OpenVPN Remote Access Configuration Example

The OpenVPN wizard on pfSense® software is a convenient way to setup a remote access VPN for mobile clients. The wizard configures all of the necessary prerequisites for an OpenVPN remote access server:

- An authentication source (Local, RADIUS server, or LDAP server)
- A certificate authority (CA)
- A server certificate
- An OpenVPN server instance

At the end of the wizard the firewall will have a fully functioning sever, ready to accept connections from users. This server configuration can then be altered as needed.

This document uses an example setup to aide in explaining the options available in the wizard.

See also

[Server Configuration Options](#)

Before Starting The Wizard

Before starting the wizard, plan the design of the VPN.

Determine an IP addressing scheme

The OpenVPN server requires a dedicated subnet for communication between the server and the OpenVPN clients. This is the **Tunnel Network** in the server configuration. The server uses the first address in this subnet for itself to act as a gateway and it allocates IP addresses within this subnet to clients.

When selecting internal subnets for a single location, ideally choose subnets which can be CIDR summarized with other internal subnets. This example uses `10.3.0.0/24` for LAN and `10.3.201.0/24`

for the remote access OpenVPN server. These two networks can be summarized with `10.3.0.0/16`, which makes routing easier to manage.

See also

[CIDR Summarization](#)

Example Network

Figure [OpenVPN Example Remote Access Network](#) shows a depiction of this example deployment.

../_images/diagrams-openvpn-server.png

OpenVPN Example Remote Access Network

OpenVPN Remote Access Server Settings

Remote Access Server	
WAN Address	198.51.100.3
LAN Subnet	10.3.0.0/24
LAN Address	10.3.0.1
Tunnel Net	10.3.201.0/24

OpenVPN Wizard Walkthrough

To start the OpenVPN Remote Access Server Setup wizard:

- Navigate to **VPN > OpenVPN**
- Click the **Wizards** tab

The GUI presents the first step of the wizard automatically

Note

The option for [OpenVPN Data Channel Offload (DCO)](#) is not included in this wizard. To use DCO on this server, run the wizard first then after completing the wizard, edit the server instance and enable the DCO option.

Choose Authentication Type

On the first screen of the wizard, select the authentication backend server type. The choices available for **Type of Server** are *Local User Access*, *LDAP*, and *RADIUS*.

See also

[Authentication Servers](#)

Local User Access

> Manage the users, passwords, and certificates using the [User Manager](#) on this firewall.
>
> Sets the server mode to *Remote Access (SSL/TLS + User Auth)* which requires user authentication as well as per-user certificates.
>
> *Local User Access* easily handles per-user certificates, managed completely in the GUI. This is much more secure, but depending on the number of users which will access the service, may be less convenient than using a central authentication system.

LDAP / RADIUS

> If the network has an existing authentication system already in place, such as Active Directory, pick *LDAP* or *RADIUS* depending on which method that system accepts.
>
> *LDAP* and *RADIUS* both set the server mode to *Remote Access (User Auth)*, which does not require per-user certificates.
>
> Note
>
> The server mode can be adjusted later to require certificates, but administrators must manually create per-user certificates for *LDAP* or *RADIUS* users.

Click fa-angle-double-right **Next** to continue.

For *Local User Access*, the wizard skips the LDAP and RADIUS configuration steps.

For *LDAP* or *RADIUS* the wizard will present appropriate authentication server configuration options next. This example uses *Local User Access*, but this document discusses the other options for completeness.

Choosing an LDAP Server

If the user manager configuration on this firewall contains one or more LDAP servers, the wizard offers these LDAP servers as options it can use for this VPN.

Click fa-angle-double-right **Add new LDAP server** to create a different LDAP server entry.

Click fa-angle-double-right **Next** to continue using the server selected in the **LDAP Servers** list.

If the firewall configuration does not contain any LDAP servers, the wizard skips this step.

See also

[Authentication Servers](#)

Adding an LDAP Server

If the user manager configuration on this firewall does not contain an LDAP server, or if the user chose to create a new LDAP server, the wizard presents a screen to define a new server.

The values for the options on this screen depend on the specific LDAP directory configuration and structure. For guidance, consult the LDAP server administrator, software vendor, or documentation.

Note

The details of LDAP servers are covered in [LDAP Authentication Servers](#).

This document omits some detail since the options are discussed in-depth by that other section.

The wizard offers the following LDAP authentication server parameters:

Name

Descriptive name for this LDAP server, for reference.

Hostname or IP address

The hostname or IP address of the LDAP server.

If the firewall will contact this server using an encrypted method, this value must match the contents of the LDAP server certificate.

Port

The port on which the LDAP server is listening for requests.

The default port is `389` for standard TCP connections and `636` for SSL.

Transport

Sets the method the firewall will use when performing LDAP queries to the server.

Standard TCP

Unencrypted connections using plain TCP.

STARTTLS Encrypted

Connects to the standard TCP port and then attempts to negotiate TLS encryption.

SSL/TLS Encrypted

Secure connections using TLS encryption.

A standard TCP connection is typically sufficient for initial testing, and potentially for local servers or those only accessible over secure connections. If the server is remote or crosses any untrusted network links, an encrypted method is essential. Using an encrypted method is always the best practice, but may not always be viable.

Warning

When the firewall uses an encrypted method to contact the LDAP server, the **Hostname or IP address** above must match a value in the LDAP server certificate.

Peer Certificate Authority

To use SSL/TLS or STARTTLS transports, the firewall must trust the CA of the LDAP server. This can be accomplished by any of the following methods:

- Import the CA into the certificate manager and select it from the list in this option.
- Import the CA into the certificate manager with the **Trust Store** option set, which adds the imported CA into the list of CAs which the firewall trusts globally. Then select *global* from this list.
- If the LDAP server certificate is signed by a globally trusted CA, such as Let's Encrypt, then select *global*.

Search Scope Level

Selects how deep the firewall will search in the LDAP directory, *One Level* or *Entire Subtree*.

In almost all cases, *Entire Subtree* is the correct choice.

Search Scope Base DN

The distinguished name (DN) upon which the firewall bases its search. For example `DC=example,DC=com`.

Authentication Containers

These values specify where the directory stores user data. For example, `CN=Users;DC=example`.

LDAP Bind User DN

If the LDAP server requires authenticated binds when performing queries, this field sets the distinguished name the firewall uses for this bind action.

If this is blank the firewall performs an anonymous bind without credentials.

LDAP Bind Password

The password for authenticated binds. The firewall only uses this value if **LDAP Bind User DN** has a value.

User Naming Attribute

Varies depending on the LDAP directory software and structure.

Typically `cn` for OpenLDAP and Novell eDirectory, and `samAccountName` for Microsoft Active Directory.

Group Naming Attribute

Varies depending on the LDAP directory software and structure, but is most typically `cn`.

Member Naming Attribute

Varies depending on the LDAP directory software and structure.

Typically `member` on OpenLDAP, `memberOf` on Microsoft Active Directory, and `uniqueMember` on Novell eDirectory.

See also

[LDAP Authentication Servers](#) explains the remaining options in detail, and when a server may require them.

Click fa-angle-double-right **Add new server** to continue.

Choosing a RADIUS Server

If the user manager configuration on this firewall contains one or more RADIUS servers, the wizard offers these RADIUS servers as options it can use for this VPN.

Click fa-angle-double-right **Add new RADIUS server** to create a different RADIUS server entry.

Click fa-angle-double-right **Next** to continue using the server selected in the **RADIUS Servers** list.

If the firewall configuration does not contain any RADIUS servers, the wizard skips this step.

See also

Adding a RADIUS Server

If the user manager configuration on this firewall does not contain a RADIUS server, or if the user chose to create a new RADIUS server, the wizard presents a screen to define a new server.

The values for the options on this screen depend on the specific RADIUS configuration and structure. For guidance, consult the RADIUS server administrator, software vendor, or documentation.

Note

The details of RADIUS servers are covered in [RADIUS Authentication Servers](#).

This document omits some detail since the options are discussed in-depth by that other section.

The wizard offers the following RADIUS authentication server parameters:

Name

Descriptive name for this RADIUS server, for reference.

Hostname or IP address

The hostname or IP address of the RADIUS server.

Authentication Port

Port used by the RADIUS server for accepting authentication requests, typically `1812`.

Shared Secret

The password the RADIUS server expects from this firewall when it submits authentication requests (e.g. password on the NAS entry.)

Click fa-angle-double-right **Add new server** to continue.

Choosing a Certificate Authority

If the certificate manager configuration on this firewall contains one or more certificate authorities, the wizard offers these CA entries as options it can use for this VPN.

Click fa-angle-double-right **Add new CA** to create a different certificate authority.

Click fa-angle-double-right **Next** to continue using the certificate authority selected in the **Certificate authority** list.

If the firewall configuration does not contain any CA entries, the wizard skips this step.

See also

[Certificate Management](#)

Creating a Certificate Authority

If the certificate manager configuration on this firewall does not contain a CA, or if the user chose to create a new CA, the wizard presents a screen to define a new CA.

See also

For more information on creating and managing CAs, see [Certificate Authority Management](#).

This document omits some detail since the options are discussed in-depth by that other section.

The firewall uses this entry as a root CA which can sign server and user certificates. Clients can use this CA to validate the server, and the server can use this CA to validate clients. Because this CA is self-signed, only clients which are supplied with a copy of this CA certificate will trust other certificates signed by this CA.

The wizard offers the following CA parameters:

Descriptive Name

`ExampleCoCA`

A name for reference to identify this certificate. This is the same as **Common Name** field for other certificates.

Note

Although this field can technically contain spaces, the best practice is to conform the contents of this field to the format allowed for fully qualified domain names.

Some clients have issues handling entries with spaces properly.

Key Length

`2048`

Size of the CA private key which the wizard will generate.

Larger keys offer increased security but larger keys are generally slower to use.

Lifetime

`3650`

The time, in days, for which this CA will remain valid.

For a self-signed CA such as this, the default of `3650` is acceptable, which is approximately 10 years.

The remaining fields are optional but define additional identifying data for the CA "subject"/distinguished name. For small deployments this may not matter much, but for larger organizations with CA entries at multiple sites, this can help ensure each CA is easily identifiable.

Country Code

`US`

(Optional) Two-letter ISO country code (e.g. US, AU, CA).

ExampleCo is located in the United States which has an ISO country code of `US`.

To locate an appropriate ISO code for other countries, use the [ISO Online Browsing Platform](#) site.

State or Province

`Texas`

(Optional) Full unabbreviated State or Province name (e.g. Texas, Indiana, California).

ExampleCo is located in `Texas`.

City

`Austin`

(Optional) City or other Locality name (e.g. Austin, Indianapolis, Toronto).

ExampleCo headquarters is in `Austin`.

Organization

`ExampleCo`

(Optional) Organization name, often the Company or Group name.

Warning

Do not use any special characters in this field, not even punctuation such as a period or comma.

Click fa-angle-double-right **Add new CA** finish the CA creation process.

Choosing a Server Certificate

If the certificate manager configuration on this firewall contains one or more certificates, the wizard offers these certificate entries as options it can use for this VPN.

Click fa-angle-double-right **Add new Certificate** to create a different certificate.

Click fa-angle-double-right **Next** to continue using the certificate selected in the **Certificate** list.

If the firewall configuration does not contain any certificate entries, the wizard skips this step.

See also

Certificate Management

Adding a Server Certificate

If the certificate manager configuration on this firewall does not contain a certificate, or if the user chose to create a new certificate, the wizard presents a screen to define a new server certificate.

See also

For more information on creating and managing certificates, see Certificate Management.

This document omits some detail since the options are discussed in-depth by that other section.

This server certificate verifies the identity of the server to the clients. The CA set in the previous wizard steps will sign this certificate. In most cases, as with this example, the server certificate uses the same information from the previous step and the wizard pre-fills the form automatically.

Descriptive Name

`vpn.example.com`

This is the common name (CN) field of the server certificate and the firewall also uses this name to reference the certificate.

The best practice is to set this to the fully qualified hostname of the firewall.

Note

Although this field can technically contain spaces, the best practice is to conform the contents of this field to the format allowed for fully qualified domain names.

Some clients have issues handling entries with spaces properly.

Key Length
`2048`

Size of the CA private key which the wizard will generate.

Larger keys offer increased security but larger keys are generally slower to use.

Lifetime
`398`

The time in days that this certificate will be valid. The best practice is to set this to `398` days or less.

Note

Some current operating systems and software limit server certificates to a maximum lifetime of `398` days for security reasons. Clients on these platforms may reject a server certificate with a longer lifetime.

The remaining fields are optional but define additional identifying data for the server certificate "subject"/distinguished name. For small deployments this may not matter much, but for larger organizations with many server certificates, this can help ensure each certificate is easily identifiable.

Country Code
`US`

(Optional) Two-letter ISO country code (e.g. US, AU, CA).

ExampleCo is located in the United States which has an ISO country code of `US`.

To locate an appropriate ISO code for other countries, use the [ISO Online Browsing Platform](#) site.

State or Province

`Texas`

(Optional) Full unabbreviated State or Province name (e.g. Texas, Indiana, California).

ExampleCo is located in `Texas`.

City

`Austin`

(Optional) City or other Locality name (e.g. Austin, Indianapolis, Toronto).

ExampleCo headquarters is in `Austin`.

Organization

`ExampleCo`

(Optional) Organization name, often the Company or Group name.

Warning

Do not use any special characters in this field, not even punctuation such as a period or comma.

Click fa-angle-double-right **Create New Certificate** to continue.

Configuring OpenVPN Server Settings

The options on this step of the wizard configure each aspect of how the OpenVPN server itself behave as well as options the server will pass on to clients.

See also

The options presented here are the same as those in [Server Configuration Options](#). Refer to that section for details.

Because the options are covered in detail in that section, this document only mentions the settings used by this example.

General OpenVPN Server Information

These options control how the OpenVPN instance operates.

Interface
: *WAN*

Protocol
: *UDP on IPv4 Only*

Local Port
: `1194`

    The wizard suggests the first unused port number starting with port `1194`. If there is an existing OpenVPN server on that port, use a different port number.

Description
: `ExampleCo Mobile VPN Clients`

Cryptographic Settings

These options control how the server encrypts and authenticates traffic in the tunnel.

TLS Authentication
: Check **Enable authentication of TLS packets**

    Using TLS authentication is the best practice.

Generate TLS Key
: Check **Automatically generate a shared TLS authentication key**

TLS Shared Key
: Blank

    The wizard disables this field when **Automatically generate a shared TLS authentication key** is checked.

DH Parameters Length
: *2048*

    This value is a good balance of speed and strength.

Data Encryption Negotiation

Checked

This allows the server to automatically negotiate encryption settings with clients.

Note

Disabling this option is deprecated, but still present on this version for compatibility.

Data Encryption Algorithms

AES-256-GCM, *AES-128-GCM*, and *CHACHA20-POLY1305*

The best practice is to use the default suggested values as noted above.

Fallback Data Encryption Algorithm

AES-256-CBC

This algorithm is used when negotiation fails, for example with a client that is too old to support negotiation.

Auth Digest Algorithm

SHA256 (256-bit)

Tunnel Settings

These options control how the server routes traffic from remote clients.

Tunnel Network

`10.3.201.0/24`

This is the tunnel network from the table at the start of this example (OpenVPN Remote Access Server Settings).

Redirect Gateway

Unchecked

For this example, The VPN will only carry traffic destined for subnets at the main office.

Local Network

`10.3.0.0/24`

This is the server-side LAN subnet from the table at the start of this example ([OpenVPN Remote Access Server Settings](#)).

Concurrent Connections

> Blank
>
> This example does not limit the number of clients which can connect at the same time.

Allow Compression

> *Refuse any non-stub compression (Most secure)*
>
> The best practice is to disable compression for security reasons.

Compression

> *Disable Compression [Omit Preference]*
>
> The best practice is to disable compression for security reasons.

Type-of-Service

> *Unchecked*
>
> There is no traffic on this example VPN which requires prioritization/QoS.

Inter-Client Communication

> *Unchecked*
>
> The clients on this VPN have no need to connect to other VPN client hosts.

Duplicate Connections

> *Unchecked*
>
> This example uses unique certificates for every client and does not allow multiple connections per client.

Client Settings

These options control specific settings the server pushes to clients when they establish a connection.

Dynamic IP

Checked

> The clients connect from all over the country and unknown mobile networks and their IP addresses are likely to change without notice.

Topology
> *Subnet*

> The method the server uses to assign IP addresses to clients.

DNS Default Domain
> `example.com`

> The domain name used by ExampleCo.

DNS Servers
> `10.3.0.5`

> A list of internal DNS servers. ExampleCo has a Windows Active Directory Domain Controller which is configured to act as a DNS server at `10.3.0.5`.

NTP Servers
> `10.3.0.6`

> A dedicated local NTP server exists at `10.3.0.6`.

Advanced
> Blank

> At this time no additional tweaks are necessary.

Click fa-angle-double-right **Next** to continue.

Firewall Rule Configuration

By default the firewall blocks all traffic from connecting to VPNs or passing over VPN tunnels. This step of the wizard adds firewall rules automatically to allow traffic to connect to the VPN and also so connected clients can pass traffic over the VPN.

Traffic from clients to server

Checked

When checked, the wizard adds a firewall rule on the chosen interface outside of the tunnel where the server is listening (e.g. *WAN*) which allows VPN clients to connect. The rule created by this option allows all clients from any source IP address to connect by default.

Since clients in this example are connecting from all over the country, the rule created by the wizard for this option is ideal.

Tip

To allow connections from a limited set of IP addresses or subnets, either make a custom rule or check this box and alter the rule it creates.

Traffic from clients through VPN tunnel

Checked

This setting allows all traffic to cross inside the OpenVPN tunnel. This is desirable for this example.

Click fa-angle-double-right **Next** to continue.

Finishing the Wizard

Click fa-angle-double-right **Finish** to complete the wizard.

At this point, the firewall now contains a full OpenVPN remote access server configuration which is ready for client connections.

From here, the next steps are to add users and configure client devices.

If this setup requires adjustments to the automatically generated firewall rules, make them now.

Verifying the Setup

Look at firewall rules (**WAN** and **OpenVPN** tabs)

- **WAN** tab rule should pass from any to the *OpenVPN* port on the *WAN address*
  ../_images/openvpn_ra-wanrule.png
- **OpenVPN** tab rule should allow all traffic from any/to any

../_images/openvpn_ra-ovpnrule.png

Adjustments

Numerous settings are not present in the wizard but might be a better fit for certain deployments than the defaults chosen by the wizard.

Server Mode

The OpenVPN **Server Mode** allows selecting a choice between requiring Certificates, User Authentication, or both. The wizard defaults to *Remote Access (SSL/TLS + User Auth)* when using local users and *Remote Access (User Auth)* for RADIUS and LDAP. The possible values for this choice and their advantages are:

Remote Access (SSL/TLS + User Auth)

- Requires both certificates **and** username/password
- Each user has a unique client configuration which includes their personal certificate and key
- Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know)

Remote Access (SSL/TLS)

- Certificates only, no authentication
- Each user has a unique client configuration which includes their personal certificate and key
- Useful if clients should not be prompted to enter a username and password
- Less secure as it relies only on something the user has (TLS key and certificate)

Remote Access (User Auth)

- Authentication only, no certificates
- Useful if the clients cannot have individual certificates
- Commonly used for external authentication (RADIUS, LDAP)
- All clients can use the same exported client configuration and/or software package
- Less secure as it relies on a shared TLS key plus only something the user knows (Username/password)

OpenVPN Data Channel Offload (DCO)

[OpenVPN Data Channel Offload (DCO)](#), a pfSense® Plus exclusive feature, can potentially increase performance of OpenVPN well beyond the capabilities of traditional OpenVPN connections.

> **❝ Note**
>
> OpenVPN DCO is generally stable but still under development.
>
> OpenVPN DCO has been successful in many scenarios in lab and production environments, but there is still a small potential for instability or undesirable behavior.
>
> Some OpenVPN features and use cases are not compatible with DCO. See [Limitations](#) for a list of known DCO limitations.
>
> If a problem occurs with DCO, start a thread on the [Netgate Forum](#) to discuss and diagnose the issue.

Certificate Revocation

Compromised certificates can be revoked by a Certificate Revocation List (CRL). CRL entries are managed at **System > Cert Manager** on the **Certificate Revocation** tab. Create a new CRL, add the certificate to it, and then select that CRL on the OpenVPN server settings.

> See also: [Certificate Revocation List Management](#)

Adding a User with a Certificate

If the server mode includes local user authentication, a user must be exist in the user manager for each client which will connect to the VPN.

See also

This is a simplified version of the process. For more detail, see:

- [Adding OpenVPN Remote Access Users](#)
- [Manage Local Users](#)
- [User Certificates](#)

- Navigate to **System > User Manager**
- Click fa-plus To add a user
- Fill in the settings as follows:
  Username
    The username for this client.
  Password/Confirm password
    The password for this client.
  Click to create a user certificate
    Checked
  Descriptive Name
    Same value as the **Username**
  Certificate Authority
    The CA used by the OpenVPN server.
  ../_images/openvpn_ra-usercert.png
- Click **Save**

OpenVPN Client Export Package

The OpenVPN Client Export Package can export client configurations formatted for a wide variety of platforms. It can also export a pre-packaged Windows installer executable which includes the configuration bundled inside for a painless client installation.

See also

Revision #1
Created 19 August 2023 18:56:06
Updated 19 January 2024 18:19:58