Troubleshooting IKEv2 IPSEC

**Labels: HPE Router, HPE Comware Switch**

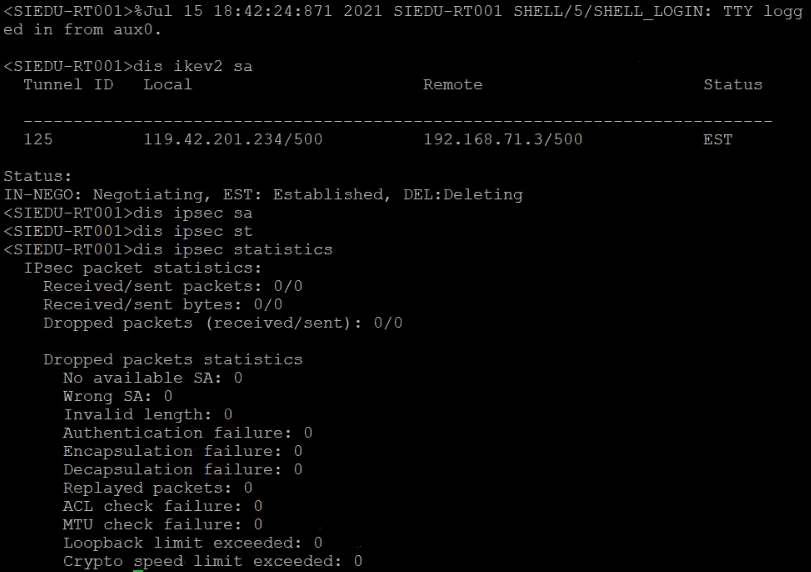
**Problem:**

-----------------------------------------------------------------------

**Scenario:** IKEv2 Phase 1 SA is already established, but phase 2 SA is not getting established between HPE MSR router 3012 (JG409B) and Fortigate Firewall 201F.

**Below could be observed:**

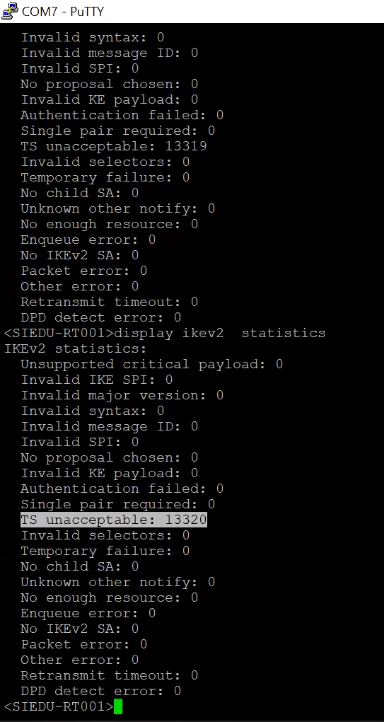
IKEv2 phase 1 SA(Security Association) is established, but phase 2 SA is down.

[](https://akb.arubanetworks.com/media/ckuploads/1110/2021/07/17/phase1-sa-is-estableshed-phase-2-is-down.PNG)

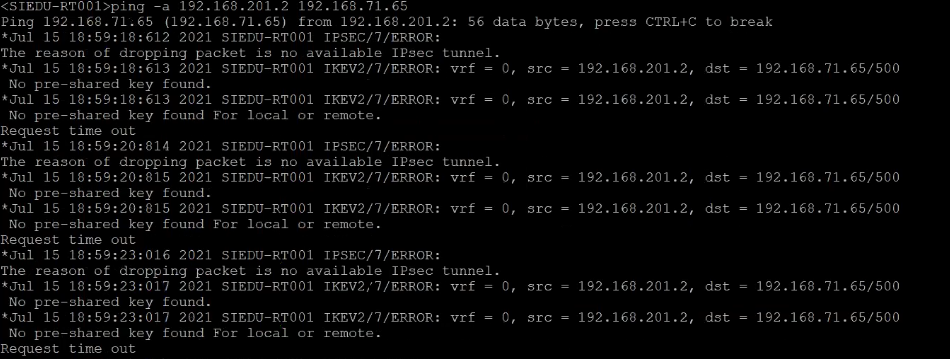
**Diagnostics:**

-----------------------------------------------------------------------

From **display ikev2 statistics** we could observe that **Unacceptable TS(Transport Selector) payload** is increasing.

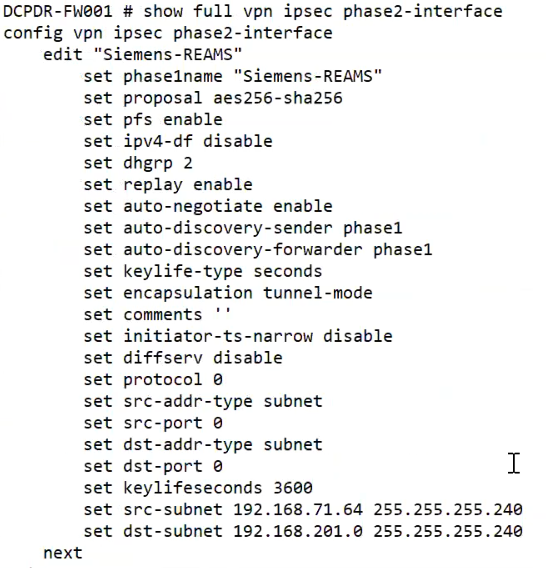


Also, debug error for ikev2 and ipsec shows ipsec tunnel is down because it could not find pre-shared key for phase 2.

[](https://akb.arubanetworks.com/media/ckuploads/1110/2021/07/17/debug-ikev2-ipsec-errors.PNG)

Config on Fortigate for Phase 2 and config on MSR router looks like below respectively:

Fortigate:



**MSR Router:**

#

interface GigabitEthernet0/0  
 port link-mode route  
 combo enable copper  
 ip address 119.42.201.234 255.255.255.252  
 tcp mss 1280  
 ipsec apply policy Siemens-REAMS-ipsec-policy

#  
acl advanced 3010  
 description IPSec Siemens  
 rule 0 permit ip source 192.168.201.0 0.0.0.15 destination 192.168.71.64 0.0.0.15  
 rule 5 permit ip source 192.168.71.64 0.0.0.15 destination 192.168.201.0 0.0.0.15

#

ipsec transform-set Siemens-REAMS-transform-set  
 esp encryption-algorithm gcm-256  
 pfs dh-group2  
#  
ipsec policy Siemens-REAMS-ipsec-policy 2 isakmp  
 transform-set Siemens-REAMS-transform-set  
 security acl 3010  
 local-address 192.168.201.2  
 remote-address 192.168.71.64  
 ikev2-profile Siemens-REAMS-profile  
 sa duration time-based 180  
#  
ikev2 keychain SiemensREAMSkeychain  
 peer DC  
  address 192.168.71.3 255.255.255.192  
  pre-shared-key local ciphertext $c$3$DJa4eQ+f5u62/G2Co9XRekhQRSNwBEmR9Xtr3yqlub1+d0Q=  
  pre-shared-key remote ciphertext $c$3$gzNYxAVGxfYSmdARtEVI+UFo8ihLRvpPD5qjpCtTRB9Weh8=  
#  
ikev2 profile Siemens-REAMS-profile  
 authentication-method local pre-share  
 authentication-method remote pre-share  
 keychain SiemensREAMSkeychain  
 identity local address 119.42.201.234  
 match remote identity address 192.168.71.3 255.255.255.192  
#  
ikev2 proposal 2  
 encryption aes-cbc-256  
 integrity sha256  
 dh group2  
#  
ikev2 policy Pol-2  
 proposal 2  
 match local address GigabitEthernet 2/0/0

**Solution:**

-----------------------------------------------------------------------

To understand ikev2 issues, knowing the configuration of ikev2 helps:

There are two sets of proposals used to establish SA in both IKEv2 Phase 1 and Phase 2.

First for Phase 1 from below config we can understand that it's using aes-cbc-256 for encryption, sha256 for integrity(HMAC) and Group2 for Diffie Hellman(DH) key exchange.

ikev2 proposal 2  
**encryption aes-cbc-256  
 integrity sha256  
 dh group2**  
#  
ikev2 policy Pol-2  
 proposal 2  
 match local address GigabitEthernet 2/0/0

Above mentioned proposals are used only in Phase 1 and for Phase 2 we have below config:

ipsec transform-set Siemens-REAMS-transform-set  
 **esp encryption-algorithm aes-cbc-256  
 esp authentication-algorithm sha256  
 pfs dh-group2**

Please note: Phase 1 and Phase 2 proposals can be different.

But the issue was not with proposals, but with below config under ipsec policy .

local-address 192.168.201.2  
remote-address 192.168.71.64

Both local and remote addresses should be interfaces facing Public(Outside) network on HPE and Fortigate respectively, but ip used was from Private(Inside) facing interfaces for each device.

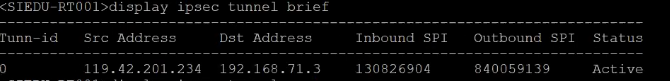
After correction, we could see that IPSEC SA got established with below SA and tunnel details:

<SIEDU-RT001>display ipsec sa  
-------------------------------  
Interface: GigabitEthernet0/0  
-------------------------------

  -----------------------------  
  IPsec policy: Siemens-REAMS-ipsec-policy  
  Sequence number: 2  
  Mode: ISAKMP  
  -----------------------------  
    Tunnel id: 0  
    Encapsulation mode: tunnel  
    Perfect Forward Secrecy: dh-group2  
    Inside VPN:  
    Extended Sequence Numbers enable: N  
    Traffic Flow Confidentiality enable: Y  
    Path MTU: 1424  
    Tunnel:  
        local  address: 119.42.201.234  
        remote address: 192.168.71.3  
    Flow:  
        sour addr: 192.168.201.0/255.255.255.240  port: 0  protocol: ip  
        dest addr: 192.168.71.64/255.255.255.240  port: 0  protocol: ip

    [Inbound ESP SAs]  
      SPI: 3544911463 (0xd34b0e67)  
      Connection ID: 700079669249  
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256  
      SA duration (kilobytes/sec): 1843200/180  
      SA remaining duration (kilobytes/sec): 1843200/139  
      Max received sequence-number: 0  
      Anti-replay check enable: Y  
      Anti-replay window size: 64  
      UDP encapsulation used for NAT traversal: N  
      Status: Active

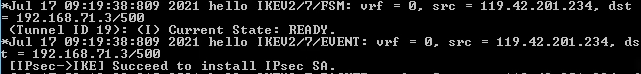
    [Outbound ESP SAs]  
      SPI: 840059309 (0x321249ad)  
      Connection ID: 365072220160  
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256  
      SA duration (kilobytes/sec): 1843200/180  
      SA remaining duration (kilobytes/sec): 1843200/139  
      Max sent sequence-number: 0  
      UDP encapsulation used for NAT traversal: N  
      Status: Active



Moreover, debug ikev2 and ipsec logs from different physical router(same MSR router model) shows similar results.

It illustrates that after Child SA gets established, it results in creation of IKEv2 phase2 SA and phase 2 IKEv2 SA takes over.

https://akb.arubanetworks.com/media/ckuploads/1110/2021/07/18/child-established.PNG



https://akb.arubanetworks.com/media/ckuploads/1110/2021/07/18/ikev2-phase-2-activated.PNG

Tags: HPE Router, HPE Comware Switch, 10.01.0040, ikev2, #ipsec, fortigate, #transport, #selector