**IKEv2 with EAP-TLS**

Under construction. Needs testing.

IKEv2 is supported starting with pfSense® software version 2.2 and one way to make it work is by using EAP-TLS, which is covered in this article.

**Setup Certificates**

Similar to OpenVPN, a set of certificates is required for the server and clients.

**Create a Certificate Authority**

If one is not already available, then the first task is to create a Certificate Authority.

* Navigate to **System > Cert Manager** in the pfSense webGUI
* Click fa-plus to create a new certificate authority
* Select *Create an internal Certificate Authority* for the **Method**
* Fill in the rest of the fields as desired with company or site-specific information
* Click **Save**

**Create a Server Certificate**

* Navigate to **System > Cert Manager**, **Certificates** tab in the pfSense webGUI
* Click fa-plus to create a new certificate
* Select *Create an internal certificate* for the **Method**
* Enter a **Descriptive Name** such as *IKEv2 Server*
* Select the appropriate **Certificate Authority** created in the previous step
* Choose the desired **Key length**, **Digest algorithm**, and **Lifetime**
* Set the **Certificate Type** to *Server Certificate*
* Fill in the regional and company values in the **Distinguished name** fields as desired, they are copied from the CA and may be left as-is
* Enter the **Common Name** as the hostname of the firewall as it exists in DNS
* Click fa-plus to add a new **Alternative Name**
* Enter *DNS* in the **Type** field
* Enter the hostname of the firewall as it exists in DNS **again** in the **Value** field – Some clients require the value in SAN not just CN!
* Click fa-plus to add a new **Alternative Name**
* Enter *IP* in the **Type** field
* Enter the WAN IP address of the firewall in the **Value** field
* Add more **Alternative Names** as needed for additional hostnames or IP address on the firewall that clients may use to connect
* Click **Save**

**Create Client Certificates**

* Navigate to **System > Cert Manager**, **Certificates** tab in the pfSense webGUI
* Click fa-plus to create a new certificate
* Select *Create an internal certificate* for the **Method**
* Enter a **Descriptive Name** such as *client1*
* Select the appropriate **Certificate Authority**
* Choose the desired **Key length**, **Digest algorithm**, and **Lifetime**
* Set the **Certificate Type** to *User Certificate*
* Fill in the regional and company values in the **Distinguished name** fields as desired, they are copied from the CA and may be left as-is
* Enter the **Common Name** as the client username, such as *client1*
* Click fa-plus to add a new **Alternative Name**
* Enter *DNS* in the **Type** field
* Enter the user name again in the **Value** field, such as *client1*
* Click **Save**

Repeat as needed for additional clients.

**Set up Mobile IPsec for IKEv2+EAP-TLS**

With the certificate structure prepared, the next task is to configure the necessary IPsec settings. The settings below have been tested and found to work, but other similar settings may function as well. Feel free to try other encryption algorithms, hashes, etc. Report any additional combinations found to work or not work on the forum.

**Mobile Clients**

* Navigate to **VPN > IPsec**, **Mobile Clients** tab in the pfSense webGUI
* Check **Enable IPsec Mobile Client Support**
* Set **User Authentication** to *Local Database*
* Check **Provide a virtual IP address to clients**
* Enter an **unused** private **Network** and appropriate subnet mask (such as */24*)
* Check **Provide a list of accessible networks to clients**
* Click **Save**

**Phase 1**

* Click the **Tunnels** Tab
* Click the **Create Phase1** button at the top if it appears, or edit the existing Mobile IPsec Phase 1
* Set **Key Exchange version** to *v2*
* Set **Authentication method** to *EAP-TLS*
* Set **My Identifier** to *Distinguished name* and enter in the hostname of the firewall

**Note**

This MUST match the Common Name of the server certificate!

* Set **Peer Identifier** to *User Distinguished name*, enter an e-mail address style identifier (e.g. *user@example.com*) – This isn’t used, but is currently required by the GUI
* Select the server certificate created previously for **My Certificate**
* Select the appropriate CA for **My Certificate Authority**
* Set **Encryption algorithm** to *AES 256*
* Set **Hash algorithm** to *SHA256*
* Set **DH key group** to *2 (1024 bit) THIS IS WRONG, CHECK LOG FOR CORRECT SETTINGS*
* Set **Lifetime** to *28800*
* Uncheck **Disable Rekey**
* Uncheck **Disable Reauth**
* Set **NAT Traversal** to *Auto*
* Check **Enable DPD**, set for *10* seconds and *5* retries
* Click **Save**

**Phase 2**

* Click fa-plus to show the Mobile IPsec Phase 2 list
* Click fa-plus to add a new Phase 2 entry if one does not exist, or click fa-pencil to edit an existing entry
* Set **Mode** to **Tunnel IPv4**
* Set **Local Network** as desired
  + To pass all traffic, including Internet traffic, across the VPN, set the **Local Network** to *0.0.0.0/0*
* Enter an appropriate **Description**
* Set **Protocol** to *ESP*
* Set **Encryption algorithms** to ONLY *AES 256*
* Set **Hash algorithms** to ONLY *SHA1*
* Set **PFS Key Group** to *off*
* Set **Lifetime** to *3600*
* Click **Save**

**Add Firewall Rules for IPsec**

Firewall rules are necessary to pass traffic from IPsec clients.

* Navigate to **Firewall > Rules**, **IPsec** tab
* Review the current rules. If there is an “allow all” style rule, then there is no need to add another. Continue to the next task.
* Click fa-plus to add a new rule
* Set the **Protocol** to *any*, and set the **Source** and **Destination** to *any* as well
* Click **Save**
* Click **Apply Changes**

**Import the CA to the Client PC**

The server setup is complete, the following tasks will configure the client side.

* Export CA Cert from the pfSense router and download it to the client PC
  + Navigate to **System > Cert Manager**, **Certificate Authorities** tab in the pfSense webGUI
  + Click fa-certificate by the CA to download *only* the certificate
* Locate the downloaded file on the client PC (e.g. *MyCA.crt*)
* Double click the CA file
* Click **Install Certificate…**
* Select *Local Machine*
* Click **Next**
* Click **Yes** at the UAC prompt if it appears
* Select *Place all Certificates in the following store*
* Click **Browse**
* Click *Trusted Root Certification Authorities*
* Click **Next**
* Click **Finish**
* Click **OK**
* Click **OK**

**Import the Client Certificate to the Client PC**

* Export client certificate from the pfSense router and download it to the client PC
  + Navigate to **System > Cert Manager**, **Certificates** tab in the pfSense webGUI
  + Click fa-archive by the certificate to download a .p12 file containing the client certificate and key
* Locate the downloaded file on the client PC (e.g. *client1.p12*)
* Double click client certificate *.p12*
* Select *Current User*
* Click **Next**
* Click **Yes** at the UAC prompt if it appears
* Confirm the proper file is selected
* Click **Next**
* Click **Next**
* Click **Next**
* Click **Finish**
* Click **OK**

**Add the Client VPN Connection**

With the certificates properly imported, now it is time to create the client VPN connection. There are several ways to add such a connection, depending on the version of Windows being used. Adapt as needed.

* Open **Network and Sharing Center** on the client PC
* Click **Set up a new connection or network**
* Select *Connect to a workplace*
* Click **Next**
* Select *No, create a new connection*
* Click **Next**
* Click **Use my Internet Connection (VPN)**
* Enter the IP address or hostname of the server into the Internet address field

**Note**

This MUST match what is in the server certificate Common Name or a configured Subject Alternative Name!

* Enter a **Destination Name** to identify the connection
* Click **Create**

The connection has been added but with several undesirable defaults. For example the type defaults to automatic and it will latch onto a PPTP connection if one exists, which is very bad. So a few settings should be set by hand first:

* In Network Connection / Adapter Settings in Windows, find the connection created above
* Right click the connection
* Click **Properties**
* Click the **Security** tab
* Set **Type of VPN** to *IKEv2*
* Set **Data Encryption** to *Require Encryption (disconnect if server declines)*
* Set **Authentication / Use Extensible Authentication Protocol** to *Microsoft: Smart Card or other certificate (encryption enabled)*
* Click **Properties**
* Select *Use a certificate on this computer*
* Click *Advanced*
* Check **Certificate Issuer**
* Choose the imported CA Certificate (e.g. *myca*)
* Check **Extended Key Usage**
* Check **Client Authentication**
* Click **OK**
* Check **Verify the servers identity by validating the certificate**
* Check **Connect to these servers**
* Enter the pfSense hostname (same as in the CN of the server certificate!)
* Select the imported CA certificate (e.g. *myca*) in the **Trusted Root Certificate Authorities** box
* Uncheck *Use a different user name for the connection*
* Click **OK**