

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>	<input checked="" type="radio"/> TUN <input type="radio"/> TAP
<u>Protocol</u>	<input type="radio"/> TCP <input checked="" type="radio"/> UDP
<u>Server Port</u>	<input type="text" value="1196"/> (Default : 1194)
<u>Authentication Mode</u>	<input checked="" type="radio"/> TLS <input type="radio"/> Static Key
<u>Keys and Certificates</u>	<input type="button" value="Edit..."/>

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

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

client	192.168.51.0	255.255.255.0	Yes	<div></div>
--------	--------------	---------------	-----	-------------

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	<div></div>
Service state	<div>Image not found or type unknown</div>
Automatic start at boot time	<div><input type="radio"/> Yes <input type="radio"/> No</div>
Description	<div>Site-to-Site HOUSE</div>
Import .ovpn file	<div><div>Choose a file</div><div>Upload</div></div>

Network Settings	
Interface Type	<div><input type="radio"/> TUN <input type="radio"/> TAP</div>
Protocol	<div><input type="radio"/> TCP <input checked="" type="radio"/> UDP</div>
Server Address and Port	<div>Address:XXXXXXXX.asuscomm.com</div> <div>Port:<div>1196</div></div>
Create NAT on tunnel	<div><input type="radio"/> Yes <input checked="" type="radio"/> No Routes must be configured manually.</div>
Inbound Firewall	<div><input type="radio"/> Block <input checked="" type="radio"/> Allow</div>
Accept DNS Configuration	<div>Disabled</div>
Redirect Internet traffic through tunnel	<div></div>

Authentication Settings	
Authentication Mode	<div><input checked="" type="radio"/> TLS <input type="radio"/> Static Key</div>
Username/Password Authentication	<div><input type="radio"/> Yes <input checked="" type="radio"/> No</div>

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

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 #6

Created 22 December 2024 15:28:42 by Steve Ling

Updated 22 December 2024 17:11:30 by Steve Ling