

03. Initial Setup

After installing PUQVPNC, follow these steps to configure the server for production use.

Step 1: Activate the License

1. Navigate to **Settings > License**
2. Enter your license key
3. Click **Save**

PUQVPNC

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

License

License Information

License Active

License KeyV1LQBS-XXXXXX-XXXXXX-XXXXXX-RYZDHL

StatusActive

Expiration DateJuly 6, 2027484 days left

VPN Client Slots5000

Last CheckedMar 10, 2026 01:20 PM

Usage

VPN Clients1828 / 5050

36%

Networks26

Active Clients1828

Available Slots3222

Total Capacity5050 (50 free + 5000 licensed)

About

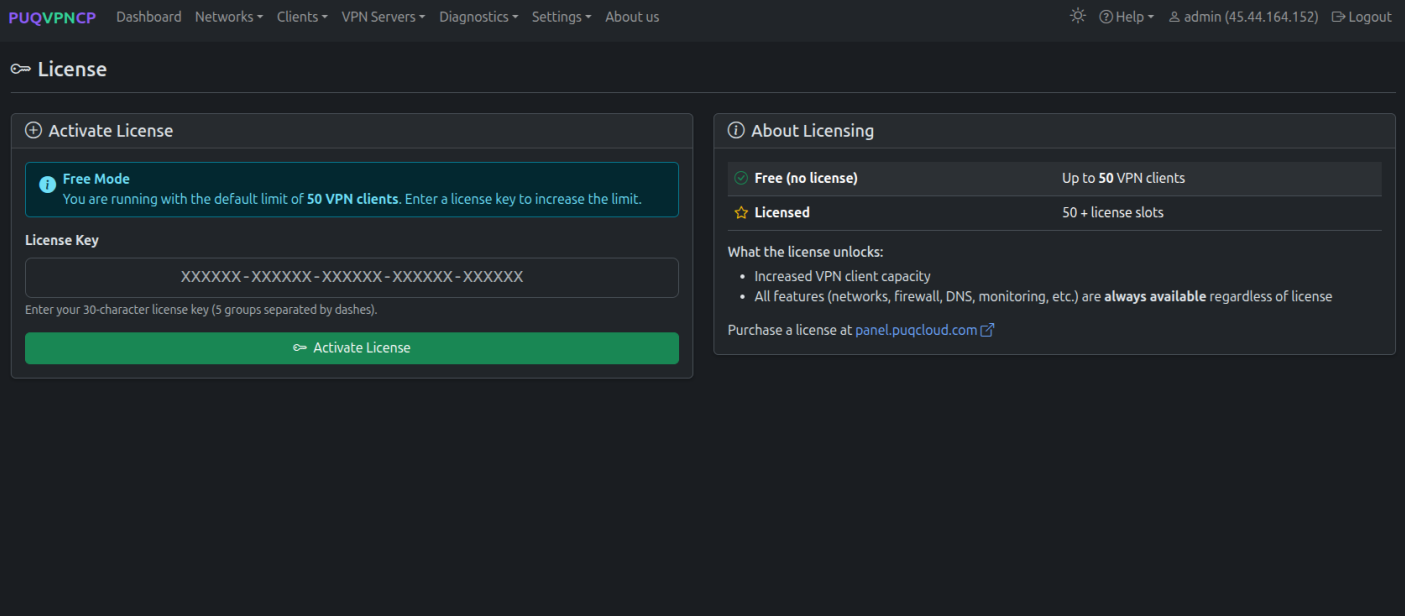
The license controls the maximum number of VPN clients you can create. Without a license, the default limit is 50 clients.

The license is verified with the PUQ license server every 24 hours. You can manually re-check using the button above.

To purchase or renew a license, visit puqcloud.com/puqvpnc.php

License page — enter your license key

After activation, the license status will show **Valid** with the expiration date.



License activated successfully

“ Purchase a license: <https://puqcloud.com/store/puqvpncp>

Step 2: System Configuration

Navigate to **Settings** > **System** to configure the core settings.

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

System Configuration

General

Traffic collection (min)

1

Traffic history (months)

2

0 = do not collect

Max bandwidth (Mbit/s)

10000

WG handshake uptime (s)

180

Offline after last handshake

VPN

VPN Domain

dev.puqvpncp.com

Domain name used in VPN client configs (WireGuard Endpoint, OpenVPN remote, IKEv2 defaults). When set, clients connect via domain instead of IP address, so changing the server IP does not require reconfiguring clients.

Security

Redirect URL

https://puqcloud.com/

For non-AllowedWebIP clients

Max login attempts

5

0 = disabled

Lockout time (min)

15

robots.txt

User-agent: *
Disallow: /

Panel

Panel title

PUQVPNCP

Default theme

Auto (system)

Maintenance mode

☒ Block all pages except login

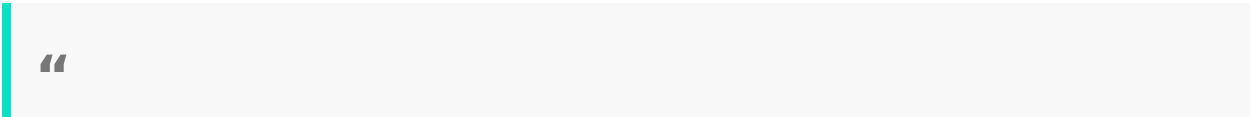
System configuration page

General Settings

Setting	Description	Default
Traffic collection (min)	How often traffic counters are read from iptables	1
Traffic history (months)	How long traffic data is retained	2
Max bandwidth (Mbit/s)	Global server bandwidth limit for TC	10000
WG handshake uptime (s)	Client considered offline after this many seconds without a WireGuard handshake	180
AWG handshake uptime (s)	Client considered offline after this many seconds without an AmneziaWG handshake	180

VPN Domain

Set the **VPN Domain** field (e.g., `vpn.example.com`) to use a domain name instead of IP in client configurations. This way, if you change your server IP, clients will not need to be reconfigured.



Tip: Point your domain's A record to the server IP before setting this field.

Security

Setting	Description
Redirect URL	URL to redirect unauthorized web access attempts
Max login attempts	Lock the account after N failed attempts (0 = disabled)
Lockout time (min)	How long the account is locked
robots.txt	Content for <code>/robots.txt</code> (blocks search engines by default)

Panel

Setting	Description
Panel title	Browser tab title
Default theme	Auto (system) / Light / Dark
Maintenance mode	Block all pages except login

Step 3: Enable SSL (Let's Encrypt)

1. Ensure your domain points to the server IP (DNS A record)
2. Go to **Settings > System**
3. In the **SSL / Let's Encrypt** section, set:
 - **Enabled** = `Yes`
 - **Domain** = your domain (e.g., `vpn.example.com`)
 - **Email** = your email for Let's Encrypt notifications
4. Click **Save** and then **Reload**

After reload, the web interface will be available on `https://your-domain.com` (port 443).

Step 4: Configure Networking

Navigate to **Settings > Networking** to manage server network interfaces and routes.

PUQVPNC P

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

Networking

+

↓

⚠

Danger Zone. Incorrect network configuration may make the server unreachable. After applying changes you will have 45 seconds to confirm. If not confirmed, the previous configuration will be restored automatically.

Interfaces

Routes

Network Interfaces

debian

25

entries per page

Filter:

Name	Type	Method	Address	Gateway	Status	MAC	
ens18	eth	static	77.87.125.200/25	77.87.125.129	UP	2e:30:5b:cc:48:27	
ens18:1	alias	static	77.87.125.201/25	-	UP	2e:30:5b:cc:48:27	
ens19	eth	manual	-	-	UP	1a:9d:1d:16:3b:d6	
ens20	eth	-	-	-	DOWN	be:4b:0f:22:e8:fe	
ens21	eth	-	-	-	DOWN	26:51:bb:1f:12:78	
lo	loopback	loopback	127.0.0.1/8 ::1/128	-	UNKNOWN	00:00:00:00:00:00	

Showing 1 to 6 of 6 entries

«

<

1

>

»

Network interfaces list

⚠ **Danger Zone.** Incorrect network configuration may make the server unreachable. After applying changes you will have **45 seconds to confirm**. If not confirmed, the previous configuration will be restored automatically.

Adding an Interface

Click the + button to add a new interface (alias or VLAN).

Server ▾ Diagnostics ▾ Settings ▾ About ▾

Add Interface ✕

Type	Name
Alias (eth0:0) ▾	ens18:1

Parent Interface

ens18 (77.87.125.200/25) ▾

Name: parent:N (e.g. ens18:0)

Method IPv4	Method IPv6	MTU
static ▾	None ▾	1500

IPv4

Address (CIDR)	Gateway	DNS Nameservers
77.87.125.202/25		8.8.8.8 8.8.4.4

IPv6

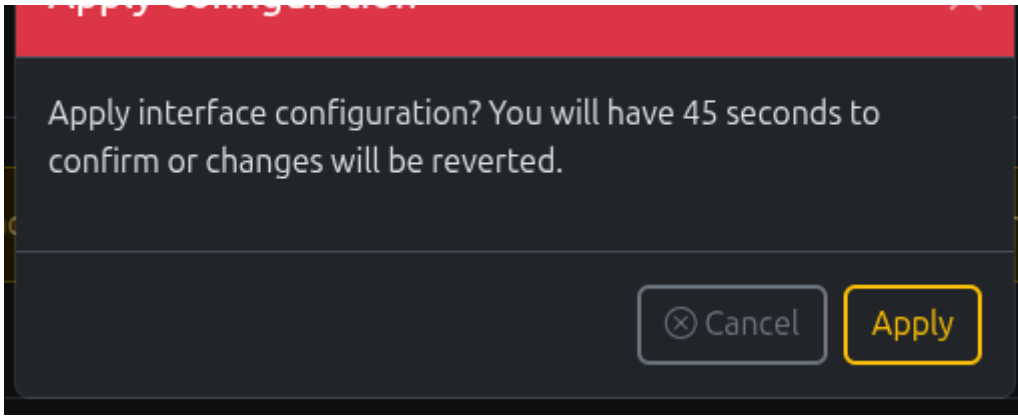
Address IPv6	Netmask IPv6	Gateway IPv6
	64	

✕ Close ✓ Save

Add network interface dialog

Applying Configuration

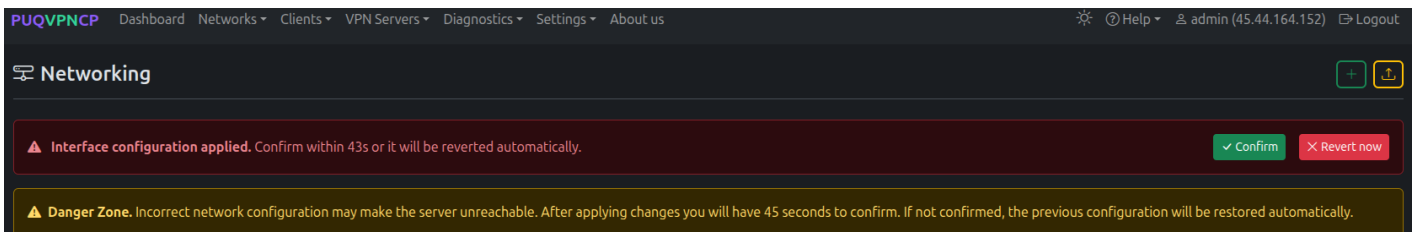
After making changes, click **Apply**. A confirmation dialog warns about the 45-second timeout:



Apply configuration

confirmation — 45-second safety timeout

Once applied, you must confirm within the timeout or changes will be reverted:



Configuration applied — confirm within 45 seconds or changes will be reverted

Routes

Switch to the **Routes** tab to view the current routing table.

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

⚙️ Help

admin (45.44.164.152)

Logout

Networking

⚠️ Danger Zone. Incorrect network configuration may make the server unreachable. After applying changes you will have 45 seconds to confirm. If not confirmed, the previous configuration will be restored automatically.

Interfaces

Routes

ⓘ Routes are applied immediately. No confirmation required.

Routing Table (live)

25 entries per page

Filter:

Destination	Gateway	Device	Metric	Type
10.0.0.0/24	-	wg51823	0	kernel
10.100.11.0/24	-	wg51822	0	kernel
10.100.12.0/24	-	wg51824	0	kernel
10.100.13.0/24	-	wg51825	0	kernel
10.100.9.0/24	-	wg51820	0	kernel
172.16.1.0/24	-	wgup0	0	kernel
77.87.125.128/25	-	ens18	0	kernel
default	77.87.125.129	ens18	0	manual

Showing 1 to 8 of 8 entries

1

System routing table (live)

Step 5: Environment Check

Navigate to **Settings > Environment** to verify all required packages are installed.

VPN Protocols

Status	Package	Description	Version	Required
✔️	wireguard	WireGuard kernel module	1.0.20210914-3	Required
✔️	wireguard-tools	WireGuard CLI tools (wg)	1.0.20210914-3	Required
✔️	amneziawg	AmneziaWG kernel module (DKMS)	1.0.20210914-0-202608130144+ee0f0a9-ubuntu24.04.1	Optional
✔️	amneziawg-tools	AmneziaWG CLI tools (awg)	1.0.20210914-0-202608130144+ee0f0a9-ubuntu24.04.1	Optional
✔️	openvpn	OpenVPN daemon	2.6.14-1+deb13u1	Required
✔️	easy-rsa	PKI management for OpenVPN	3.2.2-1	Required
✔️	strongswan	IKEv2/IPsec daemon (ipsec)	6.0.1-6+deb13u2	Required
✔️	strongswan-pki	IKEv2 certificate tools (pki)	6.0.1-6+deb13u2	Required

Environment check — VPN protocols section

The page shows:

- **VPN Protocols** — wireguard, amneziawg, amneziawg-tools, openvpn, easy-rsa, strongswan
- **Network & Firewall** — iproute2, iptables, ipset
- **DNS** — bind9, bind9-utils
- **Monitoring** — rsyslog, telegraf
- **Security** — openssl
- **System Utilities** — procps, uuid-runtime, bash, grep, gawk

DNS

Status	Package	Description	Version	Required
✔	bind9	DNS server (named)	1:9.20.18-1-deb13u1	Required
✔	bind9-utils	DNS utilities (rndc)	1:9.20.18-1-deb13u1	Required

Monitoring

Status	Package	Description	Version	Required
✔	rsyslog	System logging (iptables log)	8.2504.0-1	Required
✔	telegraf	Metrics collection (InfluxDB)	1.25.0-1	Required

Security

Status	Package	Description	Version	Required
✔	openssl	SSL/TLS certificate tools	3.5.4-1~deb13u2	Required

System Utilities

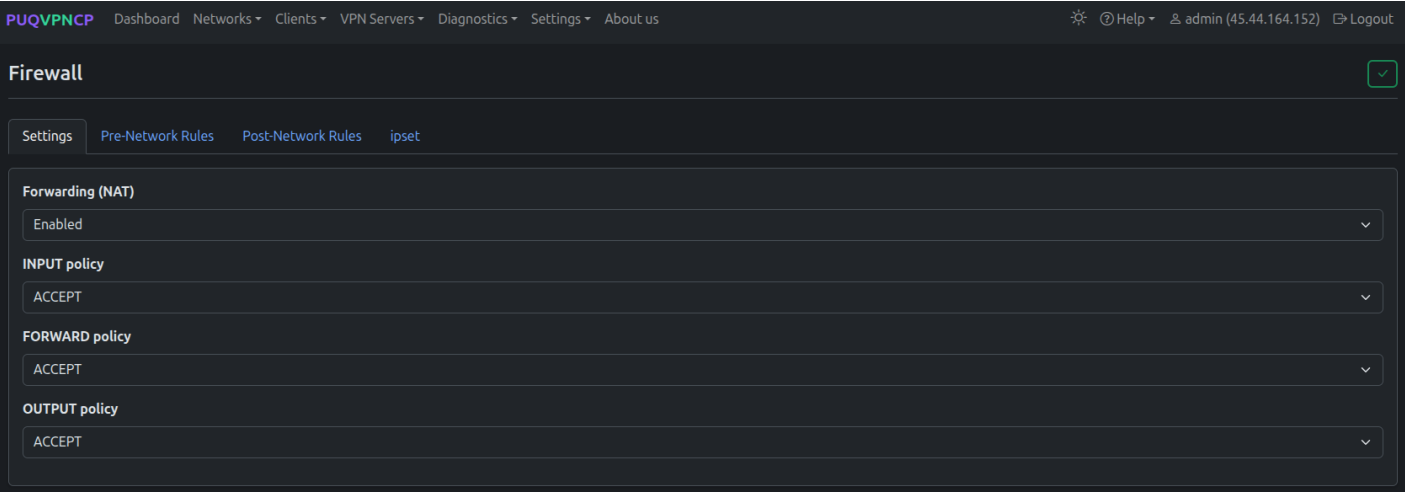
Status	Package	Description	Version	Required
✔	procps	Process tools (pgrep)	2:4.0.4-9	Required
✔	uuid-runtime	UUID generation (uuidgen)	2.41-5	Required
✔	bash	Shell for system commands	5.2.37-2+b7	Required
✔	grep	Text search utility	3.11-4	Required
✔	gawk	Text processing utility (awk)	1:5.2.1-2+b1	Required

Environment check — DNS, Monitoring, and Security sections

Missing packages are highlighted and can be installed using the copy button.

Step 6: Configure Firewall

Navigate to **Settings > Firewall** to set up global firewall policies.



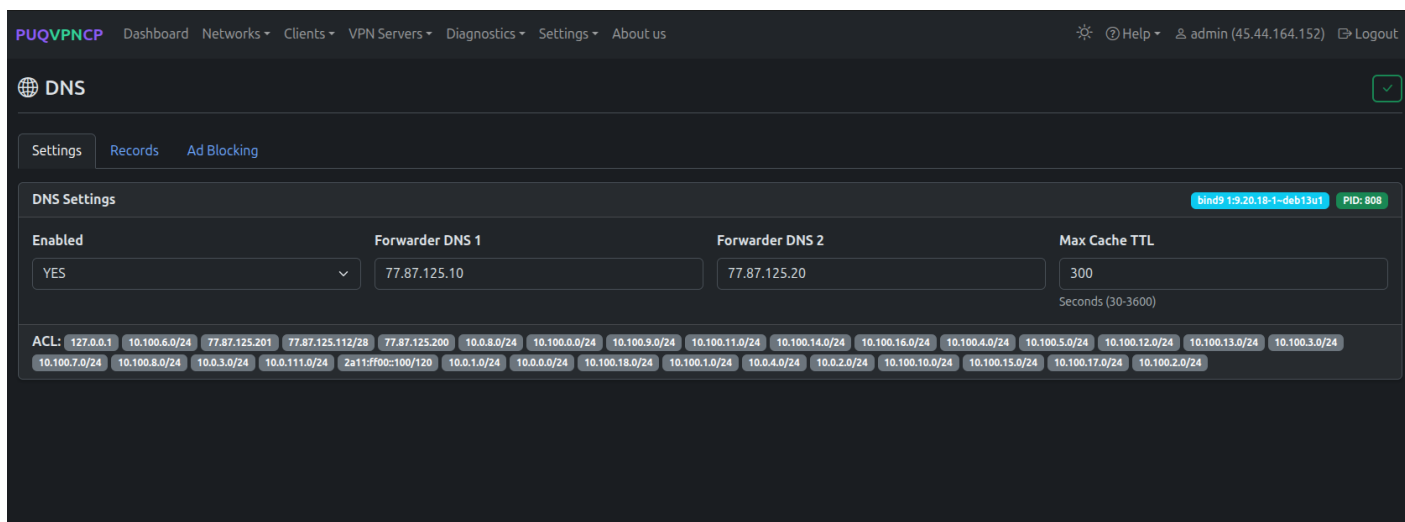
Firewall settings — global policies

Setting	Description
Forwarding (NAT)	Enable/Disable NAT for VPN clients
INPUT policy	Default action for incoming packets
FORWARD policy	Default action for forwarded packets
OUTPUT policy	Default action for outgoing packets

“ **Important:** Keep **Forwarding (NAT)** enabled for VPN clients to access the internet.

Step 7: Configure DNS

Navigate to **Settings > DNS** to configure the built-in bind9 DNS server.



DNS server configuration

Set the **Forwarders** field to upstream DNS servers (e.g., `8.8.8.8, 8.8.4.4`). This allows VPN clients to use the server as their DNS resolver.

Next Steps

After completing the initial setup:

1. **Create a Network** — define your first VPN network with a subnet
2. **Add Clients** — create VPN client accounts
3. **Configure VPN Protocols** — set up WireGuard, AmneziaWG, OpenVPN, or IKEv2

Revision #5

Created 28 September 2026 17:01:04 by Ruslan

Updated 28 September 2026 18:58:32 by Ruslan