OPENVPN™ Access Server

Follow us twitter

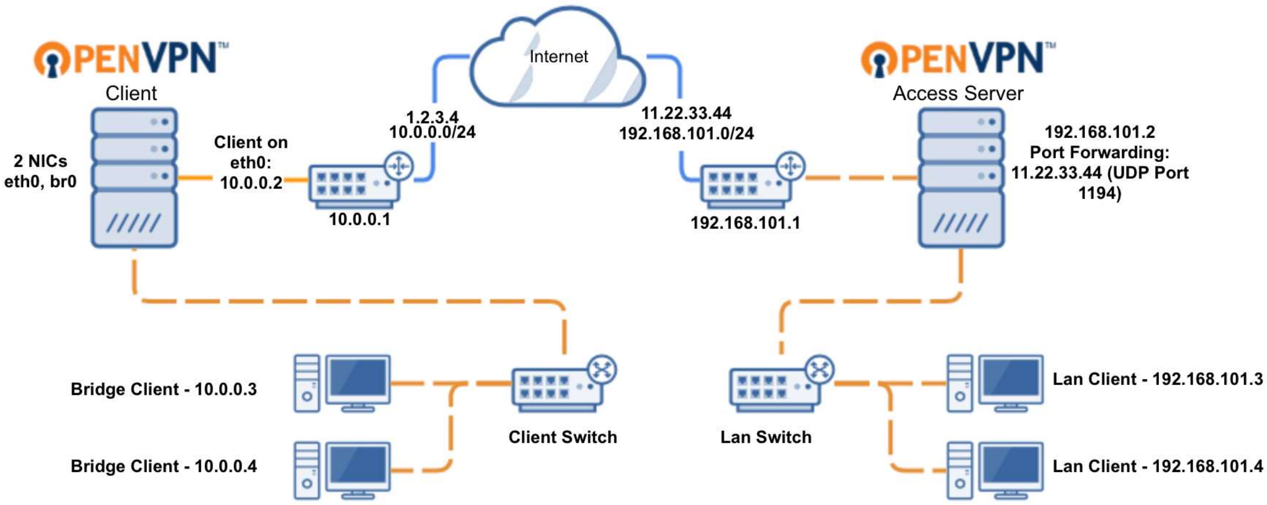
Home | Access Server CLI | Getting Started | Howto Guides | Under the hood | iOS & Android | FAQ's

Site-to-Site Layer 3 Routing Using OpenVPN Access Server and a Linux Gateway Client

Introduction

OpenVPN Access Server can be configured in a site-to-site routed setup that allows you to join two sites together using a OpenVPN gateway client. Unlike the Layer 2 method, this method does not require the OpenVPN client to have two Ethernet adapters, and since broadcast traffic is not delivered over the VPN tunnel, this saves valuable bandwidth resources. However, this setup is more complex and requires manual routing configurations on both sites. You should be advised that since multicast and broadcast traffic are not transmitted across the VPN tunnel, application and network discovery applications will not work across sites in this mode. Computers that are normally discovered thus will have to resort to communicating directly via Unicast using the other party's IP address.
In order to do this, some requirements must be met. These requirements are detailed below.

Routing Overview & Requirements



Sample Diagram Configuration

Site 1 Network (Left - Client)

Router/Firewall's Public IP Address: 1.2.3.4
Router/Firewall's LAN IP Address: 10.0.0.1
Router/Firewall's Subnet Mask: 255.255.255.0 (/24)

OpenVPN Client's LAN IP Address: **10.0.0.2**
OpenVPN Client's Subnet Mask: **255.255.255.0 (/24)**
OpenVPN Client's Default Gateway: **10.0.0.1**

Site Client 1/2's LAN IP Address: **10.0.0.3 / 10.0.0.4**
Site Client 1/2's Subnet Mask: **255.255.255.0 (/24)**
Site Client 1/2's Default Gateway: **10.0.0.1**

Site 2 Network (Right - Server)

Router/Firewall's Public IP Address: **12.34.56.78**
Router/Firewall's LAN IP Address: **192.168.101.1**
Router/Firewall's Subnet Mask: **255.255.255.0 (/24)**

OpenVPN Access Server's LAN IP Address: **192.168.101.2**
Port Forwarding for UDP Port 1194: **12.34.56.78 (UDP Port: 1194)**
OpenVPN Access Server's Subnet Mask: **255.255.255.0 (/24)**
OpenVPN Access Server's Default Gateway: **192.168.101.1**

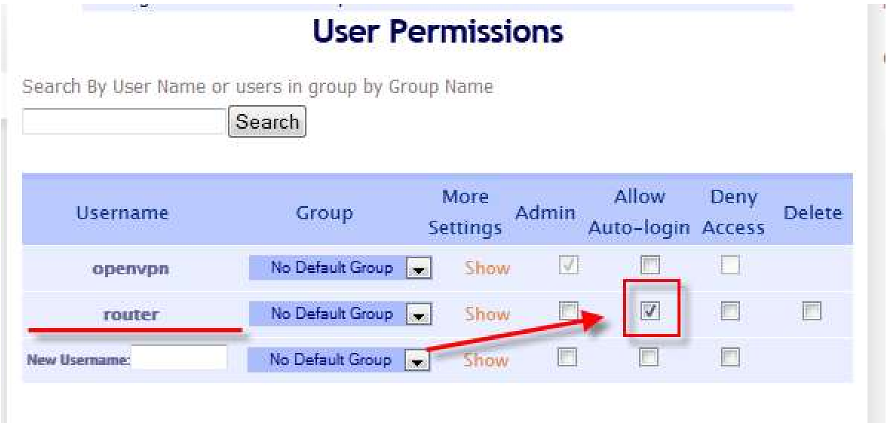
Site Client 1/2's LAN IP Address: **192.168.0.3 / 192.168.101.4**
Site Client 1/2's Subnet Mask: **255.255.255.0 (/24)**
Site Client 1/2's Default Gateway: **192.168.101.1**

The diagram above depicts a typical site-to-site layer 3 routing setup. In order to complete this setup, all of the following requirements must be met:

1. You have two sites, each one connected to the Internet. One site will be hosting the Access Server and one site will be hosting the OpenVPN client.
2. The site hosting the Access Server must be accessible from the Internet, or have its required ports forwarded to it from the Internet.
3. The OpenVPN client must have ***IP forwarding*** enabled, as well as ***openvpn*** installed, and running a ***Linux*** operating system (per these instructions).
4. You must have administrative access to the OpenVPN Client machine, including uploading files and SSH/SFTP access.
5. You must have administrative access to add static routes to both sites computers' default gateway (this is usually the router/firewall that serves the local network).
6. The two sites must not reside on the same subnet (e.g. 192.168.1.0/24 for both sites).

Routing Configuration

In order to start the routing process, you must first have Access Server generate an autologin profile. To do so, visit the ***User Permissions*** area, create an appropriate username for the bridging OpenVPN client, and then check the ***Allow Auto-login*** checkbox. Click the ***Update Running Server*** button to make sure the changes take effect.

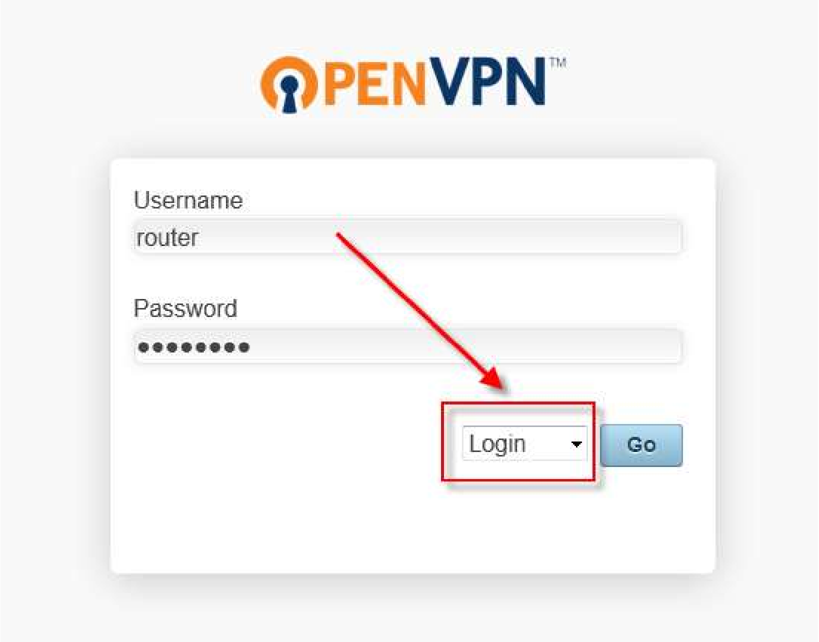


User Permissions

Search By User Name or users in group by Group Name

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group	Show	☑	□	□	
router	No Default Group	Show	□	☑	□	□
New Username:	No Default Group	Show	□	□	□	

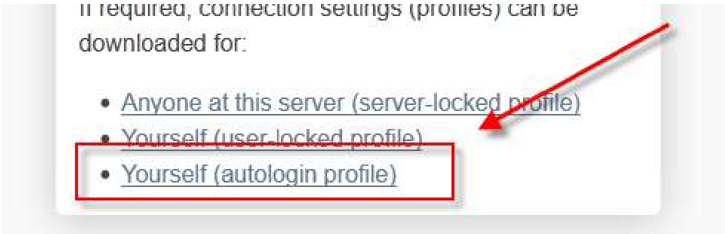
Now, login to the ***Client Web Server (CWS)*** and select the ***Login*** dropdown, when prompted.



Username: router

Password: ●●●●●●●●●

Download the ***autologin profile*** that is offered to you in the CWS.



If required, connection settings (profiles) can be downloaded for:

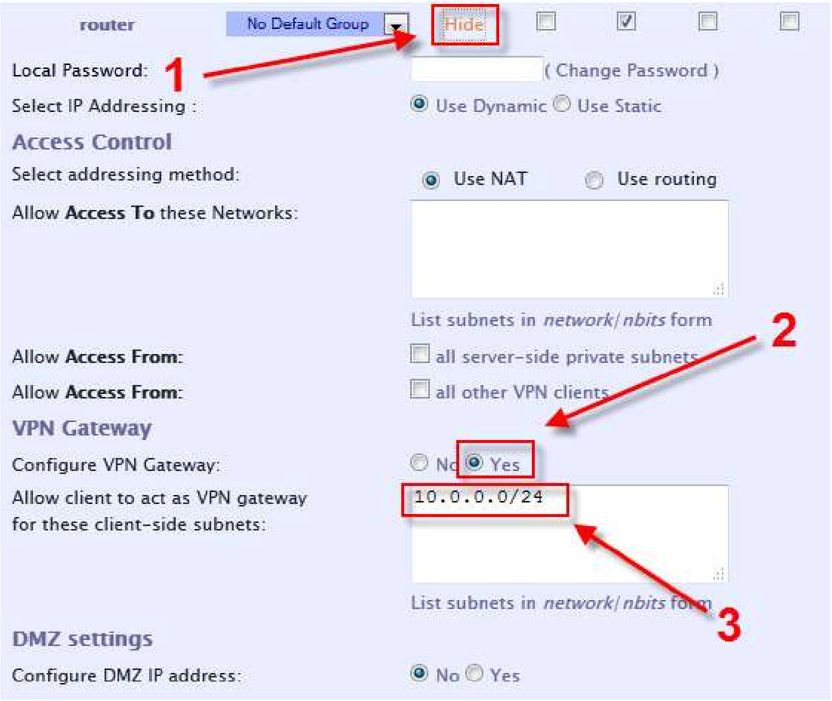
- Anyone at this server (server-locked profile)
- Yourself (user-locked profile)
- Yourself (autologin profile)

Next, we will need to make sure that the both sides know how to route their respective traffic between each other, when a link is established between the two sites.

We will begin by telling Access Server what subnet(s) the client is responsible for in its routing decisions. This allows Access Server to know where it should forward traffic to, and in our case, traffic received by the Access Server designated for ***10.0.0.0/24*** subnet should be forwarded over the ***VPN tunnel***, under the ***router*** user we

To do this, go back to the ***User Permissions*** section in your ***Admin Web UI***. Under the ***router*** user we have created previously, click the ***Show*** link to reveal more advanced options.

Afterwards, under ***Configure VPN Gateway:***, select the ***Yes*** radio box and populate the subnets that is on the OpenVPN Client's side network. Since in our example the OpenVPN Client only houses the 10.0.0.0/24 network, we will enter that in the ***Allow client to act as VPN gateway for these client-side subnets:*** text box. Please note that the subnet entered here should be in canonical notation with a CIDR style subnet mask.



router — No Default Group — Hide — □ ☑ □ □

Local Password: (Change Password)

Select IP Addressing : ● Use Dynamic ○ Use Static

Access Control

Select addressing method: ● Use NAT ○ Use routing

Allow Access To these Networks:

List subnets in *network/nbits* form

Allow Access From: □ all server-side private subnets

Allow Access From: □ all other VPN clients

VPN Gateway

Configure VPN Gateway: ○ No ● Yes

Allow client to act as VPN gateway for these client-side subnets: 10.0.0.0/24

List subnets in *network/nbits* form

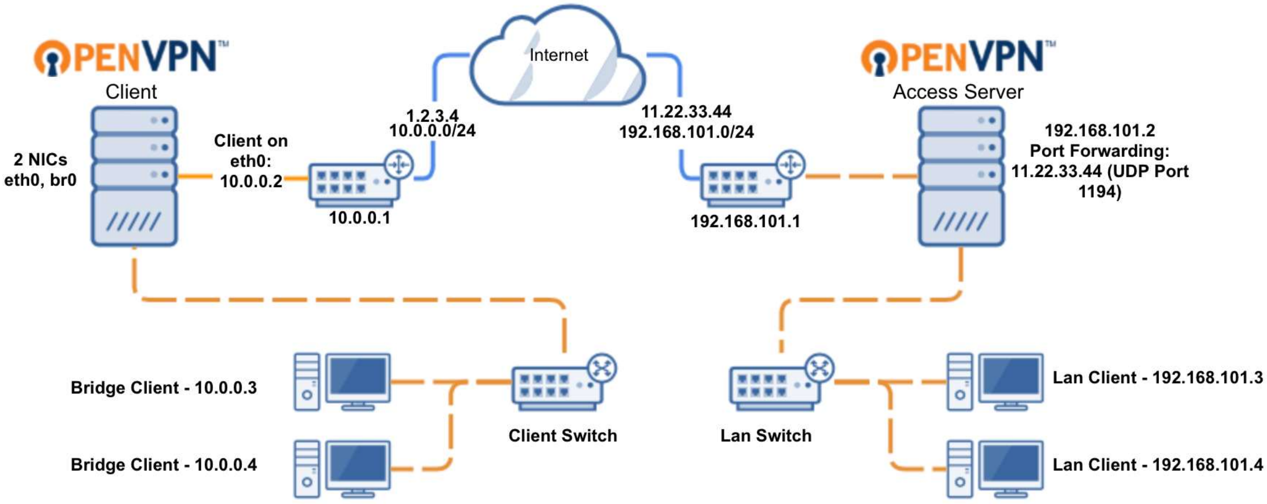
DMZ settings

Configure DMZ IP address: ● No ○ Yes

Click ***Save Settings*** and the ***Update Running Server*** buttons to update your current server's configuration.

Now that the Access Server knows where to forward your site traffic, you will need to make sure the computers on both sites also know where the appropriate traffic should go.
Since both sites' computers use a separate gateway aside from the OpenVPN box itself, static routes will have to be added at these routers to let the routers know where the other site's VPN traffic should go.

Looking at the network diagram we have above again, we have:



The client PCs on the left are using a gateway of ***10.0.0.1***, and the right side clients are using a gateway of ***192.168.101.1***. Our goal is for the left side network (***10.0.0.0/24***) to be able to communicate with the right side network (***192.168.101.0/24***), and vice versa. That being said, at the current stage of this setup, the routers themselves do not know where this traffic should go (since the traffic for the "other side" is handled by the OpenVPN boxes on each respective side, and not the router itself), and will happily drop this traffic (i.e. your site-to-site tunnel will not work).

To prevent this from happening, we must tell the routers that the appropriate "**handlers**" for the "**other side's**" VPN traffic is the "**local OpenVPN box**." (Of course, you will not have to do this if the client PCs on a particular side of the network is already using the OpenVPN "box" as a default gateway).

To do so, use the admin console for your router/firewalls, and add the static routes in this manner:

On the 10.0.0.1 (left side) router:

Subnet Mask: 255.255.255.0
Gateway / Next-hop IP Address: 10.0.0.2 (this is the local side's OpenVPN "box" - i.e. the **OpenVPN Client**)

On the 192.168.101.1 (right-side) router:
Static Route Network: 10.0.0.0 (this is the other side's subnet - i.e. on the left)
Subnet Mask: 255.255.255.0
Gateway / Next-hop IP Address: 192.168.101.2 (this is the local side's OpenVPN "box" - i.e. the **OpenVPN Access Server**)

Once the static routes are setup, you are ready to setup your OpenVPN Client to establish a link to the other site.

Using a SFTP client such as ***Filezilla*** or ***Cyberduck***, upload the ovpn profile you have obtained previously onto the ***Linux OpenVPN client machine***. Upload this to the ***/etc/openvpn/*** folder.

NOTE: If you have a ESXi host capable of running 64-bit operating systems, you can save yourself some time by deploying a preconfigured Debian OpenVPN Client here.

Login to your ***Linux OpenVPN Client*** via ***SSH***. Once logged on:

1) Rename the OpenVPN profile into a ***.conf*** extension by issuing the following commands:
cd /etc/openvpn
mv client.ovpn client.conf

2) Start the OpenVPN profile by restarting the OpenVPN Service, using the ***/etc/init.d/openvpn restart*** command.

3) Verify that the connection is active by issuing a ***ifconfig tun0*** command. If the connection is successful, the ***tun0*** interface should be configured with the IP address assigned by the Access Server software. At this point, your two sites should be able to communicate with each other via the VPN tunnel.