```
Target : GULSHAN-FF:d8:c7:c8:c8:eb:a0

show vpn status

vpn primary external ip            :202.5.140.253
vpn primary tunnel ip              :0.0.0.0
vpn backup  external ip            :0.0.0.0
vpn backup  tunnel ip              :0.0.0.0
vpn current used external ip       :202.5.140.253
vpn current remote tunnel ip       :0.0.0.0
vpn current ap's tunnel ip         :0.0.0.0
vpn is preempt status              :False
vpn hold down period               :600
vpn status                         :down

vpn primary external ip            :202.5.140.253
vpn primary tunnel ip              :0.0.0.0
vpn backup  external ip            :0.0.0.0
vpn backup  tunnel ip              :0.0.0.0
vpn current used external ip       :202.5.140.253
vpn current remote tunnel ip       :0.0.0.0
vpn current ap's tunnel ip         :0.0.0.0
vpn is preempt status              :False
vpn hold down period               :600
vpn status                         :down
end of show vpn status
=========================================================

show upgrade info

Image Upgrade Progress
----------------------
Mac                IP Adress      AP Class  Status    Image Info  Error
Detail
---                ---------      --------  ------    ----------  -------
-----
d8:c7:c8:c8:eb:a0  202.5.142.148  Orion     image-ok  image file  none
end of show upgrade info
=========================================================

show log upgrade
----------Download log start----------
download log not available
----------Download log end------------
Download status: incomplete
----------Upgrade log start----------
upgrade log not available
----------Upgrade log end------------
Upgrade status: upgrade status not available
end of show log upgrade
=========================================================

show log rapper
```

```
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i b7 1b 0c b1 c1 2d 9b ee 5c 64 71 d6 82 6c b0 91
78 32 35 4e
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={209558a10d40e8ab 3342c94120bec005} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to 202.5.140.253[4500] (3.0)
(pid:4374)  time:2012-06-02 13:30:57

Sending last fragment, size = 432


#RECV 80 bytes from 202.5.140.253[4500] (3.0)
(pid:4374)  time:2012-06-02 13:30:57

 spi={209558a10d40e8ab 3342c94120bec005} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=e4acf800)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0xcc92187e) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:4389)  time:2012-06-02 13:30:58
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
```

```
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BD0043873::d8:c7:c8:c8:eb:a0}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ca058e94
IKE_EXAMPLE: Socket created on 202.5.142.148[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:4389)  time:2012-06-02 13:30:58
 SA_INIT dest=202.5.140.253
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): e7 73 07 f8 82 d5 53 06 c0 1c 73 c6 89 f1 2f 13
f4 a1 b3 d9
   NAT_D (peer): 74 fd 44 51 53 38 86 48 21 f7 83 6f 3e b0 bc 9a
1b 49 32 e8
 spi={988c7bf60160a869 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to 202.5.140.253[4500] (0.0)
(pid:4389)  time:2012-06-02 13:30:58

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0x8c2d9359...
papi:8423

#RECV 60 bytes from 202.5.140.253[4500] (0.0)
(pid:4389)  time:2012-06-02 13:30:58
```

```
 spi={988c7bf60160a869 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={988c7bf60160a869 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to 202.5.140.253[4500] (0.0)
(pid:4389)  time:2012-06-02 13:30:58


#RECV 337 bytes from 202.5.140.253[4500] (0.0)
(pid:4389)  time:2012-06-02 13:30:58

 spi={988c7bf60160a869 86d5632442e09737} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   Notify: NAT_DETECTION_DESTINATION_IP
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 95 3f ec ae b1 eb df 7c e6 2e 74 85 78 e0 55 93
e5 c8 0c c3
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={988c7bf60160a869 86d5632442e09737} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to 202.5.140.253[4500] (3.0)
(pid:4389)  time:2012-06-02 13:31:00

Sending last fragment, size = 432


#RECV 80 bytes from 202.5.140.253[4500] (3.0)
(pid:4389)  time:2012-06-02 13:31:00

 spi={988c7bf60160a869 86d5632442e09737} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=b5fa9100)
```

```
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0x8c2d9359) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:4409)  time:2012-06-02 13:31:00
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BD0043873::d8:c7:c8:c8:eb:a0}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ca058e94
```

```
IKE_EXAMPLE: Socket created on 202.5.142.148[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:4409)  time:2012-06-02 13:31:00
 SA_INIT dest=202.5.140.253
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): 16 65 d1 3f a5 ce f0 40 35 d6 3e 67 da e9 3f 17
7b ba d2 54
   NAT_D (peer): 88 c5 04 9b f9 02 a0 6a 72 27 67 ee 5b 4c 4b fe
a4 7e 04 43
 spi={3b6694fa24869cd9 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to 202.5.140.253[4500] (0.0)
(pid:4409)  time:2012-06-02 13:31:01

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0x80760abc...
papi:8423

#RECV 60 bytes from 202.5.140.253[4500] (0.0)
(pid:4409)  time:2012-06-02 13:31:01

 spi={3b6694fa24869cd9 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={3b6694fa24869cd9 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to 202.5.140.253[4500] (0.0)
(pid:4409)  time:2012-06-02 13:31:01


#RECV 337 bytes from 202.5.140.253[4500] (0.0)
(pid:4409)  time:2012-06-02 13:31:01

 spi={3b6694fa24869cd9 c09b3b688cd481c9} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   Notify: NAT_DETECTION_DESTINATION_IP
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
```

```
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i eb 39 0b be 73 78 ca 9b bf 07 5e a0 ec 5d 3a fe
b3 de eb ac
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={3b6694fa24869cd9 c09b3b688cd481c9} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to 202.5.140.253[4500] (3.0)
(pid:4409)  time:2012-06-02 13:31:03

Sending last fragment, size = 432


#RECV 80 bytes from 202.5.140.253[4500] (3.0)
(pid:4409)  time:2012-06-02 13:31:03

 spi={3b6694fa24869cd9 c09b3b688cd481c9} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=6750b800)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0x80760abc) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:4422)  time:2012-06-02 13:31:03
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
```

```
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BD0043873::d8:c7:c8:c8:eb:a0}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ca058e94
IKE_EXAMPLE: Socket created on 202.5.142.148[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:4422)  time:2012-06-02 13:31:03
 SA_INIT dest=202.5.140.253
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): 06 e4 1f 6a ba 09 79 bd dd 57 b0 4c 08 94 c5 51
57 91 99 7d
   NAT_D (peer): 55 6b e2 29 62 a2 37 d6 d5 66 92 b9 c5 90 32 8f
51 a9 69 b8
 spi={9117b30c8d36de8f 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to 202.5.140.253[4500] (0.0)
(pid:4422)  time:2012-06-02 13:31:03

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xe661da65...
papi:8423

#RECV 60 bytes from 202.5.140.253[4500] (0.0)
(pid:4422)  time:2012-06-02 13:31:03

 spi={9117b30c8d36de8f 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
```

```
   Notify: COOKIE
 spi={9117b30c8d36de8f 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to 202.5.140.253[4500] (0.0)
(pid:4422)  time:2012-06-02 13:31:03


#RECV 337 bytes from 202.5.140.253[4500] (0.0)
(pid:4422)  time:2012-06-02 13:31:03

 spi={9117b30c8d36de8f e0d8cf0f164d229a} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   Notify: NAT_DETECTION_DESTINATION_IP
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 5a fb c5 c0 fd 2d a0 a6 59 b8 b0 c8 33 ea 92 c2
e6 e6 a7 bd
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={9117b30c8d36de8f e0d8cf0f164d229a} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to 202.5.140.253[4500] (3.0)
(pid:4422)  time:2012-06-02 13:31:06

Sending last fragment, size = 432


#RECV 80 bytes from 202.5.140.253[4500] (3.0)
(pid:4422)  time:2012-06-02 13:31:06

 spi={9117b30c8d36de8f e0d8cf0f164d229a} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=41d16200)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0
```

```
IKE_SA [v2 I] (id=0xe661da65) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:4439)  time:2012-06-02 13:31:06
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0

testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BD0043873::d8:c7:c8:c8:eb:a0}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ca058e94
IKE_EXAMPLE: Socket created on 202.5.142.148[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
```

```
(pid:4439)  time:2012-06-02 13:31:06
 SA_INIT dest=202.5.140.253
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): 78 79 58 f4 4b 9e e1 5c a5 c4 ac 04 04 a3 ed 61
5f d6 55 aa
   NAT_D (peer): c1 c0 fa 2e d7 be ca 29 be fd d5 1a 78 fc 4e 33
57 60 75 ed
 spi={34016b0eff95bbfc 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to 202.5.140.253[4500] (0.0)
(pid:4439)  time:2012-06-02 13:31:06

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0xa6718379...
papi:8423

#RECV 60 bytes from 202.5.140.253[4500] (0.0)
(pid:4439)  time:2012-06-02 13:31:06

 spi={34016b0eff95bbfc 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={34016b0eff95bbfc 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to 202.5.140.253[4500] (0.0)
(pid:4439)  time:2012-06-02 13:31:06


#RECV 337 bytes from 202.5.140.253[4500] (0.0)
(pid:4439)  time:2012-06-02 13:31:06

 spi={34016b0eff95bbfc a3e0c1a69a7119da} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   Notify: NAT_DETECTION_DESTINATION_IP
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i 31 fa fd b5 ff 49 07 9e 7a fb 3f f6 05 79 eb dd
6a 45 f9 24
```

```
OutAuth TPM sign api passed
   CFG_REQUEST
    IP4_ADDRESS
    IP4_NETMASK
   TSi: 0.0.0.0~255.255.255.255
   TSr: 0.0.0.0~255.255.255.255
 spi={34016b0eff95bbfc a3e0c1a69a7119da} np=E{IDi}
 exchange=IKE_AUTH msgid=1 len=5340
#SEND 5344 bytes to 202.5.140.253[4500] (2.0)
(pid:4439)  time:2012-06-02 13:31:09

Sending last fragment, size = 432


#RECV 80 bytes from 202.5.140.253[4500] (3.0)
(pid:4439)  time:2012-06-02 13:31:09

 spi={34016b0eff95bbfc a3e0c1a69a7119da} np=E{N}
 exchange=IKE_AUTH msgid=1 len=76
  I <--
   Notify: AUTHENTICATION_FAILED (ESP spi=1a697700)
InNotify AP authentication failed
ike2_state.c (7737): errorCode = ERR_IKE_NOTIFY_PAYLOAD
IKE SA failed reason = ERR_IKE_XAUTH_FAILED, errorcode = -8952
send_sapd_error: error:45 debug_error:0

IKE_SA [v2 I] (id=0xa6718379) flags 0x41000015 failed reason =
ERR_IKE_XAUTH_FAILED, errorcode = -8952

Switching output streamget_ike_version: Use IKE Version 2

papi_init papifd:12  ack:24

IKE_EXAMPLE: Starting up IKE server
setup_tunnel
Initialized Timers
IKE_init: completed after (0.0)
(pid:4453)  time:2012-06-02 13:31:09
 seconds.
Before getting Certs
TPM enabled
CA_MGMT_EXAMPLE_computeHostKeys init cert-len 0
Factory Device Cert is /tmp/deviceCerts/certifiedKeyCert.der
Reading DER Device Cert file
DER Device Cert file len:1768
Intermediate Cert index:0 is /tmp/deviceCerts/certifiedKeyCaCert.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1456
Intermediate Cert index:1 is /tmp/deviceCerts/caChainCert1.der
Reading DER Intermediate Cert file
DER Intermediate Cert file len:1580
Decode PEM Key length :0
testHostKeys : status 0
```

```
testHostKeys : free temp Certificate status 0

CA_MGMT_EXAMPLE_computeHostKeys after testHostKeys cert-len 1768
CA Cert index:0 is /tmp/deviceCerts/OpensslOldCA_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1416
CA Cert index:1 is /tmp/deviceCerts/MSCAV1_RootCert.der
Reading DER CA Cert file
DER CA Cert file len:1009
Got 2 Trusted Certs
After getFieldTrustedCerts ret:-1
Got 0 Field Trusted Certs
CA Cert status : 0

Before IKE_initServer
IKE_initServer: Cert length 1768
IKE_initServer: Host Certificate is set
  {CN=BD0043873::d8:c7:c8:c8:eb:a0}
IKE_EXAMPLE_addServer port:0 natt:4500

srcdev_name = br0 ip ca058e94
IKE_EXAMPLE: Socket created on 202.5.142.148[4500]
IKE_EXAMPLE_addDefaultServers Instances:0 status:0

 (0.0)
(pid:4453)  time:2012-06-02 13:31:09
 SA_INIT dest=202.5.140.253
 Initialize IKE SA
Timer ID: 1 Initialized
  I -->
   NAT_D (us): c6 93 3e 01 09 50 61 b6 18 09 73 fd 94 22 b3 c3
08 c8 04 36
   NAT_D (peer): 01 21 dc 0a 9d e3 b0 e1 c1 54 91 8b 5f b5 17 6f
8f 72 58 e2
 spi={399be200ed4a9444 0000000000000000} np=SA
 exchange=IKE_SA_INIT msgid=0 len=376
#SEND 380 bytes to 202.5.140.253[4500] (0.0)
(pid:4453)  time:2012-06-02 13:31:09

Successfully setsockopt UDP_ENCAP port 4500

IKE_EXAMPLE: IKE_keyConnect() started, id = 0x8bdccb31...
papi:8423

#RECV 60 bytes from 202.5.140.253[4500] (0.0)
(pid:4453)  time:2012-06-02 13:31:09

 spi={399be200ed4a9444 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=56
  I <--
   Notify: COOKIE
 spi={399be200ed4a9444 0000000000000000} np=N
 exchange=IKE_SA_INIT msgid=0 len=404
#SEND 408 bytes to 202.5.140.253[4500] (0.0)
```

```
(pid:4453)  time:2012-06-02 13:31:09


#RECV 337 bytes from 202.5.140.253[4500] (0.0)
(pid:4453)  time:2012-06-02 13:31:09

 spi={399be200ed4a9444 a77136f49919356d} np=SA
 exchange=IKE_SA_INIT msgid=0 len=333
  I <--
    Proposal #1: IKE[4]
     ENCR_AES 256-BITS
     PRF_HMAC_SHA1
     AUTH_HMAC_SHA1_96
     DH_2
   Notify: NAT_DETECTION_SOURCE_IP
   Notify: NAT_DETECTION_DESTINATION_IP
   VID: 40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
Fragmentation is enabled
  I -->
   Notify: INITIAL_CONTACT
OutCert: adding leaf Cert of Len:1768
OutCert: adding Cert of Len:1456
OutCert: adding Cert of Len:1580
   HASH_i fa f8 88 b1 cb bb f9 b8 78 cc 60 3b 39 23 90 86
40 7a ff a1

end of show log rapper
=======================================================
```