

BiGuard VPN Client

QIG

(74xx/75xx/85xx series VPN enabled devices)

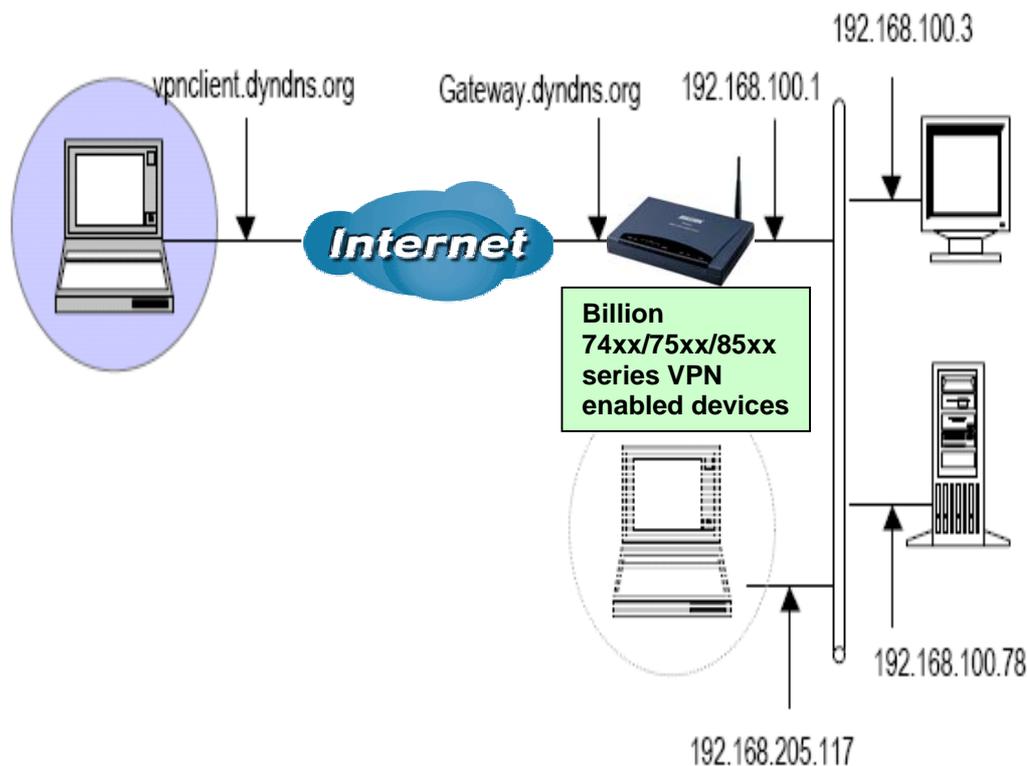
Secure access to Company Network

Your network is constantly evolving as you integrate more business applications and consolidate servers. In that environment, it is becoming extremely complex to maintain total security at the edge while users being employees or Teleworkers on the go are working with customers and partners. You need to get access to those applications and servers quickly, easily and securely.

BiGuard VPN Client is an on demand IPsec VPN Client, compliant with Billion 74xx/75xx/85xx series VPN enabled devices. Ideal for remote users and Teleworkers requiring access to the company network.

■ Network Topology

In this example, we will connect BiGuard VPN Client to the LAN behind the Billion 74xx/75xx/85xx series VPN enabled routers. The VPN Client is connected to the Internet by a DSL/dialup connection from an ISP or through a LAN. The client will have a virtual IP address in the remote LAN. All the addresses in this document are given for example purpose,



■ Billion 74xx/75xx/85xx VPN enabled devices – VPN Configuration

After connected to your Billion 74xx/75xx/85xx VPN enabled devices, you must select the menu: **【Configuration】** → **【VPN】** → **【IPSec】** .

IPSec						
VPN Tunnels						
Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal
Create 						
<input type="button" value="Apply"/>						

Click [Create](#)  and add a new IPSec VPN setting as below.

IPSec						
Create						
Connection Name	<input type="text" value="BiGuard VPN"/>					
Local						
Network	<input type="radio"/> Single Address	IP Address	<input type="text"/>			
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.100.0"/>	Netmask	<input type="text" value="255.255.255.0"/>	
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>	
Remote						
Secure Gateway Address(or Hostname)	<input type="text" value="vpnclient.dyndns.org"/>					
Network	<input checked="" type="radio"/> Single Address	IP Address	<input type="text" value="192.168.205.117"/>			
	<input type="radio"/> Subnet	IP Address	<input type="text"/>	Netmask	<input type="text"/>	
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>	
Proposal						
<input checked="" type="radio"/> ESP	Authentication	<input type="text" value="SHA1"/>				
	Encryption	<input type="text" value="AES 128"/>				
<input type="radio"/> AH	Authentication	<input type="text" value="MD5"/>				
Perfect Forward Secrecy	<input type="text" value="MODP 1024 (Group 2)"/>					
Pre-shared Key	<input type="text" value="12345678"/>					
<input type="button" value="Apply"/> Advanced Options 						

Connection Name: A user-defined name for the connection (e.g. “BiGuard VPN”).

Local:

Local Network: Set the IP address, subnet or address range of the local network.

Single Address: The IP address of the local host.

Subnet: The subnet of the local network. For example, IP: 192.168.100.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.100.1 (i.e. 192.168.100.1 through to 192.168.100.254).

IP Range: The IP address range of the local network. For example, IP: 192.168.100.1, end IP: 192.168.100.10

Remote:

Secure Gateway Address (or hostname): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel. It must be filled in with VPN Client IP address or public IP address of the router behind which the VPN Client is (“vpnclient.dyndns.org” in our example).

Network: Set the IP address, subnet or address range of the remote network. In our example, you must add a virtual IP address (192.168.205.117) for the VPN Client.

Proposal:

Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

⊙ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.

⊙ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

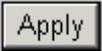
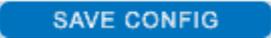
⊙ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

⊙ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

⊙ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key (“12345678” in our example). IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Select the  to submit the setting then click the  to save the settings into flash.



After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them being lost after turning off or resetting your router.

■ Billion 74xx/75xx/85xx VPN enabled devices – IKE Settings

Once **VPN Configuration** done, click on [Advanced Options](#) . In this page, you can define a Phase 1 Identity for the BiGuard VPN Client.

IPSec		
IKE Mode	Main 	
IKE Proposal		
Hash Function	SHA1 	
Encryption	3DES 	
Diffie-Hellman Group	MODP 1024 (Group 2) 	
Local ID		
Type	Default 	
Content	<input type="text"/>	
Remote ID		
Type	USER_FQDN;E-mail (User FQDN) 	
Identifier	<input type="text" value="support@billion.com"/>	
SA Lifetime		
Phase 1 (IKE)	<input type="text" value="240"/>	minutes
Phase 2 (IPSec)	<input type="text" value="60"/>	minutes
PING for keepalive		
PING to the IP	<input type="text" value="0.0.0.0"/>	(0.0.0.0 means NEVER)
Interval	<input type="text" value="10"/>	seconds (0-3600, 0 means NEVER)
Disconnection Time after no traffic	<input type="text" value="1200"/>	seconds (180 at least)
Reconnection Time	<input type="text" value="15"/>	minutes (3 at least)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

IKE (Internet Key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

IKE Proposal:

Hash Function: It is a Message Digest algorithm which converts any length of a message into a unique set of bits. It is widely used MD5 (Message Digest) and SHA1 (Secure Hash Algorithm).

SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- ⦿ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ⦿ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128,192 and 256 bits)**. 3DES and AES are more powerful but increase latency.

- ⊙ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ⊙ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ⊙ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Local ID:

- ⊙ **Type:** Specify local ID type.
- ⊙ **Content:** Input ID's information, like domain name www.ipsectest.com.

Remote ID:

- ⊙ **Type:** Specify Remote ID type ("E-mail (User QFDN)" in our example).
- ⊙ **Identifier:** Input remote ID's information ("support@billion.com" in our example).

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 240 minutes.

Phase 2 (IPSec): To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keepalive: It is used to detect IPSec tunnel connection failure. Connection failure is defined as abort or in NO response state. In such event Ping to Keepalive takes proper action to ensure the connection quality of IPSec.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Re-establish of this connection is required. Default setting is 0.0.0.0 which disables the function.

Internal: This sets the time interval between **PING to the IP** function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 seconds, 0 second disables the function.

Ping to the IP	Internal (sec)	Ping to the IP Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after to traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the **Reconnection Time** set. Default setting is **1200 seconds**; **180 seconds** is minimum time interval for this function.

Reconnection Time: It is the reconnection time interval after NO Traffic is initiated. Default setting is **15 minutes**; **3 minutes** is minimum time interval for this function.

Select the to save the setting.

■ Billion 74xx/75xx/85xx VPN enabled devices – Enable new IPSec VPN Tunnels

IPSec

VPN Tunnels

Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal		
<input checked="" type="radio"/>	<input type="radio"/>	BiGuard VPN	192.168.100.0 /255.255.255.0	192.168.205.117	vpnclient.dyndns.org	AH:none ESP:sha1,aes_128_cbc	Edit	Delete

[Create](#)

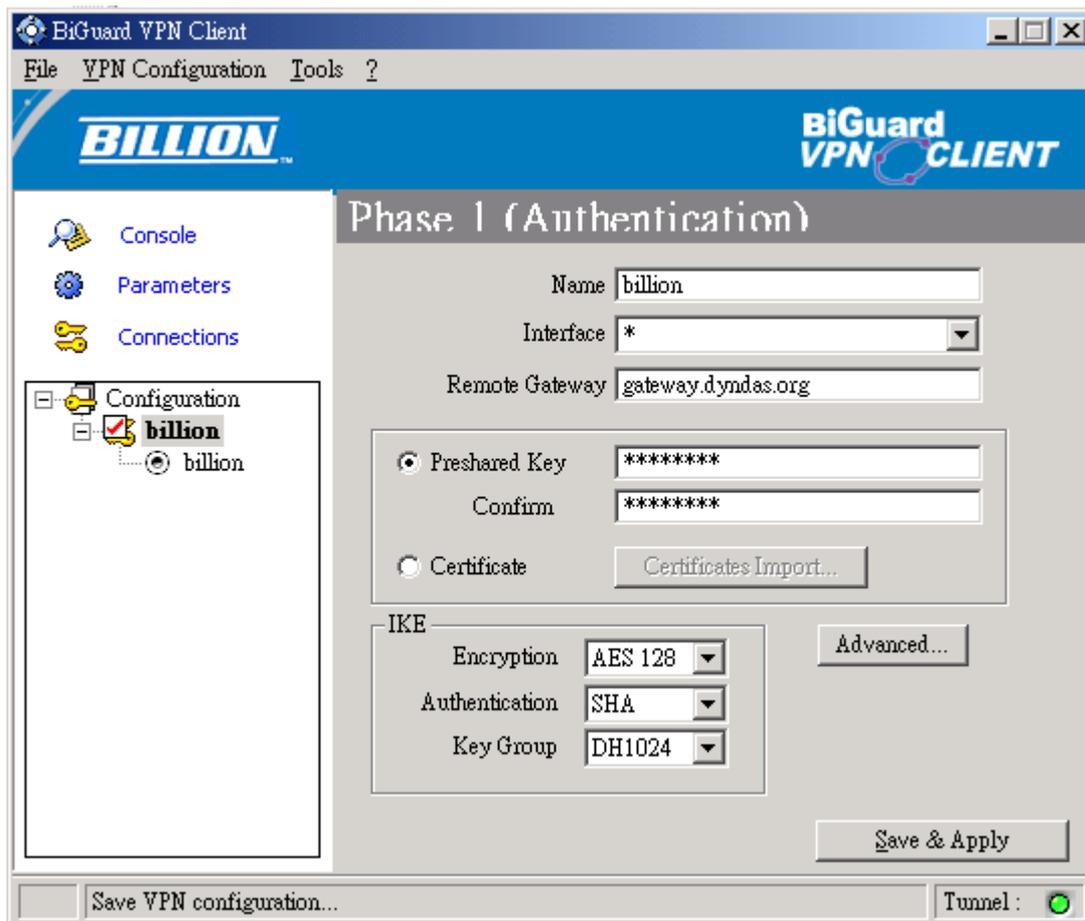
You have to select “Enable” and click on if you want to use this tunnel.

■ BiGuard VPN Client Configuration – Phase 1 Configuration

“Authentication” or “Phase 1” window will concern settings for Authentication Phase or Phase 1. It is also called IKE Negotiation Phase.

Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

You need use for the BiGuard VPN Client settings defined in Billion 74xx/75xx/85xx VPN enabled devices VPN configuration.



Name: Label for Authentication phase used only the configuration user interface. This value is never used during IKE negotiation. It is possible to change this name at any time and read it in the tree control. Two Phase 1 can not have the same name (“billion” in our example).

Interface: IP address of the network interface of the computer, through which VPN connection is established. If the IP address may change (when it is received dynamically by an ISP), select “*”.

Remote Gateway: IP address or DNS address of the remote router (in our example: gateway.dyndns.com). This field is mandatory.

Pre-shared key: Password or key shared with the remote router (“12345678” in our example).

Certificate (Please see the Appendix A): X509 certificate used by the VPN client (Please see the “Certificate Management” of on-line manual for detailed instructions).

IKE encryption: Encryption algorithm used during Authentication phase (3DES, AES, ...).

IKE authentication: Authentication algorithm used during Authentication phase (MD5, SHA, ...).

IKE key group: Diffie-Hellman key length.

You must also add phase 1 IDs in “Advanced Configuration” window, if the BiGuard VPN Client from a LAN.

The screenshot shows the 'Advanced Configuration' dialog box. It includes the following fields and options:

- Aggressive Mode
- IKE Port: []
- X-AUTH:
 - X-Auth popup
 - Login: []
 - Password: []
- Local ID:
 - Value: support@billion.com
 - Type: Email
- Remote ID:
 - Value: []
 - Type: []

Buttons: Ok, Cancel

Aggressive Mode: If checked, the VPN client will use aggressive mode as negotiation mode with the remote router.

IKE port: Negotiation port for IKE. Default value is 500.

Local ID: Local ID is the identity the BiGuard VPN client is sending during Phase 1 to VPN gateway. This identity can be:

- an IP address (type = IP address);
- an domain name (type = DNS);
- an email address (type = Email)(support@billion.com in our example)
- a string (type = KEY ID);
- a certificate issuer (type=DER ASN1 DN) (About X509 certificates, please see Appendix A) If this identity is not set, VPN client's IP address is used.

Remote ID: Remote ID is the identity the BiGuard VPN client is expecting to receive during Phase 1 from the VPN router. This identity can be:

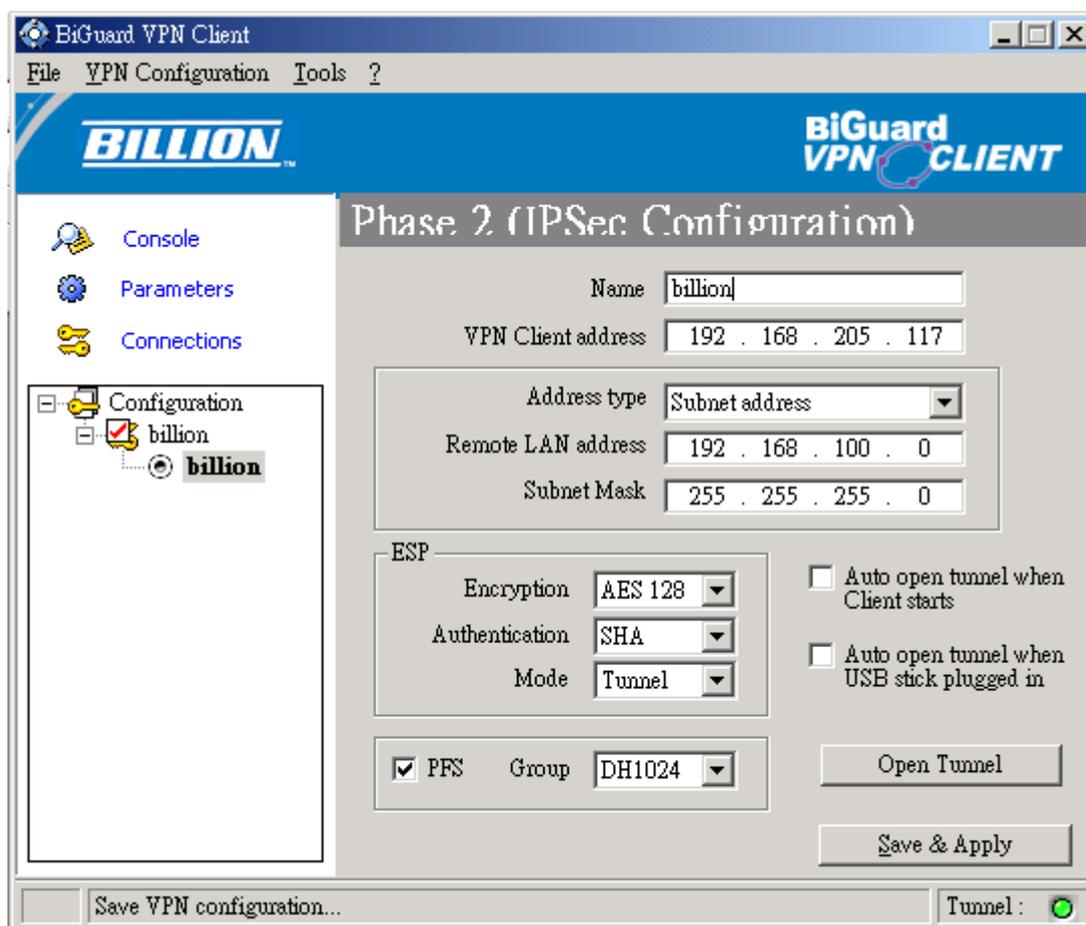
- an IP address (type = IP address);
- an domain name (type = DNS);
- an email address (type = Email);
- a string (type = KEY ID);
- a certificate issuer (type=DER ASN1 DN) (About X509 certificates, please see Appendix A) If this identity is not set, VPN gateway's IP address is used.

X-Auth(Please see the Appendix A): Here are specified the login and password of an X-AUTH IPsec negotiation.

■ BiGuard VPN Client Configuration – Phase 2 Configuration

“IPSec Configuration” or “Phase 2” window will concern settings for Phase 2.

The purpose of Phase 2 is to negotiate the IPSec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.



Name: Label for IPSec Configuration only used by the VPN client. This parameter is never transmitted during IPSec Negotiation. It is possible to change this name at any time and read it in the tree list window. Two Phases can not have the same name (“billion” in our example).

VPN Client address: Virtual IP address used by the client inside the remote LAN: The computer will appear in the LAN with this IP address (“192.168.205.117” in our example). It is important this IP address not to belong to the remote LAN.

Address type: The remote endpoint may be a LAN or a single computer. In the first case choose “Subnet address”. Choose “Single address” otherwise. When choosing “Subnet address”, the two fields “Remote LAN address” and “Subnet mask” became available. When choosing “Single address”, only the field “Remote host address” is available.

Remote address: This field may be “Remote host address” or “Remote LAN address” depending of the address type. It is the remote IP address, or LAN network address of the gateway, that opens the VPN tunnel.

Subnet mask: Subnet mask of the remote LAN. Only available when address type is equal to “Subnet address”.

ESP encryption: Encryption algorithm negotiated during IPSec phase (3DES, AES, ...).

ESP authentication: Authentication algorithm negotiated during IPSec phase (MD5, SHA, ...).

ESP mode: IPSec encapsulation mode : tunnel.

PFS group: Diffie-Hellman key length.

Auto open when Client starts: If checked, this option allows a tunnel to be automatically opened when the VPN Client starts.

Auto open when USB Stick plugged in: If checked, this option allows a tunnel to be automatically opened when a USB Stick is inserted (Please see the “USB Mode” of on-line manual for detailed instructions).

Open Tunnel: This button allows opening directly the tunnel without using a ping for example.

■ Open IPSec VPN Tunnels

Once both Billion 74xx/75xx/85xx VPN enabled devices and BiGuard VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enabled your firewall with IPSec traffic.

1. Click on  to make into account all modifications we've made on your VPN Client Configuration.
2. Click on , or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser).
3. Select  [Connections](#) to see opened VPN Tunnels.
4. Select  [Console](#) if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging.

■ Appendix A – Compatible table of Billion 74xx/75xx/85xx VPN enabled devices & BiGuard VPN Client

	BIPAC 74xx series	BIPAC 75xx series	BIPAC 85xx series
Hash algorithms			
MD5	v	v	v
SHA1	v	v	v
Encryption			
DES	v	v	v
3DES	v	v	v
AES 128	v	v	v
AES 192	v	v	v
AES 256	v	v	v
Diffie Hellman Group Support			
Group1: MODP 768	v	v	v
Group2: MODP 1024	v	v	v
Group5: MODP 1536	v	v	v
Authentication Mechanism			
Preshared key	v	v	v
X509 Certificate support (PEM)	x	x	x
X-Auth	x	x	x
Key Management			
ISAKMP (RFC2408)	v	v	v
IKE (RFC2409)	v	v	v
IPSec Mode			
ESP	v	v	v
Tunnel	v	v	v
IKE Mode			
Main	v	v	v
Aggressive	v	v	v
Quick	v	v	v

x = not support