

1. **Create CA:**  
set lifetime to 10 years.

## System: Trust: Authorities

Descriptive name	MY_CA
<b>i</b> Method	Create an internal Certificate Authority
Internal Certificate Authority	
<b>i</b> Key Type	RSA
<b>i</b> Key length (bits)	2048
<b>i</b> Digest Algorithm	SHA256
<b>i</b> Lifetime (days)	3650
Distinguished name	
<b>i</b> Country Code :	DE (Germany)
<b>i</b> State or Province :	BW
<b>i</b> City :	MyCity
<b>i</b> Organization :	MyOrg
<b>i</b> Email Address :	my@email.email
<b>i</b> Common Name :	MY_CA
<b>Save</b>	

set Common Name = Descriptive Name  
and export this CA (export CA cert, not the private key) after creating:

## System: Trust: Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	
MY_CA	YES	self-signed	0	emailAddress=my@personal.email, ST=MyProvince, O=MyOrg, L=MyCity, CN=MY_CA, C=DE,	  

## 2. Create a certificate:

System: Trust: Certificates

Method	Create an internal Certificate								
Descriptive name	My_IKEv2_Cert								
Internal Certificate									
Certificate authority	MY_CA								
Type	Server Certificate								
Key Type	RSA								
Key length (bits)	2048								
Digest Algorithm	SHA256								
Lifetime (days)	3650								
Private key location	Save on this firewall								
Distinguished name									
Country Code :	DE (Germany)								
State or Province :	MyProvince								
City :	MyCity								
Organization :	MyOrg								
Email Address :	my@personal.email								
Common Name :	gw								
Alternative Names	<table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>IP</td> <td>xxx.xxx.xxx.xxx (my external IP)</td> </tr> <tr> <td>DNS</td> <td>gw (hostname)</td> </tr> <tr> <td>DNS</td> <td>my.full.domain (FQDN)</td> </tr> </tbody> </table>	Type	Value	IP	xxx.xxx.xxx.xxx (my external IP)	DNS	gw (hostname)	DNS	my.full.domain (FQDN)
Type	Value								
IP	xxx.xxx.xxx.xxx (my external IP)								
DNS	gw (hostname)								
DNS	my.full.domain (FQDN)								

Important: Type is Server Certificate, Certificate authority (the one created in step 1)

Lifetime 10 years,

Common Name = hostname of the opnsense

SANs (Subject Alternativ Names) = IP, hostname, FQDN

### 3. Create the Mobile Client Settings:

#### VPN: IPsec: Mobile Clients

Create Phase1

Support for IPsec Mobile clients is enabled but a Phase1 definition was not found.  
Please click Create to define one.

IKE Extensions	
<div><span>?</span> Enable</div>	<input checked="" type="checkbox"/> Enable IPsec Mobile Client Support
Extended Authentication (Xauth)	
<div><span>?</span> Backend for authentication</div>	<div>Local Database</div>
<div><span>!</span> Enforce local group</div>	<div>(none)</div>
Client Configuration (mode-cfg)	
<div><span>?</span> Virtual Address Pool</div>	<input checked="" type="checkbox"/> Provide a virtual IP address to clients <div>192.168.200.1 24</div>
<div><span>?</span> Network List</div>	<input checked="" type="checkbox"/> Provide a list of accessible networks to clients
<div><span>!</span> Save Xauth Password</div>	<input type="checkbox"/> Allow clients to save Xauth passwords (Cisco VPN client only)
<div><span>?</span> DNS Default Domain</div>	<input checked="" type="checkbox"/> Provide a default domain name to clients <div>mylocal.domain</div>
<div><span>!</span> Split DNS</div>	<input type="checkbox"/> Provide a list of split DNS domain names to clients
<div><span>?</span> DNS Servers</div>	<input checked="" type="checkbox"/> Provide a DNS server list to clients <div>Server #1: 192.168.100.10</div> <div>Server #2: 192.168.100.11</div> <div>Server #3:</div> <div>Server #4:</div>
<div><span>?</span> WINS Servers</div>	<input type="checkbox"/> Provide a WINS server list to clients
<div><span>!</span> Phase 2 PFS Group</div>	<div>off</div>
<div><span>?</span> Login Banner</div>	<input checked="" type="checkbox"/> Provide a login banner to clients <div>Welcome to my VPN, all connections are logged.</div>
<div style="background-color: #ff8c00; color: white; padding: 5px 10px; border-radius: 3px;">Save</div>	

Virtual-Address Pool: use any non existing network (clients will get their IP addresses from that pool), DNS-Server: use your internal DNS if you want clients to resolve internal names.  
SAVE, then choose create phase 1

#### 4. Create Phase 1 (Tunnel Settings),

use these settings for compatibility with various clients, this will create the Firewall rules, too.

##### VPN: IPsec: Tunnel Settings

General information	
Disabled	<input type="checkbox"/> Disable this phase1 entry
Connection method	default
Key Exchange version	V2
Internet Protocol	IPv4
Interface	WAN
Description	Mobile-VPN
Phase 1 proposal (Authentication)	
Authentication method	EAP-MSCHAPv2
My identifier	My IP address
My Certificate	My_IKEv2_Cert
Phase 1 proposal (Algorithms)	
Encryption algorithm	AES 256
Hash algorithm	SHA256
DH key group	14 (2048 bits)
Lifetime	28800
Advanced Options	
Install policy	<input checked="" type="checkbox"/>
Disable Rekey	<input type="checkbox"/>
Disable Reauth	<input type="checkbox"/>
Tunnel Isolation	<input type="checkbox"/>
NAT Traversal	Enable
Disable MOBIKE	<input type="checkbox"/>
Dead Peer Detection	<input checked="" type="checkbox"/> 10 seconds 5 retries default DPD action
Margintime	
Rekeyfuzz	
<b>Save</b>	

5. Add phase 2 Tunnel for the previously created phase 1:



VPN: IPsec: Tunnel Settings

The IPsec tunnel configuration has been changed. You must wait for the daemon to reload before the changes take effect.

Type	Remote Gateway	Mode	Phase 1 Proposal	Authentication	Description
<input checked="" type="checkbox"/> IPv4 IKEv2	WAN-Hosts-Client	Remote Tunnel	15 (SHA-256 + SHA-256 + CM Group 14	ESP-Auth-PSK	Mobile-VPN

and don't forget to enable ipsec itself:

### VPN: IPsec: Tunnel Settings

Type
<input type="checkbox"/>  IPv4 IKEv2
<input type="checkbox"/>  ESP IPv4 tunnel
<input checked="" type="checkbox"/> Enable IPsec

**Save**

## 6. Tunnel Definition:

VPN: IPsec: Tunnel Settings

General information

*Disabled*
☐

*Mode*

Tunnel IPv4

*Description*

Mobile-IKE

Local Network

*Type*

LAN subnet

*Address:*

32

Phase 2 proposal (SA/Key Exchange)

*Protocol*

ESP

*Encryption algorithms*

☒ AES

auto

☐ aes128gcm16
☐ aes192gcm16
☒ aes256gcm16
☐ Blowfish

auto

☐ 3DES
☐ CAST128
☐ DES
☐ NULL (no encryption)

*Hash algorithms*

SHA256

*PFS key group*

14 (2048 bits)

*Lifetime*

3600

seconds

Advanced Options

*Automatically ping host*

Save

Important: use aes256gcm16 (for Win 10 Clients), PFS group 14 (or leave it "off").

SAVE, Apply Changes

© 2020, Ralf Gebhard, w3 GmbH

## 7. Create the users/key pairs:

### VPN: IPsec: Pre-Shared Keys

Identifier	<input type="text" value="user@email.com"/>
Pre-Shared Key	<input type="text" value="myverysecretkey"/>
Type	<div>EAP</div>
<div>Save</div>	








































### VPN: IPsec: Pre-Shared Keys

Identifier	Pre-Shared Key	Type	
user@email.com	myverysecretkey	EAP	 
user2@email.com	user2verysecretkey	EAP	 

PSK for any user can be set by using an identifier of any/ANY

it might be a good idea to restart the VPN services:

### System: Diagnostics: Services

Service	Description	Status
configd	System Configuration Daemon	  
dhcpd6	DHCPv6 Server	  
dpinger	Gateway Monitor (NC_GW)	  
flowd_aggregate	Insight Aggregator	  
ifgroups	Interface groups	  
login	Users and Groups	  
ntpd	Network Time Daemon	  
openssh	Secure Shell Daemon	  
pf	Packet Filter	  
radvd	Router Advertisement Daemon	  
samplicate	NetFlow Distributor	  
squid	Web Proxy	  
strongswan	IPsec VPN	  

## 8. Windows 10 Client, Change parameters to your needs

Important: Name "MyVPN" (should be the same in all three command)

ServerAddress: use FQDN or IP

DestinationPrefix: use your local network (or target internal network)

Open an administrative Powershell:

#Create VPN:

```
Add-VpnConnection -Name "MyVPN" -ServerAddress "gw.myopnsense.com" -TunnelType
IKEv2 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -
AllUserConnection
```

#Verschlüsselung:

```
Set-VpnConnectionIPsecConfiguration -ConnectionName "MyVPN" -
AuthenticationTransformConstants GCMAES256 -CipherTransformConstants GCMAES256 -
EncryptionMethod AES256 -IntegrityCheckMethod SHA256 -DHGroup Group14 -PfsGroup
PFS2048 -PassThru
```

#Routing:

```
Add-VpnConnectionRoute -ConnectionName "MyVPN" -DestinationPrefix 192.168.100.0/24 -
PassThru
```

- Windows 10 Client might require an additional registry key:

HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

New DWORD: DisableIKNameEkuCheck, Value: 1

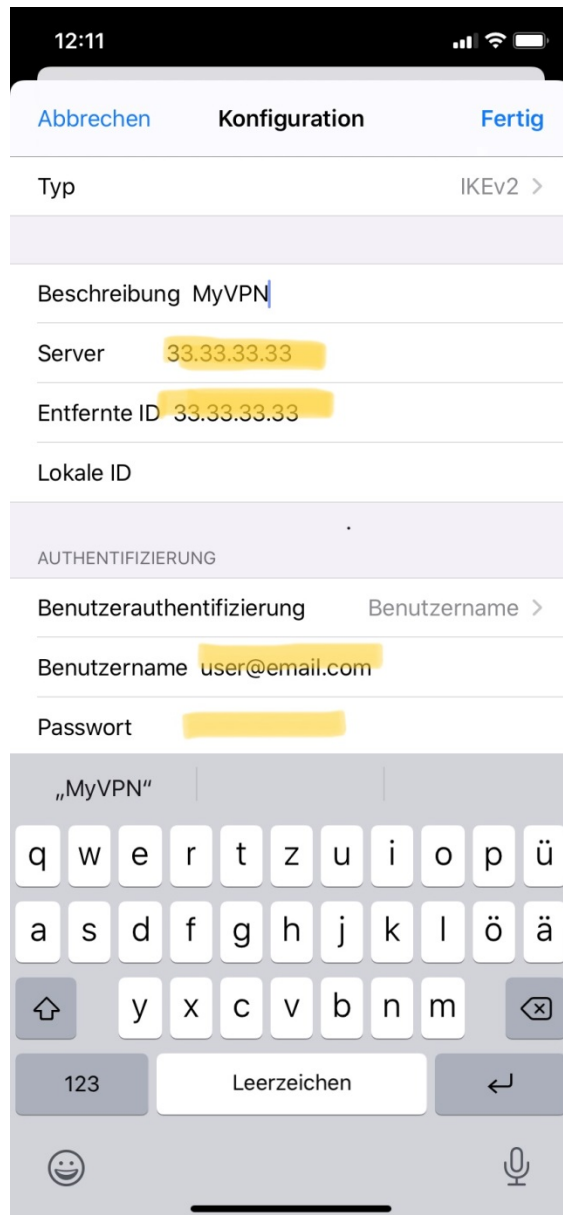
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters			
	Name	Typ	Daten
	(Standard)	REG_SZ	(Wert nicht festgelegt)
	AllocatedLuids	REG_BINARY	02 00 00 00
	AllowL2TPWeakCrypto	REG_DWORD	0x00000000 (0)
	AllowPPTPWeakCrypto	REG_DWORD	0x00000000 (0)
	DisableIKNameEkuCheck	REG_DWORD	0x00000001 (1)
	KeepRasConnections	REG_DWORD	0x00000000 (0)
	Medias	REG_MULTI_SZ	rastapi
	MiniportsInstalled	REG_DWORD	0x0000ffff (65535)
	ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\rasmans.dll
	ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

- Import the CA-Cert you exported in step 1 into Trusted Root Certification Authorities (by double-clicking and importing it into Computer ....., see other FAQ)



## 9. IOS VPN Setup

- Send your CA-Cert you created in step 1 by email (or other means) to your IOS device, klick that cert
- The cert should now show up under Settings-Profiles, where you can install it.
- Settings VPN add the new VPN:  
don't use the FQDN, use the IP, otherwise IOS will refuse to connect.





#### 10. **Android**

Since Android can't deal with EAP download the StrongSwan App in Playstore and proceed according to Step 9 (don't forget to import the CA-Cert first).