able to ping the WAN IP of VPN Router 2 from VPN Router 1 and vice versa.

1. Log in to the router interface by going to the LAN IP with your web browser. For VPN Router 1 this will be <http://192.168.0.1> and for VPN Router 2 it will be <http://192.168.1.1>. The default user name is admin and the password is blank by default.
2. Select **VPN Configuration** from the main menu on the left and click Global Setting. Check the *Enable Setting* box on the WAN1 column and click *Submit*. The TWR VPN gateway will reboot after this step.
3. After approximately 10 seconds, log back into the router, click **VPN Configuration** and click *Policy Setup*.
4. IPsec Traffic Binding:
 - Under Tunnel Name enter VPN_Router_2 (You can enter any name of your choosing). The tunnel name does not have to match the remote side. This name is only for user reference.
 - Check the *Tunnel Enable* box.
 - Select WAN1 from the WAN Port drop down box.
 - If PPPoE is used to connect to the Internet, select Session 1 from the PPPoE Session drop-down box. More PPPoE Sessions may be configured in the *Advanced Port* menu and *Advanced PPPoE* sub-menu.
 - Leave *Local Identity Type* as WAN IP.

IPSec Traffic Binding	
VPN Tunnel List	<input type="button" value="v"/>
Tunnel Name	<input type="text" value="VPN_Router_2"/>
Tunnel	<input checked="" type="checkbox"/> Enable
WAN Port	<input type="button" value="v"/> WAN 1
PPPoE Session	<input type="button" value="v"/> Session 1
Local Identity Type	<input type="button" value="v"/> Wan IP Address

5. Traffic Selector:
 - Leave the Service Protocol Type as *Any* to allow all types of packets through.
 - Under the *Local Security Network* set the Local Type as Subnet. The page will refresh allowing you to enter the Subnet Mask as well as the IP Address.
 - For IP Address enter 192.168.0.0 and 255.255.255.0 for Subnet Mask. Leave the Port Range at 0 through 0. This allows packets on any port.

- Under the *Remote Security Network*, set the Remote Type as subnet. Set the IP address to 192.168.1.0 and Subnet Mask as 255.255.255.0. Leave the Port Range at 0 through 0.
- Under the *Remote Security Gateway*, leave the Identity Type as IP Address and into the IP Address box enter the WAN IP address of the remote gateway. In this example, IP Address 10.0.20.1 is used

Traffic Selector	
Service	Protocol Type <input type="text" value="Any"/>
Local Security Network	Local Type <input type="text" value="Subnet"/>
	IP Address <input type="text" value="192.168.0.1"/> Mask Address <input type="text" value="255.255.255.0"/>
	Port Range <input type="text" value="0"/> ~ <input type="text" value="0"/>
Remote Security Network	Remote Type <input type="text" value="Subnet"/>
	IP Address <input type="text" value="192.168.1.0"/> Mask Address <input type="text" value="255.255.255.0"/>
	Port Range <input type="text" value="0"/> ~ <input type="text" value="0"/>
Remote Security Gateway	Identity Type <input type="text" value="IP Address"/>
	IP Address <input type="text" value="10.0.20.1"/>

6. Security Level:

- Set the Encryption Method to DES and set the Authentication Method to MD5.
- In this firmware release (v3.2 Rel 27) only Tunnel ESP Mode is supported. The ESP Mode is grayed out.

Security Level	
Encryption Method	<input type="text" value="DES"/>
Authentication Method	<input type="text" value="MD5"/>
ESP Mode	<input type="text" value="Tunnel"/>

7. Key Management:

- Leave the Key Type as AutoKey (IKE).
- Leave Phase 1 Negotiation as Main Mode.
- Leave Perfect Forward Secrecy as No PFS.
- Set the Preshared Key to 012345.
- Leave the Key Lifetimes as 3600 for Time and 0 for Volume.

Key Management	
Key Type	AutoKey (IKE) ▾
Phase 1 Negotiation	Main Mode ▾
Perfect Forward Secrecy	No PFS ▾
Preshared Key	012345 (Characters / Hex:0x)
Key Lifetime	In Time 3600 Seconds (Note : 0 for no expiry)
	In Volume 0 Kbytes

8. Click the Add button to create this policy.

Configuration of VPN Router 2:

1. Log in to the router interface by going to the LAN IP with your web browser.
2. Select **VPN Configuration** from the main menu on the left and click *Global Setting*. Check the *Enable Setting* box on the WAN1 column and click *Submit*. The TWR VPN gateway will reboot after this step.
3. After approximately 10 seconds, log back into the router, click **VPN Configuration** and click *Policy Setup*.
4. IPsec Traffic Binding:
 - Under Tunnel Name enter VPN_Router_1. (You can enter any name of your choosing). The tunnel name does not have to match the remote side. This name is only for user reference.
 - Check the *Tunnel Enable* box.
 - Select WAN1 from the WAN Port drop down box.
 - If PPPoE is used to connect to the Internet, select Session 1 from the *PPPoE Session* drop-down box. More PPPoE Sessions may be configured in the *Advanced Port* menu and *Advanced PPPoE* sub-menu.
 - Leave *Local Identity Type* as WAN IP.
5. Traffic Selector:
 - Leave the *Service Protocol Type* as Any to allow all types of packets through.
 - Under the *Local Security Network* set the Local Type as Subnet. The page will refresh allowing you to enter the Subnet Mask as well as the IP Address.
 - For IP Address enter 192.168.1.0 and 255.255.255.0 for Subnet Mask. Leave the Port Range at 0 through 0. This allows packets on any port.

- Under the *Remote Security Network* set the Remote Type as Subnet. Set the IP address to 192.168.0.0 and Subnet Mask as 255.255.255.0. Leave the Port Range at 0 through 0.
- Under the *Remote Security Gateway*, leave the Identity Type as IP Address and into the IP Address box enter the WAN IP address of the remote gateway, in this case its 10.0.20.1

6. Security Level:

- Set the Encryption Method to DES and set the Authentication Method to MD5.
- In this firmware release (v3.2 Rel 27) only Tunnel ESP Mode is supported. The ESP Mode is grayed out.

7. Key Management:

- Leave the Key Type as AutoKey (IKE).
- Leave Phase 1 Negotiation as Main Mode.
- Leave Perfect Forward Secrecy as No PFS.
- Set the Preshared Key to 012345.
- Leave the Key Lifetimes as 3600 for Time and 0 for Volume.

8. Click the *Add* button to create this policy.

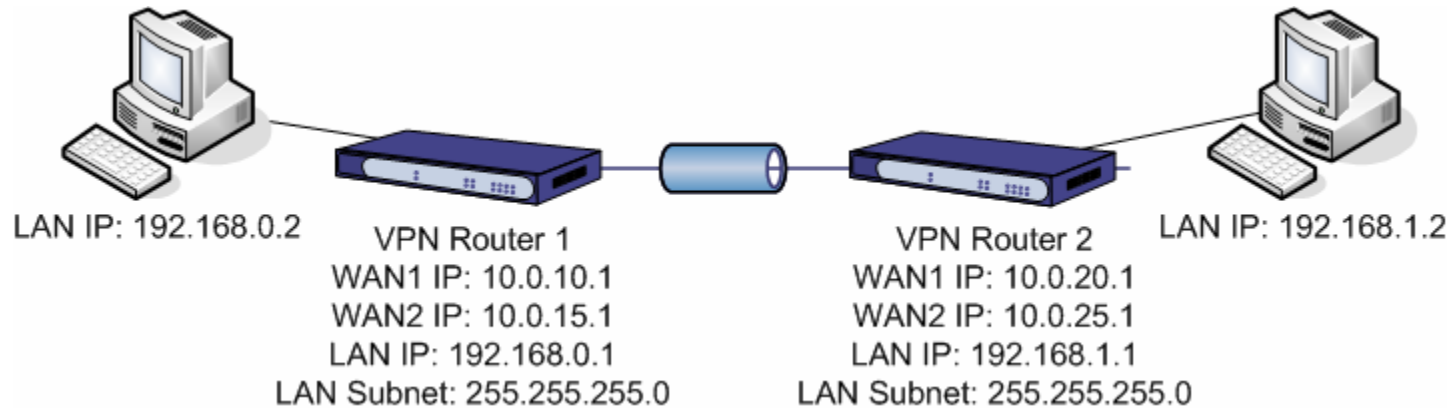
Once both remote and the local sides are configured you can press the *Connect* button to initiate the VPN tunnel. It does not matter which side initiates the connection. Shortly after, the VPN State for the tunnel will then go from *Idle* to *Established* thereby allowing IP traffic to be passed securely between the two endpoints.

Testing

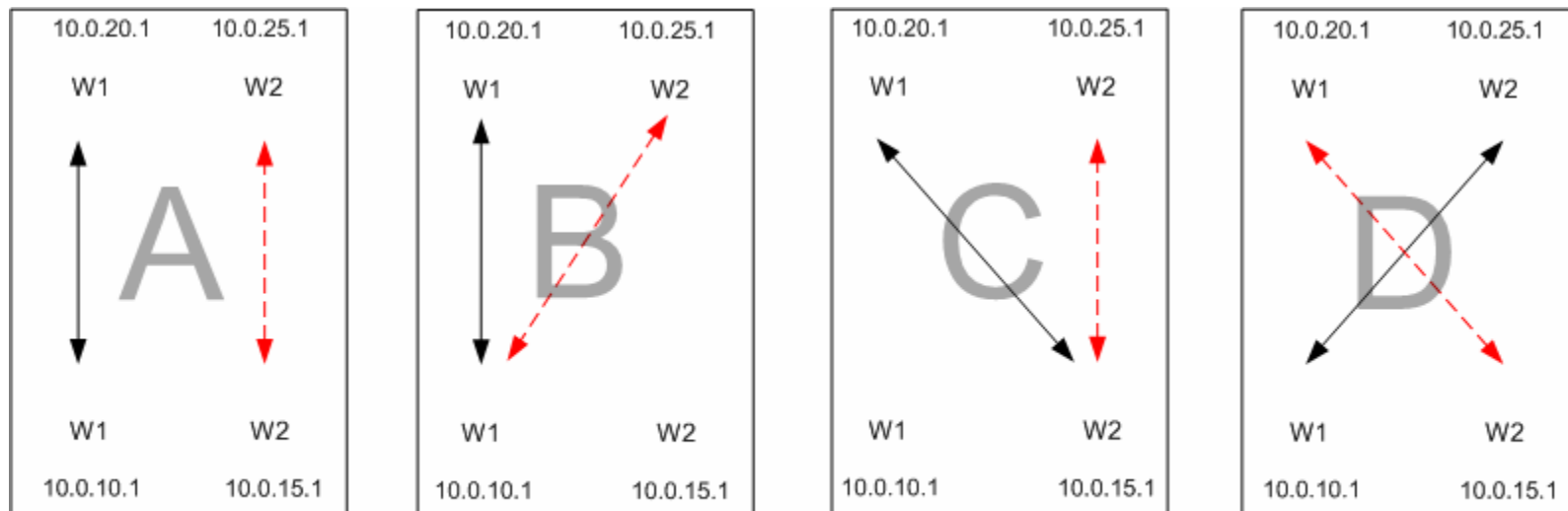
To test your VPN configuration, simply ping the PC or the router on the other side of the tunnel by using the ping utility built into your operating system. Before implementing the VPN into a live environment it is also suggested to test all services which will be used.

Basic VPN Failover Configuration

There are multiple methods of creating VPN failover. This example does not cover them all but will help give you a general idea of how to setup your VPN for failover. Since VPN failover utilizes both WAN ports, two Policies must be created on each device. For the purpose of this configuration, the VPN diagram below will be expanded to accommodate WAN1 as well as WAN2.



The following diagram displays the various methods of VPN failover that the DPG503 supports. This example only covers Type A configuration.



←→ Normal Tunnel

←- - - - - Backup Tunnel

Configuration of VPN Router 1:

Please follow the Gateway to Gateway example to create two VPN tunnels with the following settings (please follow the table left to right):

VPN Policy 1:

IPsec Traffic Binding Tunnel Name: VPN_Router_2_w1 Tunnel: Enable WAN Port: WAN1 Local Identity Type: Wan IP	Traffic Selector Service Protocol Type: Any Local Security Network Local Type: Subnet IP Address: 192.168.0.0 Subnet: 255.255.255.0 Port Range: 0 ~ 0	Remote Security Network Remote Type: Subnet IP Address: 192.168.1.0 Subnet: 255.255.255.0 Port Range: 0 ~ 0
Remote Security Gateway Identity Type: IP Address IP Address: 10.0.20.1	Key Management Key Type: AutoKey (IKE) Phase 1 Negotiation: Main Mode Perfect Forward Secrecy: No PFS Preshared Key: 012345 Key Lifetime In Time Seconds: 3600 In Volume Kbytes: 0	Security Level Encryption Method: DES Authentication Method: MD5

VPN Policy 2:

IPsec Traffic Binding Tunnel Name: VPN_Router_2_w2 Tunnel: Enable WAN Port: WAN2 Local Identity Type: Wan IP	Traffic Selector Service Protocol Type: Any Local Security Network Local Type: Subnet IP Address: 192.168.0.0 Subnet: 255.255.255.0 Port Range: 0 ~ 0	Remote Security Network Remote Type: Subnet IP Address: 192.168.1.0 Subnet: 255.255.255.0
Remote Security Gateway Identity Type: IP Address IP Address: 10.0.25.1 Port Range: 0 ~ 0	Key Management Key Type: AutoKey (IKE) Phase 1 Negotiation: Main Mode Perfect Forward Secrecy: No PFS Preshared Key: 012345 Key Lifetime In Time Seconds: 3600 In Volume Kbytes: 0	Security Level Encryption Method: DES Authentication Method: MD5

Configuration of VPN Router 2:

Please follow the Gateway to Gateway example to create two VPN tunnels with the following settings (please follow the table left to right):

VPN Policy 1:

IPsec Traffic Binding Tunnel Name: VPN_Router_1_w1 Tunnel: Enable WAN Port: WAN1 Local Identity Type: Wan IP	Traffic Selector Service Protocol Type: Any Local Security Network Local Type: Subnet IP Address: 192.168.1.0 Subnet: 255.255.255.0 Port Range: 0 ~ 0	Remote Security Network Remote Type: Subnet IP Address: 192.168.0.0 Subnet: 255.255.255.0
Remote Security Gateway Identity Type: IP Address IP Address: 10.0.10.1 Port Range: 0 ~ 0	Key Management Key Type: AutoKey (IKE) Phase 1 Negotiation: Main Mode Perfect Forward Secrecy: No PFS Preshared Key: 012345 Key Lifetime In Time Seconds: 3600 In Volume Kbytes: 0	Security Level Encryption Method: DES Authentication Method: MD5

VPN Policy 2:

IPsec Traffic Binding Tunnel Name: VPN_Router_1_w2 Tunnel: Enable WAN Port: WAN2 Local Identity Type: Wan IP	Traffic Selector Service Protocol Type: Any Local Security Network Local Type: Subnet IP Address: 192.168.1.0 Subnet: 255.255.255.0 Port Range: 0 ~ 0	Remote Security Network Remote Type: Subnet IP Address: 192.168.0.0 Subnet: 255.255.255.0
Remote Security Gateway Identity Type: IP Address IP Address: 10.0.15.1 Port Range: 0 ~ 0	Key Management Key Type: AutoKey (IKE) Phase 1 Negotiation: Main Mode Perfect Forward Secrecy: No PFS Preshared Key: 012345 Key Lifetime In Time Seconds: 3600 In Volume Kbytes: 0	Security Level Encryption Method: DES Authentication Method: MD5

Dead Peer Detection Configuration

After you configure the Policies the next step is *Dead Peer Detection* configuration. *Dead Peer Detection* will send a packet to a remote side and will await an ACK response. If the remote side does not respond, the tunnel is disconnected and the local gateway will attempt to renegotiate Phase 1 until successful. In the mean time the secondary policy you have created will be used until the primary VPN tunnel is re-established. *Dead Peer Detection* must be enabled on the remote and the local side for all policies.

1. On the *Policy Configuration* menu, select a Policy you would like to modify from the Policy List. The page will reload with the settings configured for that Policy.
2. Scroll down to the bottom of the page and click the Set Options button. A new screen will load showing DPD properties as well as other options.
3. Once there in the DPD section check the Enable box, set Check Method to ICMP and set action to Remove Tunnel you may also Enable Logging if you wish.

Dead Peer Detection Feature	
Detection	<input checked="" type="checkbox"/> Enable
Check Method	<input checked="" type="radio"/> ICMP <input type="radio"/> Heartbeat <input type="radio"/> Keepalive
Check After Idle	<input type="text" value="60"/> Seconds
Retry Times	<input type="text" value="10"/>
Action	<input type="radio"/> Do Nothing <input checked="" type="radio"/> Remove Tunnel <input type="radio"/> Keep Tunnel Alive
Logging	<input checked="" type="checkbox"/> Enable

The configuration as shown in the above example provides good tradeoffs. The Idle timeout is set to where the gateway will not waste bandwidth. In the event the VPN tunnel is severely congested, the retry is set high to a high enough that it will not allow the tunnel to be disconnected in mid-session.

Testing

It is recommended to test the settings after you have configured the tunnels. You can do this either by unplugging the WAN ports or by unplugging your cable or phone from the modem.