

PPTP VPN Configuration Using XiNCOM XC-DPG402/502/503/602/603

If you are using a PPTP VPN client or a device behind NAT using a XiNCOM XC-DPG402/502/503/602 or 603 please refer to the following configuration to solve issues with disconnected tunnels, improper authentication or dropped packets.

Overview

The Twin WAN Family product line uses an advanced SPI firewall to protect your Local Area Network against malicious users. In order to offer the best possible protection the firewall must be very strict on its policies and it will block any irregular traffic. Due to the nature of some VPN packets they can be discarded by the firewall.

System Filter Menu

By going around the Firewall through the System Filter menu the XiNCOM Twin WAN Router is able to process packets directly using the System Protocol stack. This method is not required but in certain network environments usability issues can cause dropped VPN tunnels and failed authentication attempts. If you experience these problems please follow the below instructions.

System Filter Exception Rules

Enable	Interface	Protocol	Foreign Port Range	Device Port Range
<input checked="" type="checkbox"/>	ALL	TCP	1723 ~ 1723	1723 ~ 1723
<input checked="" type="checkbox"/>	ALL	UDP	1701 ~ 1701	1701 ~ 1701
<input checked="" type="checkbox"/>	ALL	ESP	0 ~ 0	0 ~ 0
<input checked="" type="checkbox"/>	ALL	GRE	0 ~ 0	0 ~ 0

1. Check the Enable box on the first line, set the Interface to ALL, select TCP as the protocol and set the Foreign and the Device Port Range to 1723.
2. Check the Enable box on the second line, set the interface to ALL, select UDP as the protocol and set the Foreign and the Device Port Range to 1701.
3. Check the Enable box on the third line, set the interface to ALL, select ESP as the protocol and leave the Foreign and the Device Port Range at 0.
4. Check the Enable box on the third line, set the interface to ALL, select GRE as the protocol and leave the Foreign and the Device Port Range at 0.

Protocol and Port Binding

Certain types of packets such as SSL and VPN cannot be load balanced. When two IP addresses from WAN 1 and WAN 2 use the same login parameters, the server to which the connection is being established usually interprets this as a hi-jack attempt (a malicious attempt to take over a session from a valid user). The Protocol and Port Binding menu is used to force all secure outgoing traffic through either WAN 1 or WAN 2.

Protocol & Port Binding

Enable	Source IP	Destination IP	Subnet Mask	Protocol	Port Range	WAN
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	TCP	1723 ~ 1723	WAN 1
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	UDP	1701 ~ 1701	WAN 1
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	ESP	0 ~ 0	WAN 1
<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0	GRE	0 ~ 0	WAN 1

1. Check the Enable box on the first line, leave the Source IP, Destination IP and Subnet Mask at the default values, set the Protocol to TCP, set the Port Range as 1723 ~1723 and select the interface you like to bind the traffic to.
2. Check the Enable box on the first line, set the Protocol to UDP, set the Port Range as 1701 ~1701 and select the interface you like to bind the traffic to.

3. Check the Enable box on the first line, set the Protocol to ESP, leave the Port Range as 0 -0 and select the interface you like to bind the traffic to.
4. Check the Enable box on the first line, set the Protocol to GRE, leave the Port Range as 0 -0 and select the interface you like to bind the traffic to.

Conclusion

This guide was designed as a workaround for common problems when using PPTP VPN client software through the SPI firewall of the XiNCOM Twin WAN Product line. There are no guarantees stated or implied. If issues still ensue when following this guide, there might be problems elsewhere in your network.