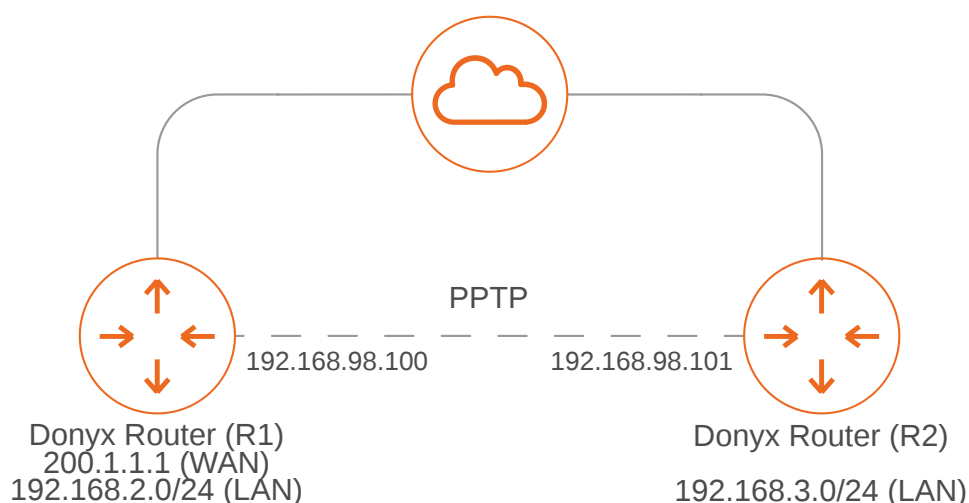


PPTP Server and Client Configuration on Donyx Routers

PPTP (Point-to-Point Tunneling Protocol) is a legacy protocol developed by Microsoft in the 1990s for establishing **Virtual Private Networks (VPN)**. While it provides basic secure connectivity, it is widely considered insecure due to outdated encryption methods. Consequently, it is recommended to implement **PPTP** in conjunction with **IPsec** rather than as a standalone protocol.

Donyx routers support both **PPTP Server** and **PPTP Client** modes. These devices feature automatic **IPsec** configuration for PPTP tunnels. Note that full mutual compatibility is guaranteed only between devices running the *dnxOS* platform; interoperability with third-party equipment may require manual adjustment.

Network integration via a PPTP tunnel:



In this scenario, router *R1* acts as the **PPTP Server** with the public IP address *200.1.1.1* and the local network *192.168.2.0/24*. Router *R2* acts as the **PPTP Client** with the local network *192.168.3.0/24*.

Configuration on Router R1 (Server)

The first step in server configuration is the creation of user accounts for connecting clients.

The following procedure is performed in the */service/client* section:



The screenshot shows a configuration form for a user named 'pptp-user'. The form is set against a dark background with white text. It includes the following fields and controls:

- Disabled:** A checkbox that is currently unchecked.
- Service:** A dropdown menu with the text "...select one or more..." and a downward arrow. Below the dropdown, a button with a minus sign and the text "pptp" is visible.
- Password:** A text input field containing seven dots, with an eye icon to its right for toggling visibility.
- Tunnel IP:** An empty text input field.
- Route:** An empty text input field.

1. Click the **Add** button and assign a name.
2. In the **Service** dropdown list, select the service for which the user is being created (e.g., *pptp*).
3. Specify the user password in the **Password** field.
4. Click **Apply**.

Once the account is created, navigate to the `/service/pptp-server` section:

1. Set the **Encryption** parameter to `ipsec` and specify the key in the **Pre-Shared Key** field. Other settings remain at their default values.

CLI Configuration

```

/service pptp-server
  auth mschap-v2
  debug -
  disabled true
  encryption ipsec
  ip-addr -
  ip-addr 192.168.98.100
  ip-pool -
  ip-pool 192.168.98.101-192.168.98.200
  ppp-option -
  ppp-option lcp-echo-failure=5,lcp-echo-interval=60
  psk password

/service pptp-server apply

```

Configuration on Router R2 (Client)

Navigate to the `/tunnel/pptp` section and click the **Add** button. Assign a name for the connection (e.g., *PPTP*).

The PPTP Client configuration for router *R2* is illustrated in the figure below.

Table 1. Parameters for Router R2 (Client)

Field	Value
Local IP	WAN (selected from the list).
Remote IP	200.1.1.1 (the server's public IP address).
User	user (must match the username created on the server).
Password	(password assigned to the user).
Encryption	ipsec
Pre-Shared Key	(the secret key, must match the server configuration).

CLI Configuration

```
/tunnel pptp add name=PPTP
  auth any
  debug -
  disabled -
  encryption ipsec
  local-ip WAN
  password password
  ppp-option -
  psk ipseckey
  remote-ip 200.1.1.1
  username user

/tunnel pptp apply
```

Firewall Configuration

When the **Encryption** parameter is set to *ipsec*, no additional firewall configuration is required on the router. However, if the *mmp* or *none* options are selected, a manual rule must be created to permit incoming traffic on TCP port 1723 for the **PPTP** server.

The rule is created in the */firewall/filter* section by clicking **Add** and completing the form with the following parameters:

Disabled	<input type="checkbox"/>
Chain	input
Source	zone-wan
Source Address	
Destination	
Destination Address	:1723
Protocol	tcp
Firewall Mark	
Action	accept
IPSec Policy	
Extra Params	

After completing the configuration, click **Apply**. In the */firewall/filter* section, the newly created rule must be moved to the top of the list, ensuring it is positioned above any rules that deny traffic.


CLI Configuration

```
/firewall filter add chain=input
  action accept
  dst-addr :1723
  protocol tcp
  src zone-wan
  reorder position=-1
  apply
/firewall filter status
```

Configuring Routes for Local Network Access

In the `/ip/route/list` section, click the **Add** button and define the routing parameters.

Router R1 (Server)



The screenshot shows a configuration dialog box with a dark background. At the top left, there are two buttons: 'OK' with a play icon and 'Close' with a close icon. Below these are four input fields:

- Target:** A text input field containing '192.168.3.0/24'.
- Source Interface:** A dropdown menu with 'in_pptp0' selected and a downward arrow.
- Gateway:** An empty text input field.
- Metric:** A text input field containing '0'.

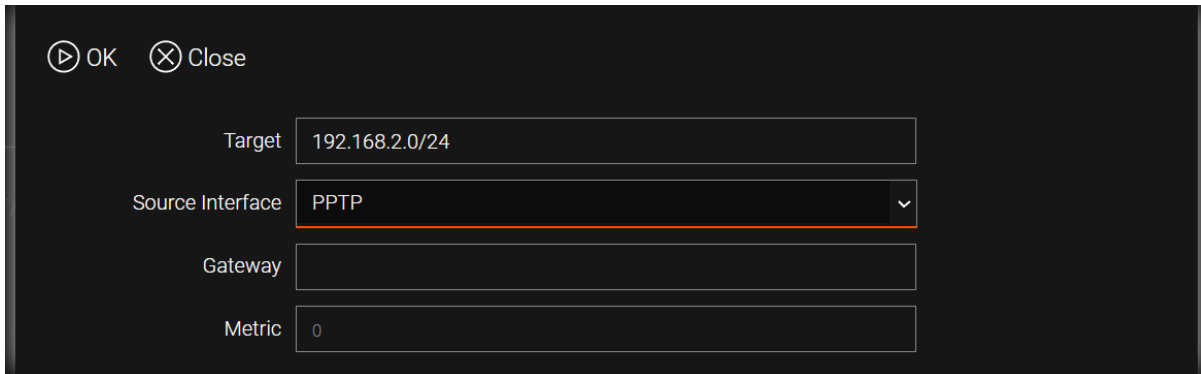
On the router acting as the server, the tunnel interface is automatically assigned the name `in_pptp0`.

1. In the **Target** field, specify the destination subnet (in this scenario, `192.168.3.0/24`).
2. In the **Source Interface** field, manually enter the interface name: `in_pptp0`.
3. The **Gateway** field should be left blank.
4. Click **OK**, then click **Apply**.

CLI Configuration

```
/ip route list add dst-addr=192.168.3.0/24 interface=in_pptp0
disabled true
metric -
src-addr -
table main
type unicast
/ip route list apply
```

Router R2 (Client)



Target: 192.168.2.0/24

Source Interface: PPTP

Gateway:

Metric: 0

The following parameters are configured in the `/ip/route/list` section:

1. In the **Target** field, specify the destination subnet (in this scenario, `192.168.2.0/24`).
2. In the **Source Interface** field, select the tunnel interface name (in this example, `PPTP`).
3. The **Gateway** field should be left blank.
4. Click **OK**, then click **Apply**.

CLI Configuration

```
/ip route list add dst-addr=192.168.2.0/24 interface=PPTP
  disabled -
  gateway -
  metric -
  src-addr -
  table main
  type unicast
/ip route list apply
```

Ping (/tools/ping) — R2 to R1

Verify connectivity from the **PPTP Client (R2)** to the **PPTP Server** network (R1):

```
⏮ Again  ✕ Stop  ✕ Close

PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_req=1 ttl=64 time=3.35 ms
64 bytes from 192.168.2.1: icmp_req=2 ttl=64 time=3.00 ms
64 bytes from 192.168.2.1: icmp_req=3 ttl=64 time=2.74 ms
64 bytes from 192.168.2.1: icmp_req=4 ttl=64 time=2.71 ms
64 bytes from 192.168.2.1: icmp_req=5 ttl=64 time=2.68 ms
64 bytes from 192.168.2.1: icmp_req=6 ttl=64 time=2.66 ms
64 bytes from 192.168.2.1: icmp_req=7 ttl=64 time=2.73 ms
64 bytes from 192.168.2.1: icmp_req=8 ttl=64 time=2.84 ms
64 bytes from 192.168.2.1: icmp_req=9 ttl=64 time=2.60 ms
64 bytes from 192.168.2.1: icmp_req=10 ttl=64 time=2.76 ms
--- 192.168.2.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 33ms
rtt min/avg/max/mdev = 2.604/2.810/3.353/0.216 ms, ipg/ewma 3.712/2.922 ms
Finished
```

Ping (/tools/ping) — R1 to R2

Verify connectivity from the **PPTP Server (R1)** to the **PPTP Client** network (R2):

```
⏮ Again  ✕ Stop  ✕ Close

PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_req=1 ttl=64 time=3.06 ms
64 bytes from 192.168.3.1: icmp_req=2 ttl=64 time=3.49 ms
64 bytes from 192.168.3.1: icmp_req=3 ttl=64 time=3.58 ms
64 bytes from 192.168.3.1: icmp_req=4 ttl=64 time=3.36 ms
64 bytes from 192.168.3.1: icmp_req=5 ttl=64 time=3.08 ms
64 bytes from 192.168.3.1: icmp_req=6 ttl=64 time=3.07 ms
64 bytes from 192.168.3.1: icmp_req=7 ttl=64 time=3.04 ms
64 bytes from 192.168.3.1: icmp_req=8 ttl=64 time=3.25 ms
64 bytes from 192.168.3.1: icmp_req=9 ttl=64 time=3.36 ms
64 bytes from 192.168.3.1: icmp_req=10 ttl=64 time=3.11 ms
--- 192.168.3.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 33ms
rtt min/avg/max/mdev = 3.045/3.243/3.581/0.194 ms, ipg/ewma 3.760/3.181 ms
Finished
```



All modifications are permanently saved to the router configuration only after executing the `/system config commit` command or clicking the **commit** button in the web interface.