OpenVPN Server and Client Setup

6350-SR

OpenVPN Server and Client Setup

Difficulty: *Intermediate*

Goal

To configure an OpenVPN server on an Accelerated device using *Server managed certificates*, and to setup the OpenVPN configuration file for remote clients.

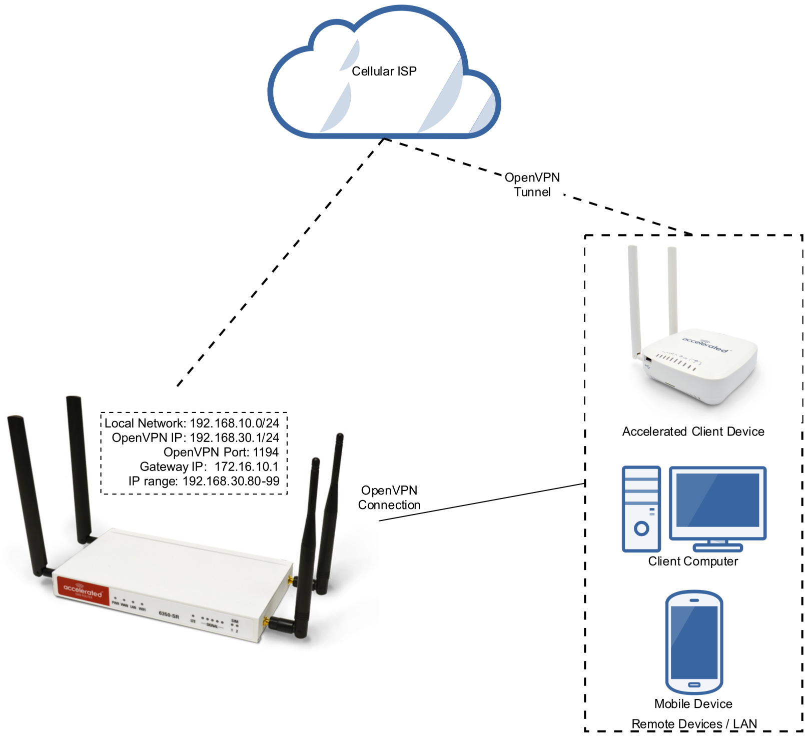
Setup

This article assumes you have an Accelerated device that supports OpenVPN, a working knowledge of networking for the infrastructure you are trying to establish, and physical connection of network hardware. The configuration of OpenVPN servers and clients that use custom key files and certificates is not in the scope of this article. However, related information are available in these links:

- Configuring an OpenVPN Server for iOS & Android OS Clients
- Configuring a TAP-styled OpenVPN Server and Client

Sample

The sample configuration below shows the connection arrangement and relevant network information between an Accelerated device as the OpenVPN server, and the remote devices which are the OpenVPN clients. The network information are used in this article.

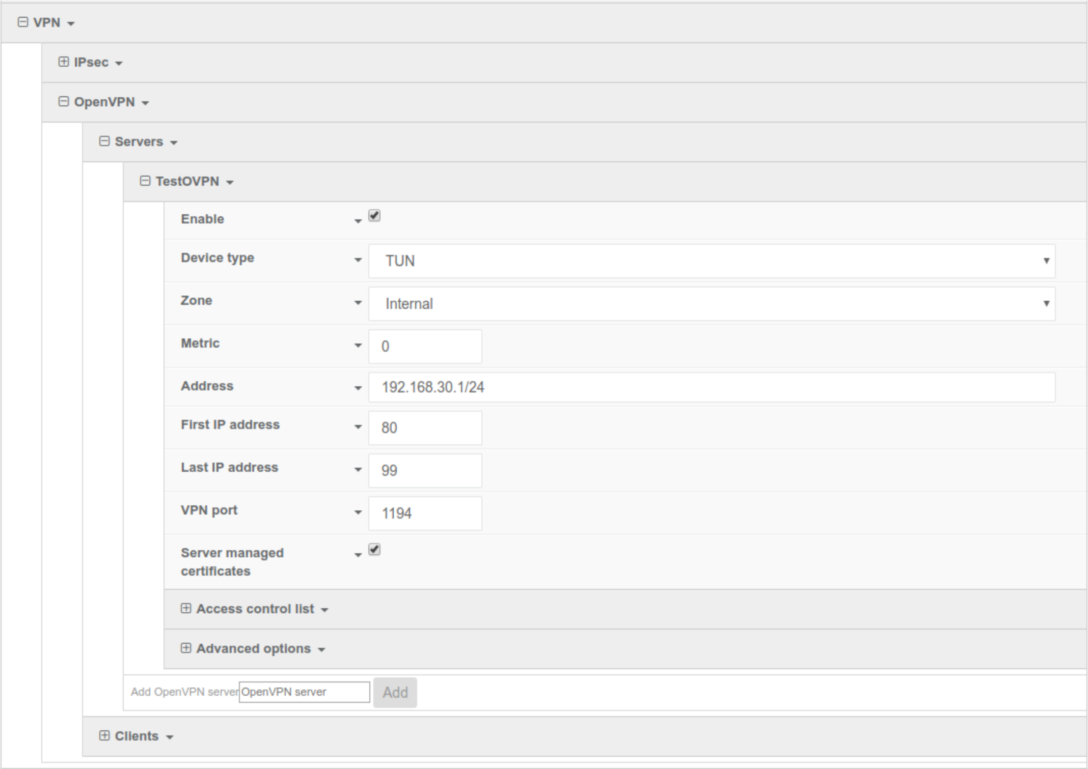


Sample Server Configuration

Open the configuration page and set the following configurations.

VPN > OpenVPN Section Configuration

1. Specify a new server name in ***Add OpenVPN server***: TestOVPN
2. Specify the type of OpenVPN device in ***Device type***: TUN/TAP *(TUN is used in this walkthrough)*
3. Specify the firewall zone in ***Zone***: internal
4. Specify the address of the OpenVPN network in ***Address***, which should be different from the LAN network: 192.168.30.1/24
5. Enable ***Server managed certificates***: Checked



⊟ VPN

⊞ IPsec

⊟ OpenVPN

⊟ Servers

⊟ TestOVPN

Enable	☑
Device type	TUN
Zone	Internal
Metric	0
Address	192.168.30.1/24
First IP address	80
Last IP address	99
VPN port	1194
Server managed certificates	☑

⊞ Access control list

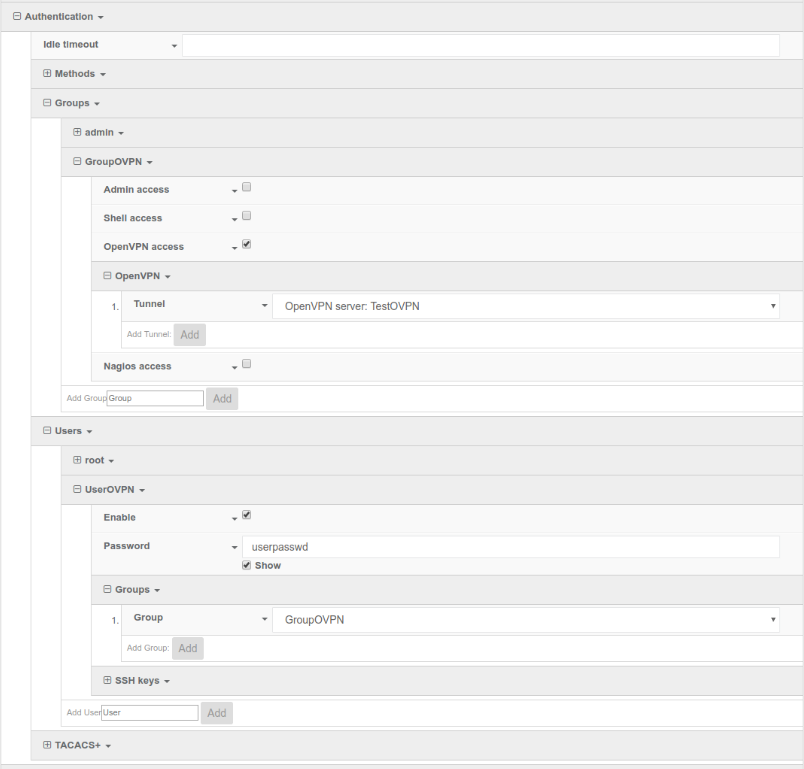
⊞ Advanced options

Add OpenVPN server OpenVPN server Add

⊞ Clients

Authentication Section Configuration *to add OpenVPN users*

1. In ***Authentication*** > ***Groups***, specify a new OpenVPN group name and click ***Add Group***: GroupOVPN
2. In the newly created group (i.e. GroupOVPN), enable ***OpenVPN access***
3. In the ***OpenVPN*** section, select the newly created OpenVPN server in the ***Tunnel*** dropdown: OpenVPN server: TestOVPN
4. In ***Authentication*** > ***Users***, specify a new OpenVPN user username and click ***Add User***: UserOVPN
5. Insert a password in the ***Password*** prompt: userpasswd
6. In the ***Groups*** section, select the newly created (or as desired) OpenVPN group in the ***Group*** dropdown: GroupOVPN



⊟ Authentication

Idle timeout

⊞ Methods

⊟ Groups

⊞ admin

⊟ GroupOVPN

Admin access □

Shell access □

OpenVPN access ☑

⊟ OpenVPN

1. Tunnel: OpenVPN server: TestOVPN

Add Tunnel: Add

Nagios access □

Add Group: Group Add

⊟ Users

⊞ root

⊟ UserOVPN

Enable ☑

Password: userpasswd

☑ Show

⊟ Groups

1. Group: GroupOVPN

Add Group: Add

⊞ SSH keys

Add User: User Add

⊞ TACACS+

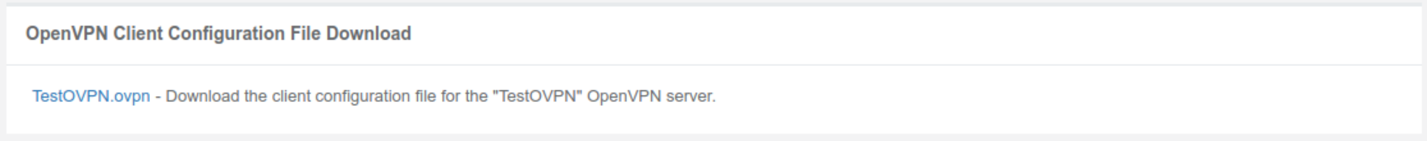
Once all configurations are correct, click *Save* at the bottom of the configuration page to save the changes. Your TUN-style OpenVPN server is now set up and ready to accept client user connection using the appropriate credentials set up in the *Authentication* section.

Sample Client Configuration File

The minimum requirements for a remote client to connect to the OpenVPN server is the OpenVPN client configuration file and an OpenVPN client. To obtain these:

- Configuration file (*.ovpn): In ***local web administration*** page (normally accessible from 192.168.210.1) > ***System*** > ***OpenVPN Configuration File Download;*** click to download *TestOVPN.ovpn*
- Client application: OpenVPN download page

The *TestOVPN.ovpn* file needs to be edited before use, and it can be edited in any text editing program.



OpenVPN Client Configuration File Download

TestOVPN.ovpn - Download the client configuration file for the "TestOVPN" OpenVPN server.

When *TestOVPN.ovpn* file is opened, change the field *<server address>* with the public external IP address of your server. In this sample, *<server address>* is replaced with *172.16.10.1*.

Custom routing (e.g. from the OpenVPN network to the internal corporate network) can also be achieved with `route <destination network> <network submask>`. In this sample, the destination (internal) network is *192.168.10.0/24*, therefore a new line `route 192.168.10.0 255.255.255.0` is added to the configuration.

```
# Note:
#
# Any lines with <...> in them need to be modified. For example
#
# remote <server address> 1234
# with a server address of 1.2.3.4, becomes
# remote 1.2.3.4 1234

#general
client
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC

# connection settings
dev tun
proto udp
# ==============================================================
# replaced 'remote <server address> 1194' with
remote 172.16.10.1 1194 # MODIFIED LINE
route 192.168.10.0 255.255.255.0 # ADDED LINE
# ==============================================================
<ca>
-----BEGIN CERTIFICATE-----
MIIFTjCCBDagAwIBAgIJALkwivgA/CCDMA0GCSqGSIb3DQEBCwUAMIHKMQswCQYD
VQQGEwJBVTEMMAoGA1UECBMDUUxEMREwDwYDVQQHEwhCcmlzYmFuZTEdMBsGA1UE
ChMUQWNjZWxlcmF0ZWQgQ29uY2VwdHMxHTAbBgNVBAsTFEFjY2VsZXJhdGVkIENv
bmNlcHRzMSAwHgYDVQQDExdBY2NlbGVyYXRlZCBDb25jZXB0cyBDQTEQMA4GA1UE
KRMHRWFzeVJTQTEoMCYGCSqGSIb3DQEJARYZamVmZi5zaGF3QGFjY2VsZXJhdGVk
LmNvbTAeFw0xNzA5MTQwMzM5MDdaFw0yNzA5MTIwMzM5MDdaMIHKMQswCQYDVQQG
EwJBVTEMMAoGA1UECBMDUUxEMREwDwYDVQQHEwhCcmlzYmFuZTEdMBsGA1UEChMU
QWNjZWxlcmF0ZWQgQ29uY2VwdHMxHTAbBgNVBAsTFEFjY2VsZXJhdGVkIENvbmNl
cHRzMSAwHgYDVQQDExdBY2NlbGVyYXRlZCBDb25jZXB0cyBDQTEQMA4GA1UEKRMH
RWFzeVJTQTEoMCYGCSqGSIb3DQEJARYZamVmZi5zaGF3QGFjY2VsZXJhdGVkLmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM7S5xFLwGCAxeJPlO2K
AWf8uOu1LuXSHSANdCgdnjsJh3l31wRQ9c6cc8JmfcbLN5B3wwvaV0LsLbPVk1jk
pw7ImVbsN2k8+dto5WzTu/RfGPbjP4yML3ZtL0lkQWw3kmZ2vhPUa3YFG1x13Yk9
yHB+FfjhJivK7f5Bw+e8clkh3t6d2nyqOlDo9nmeYnvgaSXJgkFqUgUT3s72rpz3
Hb8+m8KihZ/yU09E0e3w767TXqCjcVcKWDr2YR9d5B5nf9FbMbLWaJoCmAFHjluf
pHdKVlDiHnCKwd0PUGKiWiWH3JTmrXK4nbnba5cWFKyF+fO7Kw+2NcyGcQUVeZg5
+X8CAwEAAaOCATMwggEvMB0GA1UdDgQWBBQ3wwwxUUgvxKEJlposwCjGV4hU/TCB
/wYDVR0jBIH3MIH0gBQ3wwwxUUgvxKEJlposwCjGV4hU/aGB0KSBzTCByjELMAkG
A1UEBhMCQVUxDDAKBgNVBAgTA1FMRDERMA8GA1UEBxMIQnJpc2JhbmUxHTAbBgNV
BAoTFEFjY2VsZXJhdGVkIENvbmNlcHRzMR0wGwYDVQQLExRBY2NlbGVyYXRlZCBD
b25jZXB0czEgMB4GA1UEAxMXQWNjZWxlcmF0ZWQgQ29uY2VwdHMgQ0ExEDAOBgNV
```

```
BCkTB0Vhc3lSU0ExKDAmBgkqhkiG9w0BCQEWGWplZmYuc2hhd0BhY2NlbGVyYXRl
ZC5jb22CCQC5MIr4APwggzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IB
AQAKv7/5NNS2ow4YFNwV/0tMvNP6yekNzomiL+Yx0QwP7yK+MvvcPXsW0jgicqqW
gEVvIDP5xK/DJC2gx0BAB0ZxH9EahDHd1cuHE5JabwD8zZzMOrPflPcAYdi+B+Zn
voQvMhoH9aMBNW13oNfLHmGg7I/6tDR9NgWFSpiwlyK63HLOeSxaZ8Jioac6slSO
4qUmfef8RGcBL4tO76ebsbi7FH03bWBGf+SftAT/Xw4EJ/O/VxITS1veFn0HRUfM
6YCDou/44JTc0GD2trekCiCuvDk5QhxzUja5DXB+fsSNvGMNbuyALV7y52jSrrw5
PUj4tJcN6F1p9WKhaDXnRClb
-----END CERTIFICATE-----

</ca>

#authentication
auth-user-pass
```

The remaining configuration process of the remote client uses this configuration file. For details, visit:

- Configuring an OpenVPN Client on an Accelerated Device
- Configuring a TAP-styled OpenVPN Server and Client
- Configuring an OpenVPN Server for iOS & Android OS Clients