Configuring OpenVPN on pfSense

Configuring OpenVPN on pfSense

Posted by Glenn on Dec 29, 2013 in Networking |

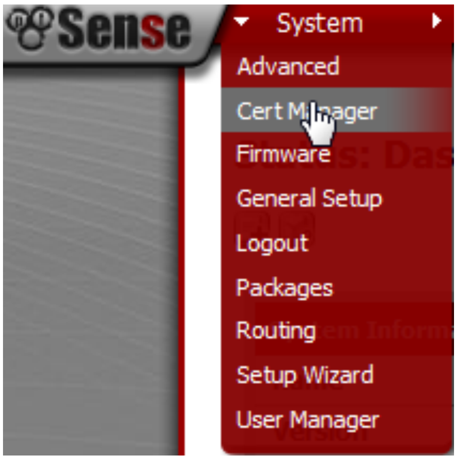
0 comments

In this article I will go through the configuration of OpenVPN on the pfSense platform. I have talked about the initial configuration of pfSense in this previous article and if you are not familiar with the platform then you can check that out to get you up and running. Let's go ahead and start by talking about VPNs first and then we will move to the configuration.

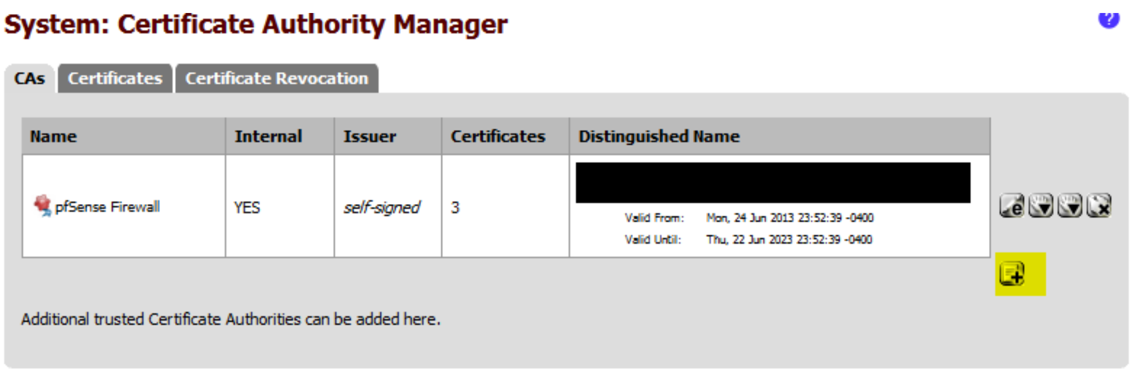
A VPN(virtual private network) allows us to connect directly to our home private network over the internet. This means that if we are in a remote location and want to have access to services hosted within our private network then we can use a VPN to do so. VPNs are used because private networks(10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are not routed in the public internet as these are reserved for private uses. A VPN gives us the ability to extend the private networks by creating a tunnel between the client in a remote location and the server in your private network. This means that once the session is up that the remote client will be able to access all the resources located within your private home network.

VPNs come in many flavors and you have different types. pfSense supports L2TP, PPTP, IPsec, and OpenVPN. You might be wondering why use OpenVPN and not the others. OpenVPN is open source and well maintained by the community which means that you can be safe in knowing that if there is a vulnerability found that it will get patched quickly. When it comes to performance OpenVPN works great on high latency connections and is capable of compression should you be limited on bandwidth on the client or server-side. With regards to authentication OpenVPN supports LDAP, Radius, and local database which makes it flexible in integrating with different types of environment. The authentication is solid because you can pair regular username and password with certificates for higher security. Encryption in OpenVPN is provided via OpenSSL which is an open source implementation of the SSL/TLS protocols and allows us to use some very strong cryptographic algorithms which can be hardware accelerated for better performance. When it comes to the networking side of things it can run over TCP or UDP depending if you want reliability or not but it will be slower should you decide on TCP. OpenVPN supports both IPv4 and IPv6 and is capable of creating a tunnel through a proxy, networks using NAT, and getting through firewalls. Overall OpenVPN is very solid compared to the other solutions which lack in many areas.

Let’s get started by configuring a certificate authority in pfSense. The certificate authority or CA will sign the certificates that we will be creating for the server and client side when we configure OpenVPN. You can access the certificate configuration by going over to System–>Cert Manager.



Under the CAs tab you might already have a CA created if you followed one of my previous articles as we needed to created one in order to sign an internal certificate to be used for securing the pfSense web interface.

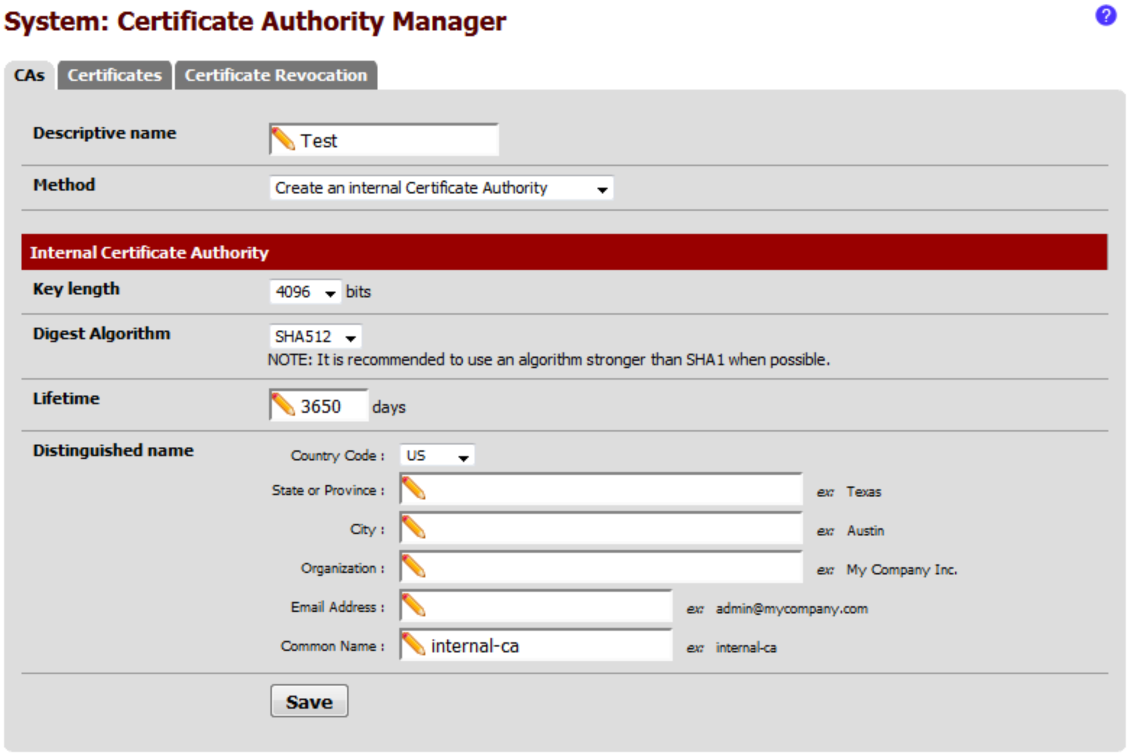


System: Certificate Authority Manager

Name	Internal	Issuer	Certificates	Distinguished Name
pfSense Firewall	YES	*self-signed*	3	[redacted] Valid From: Mon, 24 Jun 2013 23:52:39 -0400 Valid Until: Thu, 22 Jun 2023 23:52:39 -0400

Additional trusted Certificate Authorities can be added here.

If you do not have one here than you should create a CA and secure your pfSense web interface ASAP to prevent from snooping should you have it set to be accessible from the internet. Creating a CA is simple and is done by hitting the plus symbol on the right hand side. The form that you fill out should be self-explanatory.



System: Certificate Authority Manager

Descriptive name: Test

Method: Create an internal Certificate Authority

Internal Certificate Authority

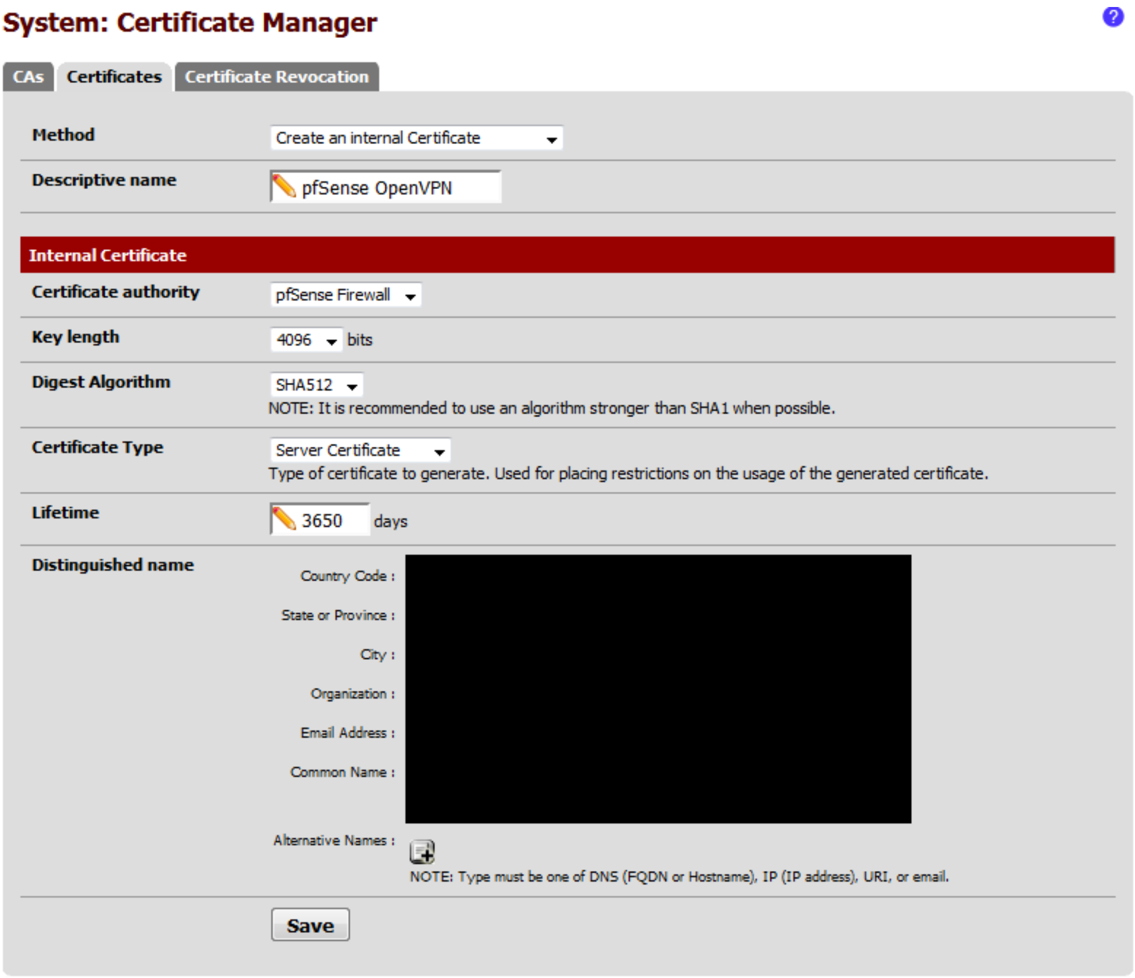
Key length: 4096 bits

Digest Algorithm: SHA512
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime: 3650 days

Distinguished name
Country Code : US
State or Province : ex: Texas
City : ex: Austin
Organization : ex: My Company Inc.
Email Address : ex: admin@mycompany.com
Common Name : internal-ca ex: internal-ca

After you finished setting up the CA the next step is to create some certificates that the recently created CA will sign for us. Since these are self-signed certificates most browsers will give you a warning if you try accessing a web site that is using them, e.g. the pfSense web GUI if you are creating a certificate to secure it. In a similar manner you want to hit the plus sign to create a certificate and go through the form. See below for the settings that I used for my OpenVPN server certificate.



System: Certificate Manager

Method: Create an internal Certificate

Descriptive name: pfSense OpenVPN

Internal Certificate

Certificate authority: pfSense Firewall

Key length: 4096 bits

Digest Algorithm: SHA512
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

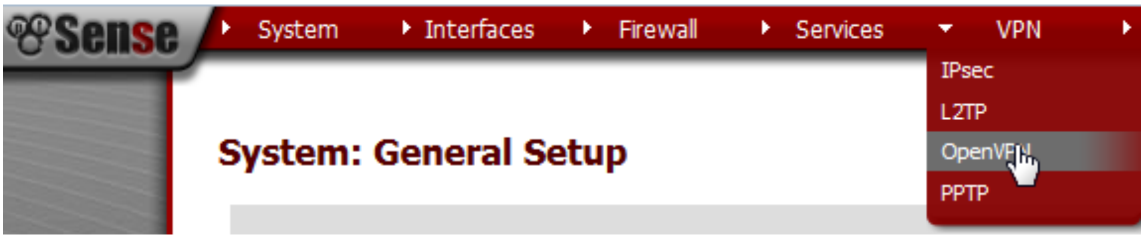
Certificate Type: Server Certificate
Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.

Lifetime: 3650 days

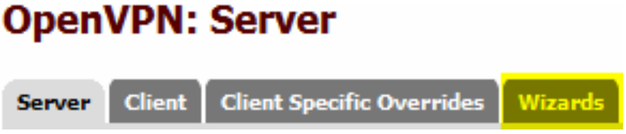
Distinguished name
Country Code :
State or Province :
City :
Organization :
Email Address :
Common Name :
[redacted]

Alternative Names :
NOTE: Type must be one of DNS (FQDN or Hostname), IP (IP address), URI, or email.

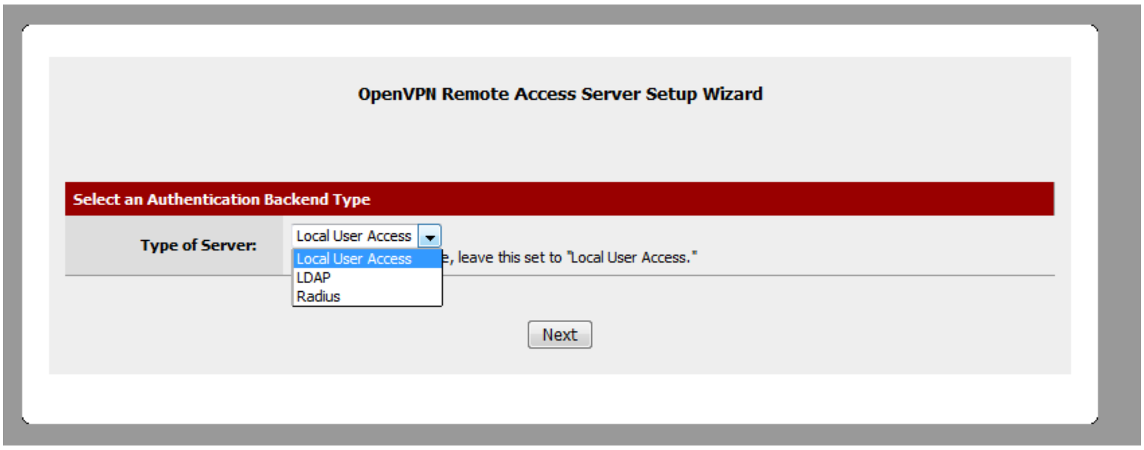
Now that we have all the components in place we can configure OpenVPN. Head over to VPN–>OpenVPN.



Go ahead and select “Wizards” from the tab at the top which will guide us step by step to configure OpenVPN.



The step by step guide will first ask you the type of authentication backend that you are using. In our case we will select the local user access database provided by pfSense. Of course, if you do have an internal LDAP or Radius server that you want to use then you can select either of those options.

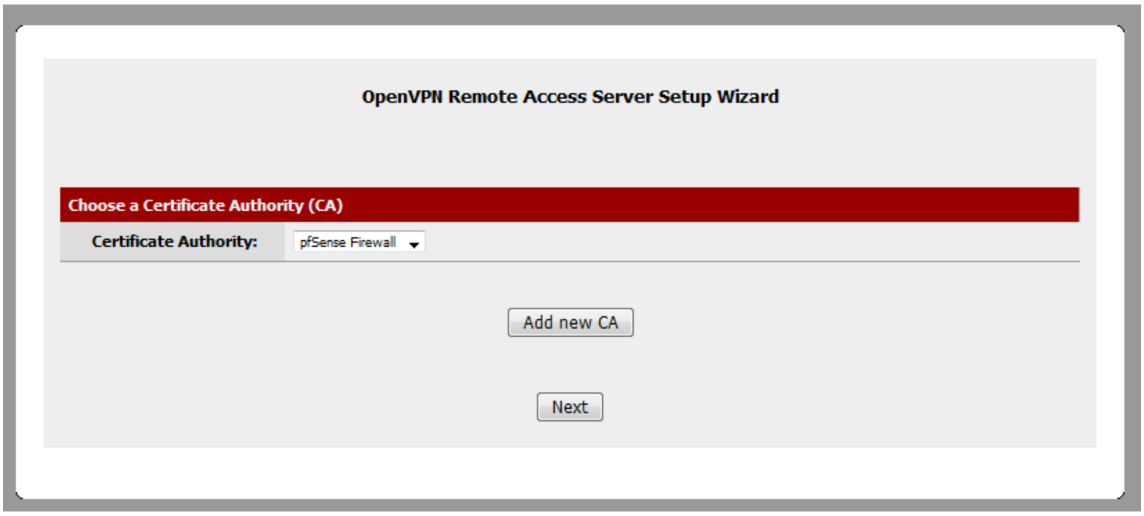

OpenVPN Remote Access Server Setup Wizard

Select an Authentication Backend Type

Type of Server: Local User Access

e, leave this set to "Local User Access."

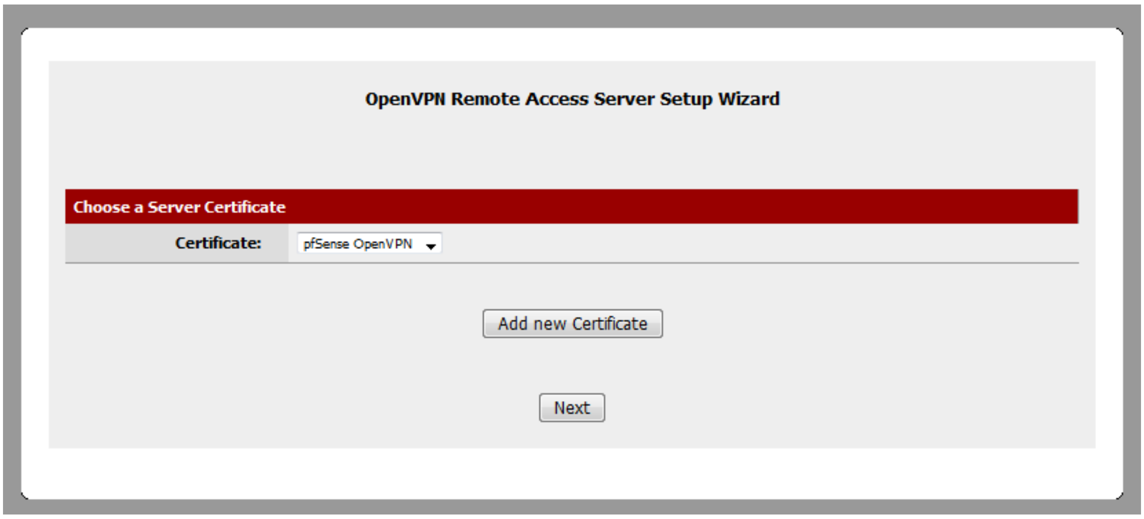
In the next step we will be selecting the CA that we created at the beginning of this article.


OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority: pfSense Firewall

Following is the Server Certificate that we will be using which is the Certificate that we recently created.


OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: pfSense OpenVPN

In the next page we will start selecting several different configuration options. The first three options involve the interface where we will listening for connections, the protocol, and port number. You should select the WAN interface where OpenVPN will bind to if you want to be able to access your network from the outside. The protocol should be UDP unless you have a specific reason for using TCP. The port can be changed or you can use the default OpenVPN port of 1194 where it listens on.

The next sections deals with the cryptographic settings. In here we will specify to use TLS authentication and have it generate a shared TLS authentication key which will give us another layer of security. See below for the explanation provided by the OpenVPN documentation.

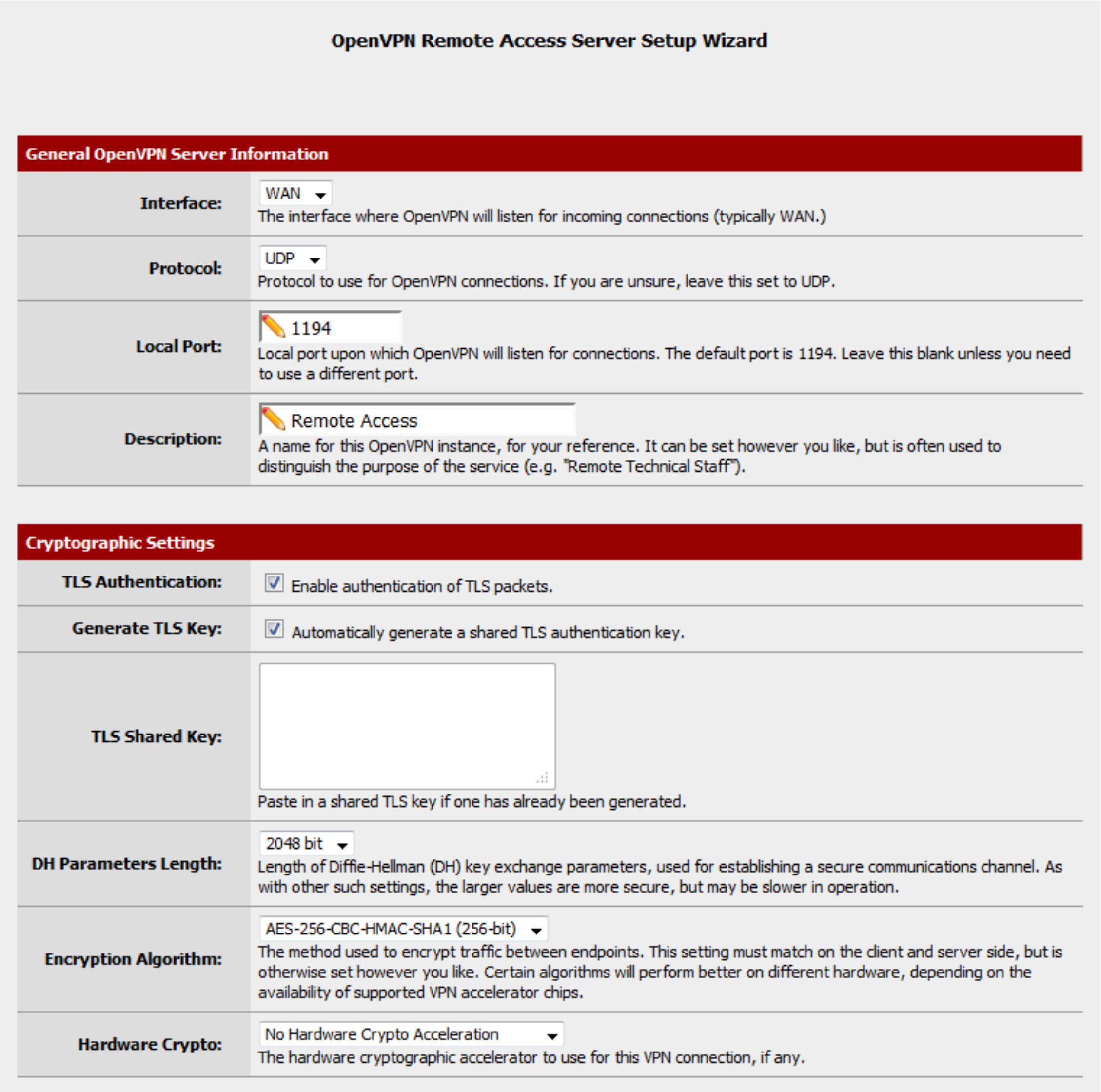
The tls-auth directive adds an additional HMAC signature to all SSL/TLS handshake packets for integrity verification. Any UDP packet not bearing the correct HMAC signature can be dropped without further processing. The tls-auth HMAC signature provides an additional level of security above and beyond that provided by SSL/TLS. It can protect against:

- DoS attacks or port flooding on the OpenVPN UDP port.
- Port scanning to determine which server UDP ports are in a listening state.
- Buffer overflow vulnerabilities in the SSL/TLS implementation.
- SSL/TLS handshake initiations from unauthorized machines (while such handshakes would ultimately fail to authenticate, tls-auth can cut them off at a much earlier point).

Using tls-auth requires that you generate a shared-secret key that is used in addition to the standard RSA certificate/key.

The DH parameter length used for public key cryptography should NOT be set to 1024 or lower. There is a lot of research that shows that 1024 bit keys can be brute force relatively quickly and RSA is recommending that all websites upgrade to 2048 bit keys by the end of this year.

At the bottom you have the option of selecting an encryption algorithm and whether your hardware can do crypto acceleration.



OpenVPN Remote Access Server Setup Wizard

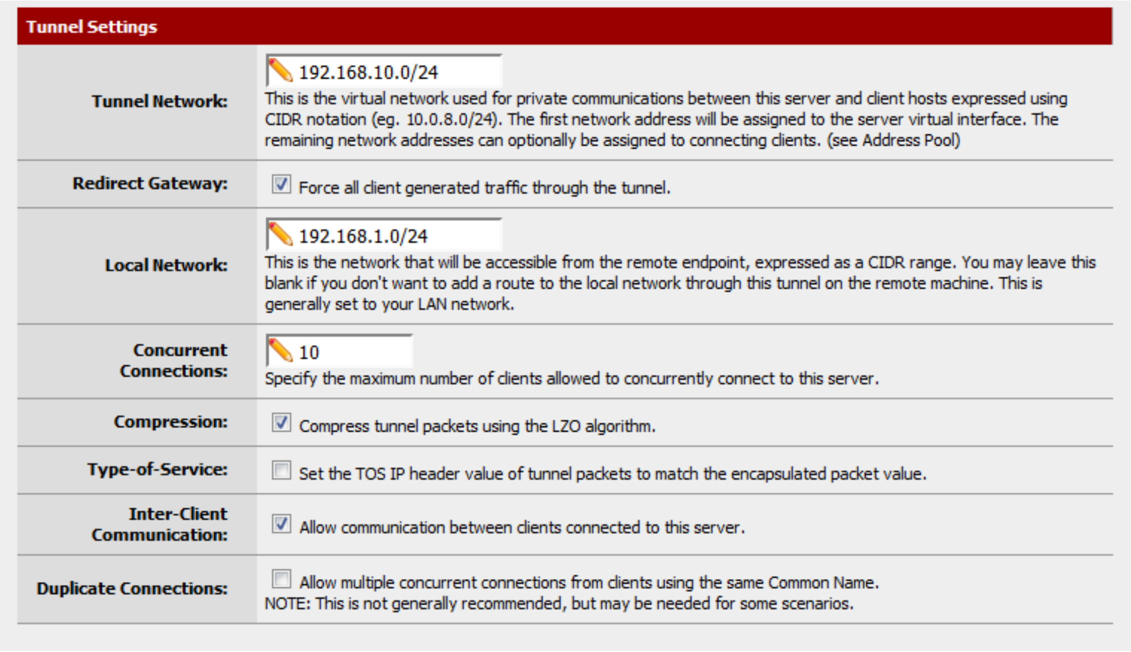
General OpenVPN Server Information

Interface:	WAN ▾ The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	UDP ▾ Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this blank unless you need to use a different port.
Description:	Remote Access A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").

Cryptographic Settings

TLS Authentication:	☑ Enable authentication of TLS packets.
Generate TLS Key:	☑ Automatically generate a shared TLS authentication key.
TLS Shared Key:	Paste in a shared TLS key if one has already been generated.
DH Parameters Length:	2048 bit ▾ Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.
Encryption Algorithm:	AES-256-CBC-HMAC-SHA1 (256-bit) ▾ The method used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.
Hardware Crypto:	No Hardware Crypto Acceleration ▾ The hardware cryptographic accelerator to use for this VPN connection, if any.

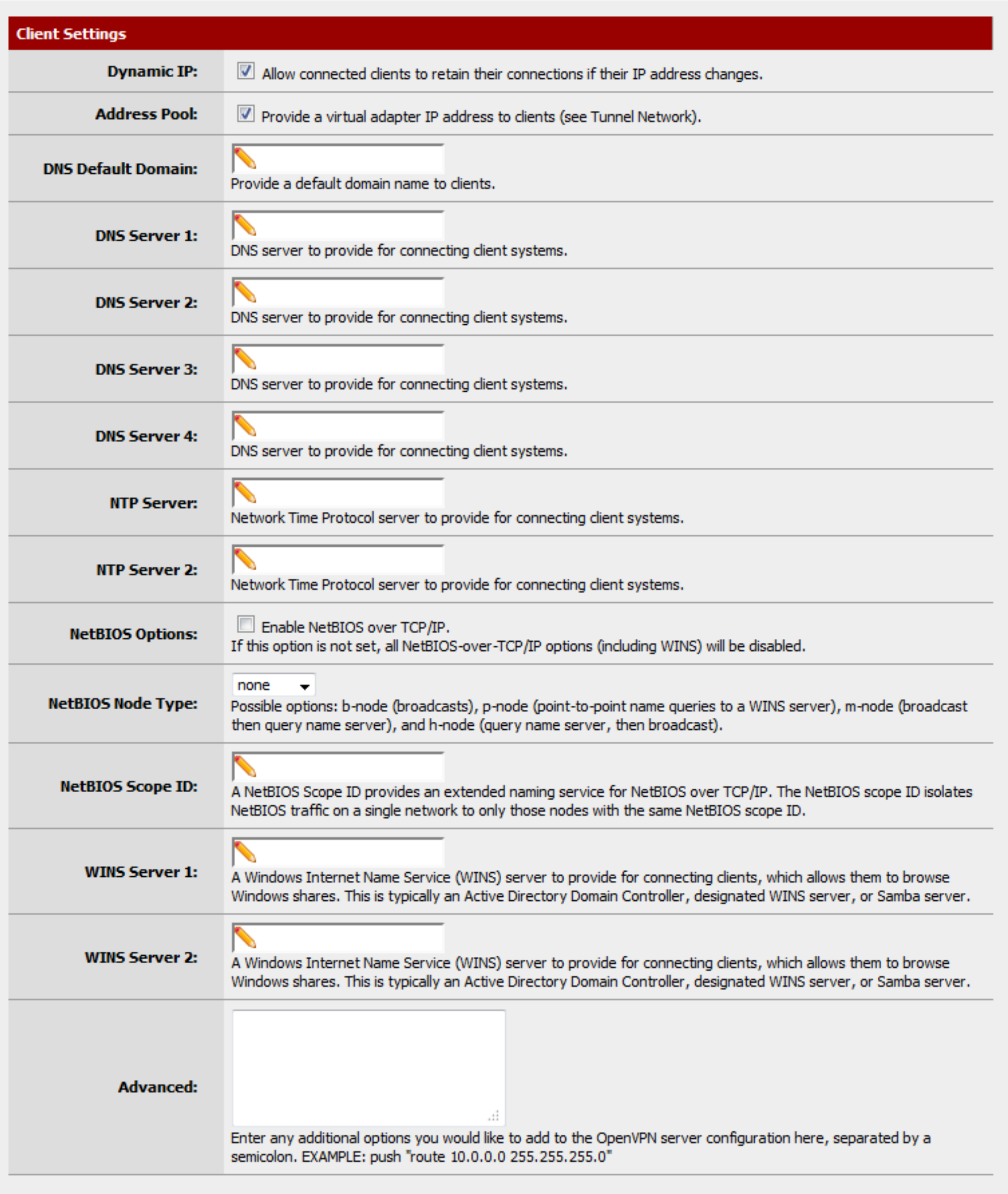
Moving onto the Tunnel settings we have the option of specifying the tunnel network which is the network that our clients connecting to the VPN will be assigned an address from. You can specify whether all traffic should be redirected through the tunnel and the local network that clients connecting from the outside can access. Near the middle we can specify the maximum number of concurrent sessions and whether we want to use compression for the data traversing the tunnel. At the bottom we have TOS fields used for QOS(quality of service), whether we want to allow communication between the clients tunneling in, and if duplicate connections should be allowed.



Tunnel Settings

Tunnel Network:	192.168.10.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	☑ Force all client generated traffic through the tunnel.
Local Network:	192.168.1.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Concurrent Connections:	10 Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	☑ Compress tunnel packets using the LZO algorithm.
Type-of-Service:	□ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-Client Communication:	☑ Allow communication between clients connected to this server.
Duplicate Connections:	□ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

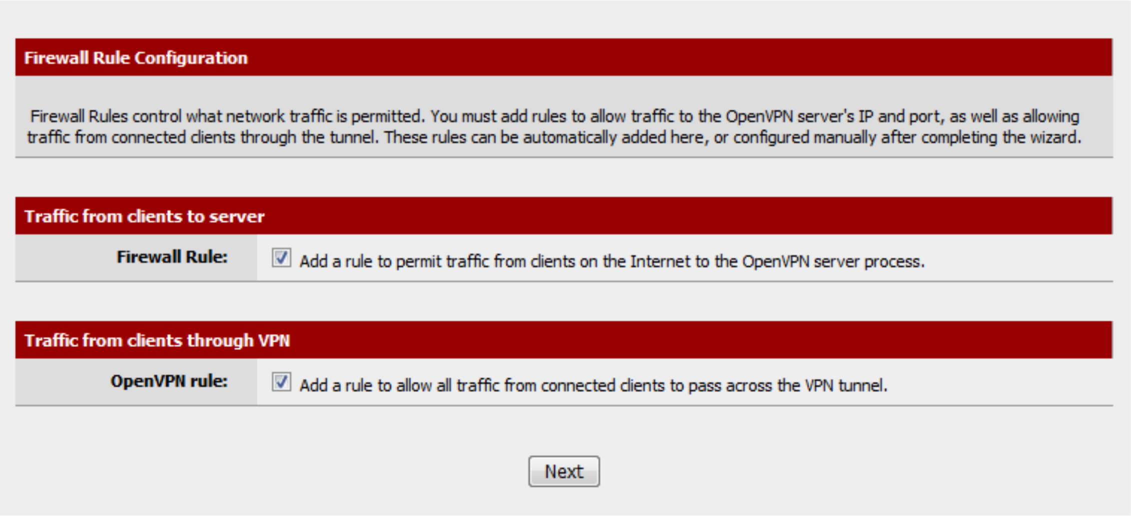
In the client settings we can specify if we want to allow clients to retain their connection should their IP address change. The second option will assign the clients an IP address from the tunnel network we configured at the top. You can configure the other options below if you want to assign certain other parameters to connecting clients.



Client Settings

Dynamic IP:	☑ Allow connected clients to retain their connections if their IP address changes.
Address Pool:	☑ Provide a virtual adapter IP address to clients (see Tunnel Network).
DNS Default Domain:	Provide a default domain name to clients.
DNS Server 1:	DNS server to provide for connecting client systems.
DNS Server 2:	DNS server to provide for connecting client systems.
DNS Server 3:	DNS server to provide for connecting client systems.
DNS Server 4:	DNS server to provide for connecting client systems.
NTP Server:	Network Time Protocol server to provide for connecting client systems.
NTP Server 2:	Network Time Protocol server to provide for connecting client systems.
NetBIOS Options:	□ Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type:	none Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID:	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1:	A Windows Internet Name Service (WINS) server to provide for connecting clients, which allows them to browse Windows shares. This is typically an Active Directory Domain Controller, designated WINS server, or Samba server.
WINS Server 2:	A Windows Internet Name Service (WINS) server to provide for connecting clients, which allows them to browse Windows shares. This is typically an Active Directory Domain Controller, designated WINS server, or Samba server.
Advanced:	Enter any additional options you would like to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"

After hitting next, we are presented with adding firewall rules. The rules are needed so that a connection can be established. Go ahead and check both boxes before finalizing.



Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

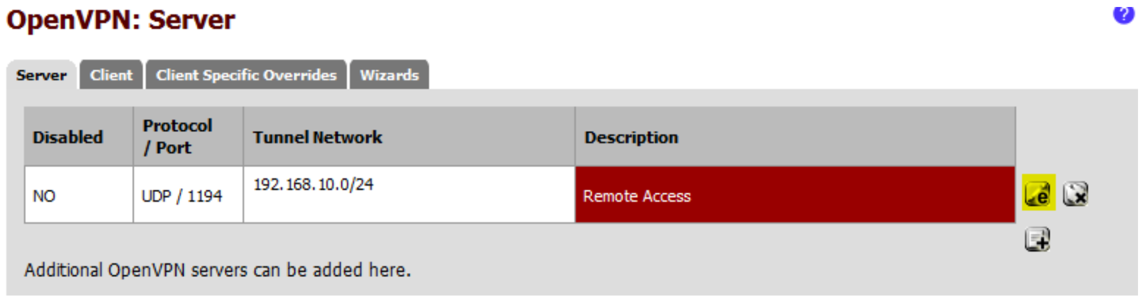
Traffic from clients to server

Firewall Rule: ☑ Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.

Traffic from clients through VPN

OpenVPN rule: ☑ Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.

Once you are done you should see an entry under the server tab of OpenVPN.

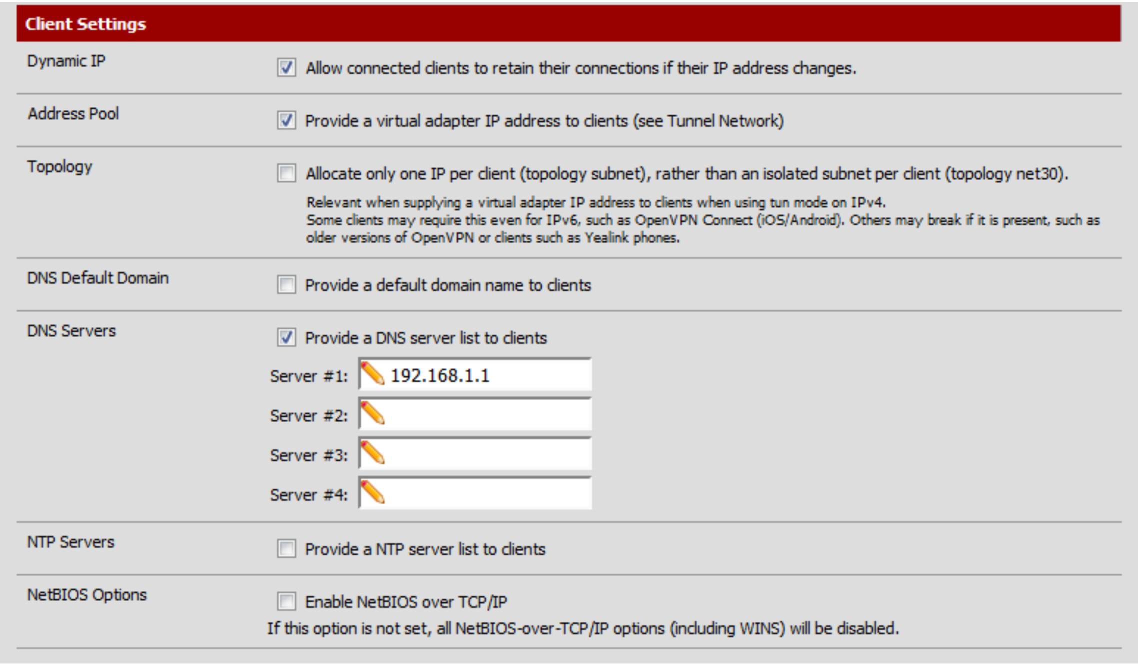


OpenVPN: Server

Disabled	Protocol / Port	Tunnel Network	Description
NO	UDP / 1194	192.168.10.0/24	Remote Access

Additional OpenVPN servers can be added here.

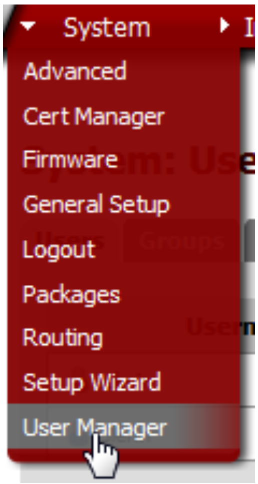
I actually did an edit on the previous entry above and configured the DNS server to point to my default gateway which is my pfSense box since it is configured as a DNS forwarder.



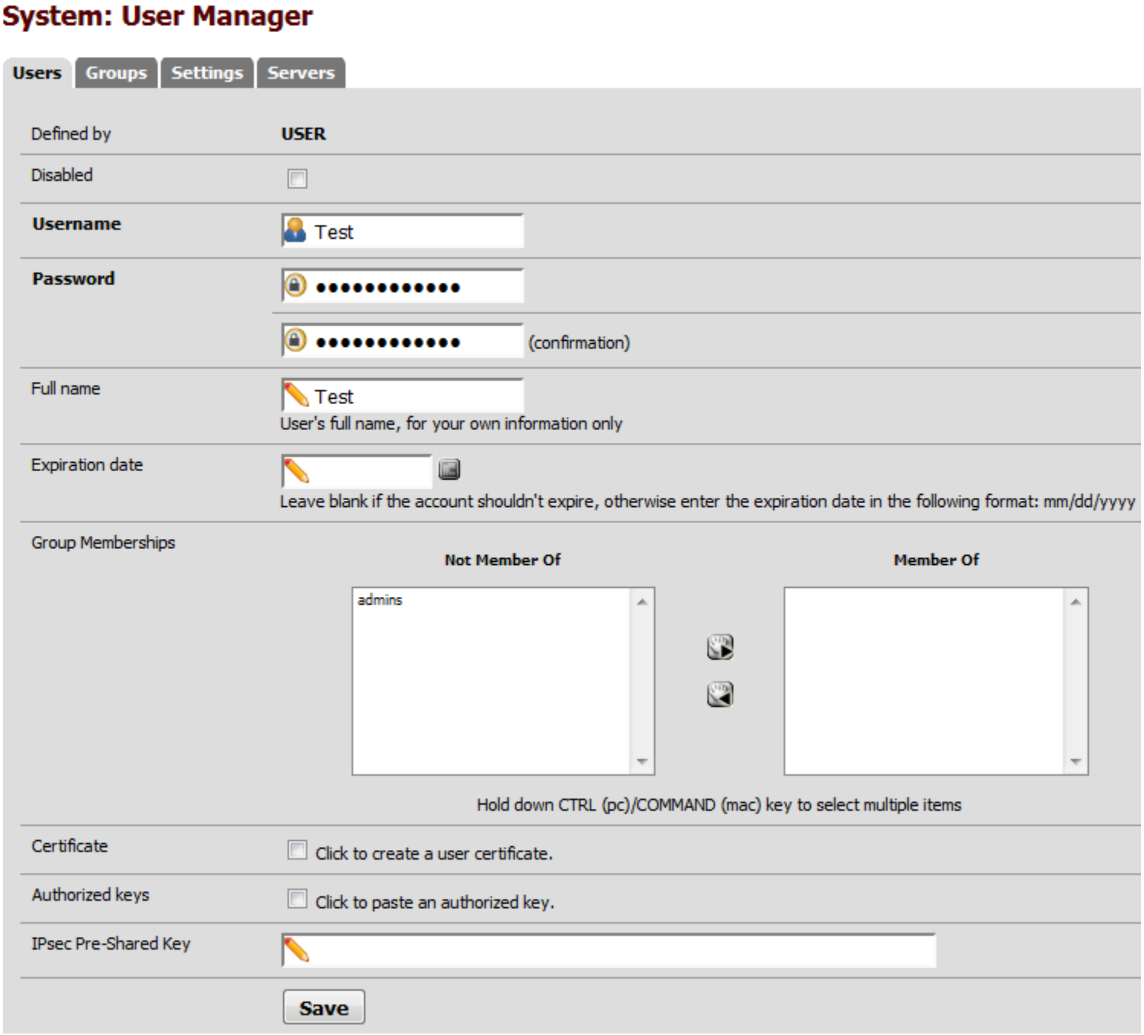
Client Settings

Dynamic IP	☑ Allow connected clients to retain their connections if their IP address changes.
Address Pool	☑ Provide a virtual adapter IP address to clients (see Tunnel Network)
Topology	☐ Allocate only one IP per client (topology subnet), rather than an isolated subnet per client (topology net30). Relevant when supplying a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this even for IPv6, such as OpenVPN Connect (iOS/Android). Others may break if it is present, such as older versions of OpenVPN or clients such as Yealink phones.
DNS Default Domain	☐ Provide a default domain name to clients
DNS Servers	☑ Provide a DNS server list to clients Server #1: 192.168.1.1 Server #2: Server #3: Server #4:
NTP Servers	☐ Provide a NTP server list to clients
NetBIOS Options	☐ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

The next step is to start creating user accounts that we will use during the authentication process. Creating user accounts is done over at System–>User Manager under the users tab.



Go ahead and hit the plus sign to create a new user and fill out the form. Everything here should be self-explanatory.

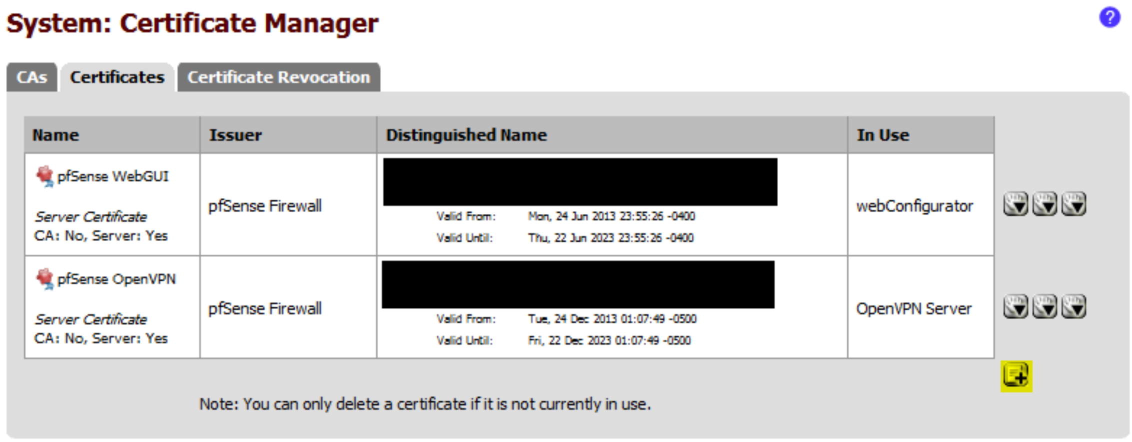


System: User Manager

Defined by	USER
Disabled	□
Username	Test
Password	●●●●●●●●●●●●
	●●●●●●●●●●●● (confirmation)
Full name	Test User's full name, for your own information only
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy
Group Memberships	Not Member Of: admins Member Of: Hold down CTRL (pc)/COMMAND (mac) key to select multiple items
Certificate	□ Click to create a user certificate.
Authorized keys	□ Click to paste an authorized key.
IPsec Pre-Shared Key	
	Save

;

Once the account has been created, we need to create a user certificate for the account. We will be going back to System–>Cert Manager and under the certificates tab create a new certificate.

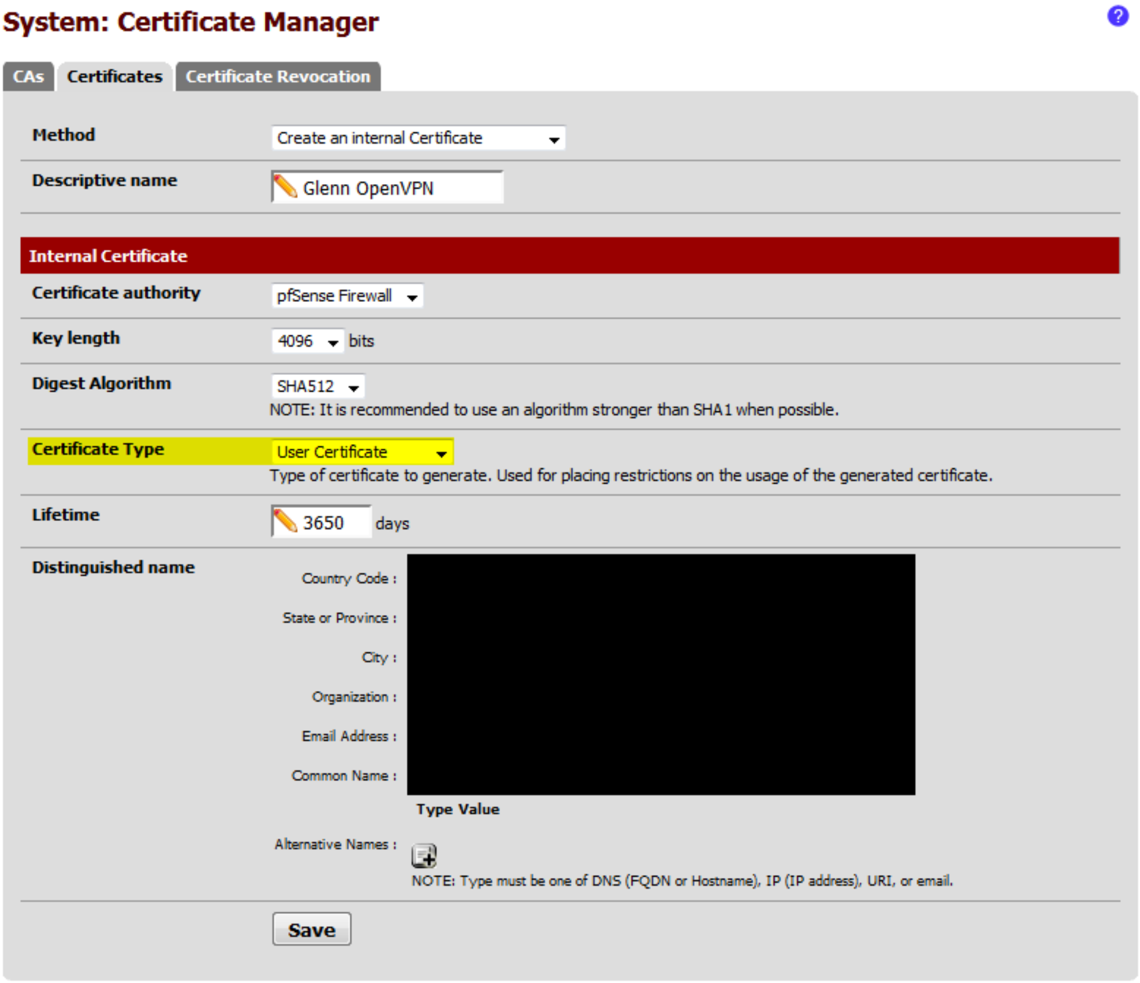


System: Certificate Manager

Name	Issuer	Distinguished Name	In Use
pfSense WebGUI *Server Certificate* CA: No, Server: Yes	pfSense Firewall	[redacted] Valid From: Mon, 24 Jun 2013 23:55:26 -0400 Valid Until: Thu, 22 Jun 2023 23:55:26 -0400	webConfigurator
pfSense OpenVPN *Server Certificate* CA: No, Server: Yes	pfSense Firewall	[redacted] Valid From: Tue, 24 Dec 2013 01:07:49 -0500 Valid Until: Fri, 22 Dec 2023 01:07:49 -0500	OpenVPN Server

Note: You can only delete a certificate if it is not currently in use.

Hit the plus sign to start the creation process. Make sure to select “User Certificate” from the dropdown as you are creating the certificate.



System: Certificate Manager

Method	Create an internal Certificate
Descriptive name	Glenn OpenVPN

Internal Certificate

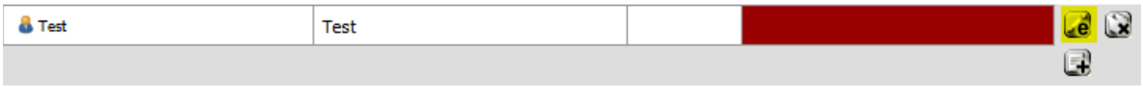
Certificate authority	pfSense Firewall
Key length	4096 bits
Digest Algorithm	SHA512 NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Certificate Type	User Certificate Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.
Lifetime	3650 days
Distinguished name	Country Code : State or Province : City : Organization : Email Address : Common Name : [redacted]

Type Value

Alternative Names :

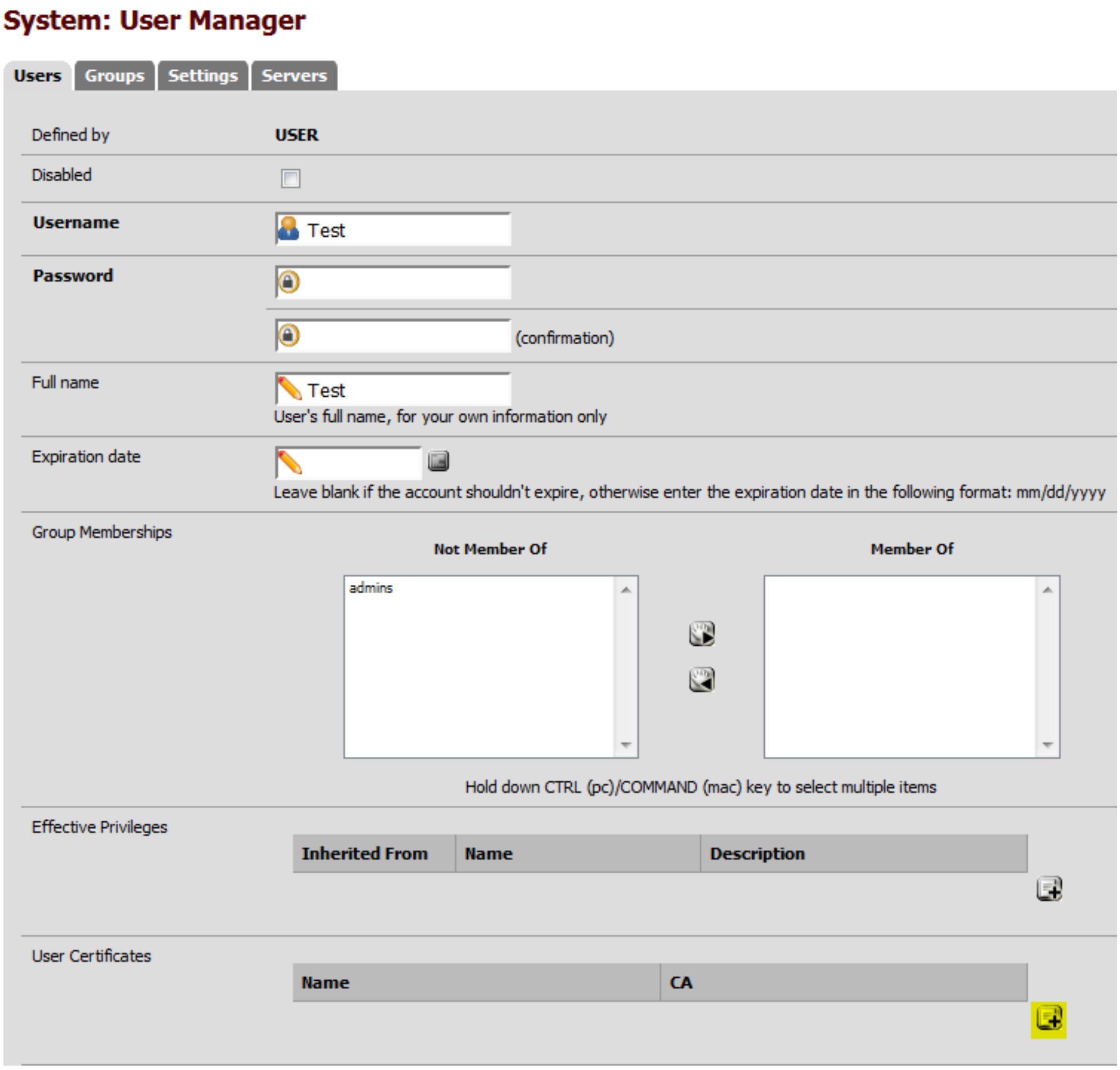
NOTE: Type must be one of DNS (FQDN or Hostname), IP (IP address), URI, or email.

Once the certificate is created, we will go back to the user account that we made and modify it.



Test	Test		[redacted]

We will assign the certificate that we just created to the user account.



System: User Manager

Defined by	USER
Disabled	□
Username	Test
Password	
	(confirmation)
Full name	Test User's full name, for your own information only
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy
Group Memberships	Not Member Of: admins Member Of: Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

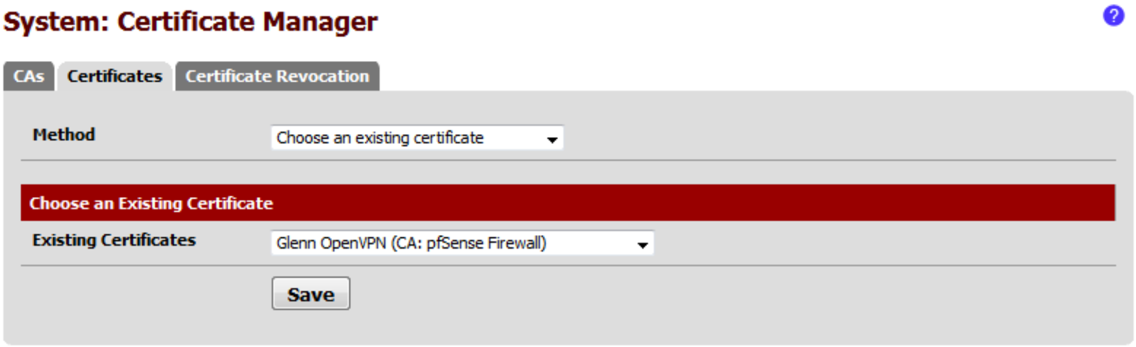
Effective Privileges

Inherited From	Name	Description

User Certificates

Name	CA

From the drop down list select the user certificate that we recently created.



System: Certificate Manager

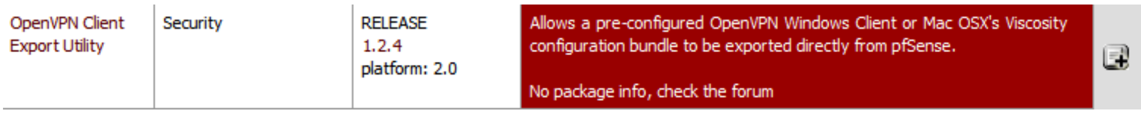
Method	Choose an existing certificate

Choose an Existing Certificate

Existing Certificates	Glenn OpenVPN (CA: pfSense Firewall)

We are almost done with the configuration and there are only a couple of small things left to do. Before we move onto the client configuration we need to export the keys and certificates from pfSense so that our clients can use them. This process is made easy by installing the OpenVPN Client Export Utility from System–

>Packages.



OpenVPN Client Export Utility	Security	RELEASE 1.2.4 platform: 2.0	Allows a pre-configured OpenVPN Windows Client or Mac OSX's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum

We will be using this tool soon but before doing so we must setup Dynamic DNS. If you are familiar with IP addressing then you know that your ISP will assign you a public IP address via DHCP on your WAN port. This IP address is dynamic which means that it can change and unless you paid your ISP extra cash for a static address. When our clients connect to the OpenVPN server it will try to reach us on the public WAN address on port 1194. If the address changes then it won’t be able to reach us unless we somehow know the new address and we modify the configuration file. This becomes a huge pain to manage and Dynamic DNS will be able to solve this problem for us.

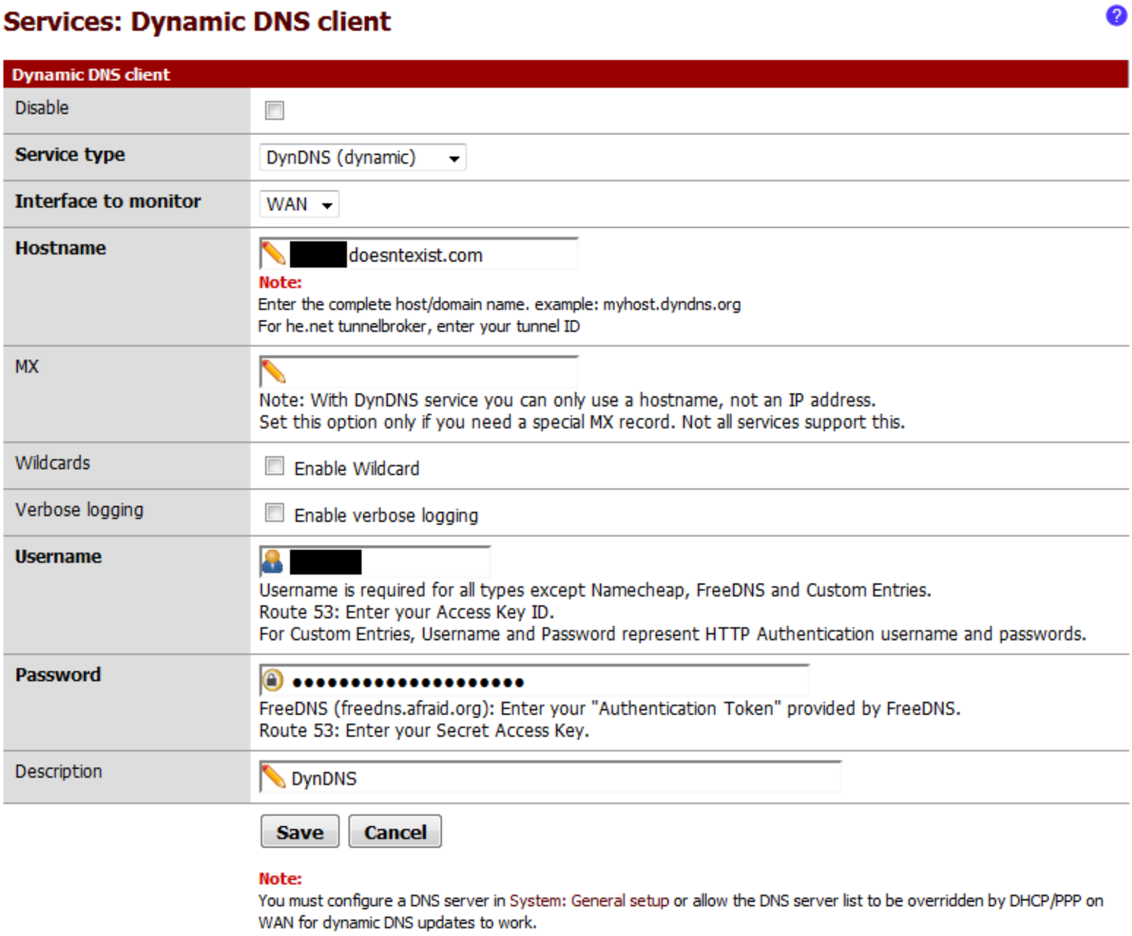
The way that dynamic DNS works is that it will map a hostname that we specify to the current WAN IP address. Dynamic DNS will check at a certain interval the WAN IP and maintain the hostname to IP address mapping current so that when we tried to reach the hostname over the internet then it will point to the correct WAN IP address of our router. In order to get a hostname we must register with a third-party and come up with a unique name that has not been taken yet. Here are a couple of different dynamic DNS provider where you can register a hostname from. Note that some of these are free.

http://dyn.com/

http://www.noip.com/

http://www.opendns.com/

Once you have register a hostname, head over to Services–>Dynamic DNS. In here under the DynDNS tab go ahead and add a new entry. From the service type menu select the provider that you registered with and make sure that you are monitoring the WAN interface. Under hostname type in your fully qualified domain name that you registered(I blacked mine out for privacy reasons). The last thing that you want to do is to type in your account information so that pfSense is capable of reaching your dynamic DNS provider and updating the hostname with your current WAN IP address.



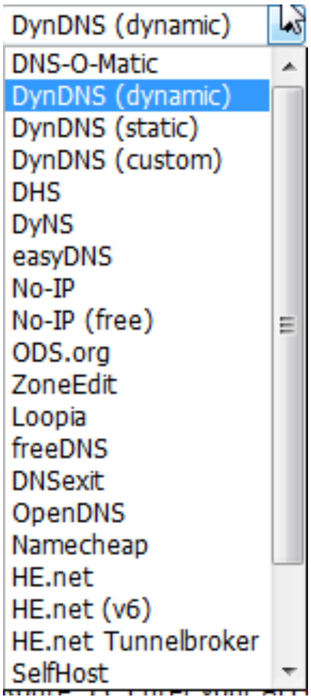
Services: Dynamic DNS client

Dynamic DNS client

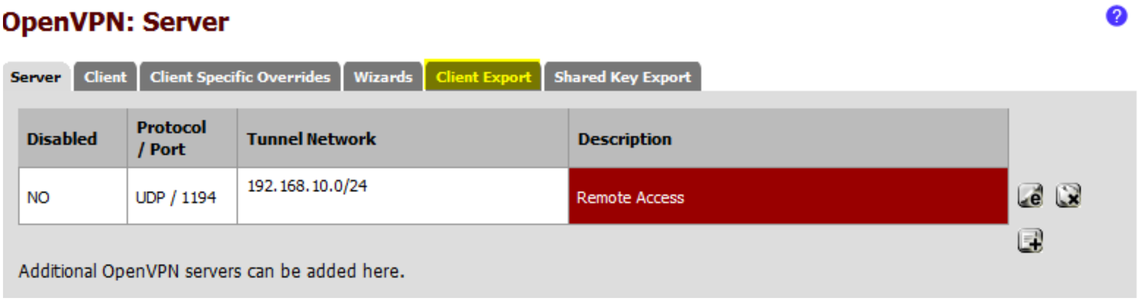
Disable	□
Service type	DynDNS (dynamic)
Interface to monitor	WAN
Hostname	[redacted]doesntexist.com Note: Enter the complete host/domain name. example: myhost.dyndns.org For he.net tunnelbroker, enter your tunnel ID
MX	Note: With DynDNS service you can only use a hostname, not an IP address. Set this option only if you need a special MX record. Not all services support this.
Wildcards	□ Enable Wildcard
Verbose logging	□ Enable verbose logging
Username	[redacted] Username is required for all types except Namecheap, FreeDNS and Custom Entries. Route 53: Enter your Access Key ID. For Custom Entries, Username and Password represent HTTP Authentication username and passwords.
Password	•••••••••••••••••••• FreeDNS (freedns.afraid.org): Enter your "Authentication Token" provided by FreeDNS. Route 53: Enter your Secret Access Key.
Description	DynDNS

Note:
You must configure a DNS server in System: General setup or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work.

Here is the list of Service Type from pfSense.



We will now go over to the VPN–>OpenVPN Section and go to the Client Export Tab.

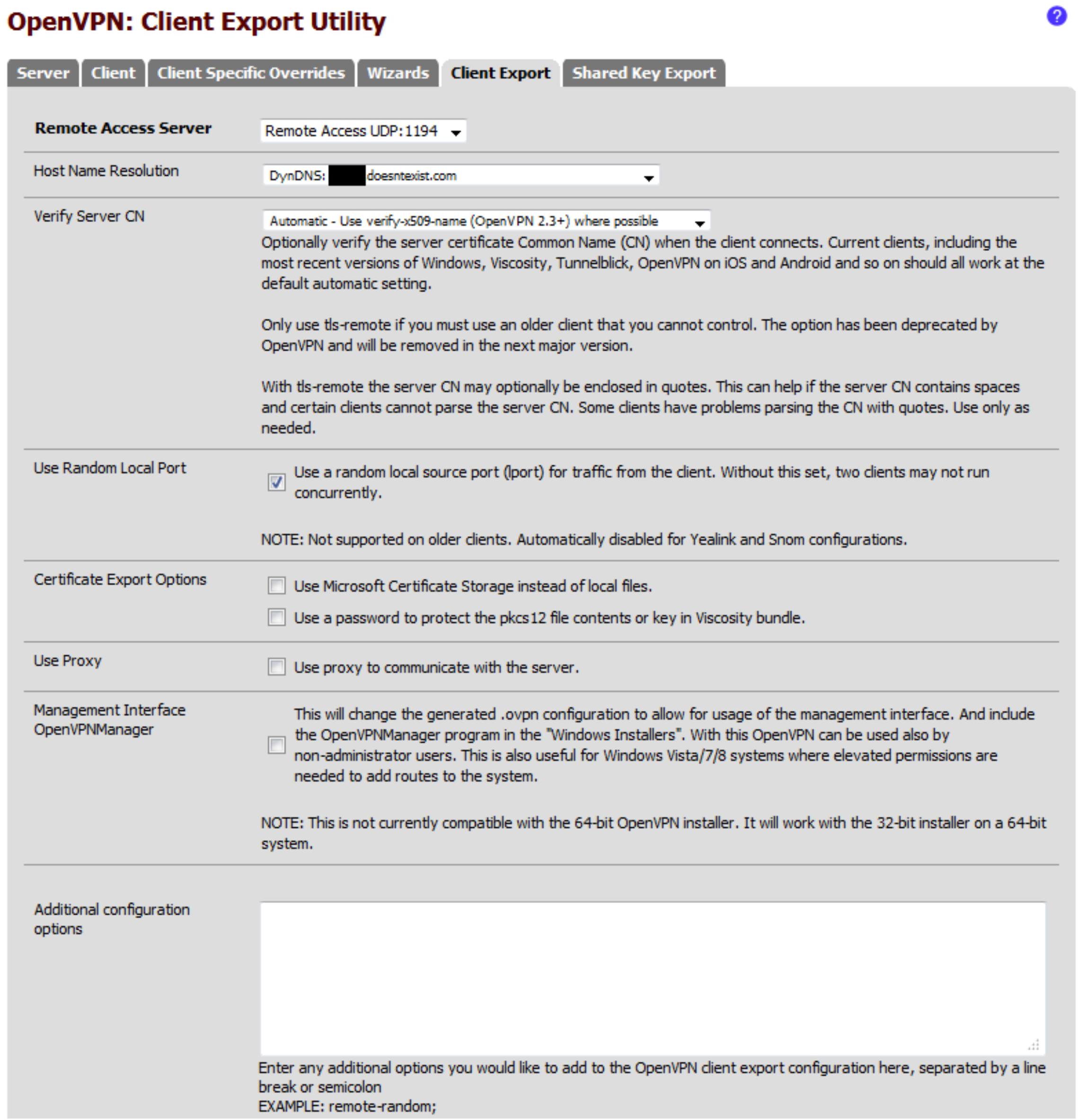


OpenVPN: Server

Disabled	Protocol / Port	Tunnel Network	Description
NO	UDP / 1194	192.168.10.0/24	Remote Access

Additional OpenVPN servers can be added here.

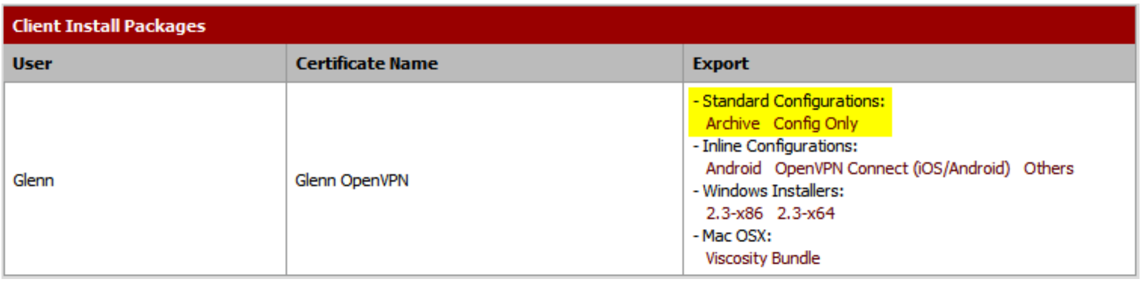
In the client export tab we will be exporting the certificates, keys, and configurations files that we will need for our VPN client. In here you will have different options to select from. The remote access server should have the port number that you specified for OpenVPN as well as the protocol whether it's TCP or UDP. For the hostname resolution we will be using Dynamic DNS which means that you will be selecting the hostname that you configured above. Everything else can be left at their default settings unless you have a reason for selecting the other options.



OpenVPN: Client Export Utility

Remote Access Server	Remote Access UDP:1194
Host Name Resolution	DynDNS: [redacted]doesntexist.com
Verify Server CN	Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting. Only use tls-remote if you must use an older client that you cannot control. The option has been deprecated by OpenVPN and will be removed in the next major version. With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.
Use Random Local Port	☑ Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently. NOTE: Not supported on older clients. Automatically disabled for Yealink and Snom configurations.
Certificate Export Options	□ Use Microsoft Certificate Storage instead of local files. □ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.
Use Proxy	□ Use proxy to communicate with the server.
Management Interface OpenVPNManager	□ This will change the generated .ovpn configuration to allow for usage of the management interface. And include the OpenVPNManager program in the "Windows Installers". With this OpenVPN can be used also by non-administrator users. This is also useful for Windows Vista/7/8 systems where elevated permissions are needed to add routes to the system. NOTE: This is not currently compatible with the 64-bit OpenVPN installer. It will work with the 32-bit installer on a 64-bit system.
Additional configuration options	Enter any additional options you would like to add to the OpenVPN client export configuration here, separated by a line break or semicolon EXAMPLE: remote-random;

At the bottom you will have options to export the configuration and files. The standard configuration is what you will need and it is a good idea to get the archive as this will include the certificates and keys needed. Note that you can also download the windows installer from here depending on which platform you are using.



Client Install Packages

User	Certificate Name	Export
Glenn	Glenn OpenVPN	- Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers: 2.3-x86 2.3-x64 - Mac OSX: Viscosity Bundle

Alternatively you can also get the installer directly from the