

# eVIP, IPsec Tunnel Fault

Evolved Virtual IP

OPERATING INSTRUCTIONS

**Copyright**

© Ericsson AB 2015, 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
<b>2</b>	<b>Alarm Description</b>	<b>3</b>
2.1	Alarm Attributes	3
<b>3</b>	<b>Procedure</b>	<b>5</b>
3.1	Validate Configuration	5
3.2	Check Network Connectivity	7



eVIP, IPsec Tunnel Fault



# 1 Introduction

This document is the Operating Instruction for the **eVIP, IPsec Tunnel Fault** alarm.

## 1.1 Prerequisites

This section describes the possible documents, tools, and conditions needed before performing the steps described in Section 3 on page 5.

### 1.1.1 Documents

Before starting this procedure, ensure that the following document have been read:

- eVIP Management Guide
- eVIP Internetworking





## 2 Alarm Description

The alarm is issued when an IPsec tunnel goes down ungracefully between an eVIP-enabled cluster and a peer.

The possible causes are as follows:

- The peer is faulty.
- The connection between the peer and the eVIP cluster is faulty.
- The configuration is incorrect.

In a normal situation, the tunnel is created after the local and remote gateway mutually authenticate each other. The second step is to set up security rules based on the configured traffic selectors. The local and remote agents negotiate an extensive set of parameters in the process. Many of the parameters can be set through configuration, rendering IPsec tunnels to be error-prone from the configuration perspective. For security reasons, the tunnels are also sensitive to loss of network connectivity.

### 2.1 Alarm Attributes

This alarm is compliant with the Ericsson SNMP Fault Management MIB, which conforms to the X.733 alarm reporting function. However, the following X.733 parameters are not supported: Correlated Notifications, Additional Info, Monitored Attributes, Proposed Repair Action, Trend Indication, Threshold Information, Backed Up Object, and State Change Definition.

The most essential statical attributes of this alarm and their values are listed in Table 1:

Table 1 Alarm Attributes

Attribute Name	Attribute Value
majorType	193
minorType	2129526787 (0x7eee0003)
class	EvipIpsecTunnel
source	ipsecPolicyId=<policy_name>,Evip_IpsecipsecTunnelId=<ikev2_tunnel_name>,Evip_HosthostId=eVIP_ALB_<alb_name> or Evip_Ipsec_Ikev1phase2PolicyId=<policy_name>,Evip_IpsecipsecTunnelId=<ikev1_tunnel_name>,Evip_HosthostId=eVIP_ALB_<alb_name>
specificProblem	eVIP, IPsec Tunnel Fault



Attribute Name	Attribute Value
eventType	COMMUNICATION
activeSeverity	MAJOR

The Alarm Type of the alarm is identified by the two integers: `majorType` and `minorType`. The Alarm Type is unique within the system type and maps to the X.733 Managed Object Instance. The `eventType`, `probableCause`, and `specificProblem` are always the same for a given Alarm Type.





## 3 Procedure

To clear the alarm, the possible error causes must be investigated.

The root cause of the problem can be:

- Misconfiguration
- Network connectivity issue

Configuration mismatch could be a primary suspect if the IPsec tunnel configuration has been added or altered on the local and/or the remote side.

**Note:**

- The alarm can also be issued after a cluster or a node restart.
- On a system, with properly configured tunnels the alarm is cleared automatically when the node(s) are successfully restarted.

### 3.1 Validate Configuration

To validate the configuration:

1. Identify the tunnel instance.

It is stated in the source attribute of the alarm.

For example:

```
ipsecpolicyId=1,Evip_IpsecipsectunnelId=1min,
Evip_HosthostId=eVIP_ALB_alb_1
```

2. Log on to COM CLI.
3. List the configuration parameters for the IPsec Tunnel in question.

```
>show all ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,IpsecTunnel=1min
IpsecTunnel=1min
  localAddressStr="10.0.20.101"
  remoteAddressStr="10.128.171.101"
  Ikev2Session=1
    ikev2PolicyProfile="ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min"
  IpsecPolicy=1
    ipsecProposalProfile="ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,IpsecProposalProfile=1min"
    localTrafficSelector
      addressRange="10.0.20.1/32"
    remoteTrafficSelector
```



```
addressRange="10.128.171.1/32"
```

4. List the referenced profiles.

```
>show all ManagedElement=1,Transport=1,  
Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min  
Ikev2PolicyProfile=1min  
ikev2Proposal  
diffieHellmanGroup  
MODP_2048_GROUP_14  
encryptionAlgorithm  
ENCR_AES_CBC_128  
integrityAlgorithm  
AUTH_HMAC_SHA1_96  
>show all ManagedElement=1,Transport=1,  
Host=eVIP_ALB_alb_1,IpssecProposalProfile=1min  
IpssecProposalProfile=1min  
childSaLifetime  
timeLimit=200  
ipsecProposal  
diffieHellmanGroup  
MODP_2048_GROUP_14  
encryptionAlgorithm  
ENCR_AES_CBC_256  
integrityAlgorithm  
AUTH_HMAC_SHA1_96
```

5. Check, if there is any mismatch between the configuration listed and the configuration on the peer.

If there is a mismatch that could cause the IKE negotiation to fail; in this case the parameters (proposals, and so on) must be adjusted.

6. Ensure that the IKE authentication information is also correct.

- In case of preshared keys: the same PSKs must be installed on both GWs. It is not possible to list/reveal the previously installed preshared key.

For example:

```
(config)>ManagedElement=1,Transport=1,  
Host=eVIP_ALB_alb_1,IpssecTunnel=1min,  
Ikev2Session=1,installPreSharedKey mySecr3t123XC
```

- In case of certificates, check certificate references:

For example:

```
>show ManagedElement=1,Transport=1,  
Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min,credential  
>show ManagedElement=1,Transport=1,  
Host=eVIP_ALB_alb_1,Ikev2PolicyProfile=1min,trustCategory
```



## 3.2 Check Network Connectivity

In most configurations, the security gateways must be able to ping each other (the addresses used as security gateways).

**Note:** The security gateway addresses cannot be pinged, for example if the traffic selectors cover these addresses as well or some discard policies are added on either side.

- The security gateway addresses can be listed in COM CLI.

For example:

```
>show ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,IpsecTunnel=1min,localAddressStr
localAddressStr="10.0.20.101"
>show ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,IpsecTunnel=1min,remoteAddressStr
remoteAddressStr="10.128.171.101"
```

- To ping the address configured in `remoteAddressStr` from eVIP, one must find a node that is part of that specific ALB instance.

To check the network connectivity:

1. Identify the ALB, the reference to the ALB can be listed from the COM CLI:

For example:

```
>show ManagedElement=1,Transport=1,
Host=eVIP_ALB_alb_1,l3Ref
l3Ref="ManagedElement=1,Transport=1,
Evip=1,EvipAlbs=1,EvipAlb=alb_1"
```

2. List Target Pools in the ALB:

For example:

```
>show all ManagedElement=1,Transport=1,
Evip=1,EvipAlbs=1,EvipAlb=alb_1,EvipTargetPools=1
EvipTargetPools=1
EvipTargetPool=6PLs_lc
distributionMethod="least_connection"
stickyGroup="no"
udpStateless="no"
EvipPayload=3
EvipPayload=4
...
```

3. Pick an `EvipPayload` from a target pool which is referenced by a flow policy having the IP address what is set as `localAddressStr`, and log on to the corresponding node in the cluster:



```
> ssh pl-2-3
```

4. Use the ping command to test connectivity between the gateway addresses:

For example:

```
PL-2-3:~ # ping -I 10.0.20.101 10.128.171.101
PING 10.128.171.101 (10.128.171.101)
from 10.0.20.101 : 56(84) bytes of data.
 64 bytes from 10.128.171.101: icmp_seq=1 ttl=60 time=0.610 ms
 64 bytes from 10.128.171.101: icmp_seq=2 ttl=60 time=0.446 ms
...
```

5. If the remote gateway cannot be reached (and there are no policies blocking this traffic), it means that the two IKE daemons cannot communicate. Ensure that there are no connectivity issues.

Contact next level of support if there is connection between the gateways and the configuration is correct on both sides, but the alarm does not disappear.