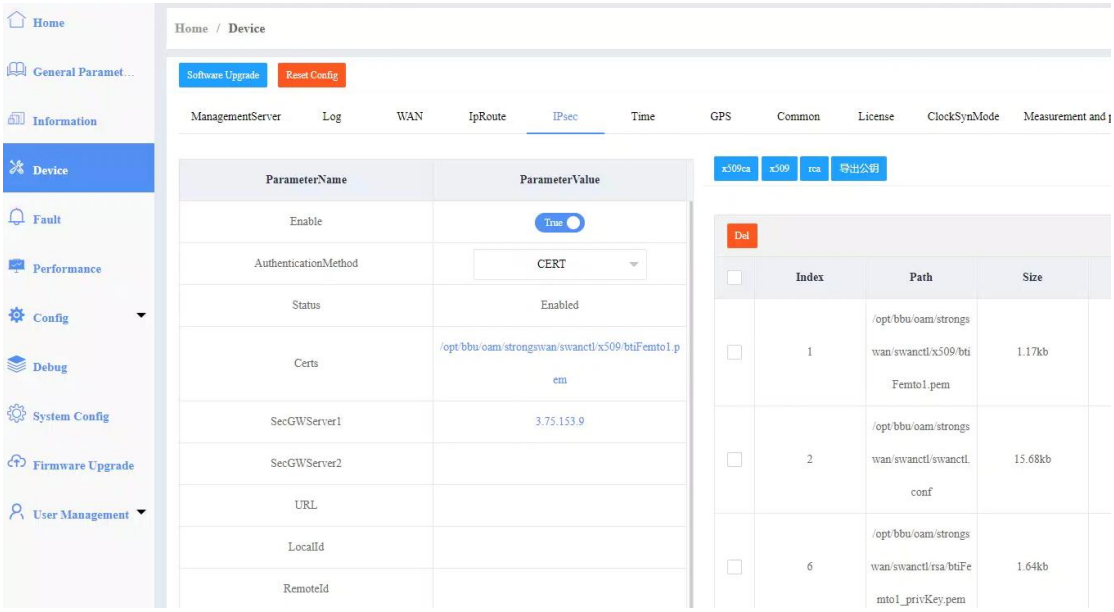
How to configure Femto Ipsec-Certification method

1. Achieve Negotiation parameter with Security gateway server

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

2. Ipsec parameter Configuration



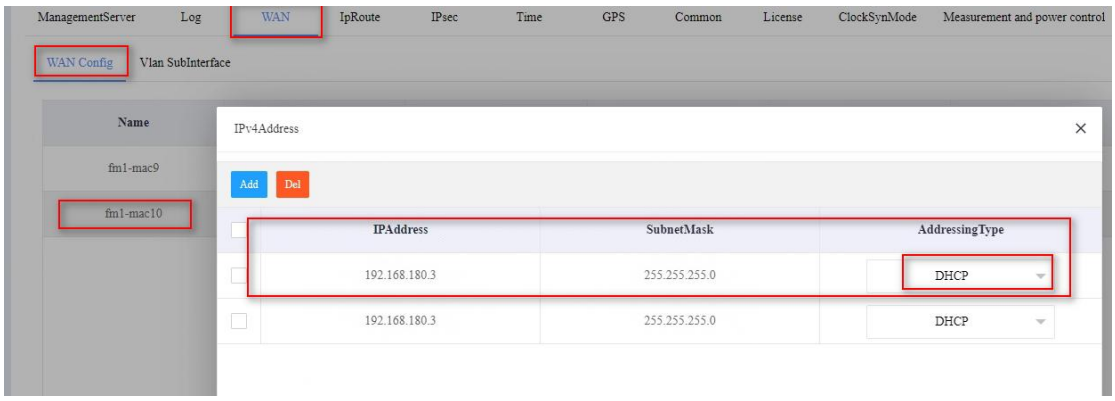
Child SA:

ChildSA

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

WAN Config: (DHCP or Static)

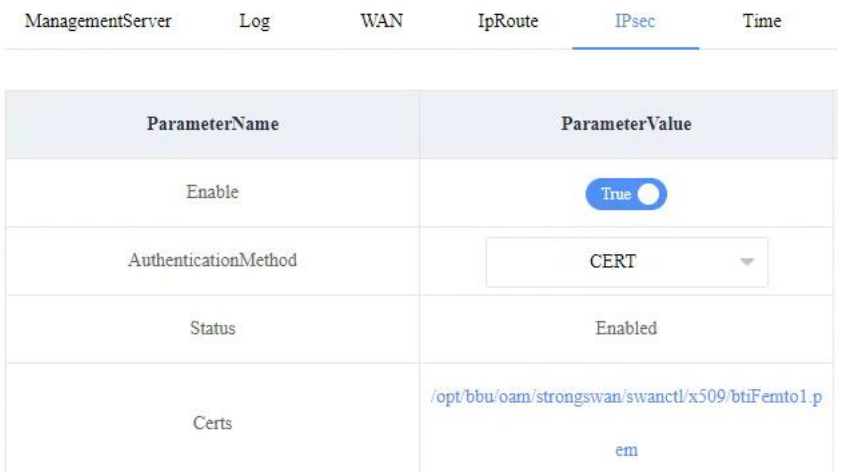
If vip of ipsec is enabled and DHCP is selected, a virtual ip will be allocated auto.



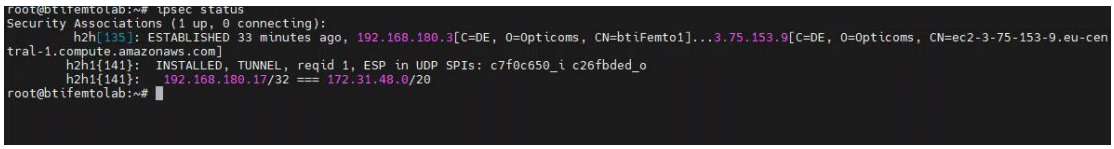
AMF LocalUpIPAdress should be configured same as VIP.

3. IPsec Status check

Check in webgui:



Check by commands: ipsec status



Check by commands: ipsec statusall

```
root@btifemtolab:~# ipsec allstatus
/usr/sbin/ipsec: unknown command `allstatus' (`ipsec --help' for list)
root@btifemtolab:~# 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: 5 days, since Oct 10 13:17:01 2023
  malloc: sbrk 4247552, mmap 0, used 2771712, free 1475840
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 10
  loaded plugins: charon aes save-keys des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem fips-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 counters
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...3.75.153.9  IKEv1/2, dpddelay=60s
        h2h:   local:  [C=DE, O=Opticoms, CN=btiFemto1] uses public key authentication
        h2h:    cert:  "C=DE, O=Opticoms, CN=btiFemto1"
        h2h:   remote: uses public key authentication
       h2h1:   child:  dynamic === 172.31.48.0/20 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
        h2h[135]: ESTABLISHED 35 minutes ago, 192.168.180.3[C=DE, O=Opticoms, CN=btiFemto1]...3.75.153.9[C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-cen
tral-1.compute.amazonaws.com]
        h2h[135]: IKEv2 SPIs: 8c49d39fa3abebf5_i fd914eac4446d093_r*, rekeying in 3 hours
        h2h[135]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
       h2h1{141}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7f0c650_i c26fbded_o
       h2h1{141}:  AES_CBC_256/HMAC_SHA2_256_128/MODP_2048, 19068 bytes_i (227 pkts, 2s ago), 19068 bytes_o (227 pkts, 428s ago), rekeying in 47 mi
nutes
       h2h1{141}:   192.168.180.17/32 === 172.31.48.0/20
```

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

```
Every 1.0s: ipsec status                                                                    btifemtolab: Mon Oct 16 00:16:23 2023

Security Associations (1 up, 0 connecting):
        h2h[135]: ESTABLISHED 36 minutes ago, 192.168.180.3[C=DE, O=Opticoms, CN=btiFemto1]...3.75.153.9[C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-cen
tral-1.compute.amazonaws.com]
       h2h1{141}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c7f0c650_i c26fbded_o
       h2h1{141}:   192.168.180.17/32 === 172.31.48.0/20
```

4. IPsec Log

```
2023/10/16 CEST 00:19:44 10[IKE] sending keep alive to 3.75.153.9[4500]
2023/10/16 CEST 00:19:53 09[CFG] vici terminate IKE_SA 'h2h'
2023/10/16 CEST 00:19:53 05[IKE] deleting IKE_SA h2h[135] between 192.168.180.3[C=DE, O=Opticoms, CN=btiFemto1]...3.75.153.9[C=DE, O=Opticoms, CN=ec
2-3-75-153-9.eu-central-1.compute.amazonaws.com]
2023/10/16 CEST 00:19:53 05[IKE] sending DELETE for IKE_SA h2h[135]
2023/10/16 CEST 00:19:53 05[ENC] generating INFORMATIONAL request 2 [ D ]
2023/10/16 CEST 00:19:53 05[NET] sending packet: from 192.168.180.3[4500] to 3.75.153.9[4500] (80 bytes)
2023/10/16 CEST 00:19:53 14[NET] received packet: from 3.75.153.9[4500] to 192.168.180.3[4500] (80 bytes)
2023/10/16 CEST 00:19:53 14[ENC] parsed INFORMATIONAL response 2 [ ]
2023/10/16 CEST 00:19:53 14[IKE] IKE_SA deleted
2023/10/16 CEST 00:20:01 15[CFG] vici terminate IKE_SA 'h2h'
2023/10/16 CEST 00:20:04 06[CFG] loaded certificate 'C=DE, O=Opticoms, CN=btiFemto1'
2023/10/16 CEST 00:20:04 06[CFG] loaded certificate 'C=DE, O=Opticoms, CN=Opticoms Root CA'
2023/10/16 CEST 00:20:04 06[CFG] loaded RSA private key
2023/10/16 CEST 00:20:04 06[CFG]   id not specified, defaulting to cert subject 'C=DE, O=Opticoms, CN=btiFemto1'
2023/10/16 CEST 00:20:04 06[CFG] updated vici connection: h2h
2023/10/16 CEST 00:20:04 06[CFG] vici initiate CHILD_SA 'h2h1'
2023/10/16 CEST 00:20:04 15[IKE] initiating IKE_SA h2h[136] to 3.75.153.9
2023/10/16 CEST 00:20:04 15[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) ]
2023/10/16 CEST 00:20:04 15[NET] sending packet: from 192.168.180.3[500] to 3.75.153.9[500] (464 bytes)
2023/10/16 CEST 00:20:04 11[NET] received packet: from 3.75.153.9[500] to 192.168.180.3[500] (497 bytes)
2023/10/16 CEST 00:20:04 11[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N
(MULT_AUTH) ]
2023/10/16 CEST 00:20:04 11[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
2023/10/16 CEST 00:20:05 11[IKE] local host is behind NAT, sending keep alives
2023/10/16 CEST 00:20:05 11[IKE] remote host is behind NAT
2023/10/16 CEST 00:20:05 11[IKE] received cert request for "C=DE, O=Opticoms, CN=Opticoms Root CA"
2023/10/16 CEST 00:20:05 11[IKE] sending cert request for "C=DE, O=Opticoms, CN=Opticoms Root CA"
2023/10/16 CEST 00:20:05 11[IKE] authentication of 'C=DE, O=Opticoms, CN=btiFemto1' (myself) with RSA_EMSA_PKCS1_SHA2_256 successful
2023/10/16 CEST 00:20:05 11[IKE] sending end entity cert "C=DE, O=Opticoms, CN=btiFemto1"
2023/10/16 CEST 00:20:05 11[IKE] establishing CHILD_SA h2h1{142}
2023/10/16 CEST 00:20:05 11[ENC] generating IKE_AUTH request 1 [ IDi CERT CERTREQ 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(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2023/10/16 CEST 00:20:05 11[ENC] splitting IKE message (1520 bytes) into 2 fragments
2023/10/16 CEST 00:20:05 11[ENC] generating IKE_AUTH request 1 [ EF(1/2) ]
2023/10/16 CEST 00:20:05 11[ENC] generating IKE_AUTH request 1 [ EF(2/2) ]
2023/10/16 CEST 00:20:05 11[NET] sending packet: from 192.168.180.3[4500] to 3.75.153.9[4500] (1236 bytes)
2023/10/16 CEST 00:20:05 11[NET] sending packet: from 192.168.180.3[4500] to 3.75.153.9[4500] (356 bytes)
2023/10/16 CEST 00:20:05 12[NET] received packet: from 3.75.153.9[4500] to 192.168.180.3[4500] (1236 bytes)
2023/10/16 CEST 00:20:05 12[ENC] parsed IKE_AUTH response 1 [ EF(1/2) ]
2023/10/16 CEST 00:20:05 12[ENC] received fragment #1 of 2, waiting for complete IKE message
2023/10/16 CEST 00:20:05 10[NET] received packet: from 3.75.153.9[4500] to 192.168.180.3[4500] (372 bytes)
2023/10/16 CEST 00:20:05 10[ENC] parsed IKE_AUTH response 1 [ EF(2/2) ]
2023/10/16 CEST 00:20:05 10[ENC] received fragment #2 of 2, reassembled fragmented IKE message (1536 bytes)
2023/10/16 CEST 00:20:05 10[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR) 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) ]
2023/10/16 CEST 00:20:05 10[IKE] received end entity cert "C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-central-1.compute.amazonaws.com"
2023/10/16 CEST 00:20:05 10[CFG]   using certificate "C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-central-1.compute.amazonaws.com"
2023/10/16 CEST 00:20:05 10[CFG]   using trusted ca certificate "C=DE, O=Opticoms, CN=Opticoms Root CA"
2023/10/16 CEST 00:20:05 10[CFG] checking certificate status of "C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-central-1.compute.amazonaws.com"
2023/10/16 CEST 00:20:05 10[CFG] certificate status is not available
2023/10/16 CEST 00:20:05 10[CFG]   reached self-signed root ca with a path length of 0
2023/10/16 CEST 00:20:05 10[IKE] authentication of 'C=DE, O=Opticoms, CN=ec2-3-75-153-9.eu-central-1.compute.amazonaws.com' with RSA_EMSA_PKCS1_SHA2
_256 successful
2023/10/16 CEST 00:20:05 10[IKE] IKE_SA h2h[136] established between 192.168.180.3[C=DE, O=Opticoms, CN=btiFemto1]...3.75.153.9[C=DE, O=Opticoms, CN
=ec2-3-75-153-9.eu-central-1.compute.amazonaws.com]
2023/10/16 CEST 00:20:05 10[IKE] scheduling rekeying in 14101s
2023/10/16 CEST 00:20:05 10[IKE] maximum IKE_SA lifetime 15541s
2023/10/16 CEST 00:20:05 10[IKE] installing new virtual IP 192.168.180.17
2023/10/16 CEST 00:20:05 10[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ
2023/10/16 CEST 00:20:05 10[IKE] CHILD_SA h2h1{142} established with SPIs c4907912_i c4f003c4_o and TS 192.168.180.17/32 === 172.31.48.0/20
2023/10/16 CEST 00:20:05 10[IKE] peer supports MOBIKE
2023/10/16 CEST 00:20:30 12[IKE] sending keep alive to 3.75.153.9[4500]
```