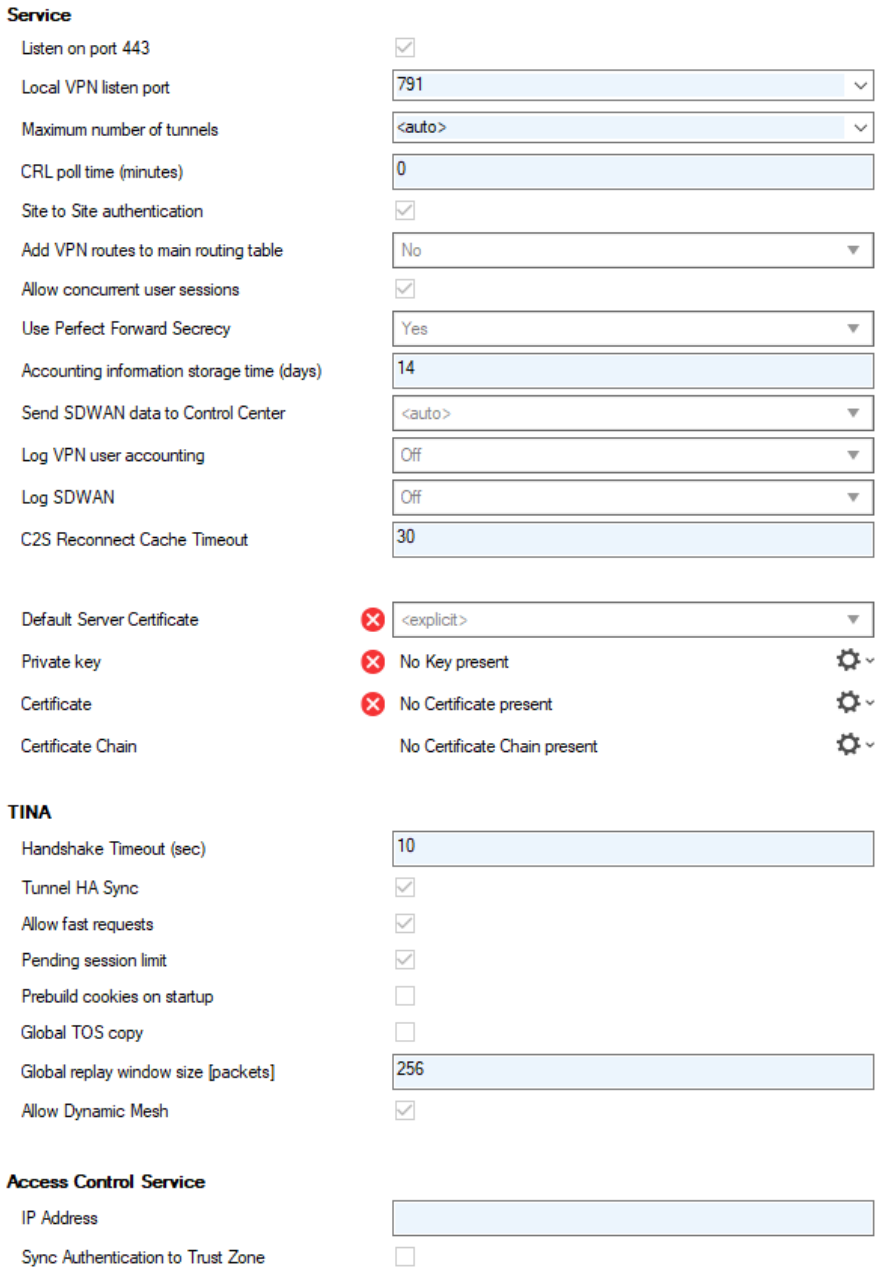
General Settings

https://campus.barracuda.com/doc/96026076/

Navigate to the following window on path **CONFIGURATION > Configuration Tree > your box > Assigned Services > VPN Service > VPN Settings > General**.



The VPN service relies on several settings necessary for operation. The parameters are grouped into the following subsections:

Service

Setting	Value(s) *=default	Description
Listen on port 443	Deactivated	The TCP tunnel transport usually uses TCP connections on port 691, the default. However, if a connection is necessary through SOCKS4 or HTTP proxies, port 443 can be used as an alternative. Port 443 can be used only by one service. If this port is redirected to another machine by the firewall service or if an SSL VPN is running, disable port 443 for client-to-site VPN connections.
Local VPN listen port		TCP tunnel transports use port 691 as default. If you want to use a different port number, you must enter it in this field.
Maximum number of tunnels	***Auto** 1 64 512 2048 8192	This value sets the maximum number of concurrent client-to-site and site-to-site tunnels accepted by the VPN service.
CRL poll time [min.]	0	The time interval in minutes for fetching the Certificate Revocation List. Entering 0 results in a poll time of 15 minutes.
Site to Site authentication	Selected Deselected	Typically, a tunnel registers itself at the firewall by creating an *auth.db* entry with the tunnel network and the tunnel credentials. You can then create an access rule with the tunnel name or credentials as a condition. This feature is rarely used.
Add VPN routes to main routing table	Selected Deselected	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	Selected Deselected	Allow a user to connect multiple times via client-to-site VPN. An Advanced Remote Access subscription is required.
Use Perfect Forward Secrecy	Enforced Yes No	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]	14	Stores information on client-to-site connections and site-to-site VPN tunnels using the TINA VPN protocol in the **/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"
Send SDWAN data to Control Center	Yes Auto No	Defines how SD-WAN data is propagated to the Control Center.
Log VPN user accounting	On Off	If set to On, this option creates a log entry for every user log-in and log-off for a client-to-site connection.
Log SDWAN	On Off	If set to On, the firewall stores the Min/Avg/Max value of the throughput rate every 5 minutes.
Default Server Certificate	Selected Deselected	Select the check box to use self-signed certificates.
Private Key	- -	Click the "add" icon to create a new private key. Click the blue "up arrow" icon to clear, import, or export the certificate.
Certificate	- -	Click the "certificate" icon to edit the current certificate. Click the "pen" icon to clear, import, or export the certificate.
Certificate Chain	-	Enter a chain of server certificates if necessary.

TINA

Setting	Value(s) *=default	Description
Handshake Timeout [sec]	10	Set the time in seconds until a handshake request times out.
Tunnel HA Sync		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.
Pending session limit	Selected Deselected	Enforces a limit of five sessions. Additional session requests are dropped.

Prebuild cookies on startup		Pre-builds 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 CloudGen 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.
Global TOS copy	Selected ***Deselected**	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 global policy settings.
Global replay window size [packets]	256	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).
Allow Dynamic Mesh	Selected Deselected	Enable Dynamic Mesh for this VPN service. For more information, see Dynamic Mesh VPN Networks.

Acccess Control Service

Setting	Value(s) *=default	Description
IP Address		The IP address of the Access Control Service.
Sync Authentication Trust Zone	Selected Deselected	If activated, propagates authentication information to systems in the same trustzone.

Figures

1. vpn_settings_general.png