IPsec IKEv1 Log Messages and Troubleshooting

https://campus.barracuda.com/doc/48203295/

This article provides a list of common issues than can occur and generate error messages in the `ike.log` file when establishing an IKEv1 IPsec VPN tunnels on the Barracuda NextGen Firewall F-Series.

Debugging in Barracuda NextGen Admin

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Click here for Server Settings** link.
4. In the **Server Settings** window, click the **Advanced** tab.
5. In the **IKE Parameters** section, select *10* from the **IPSec Log Level** list.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Logfiles

'dropped message' reported in the ike.log

- dropped message from x.x.x.x port 500 due to the PAYLOAD_MALFORMED notification type
- dropped message from x.x.x.x port 500 due to the INVALID_PAYLOAD_TYPE notification type
- dropped message from x.x.x.x port 500 due to the INVALID_COOKIE notification type

Cause

- dropped message from x.x.x.x port 500 due to the PAYLOAD_MALFORMED notification type
- dropped message from x.x.x.x port 500 due to the INVALID_PAYLOAD_TYPE notification type

These errors indicate that the preshared key does not match on the two VPN peers. As a result, the encrypted fifth main-mode packet is incorrectly decrypted or decrypted with another key.

- dropped message from x.x.x.x port 500 due to the INVALID_COOKIE notification type

This error indicates that the configuration of **Phase 1** or **Phase 2** does not match between both peers.

'INVALID_PAYLOAD_TYPE' reported in the ike.log

An IPsec tunnel does not establish: **Phase 1** and **Phase 2** settings are equal on both gateways. The following messages are displayed in the `ike.log`:

- Notice +0200 srv_sve_ike[PID]: message_parse_payloads: invalid next payload type <Unknown 118> in payload of type 8
- Notice +0200 srv_sve_ike[PID]: dropped message from x.x.x.x port 500 due to notification type INVALID_PAYLOAD_TYPE

Cause

This problem only occurs if the tunnel uses single host IP addresses for the remote and the local net. The checkpoint in this case does not insert the official gateway IP address as *ipsec_validate_id_information: IPv4:* value but uses the single host IP address from the remote and local net. To verify the value, you must set the IPsec debug level to *99* and search for this value in the ike.log.

- Info +0200 srv_sve_ike[PID]: ipsec_validate_id_information: IPv4:
- Info +0200 srv_sve_ike[PID]: c19d4f64

The c19d4f64 value is the IPv4 address that is used as ID and this IP address must be the official IP address of the active partner (normally the checkpoint).

Solution

Do not use single host IP addresses for remote and local net in the tunnel configuration. Always use a whole net (a netmask with 2 bit in Barracuda notation is enough).

'NO KEYSTATE' reported in the ike.log

If you have a "no keystate" error, verify that the preshared key is correct or if the local ID is correct (see the **Advanced** option). You should have more information in the remote endpoint logs.

- 115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
- 115319 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
- 115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
- 115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50

'received remote ID other than expected' reported in the ike.log

If you have a "received remote ID other than expected ..." error, the **Remote ID** value (see **Advanced** option) does not match what the remote VPN endpoint is expecting.

- 120351 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
- 120351 Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
- 120351 Default ike_phase_1_recv_ID: received remote ID other than expected support@thegreenbow.fr

'NO PROPOSAL CHOSEN' reported in the ike.log

If you have a "NO PROPOSAL CHOSEN" error (hereafter), verify that the **Phase 2** algorithms are the same on each side of the IPsec VPN tunnel.

- 115915 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
- 115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
- 115915 Default RECV Informational [HASH][DEL]
- 115915 Default Cnx-P1 deleted

If you have a "NO PROPOSAL CHOSEN" error (hereafter), verify that the **Phase 1** algorithms are the same on each side of the IPsec VPN tunnel.

- 115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remoteaddr
- 115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
- 115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
- 115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]

'INVALID ID INFORMATION' reported in the ike.log

If you have an "INVALID ID INFORMATION" error, verify that the **Phase 2** ID (local address and network address) is correct and matches what is expected by the remote VPN endpoint. Also verify the ID type. If **Network Mask** is not checked, you are using an IPV4_ADDR type (and not a IPV4_SUBNET type).

- 122626 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
- 122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
- 122626 Default RECV Informational [HASH][DEL]
- 122626 Default Cnx-P1 deleted

Perfect Forward Secrecy (PFS)

The Barracuda NextGen Firewall F-Series supports Perfect Forward Secrecy (PFS) for tunnel establishment. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. PFS is activated by default. If a third-party IPsec gateway tries to establish a tunnel without using PFS, errors like the following ones are generated on the Barracuda NextGen Firewall F-Series gateway and written to the `ike.log` (at the VPN service logfiles):

- Notice dropped message from 194.39.131.169 port 500 due to notification type INVALID_PAYLOAD_TYPE
- Notice message_parse_payloads: reserved field non-zero: 18
- Notice dropped message from 194.39.131.169 port 500 due to notification type PAYLOAD_MALFORMED
- Notice message_parse_payloads: reserved field non-zero: 20
- Notice dropped message from 194.39.131.169 port 500 due to notification type PAYLOAD_MALFORMED

Usage of PFS must be activated or deactivated on both gateways. Activate PFS in the **Phase 2** section of the **IPsec Tunnel** configuration window through the **DH-Group** setting. To deactivate PFS, set the value of the Phase 2 **DH-Group** to *none*.

Main keys should only be used with great care, as they will require further authentications. This can lead to additional administration effort for the domain controllers in the network. The main key does not have to be active on both gateways.