OPNsense openVPN N2N

Planning

Considerations

To set up a site-to-site (aka net-to-net or lan-to-lan) OpenVPN connection, you have several things you must consider.

1. You must designate one router to be the “master.”
    1. If you are connecting multiple remote sites to one, it is pretty obvious which would be the central location (the “main office” or something)
    2. If you are simply connecting two sites together, consider the following (in order)
        1. Static, public IP address
        2. More resources on router software
        3. Location that has the best technical support
2. You will need to collect/decide on the following
    1. remote LAN network(s) you want to access
    2. local LAN networks you want to access
    3. intermediary Private_network not used anywhere else in your networks. **Note:** there is a problem I ran into using a /24 subnet. Use a /30 subnet for this.
    4. distinct port for UDP traffic (master will suggest an unused one when you create the new server).

Overview

- Create between 1 and 3 certificates, depending on if you want to reuse existing ones or not.
- Create a server (if not reusing an existing one)
- Create Client Specific Override
- Create 1-2 Firewall rules
- Copy CA, User Certificate, TLS key to client machine
- Match parameters (TLS key, compression, algorithms) to client creation.

What is going on

Skip this if you just want to get it set up.

Basically, the client is very similar to a Road Warrior client, except that all authentication is done automatically, without human intervention. The set up is a little more complex, since we use two certificates to verify we are talking to the right machines, and a shared key to ensure initial secure communication.

To initiate the conversation, the client contacts the server on a specific (generally UDP) port. The router then knows which OpenVPN server to point to based on that. OpenVPN can have several virtual servers running on one router, similar to having multiple web sites on one web server.

The client has a certificate (which was generated by the server) by which it identifies itself (user certificate). The server identifies itself via a server certificate, which is signed by the CA (Certificate of Authority) on the server. Thus, you must copy the the CA's certificate to the client so it knows how to verify that. So, the initial conversation is the client saying “hey, I'm joe, and here is my certificate” and the server replying with “oh, I'm mary, and here is my certificate.” Thus, they begin to establish trust in each other.

Once trust is established, the server and client agree on secure communication based on TLS shared keys, an encryption algorithm and an authentication digest algorithm. Both sides must be set up the same on these.

This all happens very fast, at the beginning of the session, then traffic begins to flow. The client and server will renegotiate the secure communication regularly so traffic is less likely to be decrypted (decryption is much easier with a larger set of messages with the same keys).

So, when we create this linkage, we must create a certificate for both the client and the server, and a way of verifying it. Then, we need to agree on a shared key for encryption, and the algorithms used to secure future communications.

Set up server

1. Create or reuse the required certificates. It is just fine to use an existing Certificate of Authority (CA) and Server Certificate, but you should create a client certificate for each remote site. For more security and flexibility, you should create a new CA and server certificate for each server, since that allows you to invalidate one server without impacting others.
    1. For the following, use good descriptive names. You will not only be trying to find them when you create the OpenVPN server, but you will be exporting them to import into the client. A name like *ca1* will **not** help you find anything.
    2. one CA (you can use an existing one) **Note: with v21.1.2, it appears you have to create a separate one**
        1. System | Trust | Authorities | Add or import CA
        2. Descriptive Name: You can enter anything here, with spaces. This will be what you will select/identify this certificate with in the future
        3. **Method:** Create an internal Certificate Authority
        4. Fill in the rest of the form down to Common Name. I generally change the Lifetime depending on the application.
        5. **Common Name:** No spaces, but use something you can recognize like “VPN-N2N-office”
        6. Save
        7. Export the Certificate (do not export the key) to someplace you can use to get to the client.
    3. one Server Certificate
        1. System | Trust | Certificates | Add or import certificate
        2. Descriptive Name: You can enter anything here, with spaces. This will be what you will select/identify this certificate with in the future
        3. **Method:** Create an internal Certificate
        4. **Certificate Authority:** CA created in previous step
        5. **Type:** Server Certificate
        6. Fill in the rest of the form down to Common Name. I generally change the Lifetime

depending on the application.
7. **Common Name:** again, use something descriptive with no spaces
8. Save
9. **Do not export this certificate**

4. one Client Certificate for each remote (client) site
    1. System | Trust | Certificates | Add or import certificate
    2. Descriptive Name: You can enter anything here, with spaces. This will be what you will select/identify this certificate with in the future
    3. **Method:** Create an internal Certificate
    4. **Certificate Authority:** CA created in previous step
    5. **Type:** Client Certificate
    6. Fill in the rest of the form down to Common Name. I generally change the Lifetime depending on the application.
    7. **Common Name:** again, use something descriptive with no spaces. You should really use the target (client) name or something in this.
    8. Save
    9. Export the client certificate created
    10. Export the client key created

2. Create OpenVPN Server
    1. VPN | OpenVPN | Servers | Add (or Use a Wizard)
    2. **Server Mode:** Peer to Peer (SSL/TLS)
    3. **Protocol:** I find it best to set specifically to UDP4 or UDP6
    4. **Interface:** WAN
    5. **Local Port:** Set to some unused port. 1194 or greater is the norm
    6. **TLS Authentication** and create new key
    7. **Peer Certificate Authority:** Select the CA you are using (the one you created)
    8. **Server Certificate:** Select the Server Cert you created
    9. **IPv4 Tunnel Network:** some random private /30 network. It is important with opnSense (as of 18.7) to use a /30 subnet here as otherwise it may hand out two different pairs of IP's to the client and server. See references at bottom
    10. **IPV4 Local Networks:** Just your LAN network. You can add other networks by separating by comma's
    11. **IPV4 Remote Networks:** The LAN network(s) of the client (separated by comma's, if needed)
    12. Modify and record the Encryption Algorithm, Compression, etc.. as needed. You'll need this to match on the client.
    13. Click Save
    14. Edit the server record, and save the TLS key that was generated for the client (just copy, then paste into a file)
3. Create firewall rules to allow VPN access
    1. Firewall | Rules | OPENVPN
        1. Interface OPENVPN
        2. Everything else default (any protocol, any source, any destination, etc…)
    2. Firewall | Rules | WAN
        1. **Inteface:** WAN
        2. **Protocol:** UDP
        3. **Source:** any
        4. **Destination:** WAN address
        5. **Destination port range:** Port from server definition
4. Go into VPN | OpenVPN | Client Specific Overrides and create a new override
    1. Common Name: common name (CN) of client certificate.

2. IPv4 Remote Networks: network(s) on the client (remote) LAN

On Client Machine

1. Import CA from server
    1. System | Trust | Authorities | Add or import CA
    2. **Descriptive Name:** Something you can easily identify this with
    3. Copy/paste data you exported from server (CA)
2. Import User Cert and Key from server
    1. System | Trust | Certificates | add or import certificate
    2. **Descriptive Name:** Something you can easily identify this with
    3. Copy/paste user certificate from file you exported
    4. Copy/paste user key from file you exported
3. Create Client
    1. VPN | OpenVPN | Clients | add client
    2. **Server Host or Address:** IP or DNS name of master
    3. **Server Port:** Port used on the server
    4. **TLS Authentication**
        1. **Automatically generate a shared TLS authentication key**: uncheck
        2. paste TLS key from server
    5. **Peer Certificate of Authority:** Select CA you imported from master
    6. **Client Certificate:** Select user certificate you imported from master
    7. **Auth Digest Algorithm:** match server
    8. **Encryption Algorithm:** match server
    9. **Compression:** match server
    10. Save
4. Set up firewall rule
    1. If you want the main site to be able to access machines on the remote
        1. Firewall | Rules | OpenVPN
        2. Add
        3. Action = Pass (default)
        4. Interface = OpenVPN (default)
        5. Save (no other entries need to be made)
        6. Reload your firewall rules.

Troubleshooting

When you press save, it should immediately try to connect to the server. If you do not get a connection, check the logs on both client and server.

I had an issue where my tunnel network was using a /24 network and OpenVPN on opnSense was assigning one pair of IP's to the master router and a different set to the client router. It was causing weird behavior where I could ping the LAN behind the master router from the client router, but not from the LAN behind the client router. There were also log entries stating that the BSD route command was failing.

In my case, I simply went into the configuration on both master and client and changed the tunnel network to /30 (just changed /24 to /30, saved and restarted). It gave both routers the same pair, and

everything worked from there.

Links

- https://doc.pfsense.org/index.php/OpenVPN_Site-to-Site_PKI_%28SSL%29
- https://forum.opnsense.org/index.php?topic=11046.msg50463#msg50463