ERICSSON

Advanced Services Fault Management Guide

SYSTEM ADMINISTRATOR GUIDE

3/1543-CRA 119 1170/1-V1 Uen E

Contents

1 Alarms

You can enable or disable alarm generation for dynamic and static IPsec tunnels, as well as manual IPsec tunnels. If enabled, you then choose which alarms to generate. Alarms can be generated when a change is detected in the tunnel state. Alarms can also be generated when no valid RSA certificate is detected, or when an existing certificate is nearing expiry. Alarms are sent through SNMP and appear as events in the active alarm table until cleared.

Alarm content includes identifier strings such as the IPsec-Tunnel- Identifier string created from the remote-id-type and the remote-id value, and includes the probable cause of the failure.

1.1 Alarm Generation for an IPsec Tunnel

Before configuring the individual types of alarms to be generated, you must enable alarm generation for an IPsec tunnel.

To enable alarm generation for an IPsec tunnel:

1. In configuration mode, identify the tunnel.

   ```
   (config)#tunnel ipsec name
   ```

2. Enable alarms for that tunnel.

   ```
   (config-tunnel)#alarms
   ```

Use **no alarms** to disable alarm generation for this tunnel.

You can also configure the holddown time, which is the delay between the state change event and the alarm generation.

```
(config)#ipsec alarms holddown seconds
```

The *seconds* variable represents the number of seconds from 1 to 120 of holddown time. The default is 30 seconds.

Note: Holddown time does not apply to instant alarm generation triggered by DPD failure.

1.2 Tunnel State Alarms

A tunnel state alarm indicating IPsec tunnel failure is generated when the route to the peer is lost, an ASP or linecard is down, or a DPD failure occurs. Contents of a tunnel state alarm include the tunnel down cause.

Tunnel state alarms are cleared when:

- The tunnel is back up.
- The tunnel is deleted.
- The remote-id of the static tunnel is changed. For dynamic tunnels, the alarm corresponding to the old remote-id is not cleared.
- Alarm generation is disabled for the tunnel.

To enable IPsec tunnel state alarms:

1. Enable alarms for the IPsec tunnel. See Section 1.1 on page 1.
2. Enter the following command:

   ```
   (config-tunnel)#alarms
   ```

By default, no tunnel state alarms are generated.

Use `(config-tunnel)#no alarms` to disable alarm generation for the tunnel.

The SNMP trap used to detect state change is the **rnpIPsecTunnelStatusChangeAlarm** and is contained in the RBN-IP-SECURITY-MIB file.

1.3 RSA Certificate Expiration Alarms

Certificate expiration alarms warn you that an RSA trusted or RSA self certificate is about to expire. When you enable this alarm, you set a time interval in days that determines the amount of warning you receive before the certificate expires.

The alarm is cleared when a new certificate with the same subject name is added, the certificate is deleted by the user, or the system time is altered.

To enable certificate expiration alarms:

1. Enable alarms for the IPsec tunnel. See Section 1.1 on page 1.
2. For self certification certificates:

   ```
   [local]Redback(config)#pki alarms certificate self
   expiry interval
   ```

   For trusted certificates:

   ```
   [local]Redback(config)#pki alarms cerificate trusted
   expiry interval
   ```

   where ***interval*** is a numerical value of 1-30 days.

Use the **no** form of this command to turn off alarms for RSA certification expiration.

The related SNMP traps **rbnIpSecRSASelfCertificateNearingExpiryAlarm** and **rbnIpSecRSATrustedCertificateNearingExpiryAlarm** are contained in the RBN-IP-SECURITY-MIB file.

1.4 Valid RSA Certificate Not Found Alarms

You can enable alarms to be sent when there are no valid RSA certificates found for a context. By default, no alarm is generated. The alarm is cleared when a valid certificate is configured or when system time is change to make the existing certificate valid.

To enable invalid certificate alarms:

1. Enable alarms for the IPsec tunnel. See Section 1.1 on page 1.

2. In local configuration mode:

   For self certification certificates:

   ```
   [local]Redback(config)#pki alarms certificate self
   missing
   ```

   For trusted certificates:

   ```
   [local]Redback(config)#pki alarms certificate trusted
   missing
   ```

Use the **no** form of this command to disable the alarm.

The related SNMP traps **rbnlpSecNoValidRSASelfCertificateAlarm** and **rbnlpSecNoValidRSATrustedCertificateAlarm** are contained in the RBN-IP-SECURITY-MIB file.

1.5 Alarm Content

The content attributes for tunnel state alarms and certificate alarms are shown in Table 1

Table 1 Tunnel State Alarm Contents

Attribute	Value
IPsec-Tunnel-Identifier	String of 270 bytes. Created from the **remote-id-type** and the **remote-id** values.
Tunnel name	String of maximum 50 characters.

Attribute	Value
Tunnel type	One of the following: • static • dynamic • manual
Remote-id-type	One of the following: • ipv4 • fqdn—Fully Qualified Domain Name
Remote-id	String of maximum 256 characters
Context-ID of Source IP	
Src IP	Source IP address
Dst IP	Destination IP address
Tunnel State	Either up or down
Event Type	communications
Probable Cause	communicationsProtocolError
Tunnel Down Cause	One of the following: • general • noRoute • aspHomingFailure • ppaHomingFailure • configuredDown • keepaliveFailure • downByPeer • rekeyFailure • aspSoftReset • indeterminate
Severity	Either Major or clear

Table 2 RSA Certificate Alarms Content

Attribute	Value
Event Type	securityServiceOrMechanismViolation
self subject name	String. Maximum length 256 characters.
trusted subject name	String. Maximum length 256 characters.
certificate handle	Integer.
Time left	Expressed in days.

Attribute	Value
Probable cause	keyExpired
Severity	One of the following: • Major • warning • clear

1.6 Trap Statistics Management

All tunnel statistics are maintained at the global level. They include the number of raised alarms and the number of cleared alarms.

To show or clear tunnel state change alarm statistics:

```
#show ipsec alarms statistics

#clear ipsec alarms statistics
```

To show or clear RSA certificate alarm statistics:

```
#show pki alarms statistics

#clear pki alarms statistics
```

1.7 SNMP Configuration Example

SNMP trap generation requires configuration of system and context level alarms. For more information on configuring SNMP, see *Configuring RMON and SNMP*.

To set up general SNMP configuration:

```
snmp server enhance ifmib
snmp view eye-view internet included
snmp community public all-contexts view eye-view read-write
snmp target trapTarget 10.13.168.145 port 15162 security-name publi
```

To make entries into the clear alarm table:

```
snmp alarm model 1 state clear
notify <trapName>
vb-index <IndexValue> vb-value 1
sp-pointer <OID>
eventtype <eventTypeValue>
probablecause <probableCauseValue>
resource-id <identifier for the trap>
```

To make entries into the active alarm table:

```
snmp alarm model 1 state major
notify <trapName>
vb-index <IndexValue> vb-value 4
sp-pointer <OID>
eventtype <eventTypeValue>
probablecause <probableCauseValue>
resource-id <identifier for the trap>
```

2 Troubleshooting

There are a number of reasons that subscribers may not receive expected security services, including a variety of configuration errors. This document describes some of the troubleshooting scenarios.

2.1 ASE Card Fails to Initialize

Problem

After you insert an Advanced Services Engine (ASE) card in the SmartEdge® chassis and provision it by using the `card ase` *`slot-id`* command, error messages similar to the following appear in the console:

```
Jan 24 13:27:19:  %CSM-6-CARD: Initialization failure on
card ase in slot 2

Jan 24 13:27:19:  %CSM-3-TDM_ERR: no shut slot 1 ASP 2
failed at admin layer!  Error#:  12 [csm_card_ase_set_asp
_admin_shut]

Jan 24 13:27:19:  %CSM-3-CARD_ERR: Change admin state
for slot 2 from In Service to In Service failed at admin
layer!  Error #:  12 [csm_ase_set_admin_state]
```

The output of the `show chassis` command indicates that the ASE card did not initialize. The output of the `show hardware card` *`slot`* `details` command indicates the card state as `Card initialization:  PHY initialization failure`.

Cause

There is a possible hardware problem or transient condition.

Solution

Provision the card again in case the initialization failed due to some transient condition. Issue the following commands:

```
[local]Redback#configure

[local]Redback(config)#no card ase slot

[local]Redback(config)#commit

[local]Redback(config)#card ase slot
```

```
[local]Redback(config-card)#commit
```

Wait a maximum of 5 minutes after issuing the `card ase slot` command. You can monitor progress of the provisioning by using the `show chassis` command. Initializing is complete when the Initialized Flags value for the ASE card is *Yes P1P2UR*.

If provisioning again is unsuccessful, reload the card to ensure that the correct firmware is installed. Issue the following command:

```
[local]Redback#reload card slot
```

Reloading will take about 7 minutes. The reload sequence:

- Checks and, if necessary, reformats the file system of the compact flash on the ASE card.
- Downloads the *ase.tar.gz* file from the chassis to the ASE card.
- Upgrades any firmware on the ASE card that does not match the firmware in the *ase.tar.gz* file.

This sequence can result in more than one iteration of the reload command.

If reloading the ASE card is unsuccessful, contact your customer support representative to obtain a Return Merchandise Authorization (RMA) and return the card for replacement.

Note: For more information about the problem prior to returning the card, run On-Demand Diagnostics; see the "Troubleshoot with On-Demand Diagnostics" section in *SmartEdge 1200 Router Hardware Guide*.

2.2 ASP Configuration Error

Problem

Subscriber traffic is not treated as expected; the subscriber is connected but does not receive security services for the duration of the session.

For subscribers who log on when the problem exists, the accounting message indicates that the security service could not be applied. For subscribers already logged on when the problem occurs, security attributes are cleared, but no interim accounting is reported.

Cause

- No Advanced Services Processor (ASP) group is associated with a context.
- An ASP group is associated with a context, but there is no ASP assigned to the ASP pool or no ASE card installed in the chassis; see Reference [1].

Solution

Associate an ASP to the pool or install the ASP in the chassis; see Reference [2].

When the problem is corrected, an accounting reauthorization is sent to provide security services to subscribers.

2.3 Traffic Management Policy Missing

Problem

The subscriber traffic is not treated as expected; the subscriber is connected and receives security services defined by a default Deep Packet Inspection (DPI) traffic management policy, or if no default policy exists, the subscriber does not receive security services.

For subscribers who log on when the problem exists, the accounting message does not include the security service, indicating that the security service could not be applied for the subscriber. For subscribers logged on when the problem occurs, no interim accounting is reported.

Cause

- A DPI traffic management policy assigned to a subscriber is missing when the subscriber logs on.
- A DPI traffic management policy assigned to a subscriber is deleted when the security-enabled subscriber is logged on.

Solution

Change the subscriber configuration to reference an existing DPI traffic management policy or create the DPI traffic management policy assigned to the subscriber.

When the problem is corrected, security services are reapplied automatically, based on subscriber configuration; no accounting reauthorization is sent.

2.4 Peer for an IPsec Tunnel Cannot Be Reached

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Down* or *Wait-on-SA*, and the destination is down or unreachable, or both. No Internet Key Exchange (IKE) or Internet

Protocol Security (IPsec) negotiation messages are logged. The configured peer IP addresses do not respond to ping commands.

Cause

The peer is down or is unreachable.

Solution

Check the physical connectivity to ensure the port or interface is in the *Up* state. Check the network with a ping test to the remote endpoint.

2.5 Peer Context for an IPsec Tunnel is Not Configured

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Down*, the value for `context-for-local-ip` is *local*, and the destination is down on the management interface. No IKE or IPsec negotiation messages are logged, as shown in the following example:

```
[local]Redback#sh tunnel ipsec


::::: Tunnel : ipsec_tunnel1
   Key        : -
   Remote IP : 29.0.0.2    Local IP    : 39.0.0.1
   Tnl Type   : IPsec
   State      : Down       Bound to    :
   Circuit ID: 5           Internal Hdl: 255/28:1023:63/0/1/5
[local]Redback#
```

Cause

The peer interface context is not specified. As a result, messages are routed to the local context instead of the peer. Confirm this by using the `show configuration tunnel` command. The `peer-end-point` attribute must have three settings: *local* (an IP address), *remote* (an IP address), and a *context* (name)

Solution

Configure the context setting for the `peer-end-point` attribute.

2.6 IPsec Tunnel is Not Bound to a Tunnel Interface

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Down* and the value for the interface to which the tunnel must be bound is missing. No IKE or IPsec negotiation messages are logged.

Cause

The interface to which the tunnel must be bound is not configured. Confirm this by using the `show configuration tunnel` command. The bind interface setting between the tunnel interface and the peer context is missing.

Solution

Configure the binding of the tunnel interface to the peer context.

2.7 Mismatched Values for IKE Policy Negotiations

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Wait-on-SA*. The IKE negotiation logs contain `Mismatching Exchange Type` messages.

Cause

The IKE policy specified by one peer is in MAIN mode, and on the other peer is in AGGRESSIVE mode.

Solution

Configure the policies so that they both contain matching values for the key exchange mode.

2.8 Missing IKE or IPsec Policies

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Wait-on-SA*. The IKE negotiation logs contain messages indicating that no policy is configured for the peer.

Cause

An IKE policy for Phase 1 negotiation, or an IPsec policy for Phase II negotiation is missing in the configuration for one of the peers.

Solution

Configure the necessary policies.

2.9 Mismatched Phase II Authentication Algorithms

Problem

The tunnel does not come up. The output of the `show tunnel` command indicates that the tunnel state is *Wait-on-SA*. The IKE negotiation logs contain `Mismatching Authentication algorithm` messages.

Cause

The authentication algorithm specified on one peer does not match the algorithm specified on the other peer.

Solution

Configure IPsec policies on both peers to have matching authentication algorithms.

2.10 ASE Security Services Not Enabled with NAT Service

Problem

ASE security services are not enabled or are removed from a subscriber when Network Address Translation (NAT) service and ASE security services are applied together for a subscriber.

Cause

NAT and ASE security services are mutually exclusive and cannot be applied together for a subscriber.

- If ASE security services are configured when NAT is applied to a subscriber, ASE security services are removed and the NAT service is enabled.
- If NAT is configured when ASE security services are applied to a subscriber, ASE security services are not enabled.

- If both NAT and ASE security services are applied to a subscriber; only the NAT service is enabled.

2.11 ASP Group Congestion

Problem

Security attributes are cleared and security services are permanently bypassed for the duration of the subscriber session. Accounting information indicates that security services could not be applied for the subscriber.

Cause

ASPs in an ASP group are operating at peak capacity when a security-enabled subscriber belonging to that ASP group logs on.

Solution

Reauthorize the subscriber to restore security services.

2.12 Traffic Dropped or Bypasses ASE When Resource Failure Occurs

Problem

The security service drops traffic or bypasses the ASE, depending on the security service application. You can configure whether application traffic is dropped or bypasses the ASP when a resource failure occurs; IPsec traffic is always dropped when a resource failure occurs.

Cause

No physical ASP is associated with an ASP group due to one of the following conditions:

- ASPs configured in an ASP pool are not present.
- All ASPs in an ASP pool are shut down.
- All ASPs in an ASP group failed to recover from a failure and are now in a permanently failed state.
- All ASPs in the ASP group are in a transient failure state.
- An ASP associated with a protection group index failed, and no backup ASP is assigned.

Solution

The problem persists until the ASPs recover or the operator replaces the failed card or otherwise manually restores the ASP to an operational state.

2.13 Traffic Dropped or Bypasses ASE During Recovery From Hard Reboot

Problem

All ASPs that are configured but not physically present in the chassis are considered to have permanently failed or all ASPs that are configured and physically present in the chassis are considered to be in a transient runtime failure condition after a chassis reboot. Subscribers who log on before the ASE cards are fully operational may be mapped to ASPs that are not yet operational. In this case, the security service application drops the traffic or bypasses the ASE.

Note: You can configure a longer time-out duration for the transient runtime failure state on chassis reboot to allow the ASPs more time to become operational.

Cause

If ASE cards were added to the chassis with incorrect or missing saved binary images, when the node restarts after a hard reboot of a SmartEdge router, the order in which the ASE cards restart is not deterministic.

Glossary

ASE
Advanced Services Engine

ASP
Advanced Services Processor

DPI
Deep Packet Inspection

IKE
Internet Key Exchange

IPsec
Internet Protocol Security

NAT
Network Address Translation

RMA
Return Merchandise Authorization

Reference List

[1] *Advanced Services Infrastructure Overview*, 1/221 02-CRA 119 1170/1

[2] *Advanced Services Configuration and Operation Using the SmartEdge OS CLI*, 1/1543-CRA 119 1170/1