BILLION™

BiGuard VPN Client

QIG

(BiGuard series VPN enabled devices)

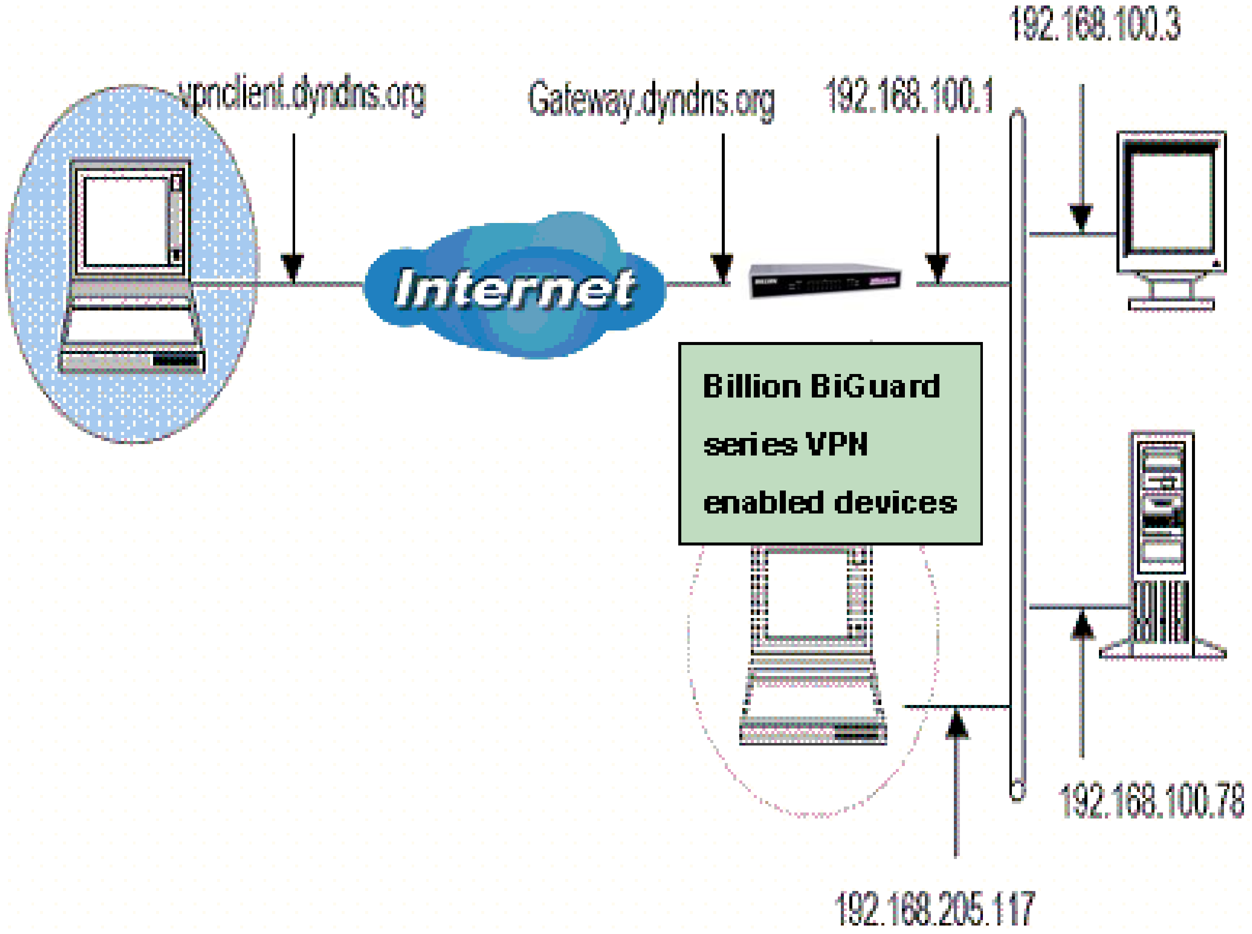
Secure access to Company Network

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 BiGuard series VPN enabled devices. Ideal for remote users and Teleworkers requiring access to the company network.

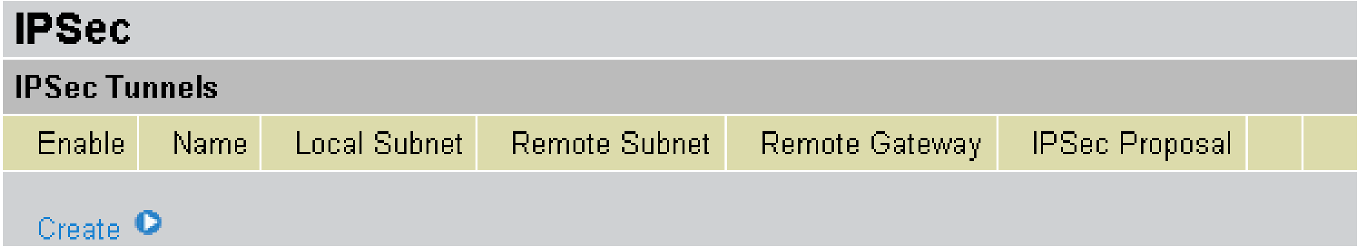
Network Topology

In this example, we will connect BiGuard VPN Client to the LAN behind the Billion BiGuard 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 addressed in this document are given for example purpose,



Billion BiGuard VPN enabled devices – VPN Configuration

After connected to your Billion BiGuard VPN enabled devices, you must select the menu: 【Configuration】→ 【IPSec】.



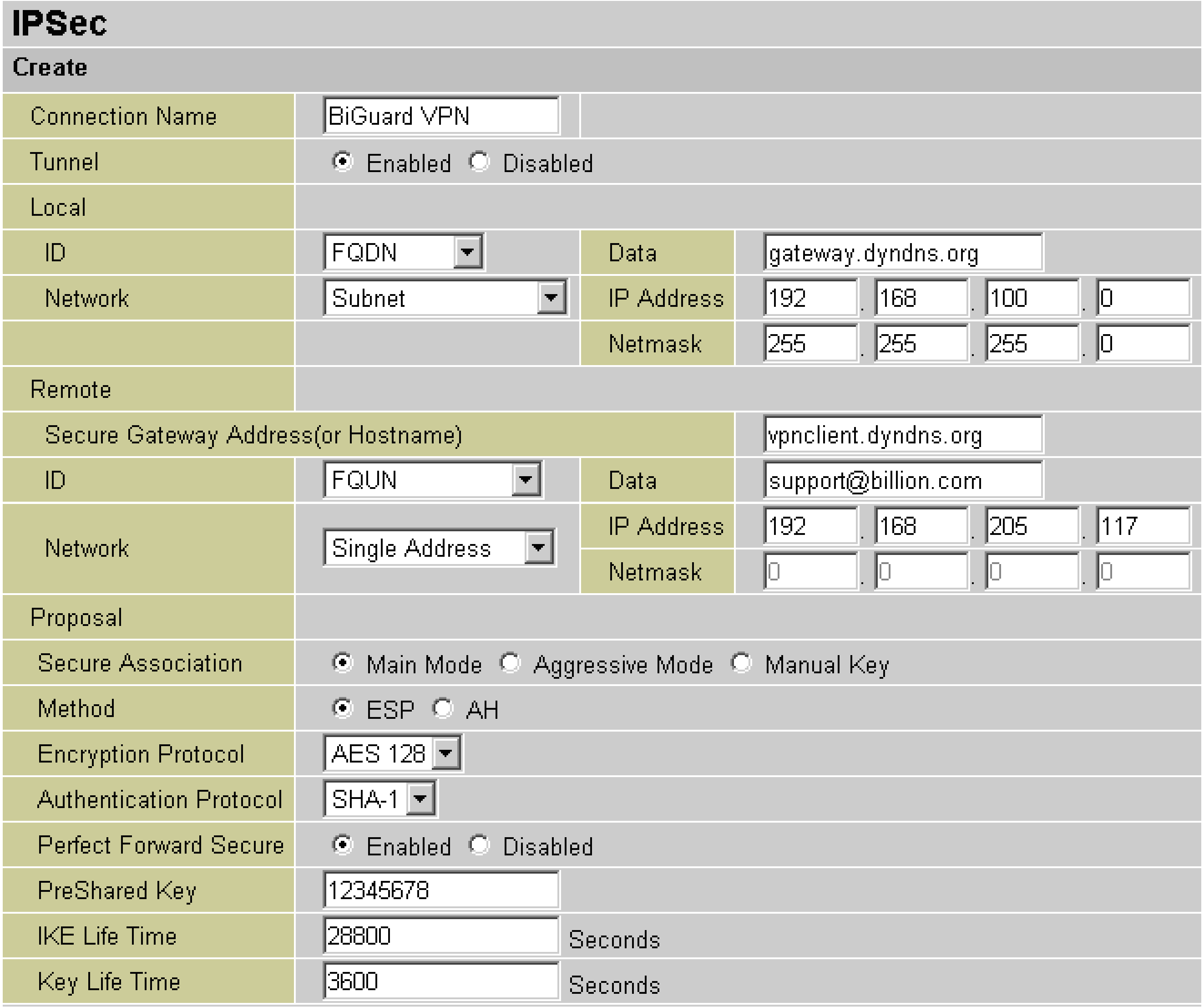
IPSec

IPSec Tunnels

Enable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal		

Create

Click Create and add a new IPSec VPN setting as below.



IPSec

Create

Connection Name	BiGuard VPN		
Tunnel	● Enabled ○ Disabled		
Local			
ID	FQDN	Data	gateway.dyndns.org
Network	Subnet	IP Address	192 . 168 . 100 . 0
		Netmask	255 . 255 . 255 . 0
Remote			
Secure Gateway Address(or Hostname)			vpnclient.dyndns.org
ID	FQUN	Data	support@billion.com
Network	Single Address	IP Address	192 . 168 . 205 . 117
		Netmask	0 . 0 . 0 . 0
Proposal			
Secure Association	● Main Mode ○ Aggressive Mode ○ Manual Key		
Method	● ESP ○ AH		
Encryption Protocol	AES 128		
Authentication Protocol	SHA-1		
Perfect Forward Secure	● Enabled ○ Disabled		
PreShared Key	12345678		
IKE Life Time	28800	Seconds	
Key Life Time	3600	Seconds	

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

Tunnel: Activates or deactivates the IPSec connection

Local:

ID: Select local ID type

Data: Input ID's information, like domain name www.ipsectest.com.

Network: Set the Any local address, subnet or single address of the local network.

⊙**Any Local Address:** All IP address of the local network

⊙ **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).

⊙ **Single Address:** The IP address of the local host.

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).

ID: Select remote ID type

Data: Input ID's information, like domain name www.ipsectest.com.

Network: Set the IP address, subnet or address range of the remote network. In our example, you must add FQDN (vpnclient.dyndns.org) for the VPN Client.

Proposal:

Secure Association: (SA) is a method of establishing a security policy between two points. There are three methods of creating a Secure Association, each varying in degrees of security and speed of negotiation.

⊙ **Main Mode:** Uses the automated Internet Key Exchange (IKE) setup; most secure method with the highest level of security.

⊙ **Aggressive Mode:** Uses the automated Internet Key Exchange (IKE) setup; mid-level security. Speed is faster than Main mode.

⊙ **Manual Key:** Manual; standard level of security. It is the fastest of the three methods.

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.

Encryption: Select the encryption method from the pull-down menu. There are several options, DES, 3DESand AES (128, 192 and 256). 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.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are two options, Message Digest 5 (**MD5**), and Secure Hash Algorithm (**SHA1**). 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.

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 two modes, MODP 768-bit, and MODP 1024-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol. Both sides should use the same key. 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).

IKE Life Time: Allows you to specify the timer interval for renegotiation of the IKE security association. The value is in seconds, eg. 28800 seconds = 8 hours.

Key Life: Allows you to specify the timer interval for renegotiation of another key. The value is in seconds eg. 3600 seconds = 1 hour.

Select the [Apply] to submit the setting then click the [SAVE CONFIG] to save the settings into flash.

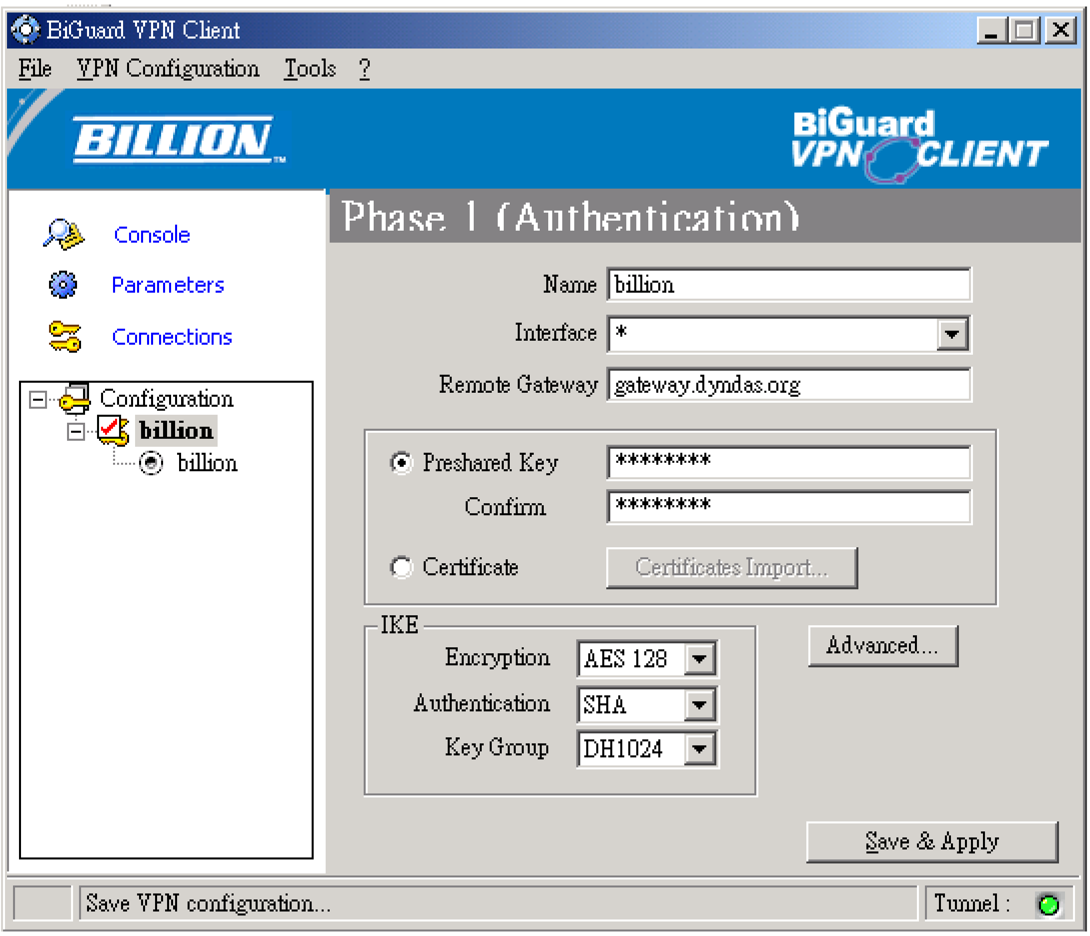
NOTE: After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them being lost after turning off or resetting your router.

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 BiGuard series VPN enabled devices VPN configuration.



Name: billion

Interface: *

Remote Gateway: gateway.dyndas.org

Preshared Key: ********

Confirm: ********

Encryption: AES 128

Authentication: SHA

Key Group: DH1024

Save 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 "*".

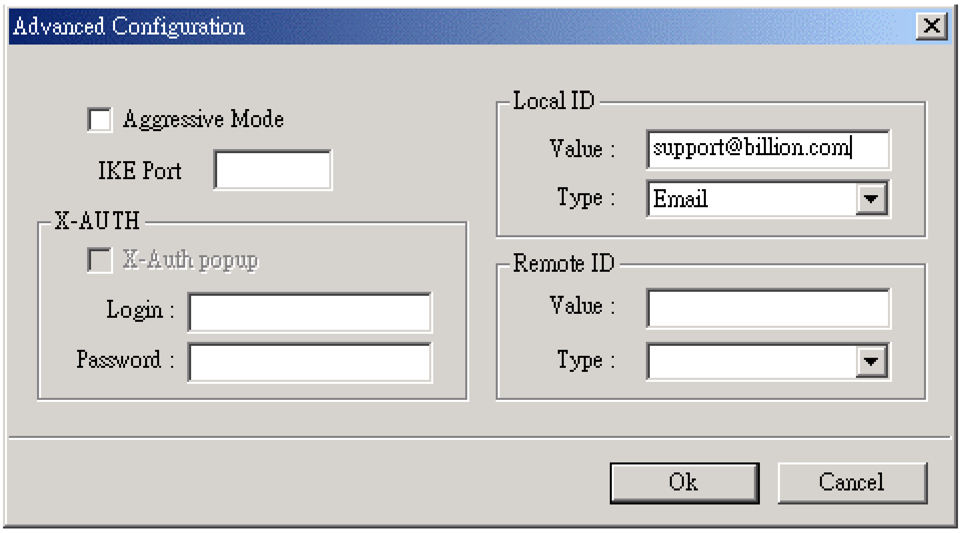
Remote Gateway: IP address or DNS address of the remote router (in our example: gateway.dyndns.com). This field is mandatory.

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 (see certificate configuration).

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.



Local ID

Value : support@billion.com

Type : Email

Aggressive Mode: If checked, the VPN client will used 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 domaine 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.

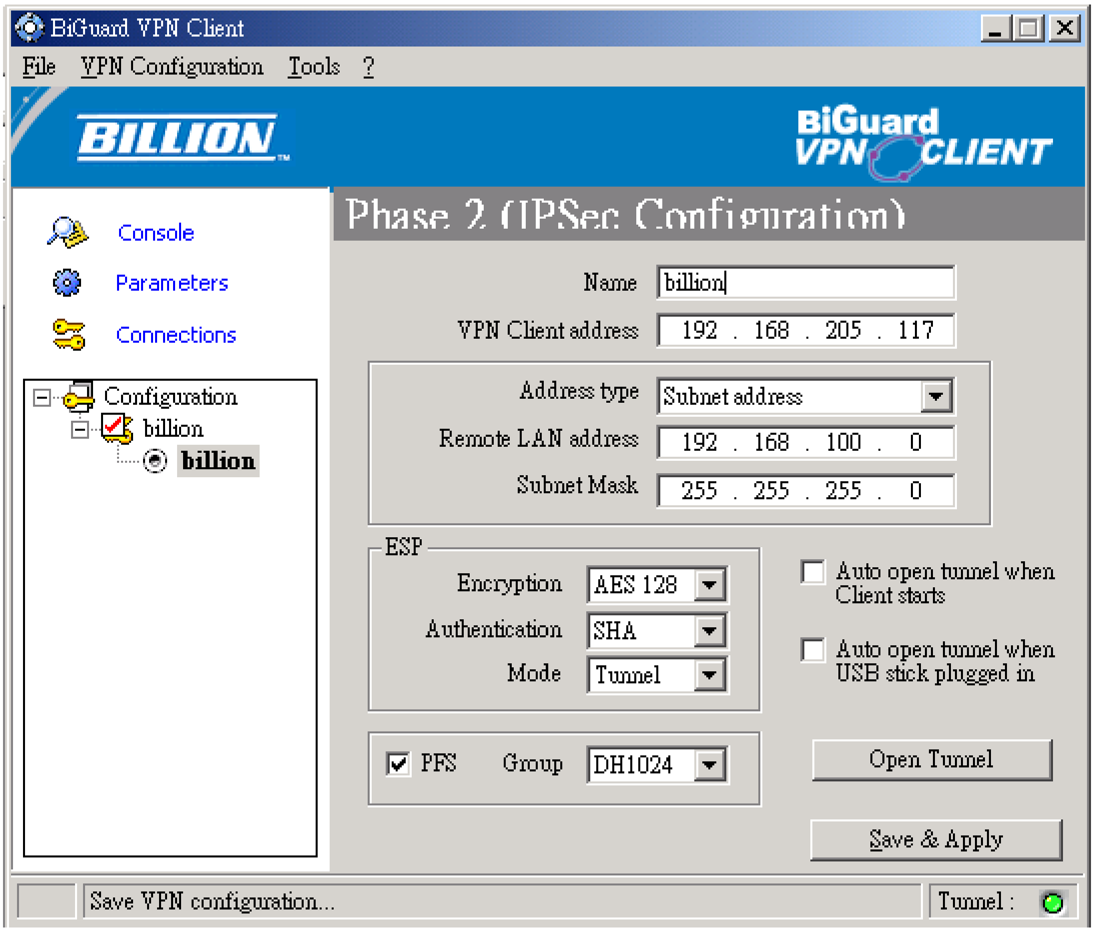
Remote ID: Remote ID is the identity the BiGuard VPN client is expecting to receive during Phase 1 from the VPN router. This identity can be: an IP address (type = IP address);
an domaine name (type = DNS);
an email address (type = Email);
a string (type = KEY ID);
a certificate issuer (type=DER ASN1 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 thought tunnels negotiated during Phase 1.



Phase 2 (IPSec Configuration)

Name: billion

VPN Client address: 192 . 168 . 205 . 117

Address type: Subnet address

Remote LAN address: 192 . 168 . 100 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: AES 128

Authentication: SHA

Mode: Tunnel

☐ Auto open tunnel when Client starts

☐ Auto open tunnel when USB stick plugged in

☑ PFS Group: DH1024

Save VPN configuration...

Tunnel : ●

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 negociated during IPSec phase (3DES, AES, ...).

ESP authentication: Authentication algorithm negociated 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. Note: as the VPN Client may also start during the boot (see section VPN Tools), tunnels can be configured to be opened automatically during the boot of the computer.

Auto open when USB Stick plugged in: If checked, this option allows a tunnel to be automatically opened when a USB Stick is inserted (see section "USB Mode").

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

Open IPSec VPN Tunnels

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

1. Clink on Save & Apply to make into account all modifications we've made on your VPN Client Configuration.
2. Click on Open Tunnel, 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 BiGuard VPN enabled devices & BiGuard VPN Client

	BiGuard 2	BiGuard 10	BiGuard 30
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	x	x	x
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