VPN Settings

The following sections provide more details on the VPN server settings:

General Settings

From the **General Settings** tab of the **Server Settings** window, you can configure the following settings:

Section	Setting	Description
Access Control Service	**IP Addresses**	The IP address of the access control service to use.
	Sync Authentication to Trustzone	Propagates authentication information to the other systems in the same trustzone.

Server Configuration	**Use port 443** [default: **Yes**]	Defines whether incoming VPN connections on port 443 should be accepted. VPN tunnels connecting to this port are limited to the TCP transport protocol. Port 443 can only be used by one service. If this port is redirected to another machine by the firewall service or an SSL VPN is running, disable port 443 for client-to-site VPN connections.
	CRL Poll Time	The time interval in minutes for fetching the Certificate Revocation List. Entering `0` results in a poll time of 15 minutes.
	Global TOS Copy	Enables the Type of Service (ToS) flag for site-to-site tunnels. By default, the ToS flag is globally disabled (setting: *Off*). Individual tunnel ToS policies override the global policy settings.
	Global Replay Window Size [0]	If ToS policies assigned to VPN tunnels or transport packets are not forwarded instantly according to their sequence number, you can configure the replay window size for sequence integrity assurance to avoid IP packet "replaying." The window size specifies a maximum number of IP packets that can be on hold until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. Individual window size settings are configurable per tunnel and transport, overriding global policy settings. To specify that tunnel and transport settings should be used, enter *0* (default). To view the specified replay window size, double-click the tunnel on the **VPN** page to open the **Transport Details** window (attribute: transport_replayWindow).
	Use Site to Site Tunnels for Authentication [Yes]	Typically, a tunnel registers itself at the firewall, creating an auth.db entry with the tunnel network and the tunnel credentials. You can then create a firewall rule with the tunnel name or credentials as a condition. This feature is rarely, if ever, used.
	Pending Session Limitation [Yes]	Enforces a limit of five sessions. Additional session requests are dropped.
	Prebuild Cookies on Startup [No]	Prebuilds the cookies when the VPN service is started. This can slow the VPN service startup but increases the speed of tunnel builds. Typically, cookies are built on demand while a VPN tunnel is initiated. Enable this setting to prevent high system load on F-Series Firewalls that are concentrating a large number of VPN tunnels. High system load caused by the VPN service can occur if a large number of VPN tunnels are established simultaneously after a reboot or Internet Service Provider outage.
	Tunnel HA Sync	Synchronization is provided only for TINA tunnels and transports using either UDP or ESP. Synchronization of hybrid, TCP, or IPsec tunnels is not available. During an HA takeover, the initialization of all VPN tunnels and transports requires a very CPU-intensive RSA handshake procedure. As long as less than approximately 200 tunnels and transports are terminated, this initialization happens very quickly and does not decrease overall system performance. Due to real-time synchronization to the HA partner unit, the system load during a takeover can be decreased, providing faster tunnel re-establishment. By default, this setting is disabled. It can be activated using **Tunnel HA Sync** through the VPN server settings. Barracuda Networks recommends that you only activate this setting when using more than 200 ESP or UDP TINA tunnels.
	Maximum Number of Tunnels	The maximum number of concurrent client-to-site and site-to-site tunnels accepted by the VPN service. Leave the default setting **<auto>**, or select one of the values available from the drop-down list. Barracuda NextGen Firewall F10, F100, F101, F200, F201, F300, and F301 are limited to 256 VPN tunnels.
	Allow Fast Requests	Allows a fast request rate.
	Handshake Timeout (sec)	Set the time in seconds until a handshake request times out.
	Allow Dynamic Mesh	Enable Dynamic Mesh for this VPN service. For more information, see Dynamic Mesh VPN Networks.
	Add VPN Routes to Main Routing Table (Single Routing Table)	Add the routes for published VPN networks to the main routing table with a metric of 10. For more information, see Authentication, Encryption, Transport, IP Version and VPN Routing.
	Allow Concurrent User Sessions	Allow a user to connect multiple times via client-to-site VPN. An Advanced Remote Access subscription is required. For more information, see Licensing.
	Use Perfect Forward Secrecy	Enable perfect forward secrecy and elliptic curve cryptography for TINA site-to-site VPN tunnels. For more information, see Authentication, Encryption, Transport, IP Version and VPN Routing.
	Accounting Information Storage Time (Days)	Stores information on client-to-site connections and site-to-site VPN tunnels using the TINA VPN protocol in the **/your_virtual_server/VPNservice/VPN** log file. For client-to-site VPN connections both the login and logout are logged. To disable this feature, set to `0`. This information is also used by the Report Creator. For more information, see Barracuda Report Creator. **Example login log entry:** Session PGRP-AUTH-user1-b607769a27fdf6e: Accounting LOGIN - user=user1 IP=REMOTE_IP start="2016/05/27 15:00:00" **Example logout log entry:** Session PGRP-AUTH-user1-b607769a27fdf6e: Accounting LOGOUT - user=user1 IP=REMOTE_IP start="2016/05/27 15:00:00" duration=0:03:36 inBytes=0 outBytes=0 lastOS="Android 6.0" lastClient="Android 2.0.1"

Default Server Certificate Section	**Subject/Issuer**	These two fields display the certificate subject and issuer. Note that L2TP and IPsec require server certificates with SubAltName: DNS:your.vpnserver.com
	Default Key	If the VPN server demands a key but the key is not stated explicitly, you can generate it by clicking **Ex/Import** and selecting a suitable option.

For a successful client-to-site connection, you must define a default server certificate.

Advanced Settings

From the **Advanced Settings** tab of the **Server Settings** window, you can configure these settings:

Section	Description
VPN Interface Configuration | VPN Next Hop Interface Configuration	In these sections, configure the VPN interfaces and next hop interfaces. To add and configure virtual interfaces equipped with unique index numbers, click **Add**. VPN next hop interfaces are required for routed VPN, BGP and OSPF over VPN configurations. After assigning the interface with a local IP address, it may be directly used within the OSPF or BGP router configuration. The interfaces are active and visible on the **Control > Network** page as soon as the IP address of the interface has been introduced as a virtual server IP address. Next Hop VPN Interfaces are labeled as follows: *vpnr[INDEX]* In the **VPN Interface Properties** window, edit the following settings for each interface: • **VPN Interface Index** – The unique index number of the VPN interface. • **MTU** – The Maximum Transmission Unit size. You can enter values between 1398 and 4000. • **IP Addresses** – The IP addresses that should be started on the *vpnX* interface. You can enter a space-delimited list of IP addresses. • **Multicast Addresses** – The multicast addresses that should be propagated into this field. You can enter a space-delimited list of IP addresses. For example, to transport OSPF multicast via the VPN tunnel, enter `224.0.0.5 224.0.0.6`
IKE Parameters	In this section, configure the global IKE settings for all configured IPsec tunnels. You can edit the following settings: • **Exchange Timeout (s)** – The maximum period to wait until the request for IPsec tunnel connection establishment has to be approved by the remote peer (default: *30* seconds). • **Tunnel Check Interval (s)** – The interval between queries for a valid exchange that is assignable to an IPsec tunnel (default: *5* seconds). If a tunnel that is configured with direction assignment *Active* has been terminated, it will be re-established automatically when the check interval expires. If a tunnel that is configured with direction assignment *Passive* has been terminated, a corresponding status message is triggered and the interface is updated on the **VPN** page. • **Dead Peer Detection Interval (s)** – The interval between keep-alive checks on the remote peer (default: 5 seconds). • **Use IPSec dynamic IP** – If the service is connected to the Internet via a dynamic link (dynamic IP address), select *Yes*. The server IP address is not yet known at configuration time and IKE then listens to all local IP addresses. • **IPSec Log Level** – The debug log level of IKE. The debug log may be very “noisy.” Do not select a log level greater than *0* if the log is not required for solving an issue.
Custom Ciphers	In this section, add or remove custom ciphers.