

Asus - OpenVPN Site to Site or Point to Point

ASUS Asuswrt Merlin

Most of the documents online are missing steps or the folks writing the document are assuming that the folks setting this up are network traffic wizards.

GOAL:

With one of the Asus routers being the server and the other being a client, we want to be able from either side hit IPs or hostnames of any of any device.

Both Routers:

VPN Type: TUN as TAP maybe overkill for this case

Protocol: UDP

Static Routes: Both servers

When you export the OpenVPN certificates from the router (as opposed to supplying your own), they have the CN set as '**client**'. This is relevant/confusing for the server config, as our other router is a client named client.

Server:

ASUS RT-AC5300 with 192.168.53.1/24

<u>Interface Type</u>	☒ TUN ☐ TAP
<u>Protocol</u>	☐ TCP ☒ UDP
<u>Server Port</u>	1196 (Default : 1194)
<u>Authentication Mode</u>	☒ TLS ☐ Static Key
<u>Keys and Certificates</u>	Edit...

Username/Password Authentication	☐ Yes ☒ No	
<u>TLS control channel security</u> <i>(tls-auth / tls-crypt)</i>	Encrypt channel ▼	
<u>HMAC Authentication</u>		
<u>VPN Subnet / Netmask</u>	10.100.100.0	255.255.255.0
<u>Advertise DNS to clients</u>	☒ Yes ☐ No	
<u>Data ciphers</u>	AES-128-GCM:AES-256-GCM:AES-128-CBC:AES-256-CBC	
<u>Compression</u>	LZO Adaptiv ▼	
<u>Log verbosity</u>	3	(Between 0 and 6. Default: 3)
<u>Manage Client-Specific Options</u>	☒ Yes ☐ No	
<u>Allow Client <-> Client</u>	☒ Yes ☐ No	
<u>Allow only specified clients</u>	☐ Yes ☒ No	

Allowed Clients				
Common Name(CN)	Subnet	Mask	Push	Add / Delete
			No	▼

client	192.168.51.0	255.255.255.0	Yes	
--------	--------------	---------------	-----	-------------

Custom Configuration

```
reneg-sec 432000
push "route 192.168.53.0 255.255.255.0"
route 192.168.51.0 255.255.255.0
```

Custom Explained:

```
reneg-sec 432000 #optional
push "route 192.168.53.0 255.255.255.0" #server LAN IP
route 192.168.51.0 255.255.255.0 #client LAN IP
```

Export the .ovpn files from the new server config

Client:

ASUS RT-AC5300 with 192.168.51.1/24

Import .ovpn config file exported from server, to set the certificates and some of the basic settings.

Select client instance	
Service state	Image not found or type unknown
Automatic start at boot time	☐ Yes ☐ No
Description	Site-to-Site HOUSE
Import .ovpn file	Choose a file Upload

Network Settings	
Interface Type	☐ TUN ☐ TAP
Protocol	☐ TCP ☒ UDP
Server Address and Port	Address:XXXXXXXX.asuscomm.com Port: 1196
Create NAT on tunnel	☐ Yes ☒ No Routes must be configured manually.
Inbound Firewall	☐ Block ☒ Allow
Accept DNS Configuration	Disabled
Redirect Internet traffic through tunnel	

Authentication Settings	
Authentication Mode	☒ TLS ☐ Static Key
Username/Password Authentication	☐ Yes ☒ No

Crypto Settings	
Keys and Certificates	Edit...
Data ciphers	AES-128-GCM:AES-256-GCM:AES-128-CBC:AES-256-CBC

Crypto Settings	
<u>TLS control channel security</u> <i>(tls-auth / tls-crypt)</i>	Encrypt Channel ▼
<u>Auth digest</u>	▼

Advanced Settings	
Log verbosity	3 (Between 0 and 6. Default: 3)
Compression	LZO Adaptive ▼
<u>TLS Renegotiation Time</u>	-1 (in seconds, -1 for default)
Connection Retry attempts	0 (0 for infinite)
Verify Server Certificate Name	No ▼

Custom Configuration
resolv-retry infinite float keepalive 15 60 remote-cert-tls server

Applied the "automatic start at boot time"

Turn on the client VPN

Server Connection:

OpenVPN Server 2 - Running

Confusion:

The problem is that from the server I cannot access the the LAN on the client side without adding a route vis the JFFS scripts folder using the "nat-start" script.

```
#!/bin/sh
#https://github.com/RMerl/asuswrt-merlin.ng/wiki/User-scripts
#
DATE=$(date +"%Y-%m-%d-%H%M%S")
echo "deleting the route to router if it exists" $DATE >> /tmp/nat-start.log
route delete -net 192.168.51.0 netmask 255.255.255.0 gw 10.100.100.2
echo "done deleting the route" $DATE >> /tmp/nat-start.log
echo "adding route to router" $DATE >> /tmp/nat-start.log
route add -net 192.168.51.0 netmask 255.255.255.0 gw 10.100.100.2
echo "done adding route to router" $DATE >> /tmp/nat-start.log
```

References:

<https://medium.com/@kylemattimore/asuswrt-merlin-openvpn-tunnel-site-to-site-69b9011b079a>

<https://www.senia.org/2018/03/12/router-to-router-vpn-tunnel-using-asus-routers/>

<https://www.asus.com/us/support/faq/1011706/>

Revision #1

Created 11 February 2026 13:20:55 by Steve Ling

Updated 11 February 2026 13:20:55 by Steve Ling