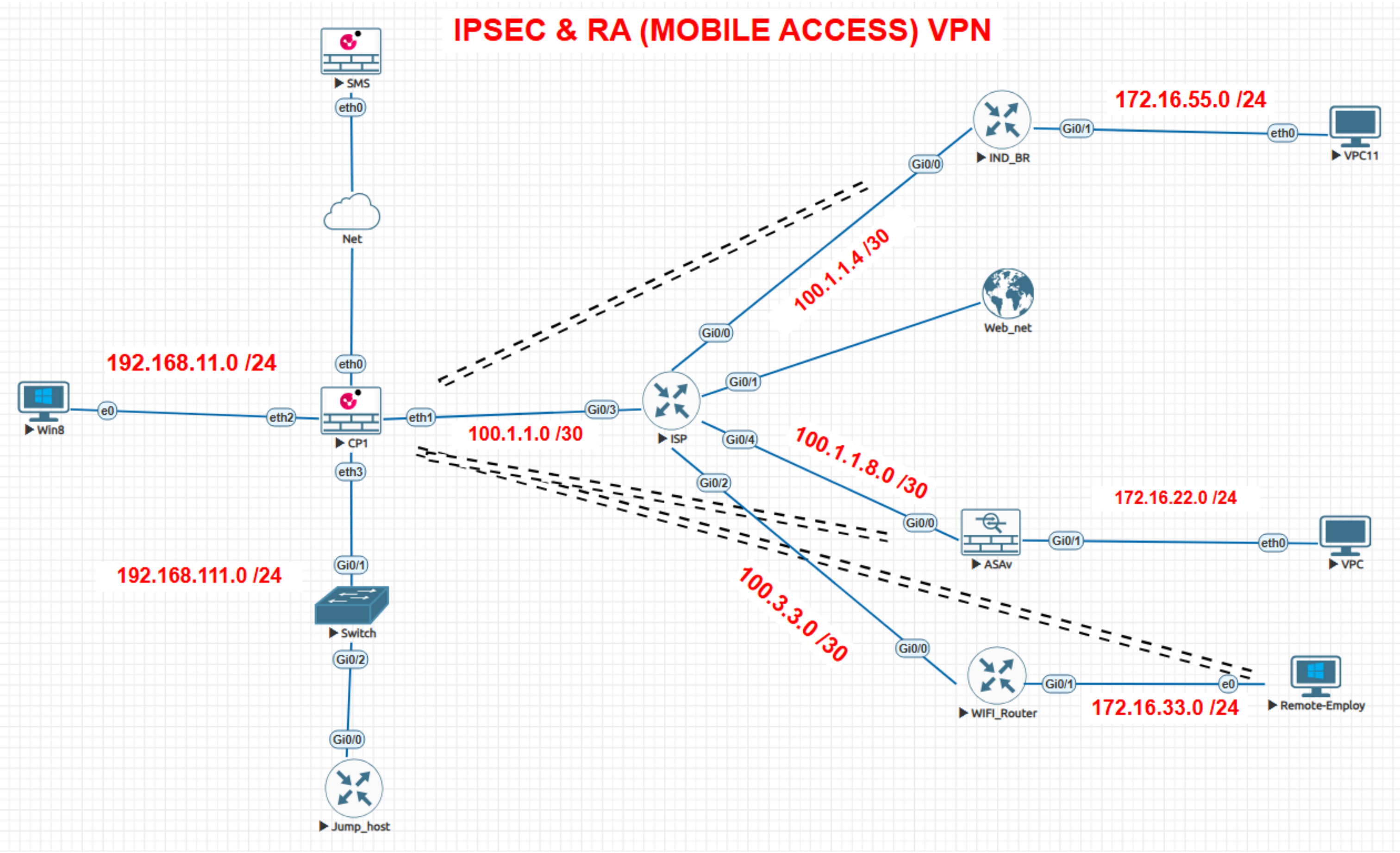
TOPOLOGY



Checkpoint:

INT	IP
LAN -	192.168.11.254
WAN -	100.1.1.1
DMZ -	192.168.111.254

ASA:

INT	IP
INSIDE -	172.16.22.9
OUTSIDE -	100.1.1.9

Router:

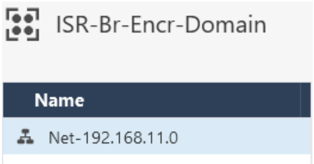
INT	IP
g0/1 -	172.16.55.5
g0/0 -	100.1.1.5

SA - (Security Association): a one-way (inbound or outbound) agreement between two communicating peers that specifies the IPsec protections to be provided to their communications. This includes the specific security protections, cryptographic algorithms, and secret keys to be applied, as well as the specific types of traffic to be protected.

Checkpoint Configuration

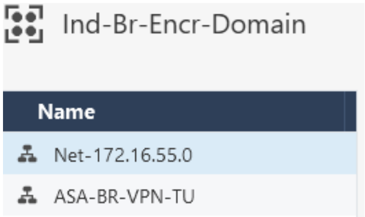
1. Create Groups:

IN 1st group, I have set 1 encryption domain. In 2nd group, I have set 2 encryption domains (Remote-Branch).



ISR-Br-Encr-Domain

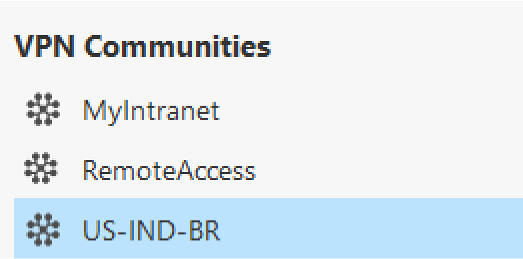
Name
Net-192.168.11.0



Ind-Br-Encr-Domain

Name
Net-172.16.55.0
ASA-BR-VPN-TU

2. Create a VPN Community (Gateway, Encryption methods, Lifetime, Shared Secret)

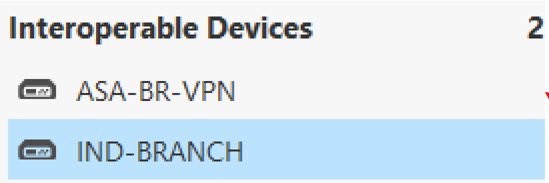


VPN Communities

- MyIntranet
- RemoteAccess
- US-IND-BR

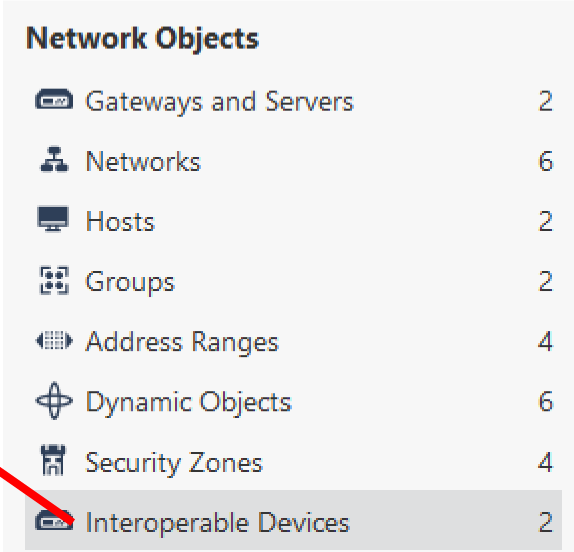
3. Create an Interoperable Devices

i. Remote-public ip
ii. Remote-Encryption domain



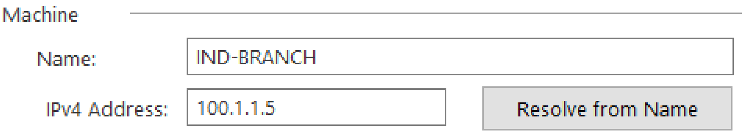
Interoperable Devices 2

- ASA-BR-VPN
- IND-BRANCH



Network Objects

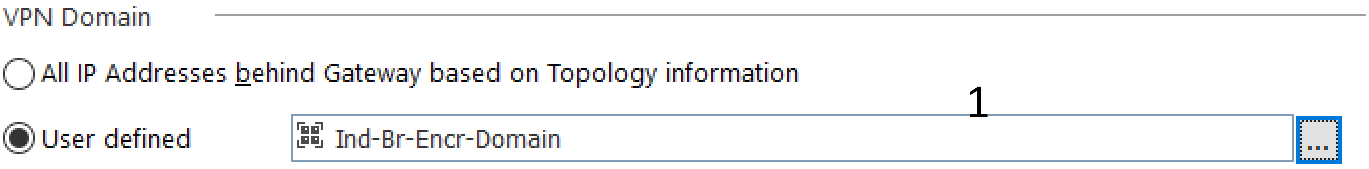
Gateways and Servers	2
Networks	6
Hosts	2
Groups	2
Address Ranges	4
Dynamic Objects	6
Security Zones	4
Interoperable Devices	2



Machine

Name: IND-BRANCH

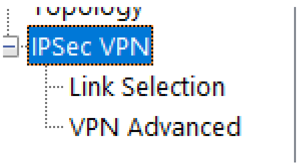
IPv4 Address: 100.1.1.5

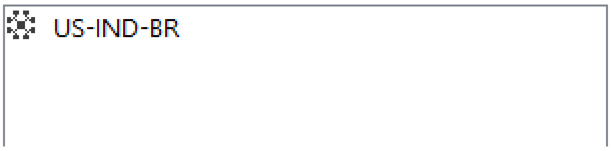


VPN Domain

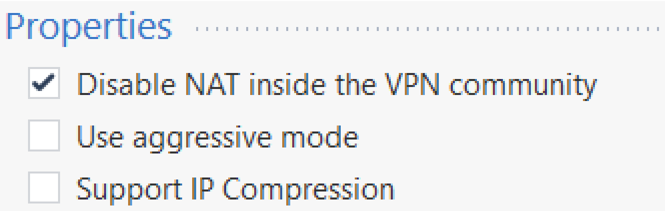
○ All IP Addresses behind Gateway based on Topology information

● User defined Ind-Br-Encr-Domain





US-IND-BR



Properties

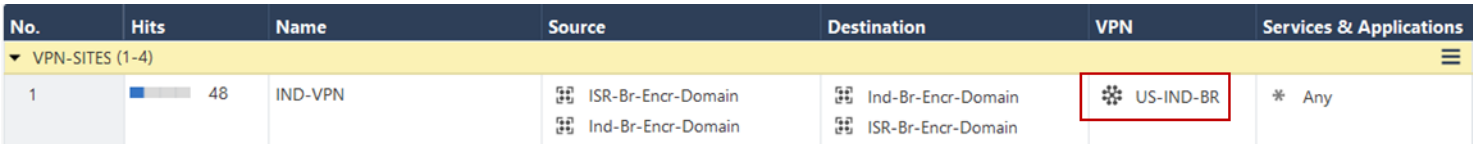
☑ Disable NAT inside the VPN community

☐ Use aggressive mode

☐ Support IP Compression

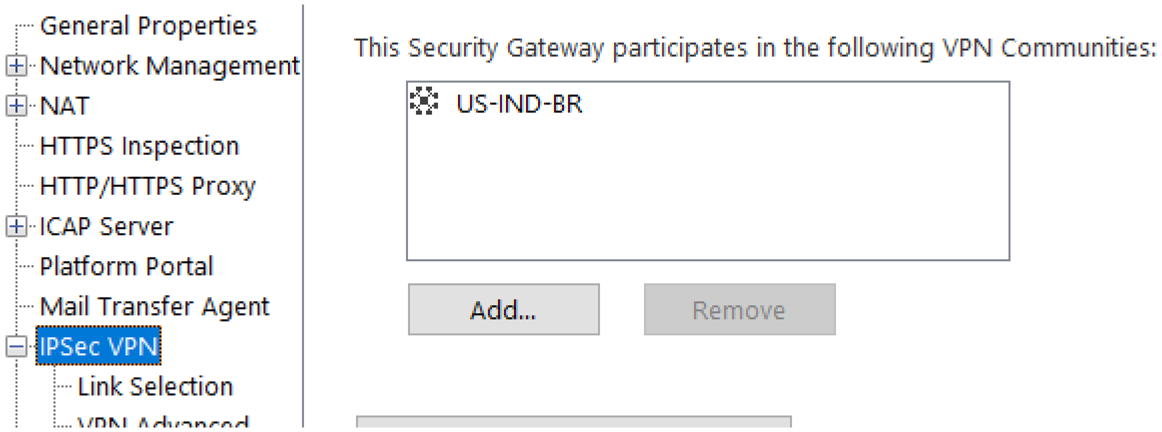
Checkpoint Configuration

4. Create a policy so that matched traffic go through tunnel



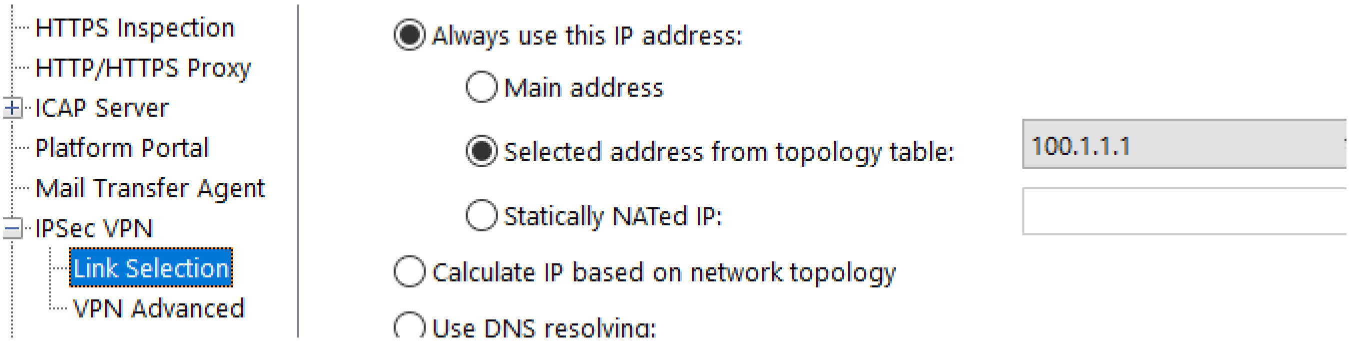
No.	Hits	Name	Source	Destination	VPN	Services & Applications
▾ VPN-SITES (1-4)						
1	48	IND-VPN	ISR-Br-Encr-Domain Ind-Br-Encr-Domain	Ind-Br-Encr-Domain ISR-Br-Encr-Domain	US-IND-BR	Any

5. Define which public IP the gateway should use to send VPN traffic (by default, the gateway's management interface IP is used).



This Security Gateway participates in the following VPN Communities:

US-IND-BR



● Always use this IP address:

○ Main address

● Selected address from topology table: 100.1.1.1

○ Statically NATed IP:

○ Calculate IP based on network topology

○ Use DNS resolving:

ASA COFIGURATION

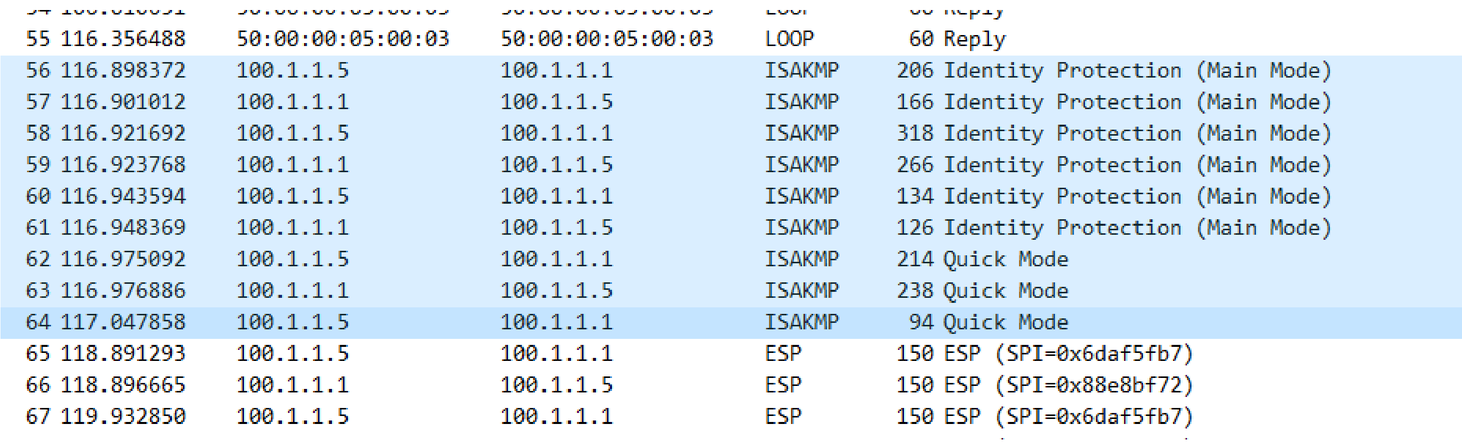
```
crypto ikev1 enable outside
crypto ikev1 policy 10
    hash md5
    authentication pre-share
    group 2
    lifetime 86400
    encryption des
tunnel-group 100.1.1.1 type ipsec-l2l
tunnel-group 100.1.1.1 ipsec-attributes
    ikev1 pre-shared-key Shan_home-Car@1234334324
object network LOCAL-NET
    subnet 172.16.22.0 255.255.255.0
object network REMOTE-NET
    subnet 192.168.11.0 255.255.255.0
nat (inside,outside) source static LOCAL-NET LOCAL-NET destination static REMOTE-NET REMOTE-NET
access-list VPN-ACL extended permit ip 172.16.22.0 255.255.255.0 192.168.11.0 255.255.255.0
crypto ipsec ikev1 transform-set TSET esp-des esp-md5-hmac
crypto map CMAP 10 match address VPN-ACL
crypto map CMAP 10 set peer 100.1.1.1
crypto map CMAP 10 set ikev1 transform-set TSET
crypto map CMAP interface outside


route outside 0 0 100.1.1.10 1
```

IND-Router Configuration

```
crypto isakmp policy 10
    authentication pre-share
    hash sha
    group 2
    lifetime 86400
    encryption aes
crypto isakmp key Shan_home-Car@5663355236
address 100.1.1.1
access-list 100 permit ip 172.16.55.0  0.0.0.255
192.168.11.0   0.0.0.255
crypto ipsec transform-set TR-SET esp-aes  esp-sha-hmac
crypto map CMAP 10 policy ipsec-isakmp
     set peer 100.1.1.1
     set transform-set TR-SET
     match address 100
int g0/0
     crypto map CMAP
ip access-list extended dontFragment
     deny icmp any any fragement
     permit ip any any
int g0/0
     ip access-group dontFragment in
```

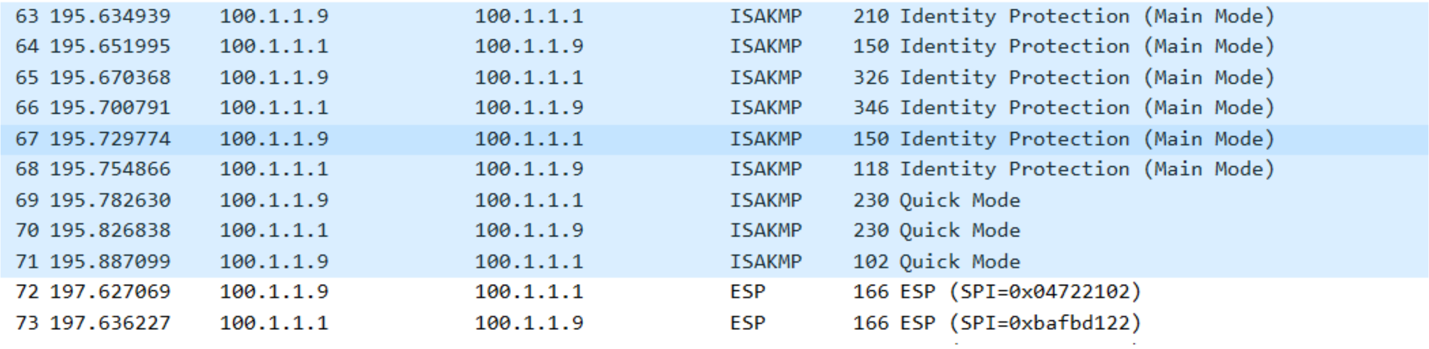
PING

ping from 172.16.55.1 to 192.168.11.11



```
55 116.356488   50:00:00:05:00:03   50:00:00:05:00:03   LOOP     60 Reply
56 116.898372   100.1.1.5           100.1.1.1           ISAKMP  206 Identity Protection (Main Mode)
57 116.901012   100.1.1.1           100.1.1.5           ISAKMP  166 Identity Protection (Main Mode)
58 116.921692   100.1.1.5           100.1.1.1           ISAKMP  318 Identity Protection (Main Mode)
59 116.923768   100.1.1.1           100.1.1.5           ISAKMP  266 Identity Protection (Main Mode)
60 116.943594   100.1.1.5           100.1.1.1           ISAKMP  134 Identity Protection (Main Mode)
61 116.948369   100.1.1.1           100.1.1.5           ISAKMP  126 Identity Protection (Main Mode)
62 116.975092   100.1.1.5           100.1.1.1           ISAKMP  214 Quick Mode
63 116.976886   100.1.1.1           100.1.1.5           ISAKMP  238 Quick Mode
64 117.047858   100.1.1.5           100.1.1.1           ISAKMP   94 Quick Mode
65 118.891293   100.1.1.5           100.1.1.1           ESP     150 ESP (SPI=0x6daf5fb7)
66 118.896665   100.1.1.1           100.1.1.5           ESP     150 ESP (SPI=0x88e8bf72)
67 119.932850   100.1.1.5           100.1.1.1           ESP     150 ESP (SPI=0x6daf5fb7)
```

ping from 172.16.22.1 to 192.168.11.11



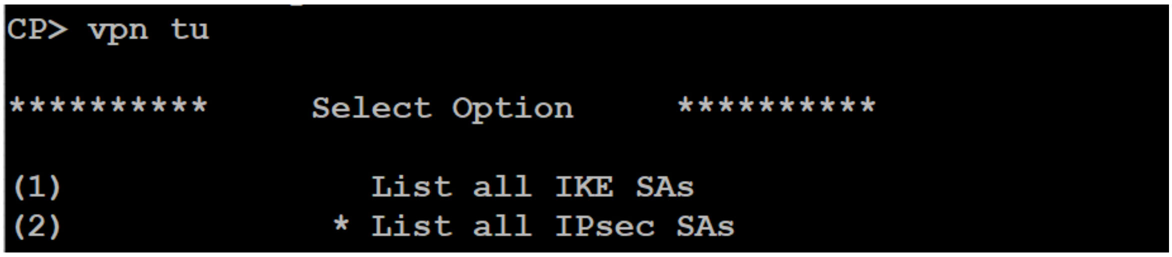
```
63 195.634939   100.1.1.9   100.1.1.1   ISAKMP  210 Identity Protection (Main Mode)
64 195.651995   100.1.1.1   100.1.1.9   ISAKMP  150 Identity Protection (Main Mode)
65 195.670368   100.1.1.9   100.1.1.1   ISAKMP  326 Identity Protection (Main Mode)
66 195.700791   100.1.1.1   100.1.1.9   ISAKMP  346 Identity Protection (Main Mode)
67 195.729774   100.1.1.9   100.1.1.1   ISAKMP  150 Identity Protection (Main Mode)
68 195.754866   100.1.1.1   100.1.1.9   ISAKMP  118 Identity Protection (Main Mode)
69 195.782630   100.1.1.9   100.1.1.1   ISAKMP  230 Quick Mode
70 195.826838   100.1.1.1   100.1.1.9   ISAKMP  230 Quick Mode
71 195.887099   100.1.1.9   100.1.1.1   ISAKMP  102 Quick Mode
72 197.627069   100.1.1.9   100.1.1.1   ESP     166 ESP (SPI=0x04722102)
73 197.636227   100.1.1.1   100.1.1.9   ESP     166 ESP (SPI=0xbafbd122)
```

SITE-TO-SITE VPN (TROUBLESHOOT) On Checkpoint

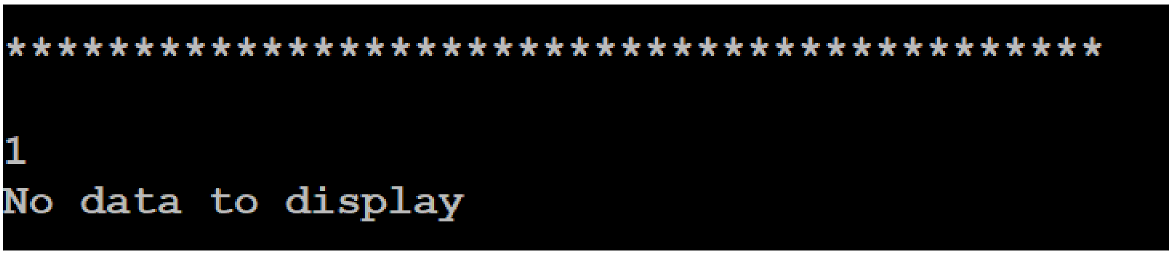
1. SA MISAMTCH:

Hagle Parameter Mismatch

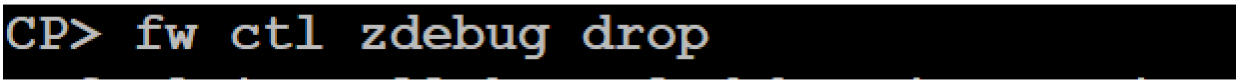
H – Hash - md5, sha
A – Authentication -
G – DH Group – 2,5 ……
L – Lifetime - <60-86400> seconds
E – Encryption - des, 3des, aes, aes-gcm



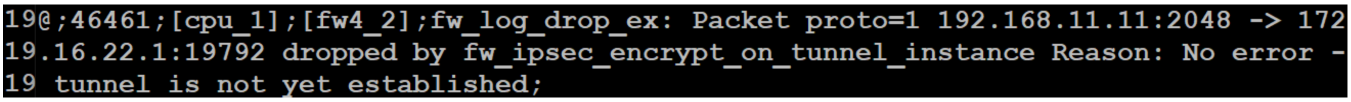
```
CP> vpn tu

**********     Select Option     **********

(1)                 List all IKE SAs
(2)               * List all IPsec SAs
```



```
*******************************************

1
No data to display
```

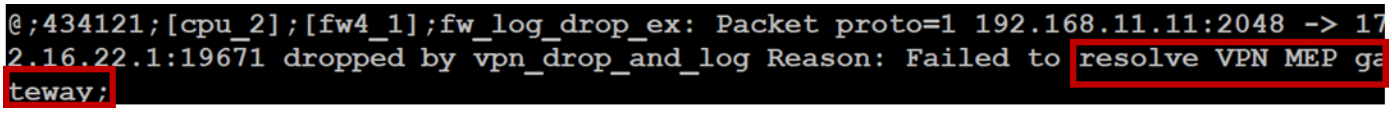


```
CP> fw ctl zdebug drop
```



```
19@;46461;[cpu_1];[fw4_2];fw_log_drop_ex: Packet proto=1 192.168.11.11:2048 -> 172
19.16.22.1:19792 dropped by fw_ipsec_encrypt_on_tunnel_instance Reason: No error -
19 tunnel is not yet established;
```

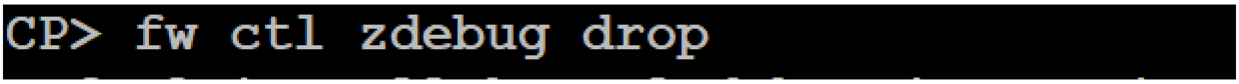
2. MM_KEY_EXCH:



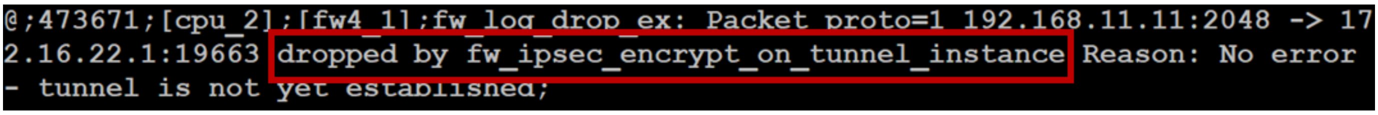
```
@;434121;[cpu_2];[fw4_1];fw_log_drop_ex: Packet proto=1 192.168.11.11:2048 -> 17
2.16.22.1:19671 dropped by vpn_drop_and_log Reason: Failed to resolve VPN MEP ga
teway;
```

(specific: fw ctl zdebug drop + grep 100.1.1.9)

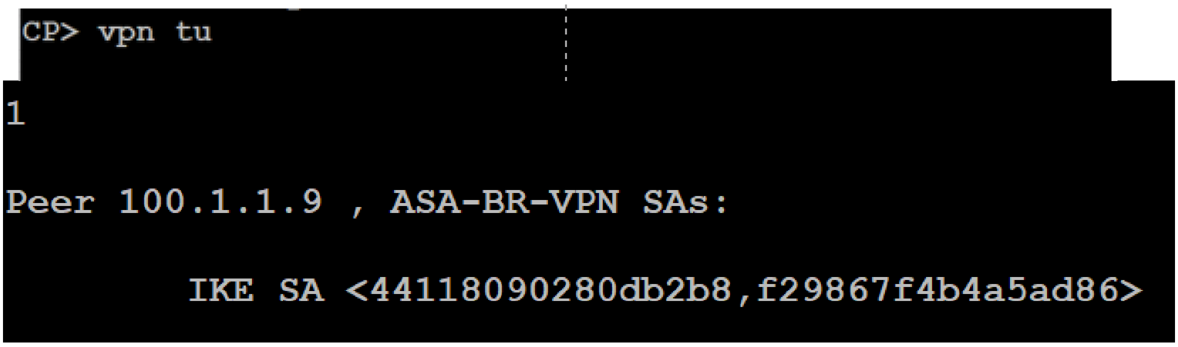
3. Phase 2 transform-set mismatch: (esp, ah)



```
CP> fw ctl zdebug drop
```



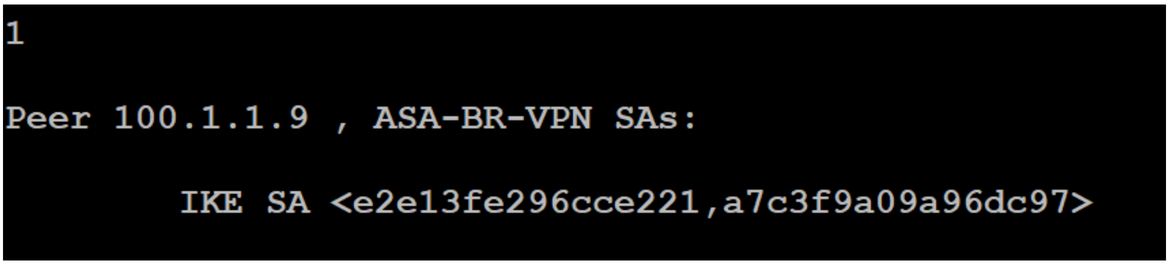
```
@;473671;[cpu_2];[fw4_1];fw_log_drop_ex: Packet proto=1 192.168.11.11:2048 -> 17
2.16.22.1:19663 dropped by fw_ipsec_encrypt_on_tunnel_instance Reason: No error
- tunnel is not yet established;
```



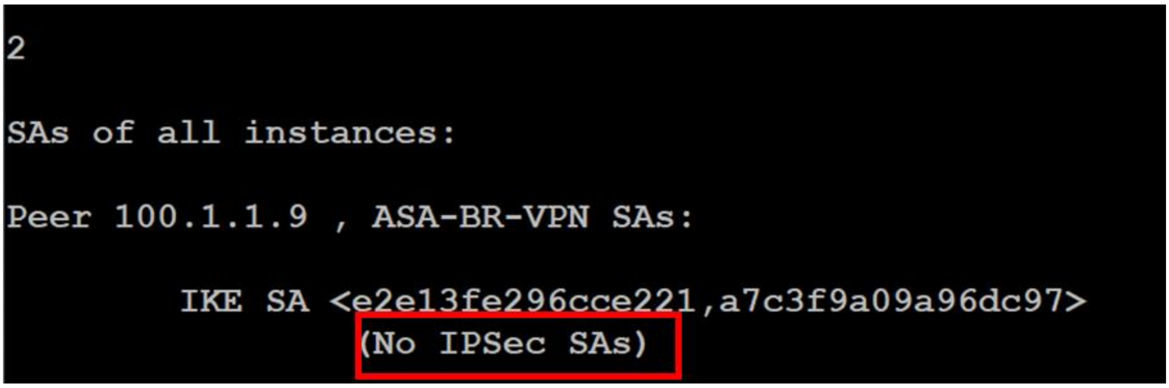
```
CP> vpn tu

1

Peer 100.1.1.9 , ASA-BR-VPN SAs:

        IKE SA <44118090280db2b8,f29867f4b4a5ad86>
```

SITE-TO-SITE VPN (TROUBLESHOOT) On Checkpoint

4. No crypto acl or Encryption Domain otherside



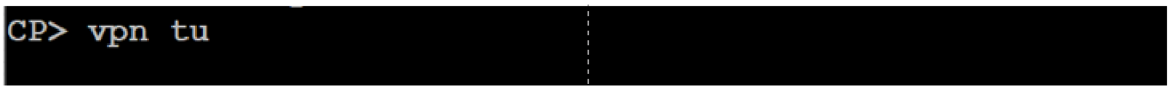
```
1

Peer 100.1.1.9 , ASA-BR-VPN SAs:

        IKE SA <e2e13fe296cce221,a7c3f9a09a96dc97>
```



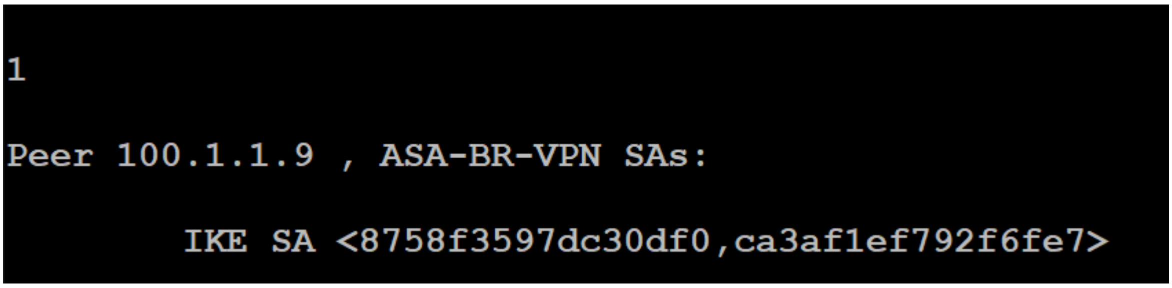
```
2

SAs of all instances:

Peer 100.1.1.9 , ASA-BR-VPN SAs:

        IKE SA <e2e13fe296cce221,a7c3f9a09a96dc97>
                (No IPSec SAs)
```

4. Both phases success:

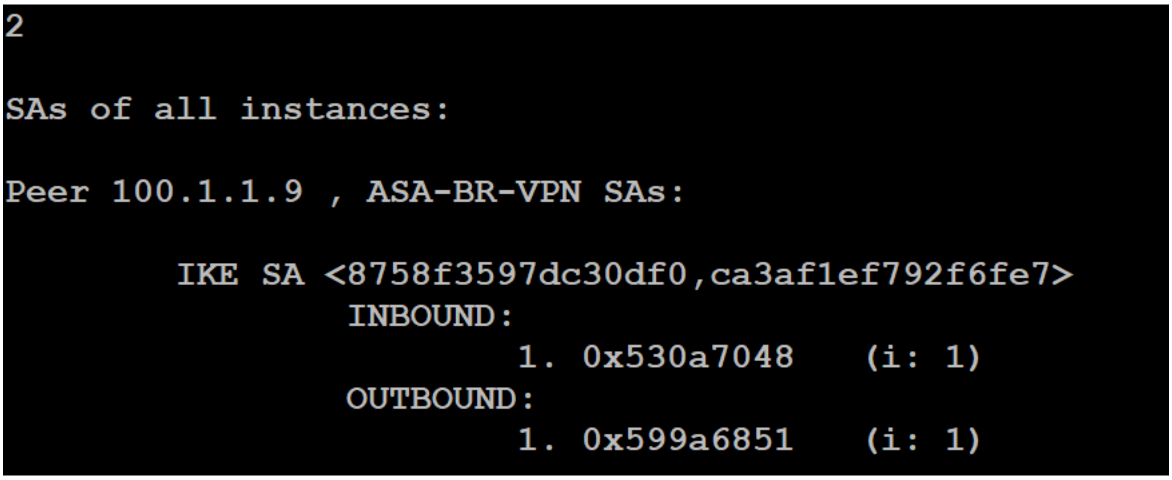
Once an IKE negotiation is successfully completed, the peers have established two pairs of one-way (inbound and outbound) SAs. Since IKE always negotiates pairs of SAs, the term "SA" is generally used to refer to a pair of SAs (e.g., an "IKE SA" or an "IPsec SA" is in reality a pair of one-way SAs).



```
CP> vpn tu
```



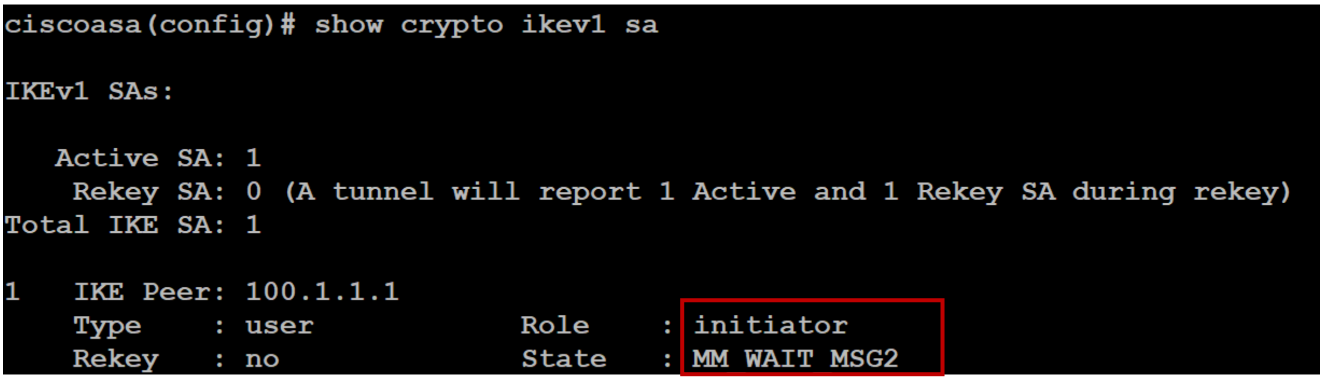
```
1

Peer 100.1.1.9 , ASA-BR-VPN SAs:

        IKE SA <8758f3597dc30df0,ca3af1ef792f6fe7>
```



```
2

SAs of all instances:

Peer 100.1.1.9 , ASA-BR-VPN SAs:

        IKE SA <8758f3597dc30df0,ca3af1ef792f6fe7>
                INBOUND:
                        1. 0x530a7048   (i: 1)
                OUTBOUND:
                        1. 0x599a6851   (i: 1)
```

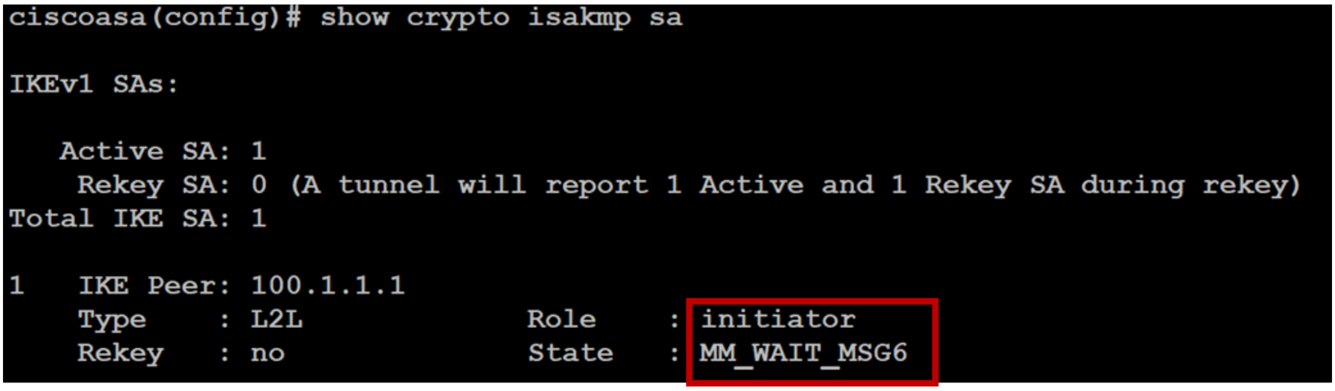
SITE-TO-SITE VPN (TROUBLESHOOT) On ASA

1. SA MISAMTCH:



```
ciscoasa(config)# show crypto ikev1 sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 100.1.1.1
    Type    : user            Role    : initiator
    Rekey   : no              State   : MM WAIT MSG2
```

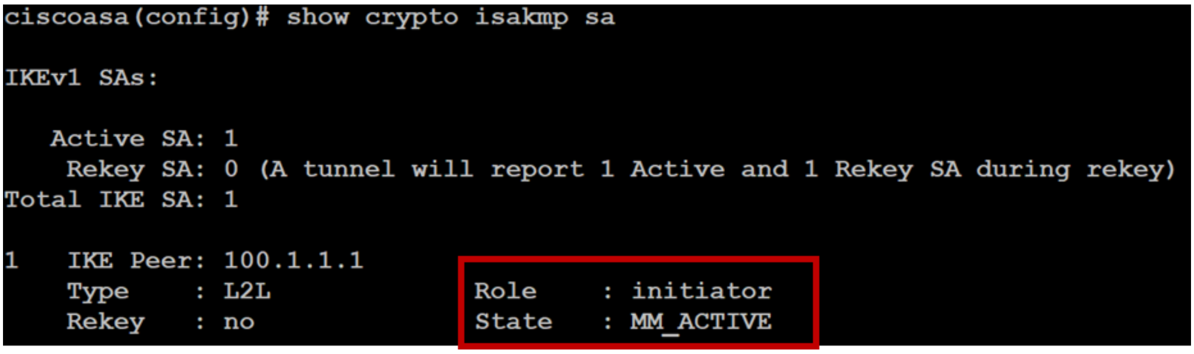
2. MM_KEY_EXCH:



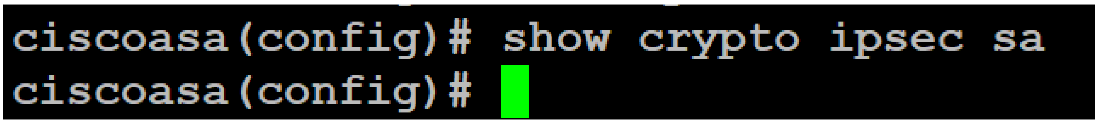
```
ciscoasa(config)# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 100.1.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG6
```

3. Phase 2 transform-set mismatch: (esp, ah)

Phase1 – UP
Phase2 - Down



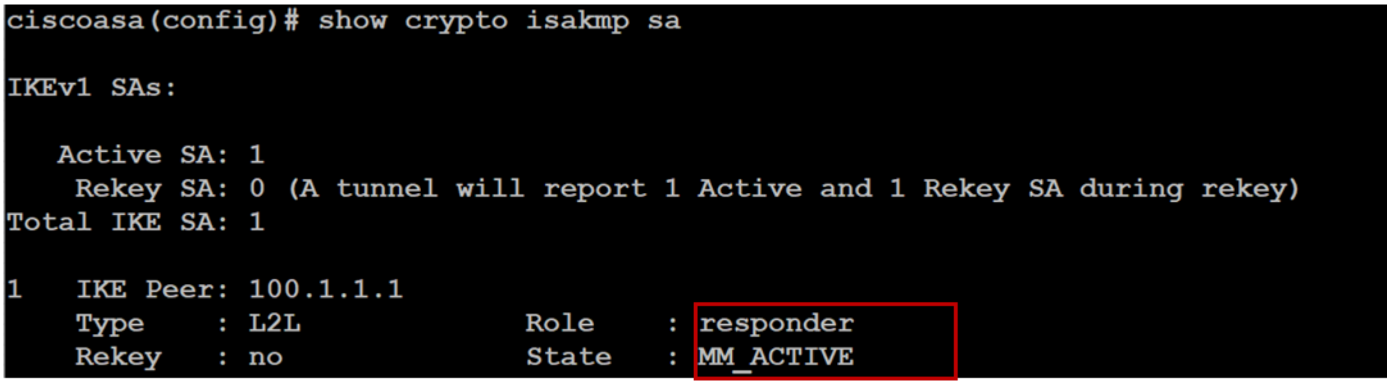
```
ciscoasa(config)# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 100.1.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```



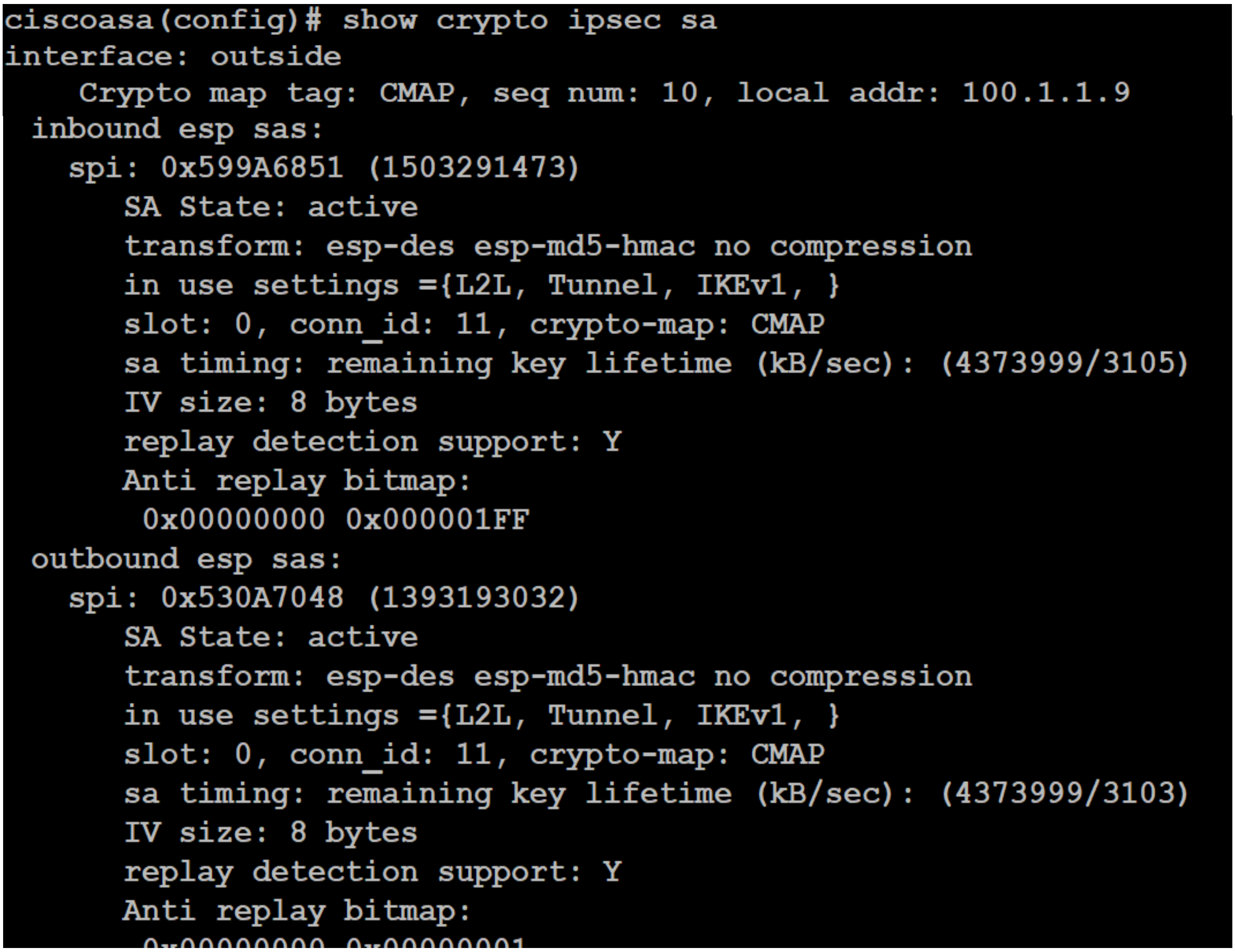
```
ciscoasa(config)# show crypto ipsec sa
ciscoasa(config)#
```

SITE-TO-SITE VPN (TROUBLESHOOT) On ASA

4. Both phases success:



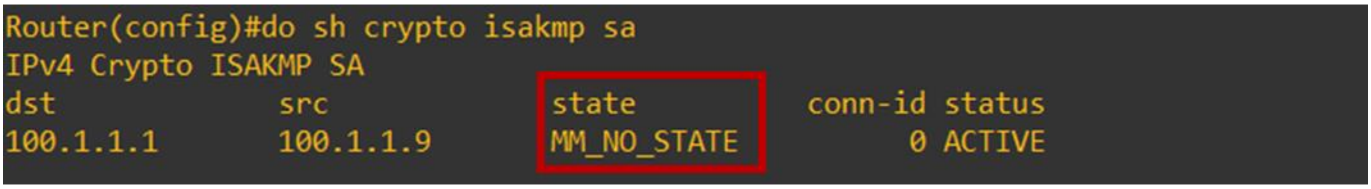
```
ciscoasa(config)# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 100.1.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```



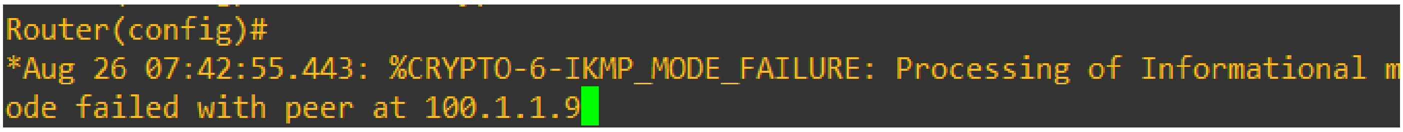
```
ciscoasa(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: CMAP, seq num: 10, local addr: 100.1.1.9
  inbound esp sas:
    spi: 0x599A6851 (1503291473)
       SA State: active
       transform: esp-des esp-md5-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 11, crypto-map: CMAP
       sa timing: remaining key lifetime (kB/sec): (4373999/3105)
       IV size: 8 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000001FF
  outbound esp sas:
    spi: 0x530A7048 (1393193032)
       SA State: active
       transform: esp-des esp-md5-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 11, crypto-map: CMAP
       sa timing: remaining key lifetime (kB/sec): (4373999/3103)
       IV size: 8 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

SITE-TO-SITE VPN (TROUBLESHOOT) On Router

1. SA MISAMTCH:
   Hagle Parameter Mismatch

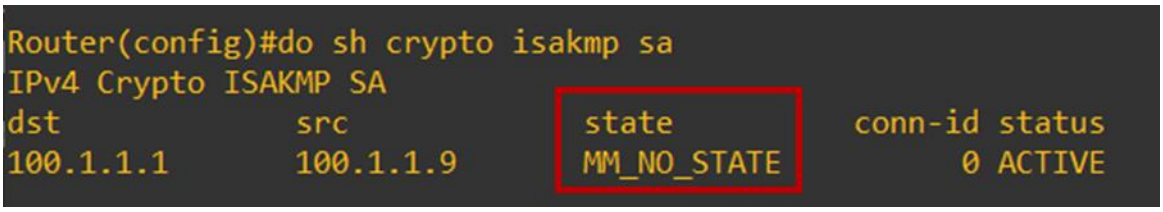


```
Router(config)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.1.9       MM_NO_STATE          0 ACTIVE
```



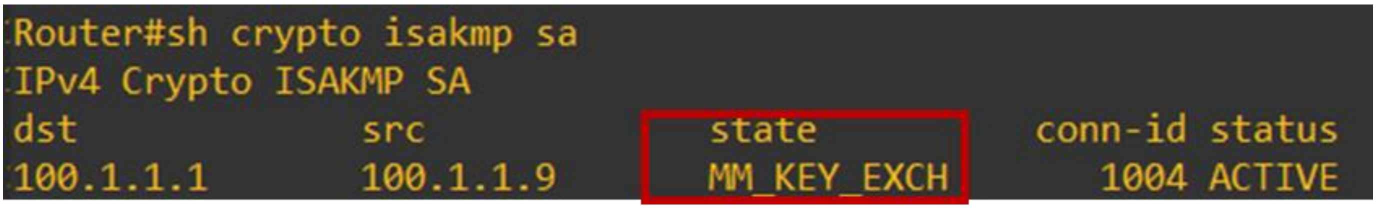
```
Router(config)#
*Aug 26 07:42:55.443: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational m
ode failed with peer at 100.1.1.9
```

2. If No crypto ACL on remote device only single message appears

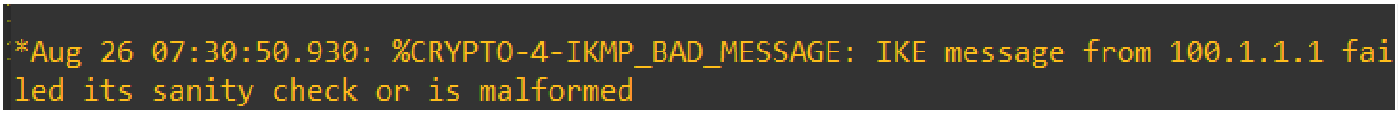


```
Router(config)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.1.9       MM_NO_STATE          0 ACTIVE
```

2. MM_KEY_EXCH:
   Authentication key mismatch.

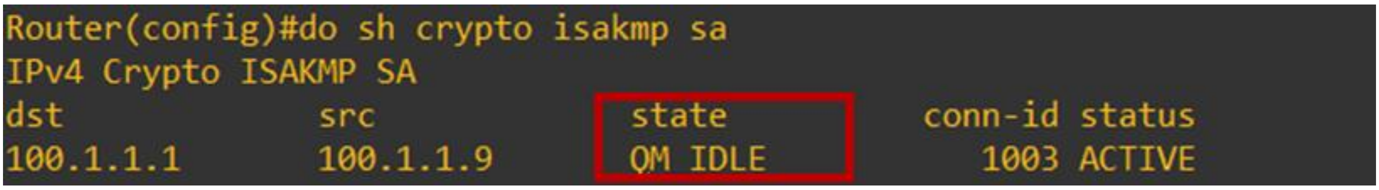


```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.1.9       MM_KEY_EXCH       1004 ACTIVE
```



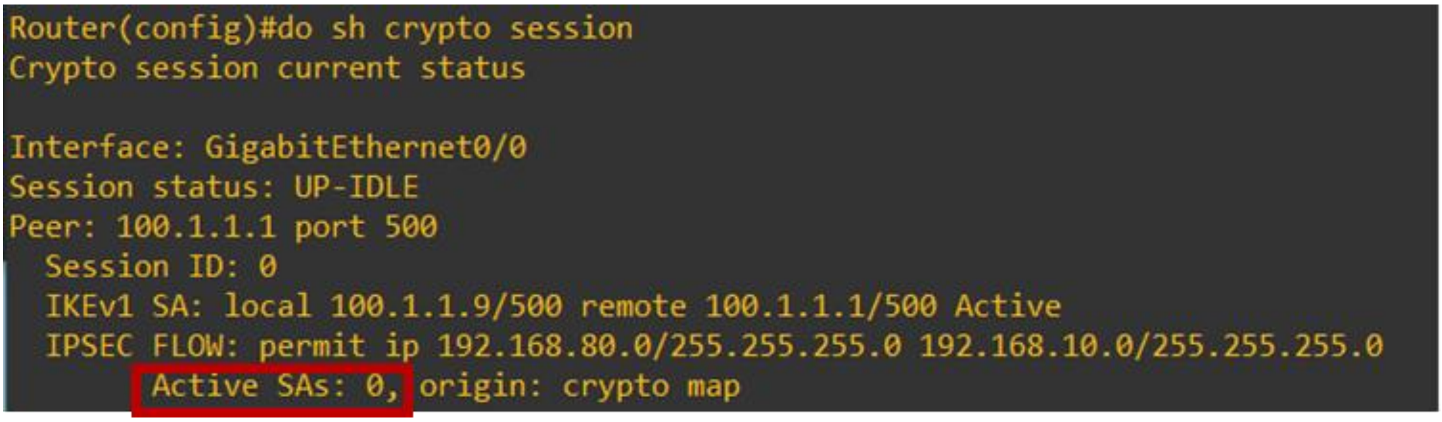
```
*Aug 26 07:30:50.930: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 100.1.1.1 fai
led its sanity check or is malformed
```

3. Phase 2 transform-set mismatch: (esp, ah)



```
Router(config)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.1.9       QM_IDLE           1003 ACTIVE
```

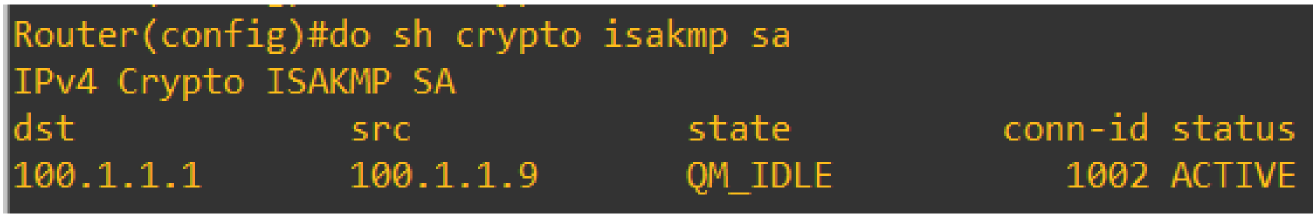
(QM_IDLE - phase 1 tunnel is successfully established.)



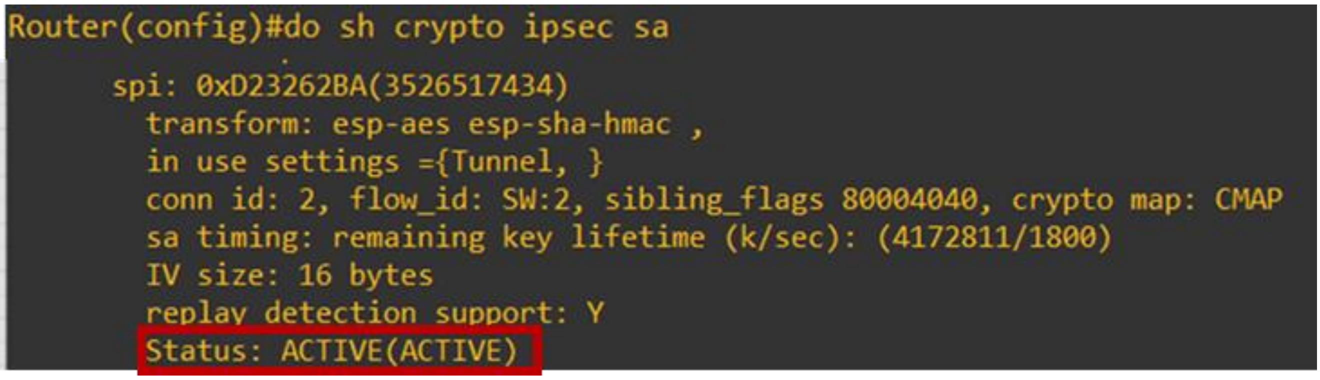
```
Router(config)#do sh crypto session
Crypto session current status

Interface: GigabitEthernet0/0
Session status: UP-IDLE
Peer: 100.1.1.1 port 500
  Session ID: 0
  IKEv1 SA: local 100.1.1.9/500 remote 100.1.1.1/500 Active
  IPSEC FLOW: permit ip 192.168.80.0/255.255.255.0 192.168.10.0/255.255.255.0
        Active SAs: 0, origin: crypto map
```

SITE-TO-SITE VPN (TROUBLESHOOT) On Router

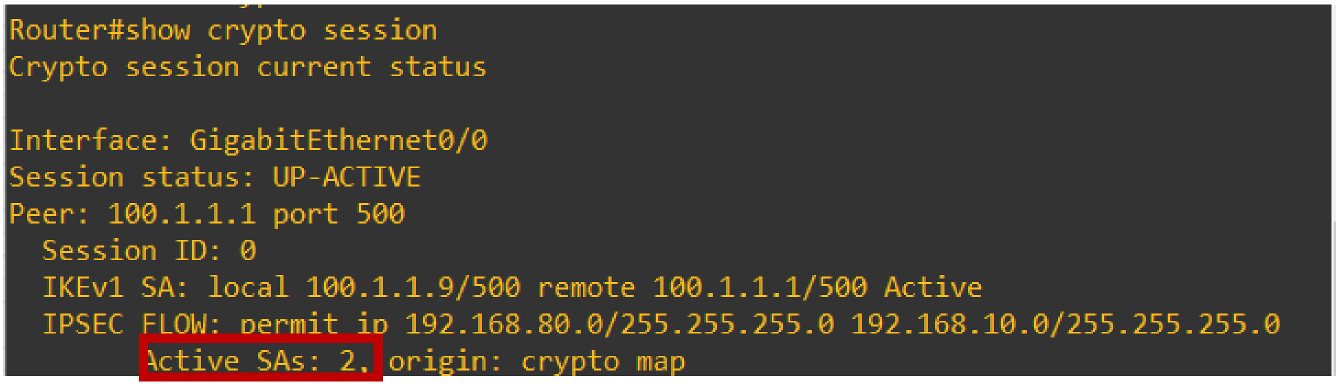
4. Both phases success:



```
Router(config)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
100.1.1.1       100.1.1.9       QM_IDLE           1002 ACTIVE
```



```
Router(config)#do sh crypto ipsec sa

      spi: 0xD23262BA(3526517434)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4172811/1800)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```



```
Router#show crypto session
Crypto session current status

Interface: GigabitEthernet0/0
Session status: UP-ACTIVE
Peer: 100.1.1.1 port 500
  Session ID: 0
  IKEv1 SA: local 100.1.1.9/500 remote 100.1.1.1/500 Active
  IPSEC FLOW: permit ip 192.168.80.0/255.255.255.0 192.168.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

Other possible causes & Solution

Configuration need to check or perform:

I. DNS resolution check

II.MTU mismatch & Fragmentation
(ping ip-address df-bit <size>, show ip traffic)

III. Asymmetric route (check using traceroute)

IV.Device-health or CPU utilisation
(show platform resources, show process cpu sorted)

V. Perform Quality Of service for TCP or interesting traffic

VI.Firewall Policy
(use inline and ordered layer policy as it provides hierarchical policy structure)

VII.Use Policy trace (virtual check)