Error Log Message	Possible Cause	Solution
Retransmission count exceeded the limit **Log message example** 2013-02-04 15:47:52 [PROTO_ERR]: ikev2.c:616:ikev2_timeout(): 3:5.5.5.2[500] - 5. 5.5.1[500]:0x0:retransmission count exceeded the limit	The tunnel on the other end is not yet configured, or firewall routing issues are preventing the exchange of IKE related packets (UDP port 500/4500).	• If the tunnel on the other end point is not configured, configure it. • If the tunnel settings (IKE Version, Encryption/Hash Algorithm, PSK/certificates) on one end point do not match those on the other end point, no proposal is agreed upon between the end points. Specify the same settings on both end points. • After you configure a CloudBridge Connector tunnel between two end points, if the IP tunnel entity in an end point does not enter the UP state within a few minutes, remove the IP tunnel entity and add it again. One minute is usually sufficient for tunnel establishment if both ends are Citrix NetScaler appliances. • If none of the above measures correct the problem, configure, between the same end points, another CloudBridge that uses only the GRE protocol. Configure the firewalls on both ends to allow GRE (protocol number 47) packets. Verify that you are able to ping the network at one end of CloudBridge Connector tunnel from the other end.
Authentication failure **Log message example** 2013-02-04 16:05:16 [PROTO_ERR]: ikev2_auth.c:615:ikev2_verify(): 8:5.5.5.2[500] - 5. 5.5.1[500]:0x8104290:authenticatio n failure	The IPSec authentication parameters (PSK or the public and private key) are set to incorrect values.	• Configure the authentication parameters correctly on both NetScaler appliances.
Failed to find a socket for retransmission or could not find configuration **Log message example**	The tunnel IP address is not yet available for IKE purposes, or the tunnel does not exist.	• Remove the IP tunnel entities on both tunnel end points and add them again. • If another IP tunnel entity exists, with Local IP set to the same IP address but with IPSec profile set to NONE, remove these two tunnel entities and add them again. First add

```
2013-02-04 15:47:44
[INTERNAL_ERR]: i
sakmp.c:1844:isak
mp_retransmit(): failed
to find a socket for
retransmission 2013-01-
10 21:21:46
[PROTO_ERR]: ike
v1.c:950:isakmp_
ph1begin_r(): couldn't
find configuration.
```

The source port and destination ports shown in the /tmp/iked.debug are other than port 500. That is: src=<srcip>[<srcPort != 500>] dst=<dst tip>[<dstPort != 500>])

Log message example

```
2013-02-04 16:08:59
[INFO]: i
ke_pfkey.c:490:sa
db_log_add():
SADB_UPDATE
ul_proto=255
src=5.5.5.1[4500]
dst=5.5.5.2[4500]
satype=ESP
samode=transport
spi=0x055fdd6d au
thtype=HMAC-SHA -
256 enctype=AES-CBC
lifetime soft time=25741
bytes=0 hard
time=28800 bytes=0
```

the one with a valid IPSec profile, and then add the one with IPSec profile NONE.

- Verify that the IP address is available for IKE purposes, by typing the following commands at the CloudBridge shell prompt:
  - **ifconfig -a | grep**<LocalTunnelEndPoint-IP>

    Example

    ```
    root@ns# ifconfig -a | grep 5.5.5.2
    inet 5.5.5.2 netmask 0xffffff00
    broadcast 5.5.5.255
    ```
  - **netstat | grepudp | grep**<LocalTunnelEndPoint-IP>

    Example

    ```
    root@ns# netstat | grepudp | grep
    5.5.5.2 udp4 0 0 5.5.5.2.sae-urn *.*
    udp4 0 0 5.5.5.2.isakmp *.*
    ```