How to configure Femto Ipsec-PSK method

1. Achieve Negotiation parameter with Security gateway server

AuthenticationMethod	LocalId and RemoteId	EncryptionAlgorithms
PreSharedKey	LocalTs and RemoteTs	IntegrityAlgorithms
SecGWServer1	EnableVips switch	DiffieHellmanGroupTransforms

2. Ipsec parameter Configuration

ParameterName	ParameterValue
AuthenticationMethod	PSK
Status	Enabled
PreSharedKey	
Certs	
SecGWServer1	88.217.136.214
SecGWServer2	
URL	
LocalId	
RemoteId	
EncryptionAlgorithms	aes256
IntegrityAlgorithms	sha256
DiffieHellmanGroupTransforms	modp2048
EnableVips	True

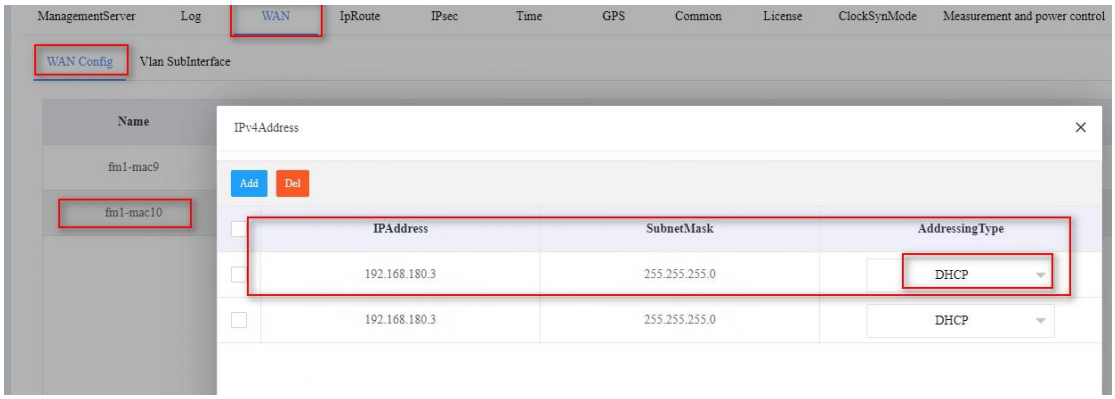
Child SA:

ChildSA

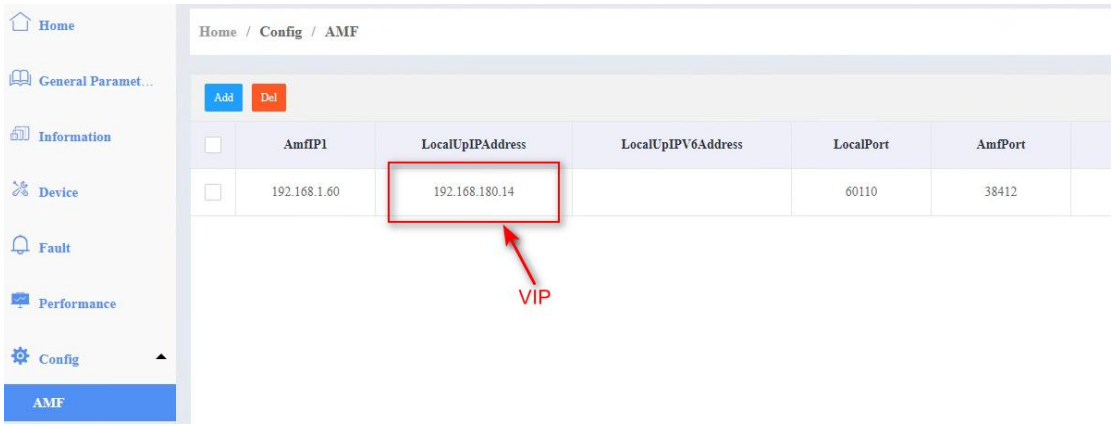
ParameterName	ParameterValue
Index	1
LocalTs	
RemoteTs	192.168.1.0/24
EncryptionAlgorithms	aes256
IntegrityAlgorithms	sha256
DiffieHellmanGroupTransforms	modp2048

WAN Config: (DHCP or Static)

If vip of ipsec is enabled and DHCP is selected, a virtual ip will be allocated auto.



AMF LocalUpIPAdress should be configured same as VIP.



3. IPsec Status check

Check in webgui:

Check by commands: ipsec status

```
root@localhost:/opt/bbu/oam/pm/1# ipsec status
Security Associations (1 up, 0 connecting):
         h2h[13]: ESTABLISHED 10 minutes ago, 192.168.180.3[tef1@opticoms.vpn.de]...88.217.136.214[cle@opticoms.vpn.de]
        h2h1{1244}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7e20fa3_i 639c7450_o
        h2h1{1244}:   192.168.180.14/32 === 192.168.1.0/24
root@localhost:/opt/bbu/oam/pm/1#
```

Check by commands: ipsec statusall

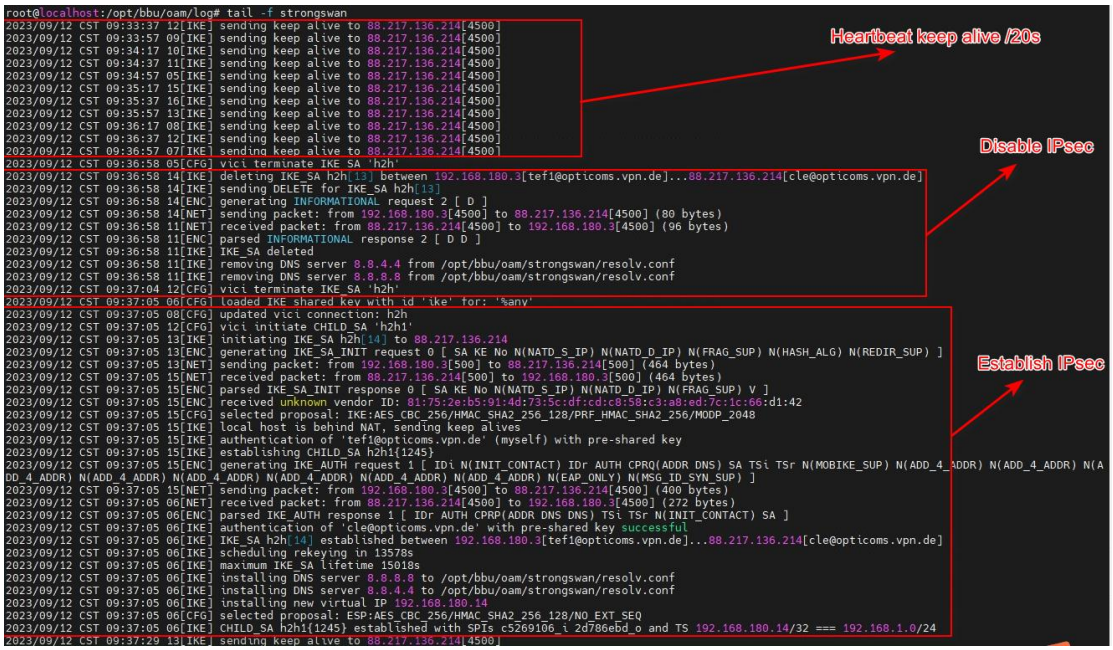
```
root@localhost:/opt/bbu/oam/pm/1# ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.5, Linux 4.19.68-241.00.2_N78_20230823_v2.5.4, aarch64):
  uptime: 13 hours, since Sep 11 19:24:39 2023
  malloc: sbrk 2658304, mmap 0, used 1647376, free 1010928
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 9
  loaded plugins: charon aes save-keys des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey
s-prf gmp curve25519 xcbc cmac hmac drbg attr kernel-netlink resolve socket-default stroke vici updown eap-sim eap-aka eap-aka-3gpp xauth-generic cou
Listening IP addresses:
  10.10.100.120
  192.168.180.3
  192.0.2.1
  192.0.2.2
  192.0.2.3
  192.0.2.10
  192.0.2.11
  192.0.2.12
  192.0.2.13
  192.0.3.1
Connections:
        h2h:  %any...88.217.136.214  IKEv1/2, dpddelay=60s
        h2h:   local:  [tef1@opticoms.vpn.de] uses pre-shared key authentication
        h2h:   remote: [cle@opticoms.vpn.de] uses pre-shared key authentication
       h2h1:   child:  dynamic === 192.168.1.0/24 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
        h2h[13]: ESTABLISHED 34 minutes ago, 192.168.180.3[tef1@opticoms.vpn.de]...88.217.136.214[cle@opticoms.vpn.de]
        h2h[13]: IKEv2 SPIs: fa3e1445a0bbea5d_i* 36580d084e3d0073_r, rekeying in 3 hours
        h2h[13]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
       h2h1{1244}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7e20fa3_i 639c7450_o
       h2h1{1244}:  AES_CBC_256/HMAC_SHA2_256_128, 89880 bytes_i (1070 pkts, 1s ago), 89880 bytes_o (1070 pkts, 2085s ago), rekeying in 20 minutes
       h2h1{1244}:   192.168.180.14/32 === 192.168.1.0/24
root@localhost:/opt/bbu/oam/pm/1#
```

Check established time: watch -n 1 "ipsec status"

```
Every 1.0s: ipsec status

Security Associations (1 up, 0 connecting):
         h2h[13]: ESTABLISHED 41 minutes ago, 192.168.180.3[tef1@opticoms.vpn.de]...88.217.136.214[cle@opticoms.vpn.de]
        h2h1{1244}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7e20fa3_i 639c7450_o
        h2h1{1244}:   192.168.180.14/32 === 192.168.1.0/24
```

4. IPsec Log




```
root@localhost:/opt/bbu/oam/log# tail -f strongswan
2023/09/12 CST 09:33:37 12[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:33:57 09[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:34:17 10[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:34:37 11[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:34:57 05[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:35:17 15[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:35:37 16[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:35:57 13[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:36:17 08[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:36:37 12[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:36:57 07[IKE] sending keep alive to 88.217.136.214[4500]
2023/09/12 CST 09:36:58 05[CFG] vici terminate IKE_SA 'h2h'
2023/09/12 CST 09:36:58 14[IKE] deleting IKE_SA h2h[13] between 192.168.180.3[tef1@opticoms.vpn.de]...88.217.136.214[cle@opticoms.vpn.de]
2023/09/12 CST 09:36:58 14[IKE] sending DELETE for IKE_SA h2h[13]
2023/09/12 CST 09:36:58 14[ENC] generating INFORMATIONAL request 2 [ D ]
2023/09/12 CST 09:36:58 14[NET] sending packet: from 192.168.180.3[4500] to 88.217.136.214[4500] (80 bytes)
2023/09/12 CST 09:36:58 11[NET] received packet: from 88.217.136.214[4500] to 192.168.180.3[4500] (96 bytes)
2023/09/12 CST 09:36:58 11[ENC] parsed INFORMATIONAL response 2 [ D D ]
2023/09/12 CST 09:36:58 11[IKE] IKE_SA deleted
2023/09/12 CST 09:36:58 11[IKE] removing DNS server 8.8.4.4 from /opt/bbu/oam/strongswan/resolv.conf
2023/09/12 CST 09:36:58 11[IKE] removing DNS server 8.8.8.8 from /opt/bbu/oam/strongswan/resolv.conf
2023/09/12 CST 09:37:04 12[CFG] vici terminate IKE_SA 'h2h'
2023/09/12 CST 09:37:05 06[CFG] loaded IKE shared key with id 'ike' for: '%any'
2023/09/12 CST 09:37:05 08[CFG] updated vici connection: h2h
2023/09/12 CST 09:37:05 12[CFG] vici initiate CHILD_SA 'h2h1'
2023/09/12 CST 09:37:05 13[IKE] initiating IKE_SA h2h[14] to 88.217.136.214
2023/09/12 CST 09:37:05 13[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
2023/09/12 CST 09:37:05 13[NET] sending packet: from 192.168.180.3[500] to 88.217.136.214[500] (464 bytes)
2023/09/12 CST 09:37:05 15[NET] received packet: from 88.217.136.214[500] to 192.168.180.3[500] (464 bytes)
2023/09/12 CST 09:37:05 15[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) V ]
2023/09/12 CST 09:37:05 15[ENC] received unknown vendor ID: 81:75:2e:b5:91:4d:73:5c:df:cd:c8:58:c3:a8:ed:7c:1c:66:d1:42
2023/09/12 CST 09:37:05 15[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
2023/09/12 CST 09:37:05 15[IKE] local host is behind NAT, sending keep alives
2023/09/12 CST 09:37:05 15[IKE] authentication of 'tef1@opticoms.vpn.de' (myself) with pre-shared key
2023/09/12 CST 09:37:05 15[IKE] establishing CHILD_SA h2h1{1245}
2023/09/12 CST 09:37:05 15[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH CPRQ(ADDR DNS) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2023/09/12 CST 09:37:05 15[NET] sending packet: from 192.168.180.3[4500] to 88.217.136.214[4500] (400 bytes)
2023/09/12 CST 09:37:05 06[NET] received packet: from 88.217.136.214[4500] to 192.168.180.3[4500] (272 bytes)
2023/09/12 CST 09:37:05 06[ENC] parsed IKE_AUTH response 1 [ IDr AUTH CPRP(ADDR DNS DNS) TSi TSr N(INIT_CONTACT) SA ]
2023/09/12 CST 09:37:05 06[IKE] authentication of 'cle@opticoms.vpn.de' with pre-shared key successful
2023/09/12 CST 09:37:05 06[IKE] IKE_SA h2h[14] established between 192.168.180.3[tef1@opticoms.vpn.de]...88.217.136.214[cle@opticoms.vpn.de]
2023/09/12 CST 09:37:05 06[IKE] scheduling rekeying in 13578s
2023/09/12 CST 09:37:05 06[IKE] maximum IKE_SA lifetime 15018s
2023/09/12 CST 09:37:05 06[IKE] installing DNS server 8.8.8.8 to /opt/bbu/oam/strongswan/resolv.conf
2023/09/12 CST 09:37:05 06[IKE] installing DNS server 8.8.4.4 to /opt/bbu/oam/strongswan/resolv.conf
2023/09/12 CST 09:37:05 06[IKE] installing new virtual IP 192.168.180.14
2023/09/12 CST 09:37:05 06[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
2023/09/12 CST 09:37:05 06[IKE] CHILD_SA h2h1{1245} established with SPIs c5269106_i 2d786ebd_o and TS 192.168.180.14/32 === 192.168.1.0/24
2023/09/12 CST 09:37:29 13[IKE] sending keep alive to 88.217.136.214[4500]
```