**Configuring an IPsec Remote Access Mobile VPN using IKEv2 with EAP-MSCHAPv2**

IKEv2 is supported in current pfSense® software versions, and one way to make it work is by using EAP-MSCHAPv2, which is covered in this article.

**Warning**

Server certificates generated before pfSense software version 2.2.4-RELEASE did not have an **Extended Key Usage** flag set that Windows typically expects. A new server certificate must be generated after upgrading to a current pfSense software release.

**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 through the pfSense webGUI to **System > Cert Manager**
* Click  **Add** 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
* Click  **Add** 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. If clients will connect by IP address, place the IP address here.
* Click  **Add** 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 CN!
* Click  **Add** to add another new **Alternative Name**
* Enter *IP address* 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 addresses on the firewall that clients may use to connect
* Click **Save**

**Set up Mobile IPsec for IKEv2+EAP-MSCHAPv2**

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
* 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**
* Click the **Create Phase1** button at the top when it appears (if there is no existing Mobile IPsec P1)

**Phase 1**

* If there is an existing Mobile IPsec P1 entry, click the **Tunnels** Tab and edit it there
* Set **Key Exchange version** to *v2*
* Set **Authentication method** to *EAP-MSChapv2*
* 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 *any*
* Select the server certificate created previously for **My Certificate**
* Select the appropriate CA for **My Certificate Authority**
* Set **Algorithm** to *AES*
* Set **Key length** to *256 bits*
* Set **Hash** to *SHA256*
* Set **DH Group** to *14 (2048 bit)*
	+ Multiple combinations of encryption, hashing, and DH options may be created to accommodate various clients with different requirements. Click  **Add Algorithm** to add more entries.
* Set **Lifetime** to *28800*
* Uncheck **Disable Rekey**
* Uncheck **Disable Reauth**
* Check **Enable DPD**, set for *10* seconds and *5* retries
* Click **Save**

**Phase 2**

* Click  **Show Phase 2 Entries** to show the Mobile IPsec Phase 2 list
* Click  **Add P2** to add a new Phase 2 entry if one does not exist, or click  to edit an existing entry
* Set **Mode** to **Tunnel IPv4**
* Set **Local Network** as desired, e.g. *LAN subnet*
	+ 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 *AES Auto*.
* Set **Hash Algorithms** to *SHA256*
* Set **PFS key group** to *off*
* Set **Lifetime** to *3600*
* Click **Save**

**Create Client Pre-Shared Keys**

With the IPsec tunnel itself ready, now the users need pre-shared keys.

* Navigate to **VPN > IPsec**, **Pre-Shared Keys** tab to add EAP users
* Click  **Add** to add a new user
* Enter an e-mail address style username, such as user@example.com
* Set **Secret Type** to *EAP*
* Enter a **Pre-Shared Key** (password) for the user
* Click **Save**

Repeat as needed for additional clients.

In situations where entering pre-shared keys on the firewall in plain text is undesirable, a RADIUS server may be used instead by selecting the *EAP-RADIUS* authentication type rather than *EAP-MSCHAPv2*. The setup is nearly identical. Follow the directions on this page and then see [IKEv2 with EAP-RADIUS](https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/ikev2-with-eap-radius.html) for the needed adjustments.

**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  **Add** 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**

**Windows Client Setup**

**Import the CA to the Client PC**

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

* Export the CA Cert from the pfSense router and download it to the client PC
	+ Navigate through the pfSense webGUI to **System > Cert Manager**, **Certificate Authorities**tab
	+ Click  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**

**Setup the 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:

* 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: Secured password (EAP-MSCHAP v2) (encryption enabled)*
* Click **OK**

**Disable EKU Check**

In some cases it may be necessary to disable the check on Windows for a certificate’s Extended Key Usage parameters. Disabling this check also disables validation of the certificate’s common name and SAN fields, so it is potentially dangerous. Any certificate from the same CA could be used for the server when this is disabled, so proceed with caution.

To disable the extended key usage checks, open up **Registry Editor** on the Windows client and navigate to the following location in the client registry:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\Parameters\

In there, add a new **DWORD** entry named DisableIKENameEkuCheck and set it to 1.

A reboot may be required to activate the setting.

**Ubuntu-based Client Setup**

Before starting, install **network-manager-strongswan** and **strongswan-plugin-eap-mschapv2** using apt-get or a similar mechanism.

**Setup the VPN Connection**

* Copy the CA Certificate for the VPN from the firewall to the workstation
* Click **Network Manager** icon in the notification tray by the clock (Icon varies depending on the type of network in use)
* Click **Network Connections**
* Click **Add**
* Select **IPsec/IKEv2 (strongswan)** under **VPN** (If the option is not present, ensure that network-manager-strongswan is installed)
* Click **Create**
* Enter a **Description** (e.g. *Work VPN*)
* Select the **VPN** Tab
* Enter the **Address** of the firewall (e.g. *vpn.example.com*)
* Select the control next to **Certificate** and browse to find the downloaded CA Certificate
* Select **EAP** for **Authentication**
* Enter the **Username** to be used for this connection (e.g. *alice*)
* Check **Request an inner IP address**
* Click **Save**
* Click **Close**

**Connecting and Disconnecting**

To Connect:

* Click the Network Manager icon
* Click the VPN Name or click **VPN Connections** to move the slider to the **On** (1) position

**Note**

If a password prompt does not appear, the network manager service may need restarted or a reboot of the workstation may be necessary.

To Disconnect:

* Click the Network Manager icon
* Click **VPN Connections** to move the slider to the **Off** (0) position

**Android Client Setup**

Before starting, install the strongSwan app from the Play Store:<https://play.google.com/store/apps/details?id=org.strongswan.android>

**Setup the VPN Connection**

* Copy the CA Certificate to the device
* Open the strongSwan app
* Import the CA:
	+ Tap the settings icon (Three vertical dots in the upper right)
	+ Tap CA Certificates
	+ Tap the settings icon (Three vertical dots in the upper right)
	+ Tap Import Certificate
	+ Locate the CA Certificate copied earlier and tap it.
* Tap **Add VPN Profile**
* Enter a **Profile Name** (optional, if left blank, the gateway address will be used)
* Enter the address of the firewall as the **Gateway** (e.g. vpn.example.com)
* Select **IKEv2 EAP (Username/Password)** for the **Type**
* Enter the **Username**
* Enter the **Password** if it should be saved, leave blank to prompt for the password.
* Check **Select automatically** under **CA Certificate**

**Connecting and Disconnecting**

To Connect:

* Open the strongSwan app
* Tap the desired VPN
* Check **I trust this application** at the security prompt
* Tap OK

To Disconnect:

* Swipe down from the top
* Tap the strongSwan entry in the notification list
* Tap Disconnect

-or-

* Open the strongSwan app
* Tap Disconnect on the desired VPN

**OS X 10.11+ Setup**

**Import the CA Certificate**

* Copy the CA Certificate to the OS X system
* Double click the CA Certificate File in Finder, which opens Keychain Access
* Enter the login credentials and click **Modify Keychain**
* Locate the imported certificate under **Login**, **All Items**
* Drag the certificate on to **System**
* Click the Certificate
* Click **File > Get Info**
* Expand **Trust**
* Set **When using this certificate** to *Always Trust*

**Setup the VPN Connection**

* Open System Preferences
* Click **Network**
* Click + to add a new VPN entry
* Select *VPN* for the **Interface**
* Select *IKEv2* for the **VPN Type** (default)
* Set **Service Name** to a description for the VPN
* Enter the hostname of the firewall in DNS as the **Server Address**
* Enter the hostname of the firewall again in **Remote ID** – This must match the server certificate’s Common Name and SAN entry.
* Leave **Local ID** blank
* Click **Authentication Settings**
* Select **Username**
* Enter the **Username** (EAP Key ID for this user) and **Password**
* Check **Show VPN status in the menu bar** (if desired)
* Click **Apply**

**iOS 9+ Setup**

**Import the CA Certificate**

* Send the CA Certificate file to the iOS device via E-mail (or use an alternate method to get the file to the device)
* Open the Mail app
* Open the message with the CA Certificate
* Open the attachment
* Tap **Install** at the upper right
* Tap the **Install** button that appears to confirm the installation

**Setup the VPN Connection**

* Open Settings
* Tap **General**
* Tap **VPN**
* Tap **Add VPN Configuration**
* Set the **Type** to *IKEv2* (default)
* Enter some text for the **Description** (e.g. **ExampleCo VPN**)
* Enter the hostname of the firewall in DNS as the **Server**
* Enter the hostname of the firewall again in **Remote ID** – This must match the server certificate’s Common Name and SAN entry.
* Leave **Local ID** blank
* Set **User Authentication** to *Username*
* Enter the **Username** (EAP Key ID for this user) and **Password**
* Tap **Done**