ERICSSON

IPsec VPN Command Reference

MANUAL PAGE

Copyright

© Ericsson AB 2009–2011. 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

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Commands

This document provides command syntax and usage guidelines for commands used in the configuration and operation of the Internet Protocol Security (IPsec) Virtual Private Network (VPN) application. For an overview of IPsec VPN, see Reference [1]. For configuration tasks, see Reference [2].

1.1 add pki key-pair

```
add pki key-pair key-pair-name rsa size
```

1.1.1 Command Mode

exec

1.1.2 Syntax Description

`key-pair`	Unique name for the key pair; up to 39 characters.
`rsa`	Size of the key (in bits). One of: • 512 • 1024 • 2048

1.1.3 Default

No key pair is configured.

1.1.4 Usage Guidelines

This command configures a private-public key pair for use by the Public Key Infrastructure (PKI) in the specified context.

1.1.5 Examples

The following example configures the key pair `first_key_pair` with 1028-bit keys in the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#add pki key-pair first_key_pair rsa 1028
```

1.2 add pki certificate request rsa

add pki certificate-request rsa ***cert-req-name*** **file** ***file-name***

1.2.1 Command Mode

exec

1.2.2 Syntax Description

cert-req-name	The name of the certificate request.
file *file-name*	Full path to the location where the file is created.

1.2.3 Default

No certificate request is configured.

1.2.4 Usage Guidelines

This command configures a certificate request and prompts for the information to create a file in PEM format required by a Certificate Authority (CA) to generate a self certificate. After the command is issued, you are prompted for the information required for the file required by the CA:

```
Key-Pair: key-name
Subject: DN
IPv4-Address: pv4-addr
FQDN: fqdn-name
Domain-Name:  name
File: file-name
```

1.2.5 Examples

```
[local]Redback#add pki certificate-request rsa cert.req
Key-Pair: key1
Subject :  cn=se1,ou=rbak,o=Ericsson,c=us
IPv4-Address : 10.1.1.1
Domain-Name : se1.rbak.com
File  : /flash/cert1.req
```

1.3 address allocation aaa

address-allocation aaa

1.3.1 Command Mode

IKEv2 policy configuration

1.3.2 Syntax Description

This command has no keywords or arguments.

1.3.3 Default

None

1.3.4 Usage Guidelines

This command configures specifies AAA as the source of address allocation for the remote access clients using this IKEv2 policy. Using the **no** form of the command removes the address allocation from the IKEv2 policy.

1.3.5 Examples

```
[local]Redback(config-ike2-policy)#address-allocation aaa
```

1.4 ah

ah [**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcbc**]

no ah

1.4.1 Command Mode

IPsec proposal configuration

1.4.2 Syntax Description

hmac-md5-96	hmac-md5-96 algorithm
hmac-sha1-96	hmac-sha1-96 algorithm
hmac-aes-xcbc	hmac-aes-xcbc algorithm

1.4.3 Default

hmac-sha1-96

1.4.4 Usage Guidelines

This command configures the Authentication Header (AH) authentication algorithm for an IPsec proposal. Using the **no** form of the command removes the AH configuration.

1.4.5 Examples

```
[local]Redback(config-ipsec-proposal)#ah hmac-aes-xcbc
```

1.5 ah key

ah [**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcbc**] **key** {**hex** ***hex-number*** |***ASCII-value***}

no ah [**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcbc**] **key** {**hex** ***hex-number*** |***ASCII-value***}

1.5.1 Command Mode

IPsec Security Association (SA) Security Parameter Index (SPI) configuration (manual key mode)

1.5.2 Syntax Description

hex ***hex-number***	Hexadecimal number. The length of the value is specified in Table 1.
ASCII-value	ASCII value. The length of the value is specified in Table 1.

1.5.3 Default

aes-128-cbc

1.5.4 Usage Guidelines

Specifies the AH authentication algorithm and the manual key for authenticating inbound, outbound, or bidirectional traffic SAs.

Table 1 lists the valid key length values for each of the supported AH authentication algorithms.

Table 1 Valid Key Length Values for AH Authentication Algorithms

Keyword	ASCII Text Key Length	Hexadecimal Number Key Length
`hmac-md5-96,`	16	32
`hmac-sha1-96`	20	40
`hmac-aes-xcbc`	16	32

1.5.5 Examples

```
[local]Redback(config-ipsec-sa-spi)#ah hmac-md5-96
key hex 0fa20fa20fa20fa2
```

1.6 ah spi

```
ah spi spi-value
```

```
no ah spi spi-value
```

1.6.1 Command Mode

IPsec SA SPI configuration

1.6.2 Syntax Description

`spi-value`	256-0x1ffff: in, both; 1-0xffffffff: out

1.6.3 Default

No SPI value is configured.

1.6.4 Usage Guidelines

Specifies the AH SPI value for the inbound traffic, outbound traffic, or bidirectional traffic SAs. Using the `no` value of the command removes the SPI value.

1.6.5 Examples

```
[local]Redback(config-ipsec-sa-spi)#ah spi 48354
```

1.7 alarms

alarms

no alarms

1.7.1 Command Mode

Tunnel configuration

1.7.2 Default

By default, no alarms are generated.

1.7.3 Usage Guidelines

This command controls the generation of tunnel-state alarms.

1.7.4 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#alarms
```

1.8 anti-replay-window

anti-replay-window ***window_size***

no anti-replay-window

1.8.1 Command Mode

IPsec policy configuration

IPsec SA configuration

1.8.2 Syntax Description

window_size	0, 32 to 1024, in multiples of 32.

1.8.3 Default

64

1.8.4 Usage Guidelines

Configures the anti-replay window size. The anti-replay window prevents the replay attack and potential Denial of Service (DoS) attack. Size 0 disables the anti-replay window. Using the **no** form of the command resets the configuration to the default.

1.8.5 Examples

```
[local]Redback(config-ipsec-policy)#anti-replay-window 128
```

1.9 authentication

authentication {**preshared-key**|**rsa-signature**}

1.9.1 Command Mode

IKEv2 policy configuration

IKE proposal configuration

1.9.2 Syntax Description

preshared-key	Authenticate using pre-shared keys
rsa-signature	Authenticate using certificates

1.9.3 Default

Pre-shared key

1.9.4 Usage Guidelines

This command configures the authentication method used by the Internet Key Exchange version 2 (IKEv2) policy or Internet Key Exchange version 1 (IKEv1) proposal. The authentication method specified using IKEv2 protocol in an IKEv2 policy need not match on both peers. The authentication method specified using IKEv1 protocol in an IKE proposal must match on both peers. Using the **no** form of the command removes the authentication configuration.

1.9.5 Examples

The following example shows the authentication specified by an IKEv2 policy.

```
[local]Redback(config-ctx)#ike2 policy ike2-pol1
[local]Redback(config-ike-policy)#authentication rsa-signature
```

The following example shows the authentication specified by an IKE proposal.

```
[local]Redback(config)#ike proposal ike-prop1
[local]Redback(config-ike-proposal)#authentication rsa-signature
```

1.10 authentication algorithm

authentication algorithm {**hmac-md5-96**|**hmac-sha1-96**}

no authentication algorithm

1.10.1 Command Mode

IKEv1 proposal configuration

IKEv2 proposal configuration

1.10.2 Syntax Description

hmac-md5-96	hmac-md5-96 algorithm
hmac-sha1-96	hmac-sha1-96 algorithm

1.10.3 Default

hmac-sha1-96

1.10.4 Usage Guidelines

Specifies the authentication algorithm of an IKE proposal. Using the **no** form of the command resets the configuration to the default.

1.10.5 Examples

```
[local]Redback(config-ike-proposal)#authentication
algorithm hmac-md5-96
```

1.11 bind interface (IPsec)

bind interface *if-name context-name*

```
no bind interface if-name [context-name]
```

1.11.1 Command Mode

tunnel configuration

1.11.2 Syntax Description

if-name	Name of a previously created interface.
context-name	Name of the context under which the specified interface is bound.

1.11.3 Default

No IPsec tunnel endpoints are bound.

1.11.4 Usage Guidelines

Statically binds the IPsec tunnel to a previously created interface. For on-demand IPsec tunnels, bind the on-demand tunnel to the IPsec multibind interface configured for this on-demand IPsec tunnel.

Use the **no** form of this command to remove the binding. You must remove any existing binding before you can create a new binding for the IPsec tunnel.

1.11.5 Examples

The following example shows how to create or modify the **rec_2_1** tunnel and bind it to the **ipsec-if1** interface in the Security service enabled **ipsec-context** context:

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#bind interface ipsec-if1 ipsec-context

[local]Redback(config)#tunnel ipsec profile1-se on-demand
[local]Redback(config-tunnel)#bind interface ipsec-mb-se local
```

1.12 both

```
both

no both
```

1.12.1 Command Mode

IPsec SA configuration

1.12.2 Syntax Description

This command has no keywords or arguments.

1.12.3 Default

No SA values for traffic are configured.

1.12.4 Usage Guidelines

Enters IPsec SA SPI configuration mode for configuring the same SA values for both inbound and outbound traffic. Using the `no` form of the command removes the bidirectional traffic configuration.

This command cannot be used with either the `in` or `out` command. If the `both` command is configured, neither inbound nor outbound SA traffic attributes can be configured separately. To configure the different SA traffic attributes for inbound and outbound traffic see the `in` command in Section 1.40 on page 36 and the `out` command in Section 1.57 on page 53, respectively.

1.12.5 Examples

```
[local]Redback(config-ipsec-sa)#both
```

1.13 bulkstats ipsec schema

bulkstats ipsec schema ***sch-prof-name*** **policy** ***bulk-pol-name ctx-name***

no bulkstats ipsec schema ***sch-prof-name*** **policy** ***bulk-pol-name ctx-name***

1.13.1 Command Mode

IPsec tunnel configuration

1.13.2 Syntax Description

`sch-prof-name`	Name of the bulkstats schema profile. Alphanumeric string with up to 19 characters.
`bulk-pol-name`	Name of the bulkstats policy. Alphanumeric string with up to 19 characters.
`ctx-name`	Name of the context in which the bulkstats policy is configured. Alphanumeric string with up to 31 characters. Optional in context and subscriber configuration modes.

1.13.3 Default

None

1.13.4 Usage Guidelines

Use the **`bulkstats ipsec schema`** command with the *`ctx-name`* argument to collect data for a tunnel.

Caution!

Risk of system performance degradation. Although you can apply multiple bulkstats schema profiles that collect different types and formats of data, you should minimize the number of bulkstats schema profile applications to preserve system performance. To reduce the performance impact, create one bulkstats schema profile that records several subsets of data. Separate each subset within the format string by entering the **`\n`** character sequence, which creates a new starting line in the output file. You can then apply this single bulkstats schema profile.

Caution!

Risk of system performance degradation. Applying multiple bulkstats policies can reduce system performance. To reduce the risk, minimize the number of policies applied to a port, channel, channel group, or profile.

Use the **`no`** form of this command to remove the application of the specified bulkstats schema profile and policy from the context, port, channel, channel group, profile for an 802.1Q PVC, ATM PVC, Frame Relay PVC, or default subscriber profile.

1.13.5 Examples

The example shows command for collecting statistics for a **`ipsec_tunnel`** tunnel, where schema profile is tunnelstats and context name is **`local`**.

```
[local]Redback(config)#tunnel ipsec ipsec_tunnel

[local]Redback(config-ctx)# bulkstats ipsec schema  tunnelstats  policy ipsec_stats local
```

1.14 clear ike sa tunnel

`clear ike sa tunnel` ***`tunnel-name`***

1.14.1 Command Mode

exec

1.14.2 Syntax Description

`tunnel` ***`tunnel-name`***	Name of a previously created IPsec tunnel.
`remote-ip` ***`remote-ip-addr`***	IP address of the remote peer.
`local-ip` ***`local-ip-addr`***	IP address of the local peer.

1.14.3 Usage Guidelines

Clears any Service Association (SA) associated with the specified Internet Protocol Security (IPsec) tunnel name or remote and local endpoints. Commands that clear SAs delete and renegotiate the SAs (with the new IKE configuration). Does not apply to on-demand IPsec tunnels.

1.14.4 Examples

```
[local]Redback#clear ike sa tunnel rec_2_1
```

1.15 clear ipsec alarms statistics

`clear ipsec alarms statistics`

1.15.1 Command Mode

exec

1.15.2 Usage Guidelines

Clears the IPsec alarms statistics for tunnel-state traps.

1.16 clear ipsec sa tunnel

`clear ipsec sa tunnel` ***`tunnel-name`***

1.16.1 Command Mode

exec

1.16.2 Syntax Description

`tunnel-name`	Name of a previously created IPsec tunnel.

1.16.3 Usage Guidelines

Clears the IPsec SAs associated with the given tunnel name. Commands that clear SAs delete and renegotiate the SAs (with the new IPsec configuration). For on-demand IPsec tunnels, the ***`tunnel-name`*** argument is dynamically assigned by the system.

1.16.4 Examples

```
[local]Redback#clear ipsec sa tunnel rec_2_1
```

1.17 clear pki alarms statistics

`clear pki alarms statistics`

1.17.1 Command Mode

exec

1.17.2 Usage Guidelines

Clears the expiry warning and certificate missing alarms for RSA trusted and self certificates.

1.18 connection-type

connection-type {**initiator-only**|**responder-only**|**both**}

no connection-type

1.18.1 Command Mode

IKE policy configuration

IKEv2 policy configuration

1.18.2 Syntax Description

initiator-only

responder-only

both

1.18.3 Default

both

1.18.4 Usage Guidelines

Specifies the IKE connection type of an IKE policy, which assigns the role for the local IKE peer when establishing connections to set up an IPsec tunnel. For on-demand IPsec tunnels, you cannot change the connection type to initiator-only when using aggressive mode. You cannot change the connection type from responder-only if more than one IKE proposal exists in the IKE policy when using aggressive mode. Using the **no** form of the command resets it to the default.

1.18.5 Examples

The following example shows how to assign the role of initiator-only to any local peer that has this IKE policy assigned to it:

```
[local]Redback(config-ike-policy)#connection-type initiator-only
```

1.19 debug ike card

debug ike card ***slot-id*/*asp-id* *message-type*** {**trace**|**log**} {**console**|**external**} [**level** ***level***]

1.19.1 Command Mode

exec

1.19.2 Syntax Description

card ***slot-id***

Chassis slot number where the Advanced Services Engine (ASE) card is installed. The range of values depends on the chassis:

- SmartEdge® 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

The ID of the Advanced Services Processor (ASP) on the ASE card. Possible values are 1 and 2.

message-type

Type of debug message to forward:

- **all**
- **ikebase** — Base IKE messages
- **ikev1**—IKE version 1 messages
- **packet**—Packet messages
- **policy**—IKE policy messages

trace

Enables generation of trace messages.

log

Enables generation of log messages.

console

Sends debug information to the console.

`external`

Sends debug information to an external system.

`level` ***`level`***

Optional. Specifies the debug logging level, where *`level`* is one of the following (in descending severity order):

- `0`—Only emergency events.
- `1`—Alert and more severe events.
- `2`—Critical and more severe events.
- `3`—Error and more severe events.
- `4`—Warning and more severe events.
- `5`—Notice and more severe events.
- `6`—Informational and more severe events.
- `7`–All events, including debug events.

1.19.3 Usage Guidelines

Enables the generation of debug messages for the IKE configuration of a specific ASP on a specific ASE card.

Caution!

Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of debug messages on a production system.

1.19.4 Examples

The following example shows how to enable the generation of IKE debug messages for the IKE configuration on the ASP:

```
[local]Redback#debug ike card 2/1 ikev1 log console level 4
```

1.20 debug ike config

```
debug ike config
```

1.20.1 Command Mode

exec

1.20.2 Syntax Description

This command has no keywords or arguments.

1.20.3 Usage Guidelines

Enables the generation of debug messages for the IKE configuration.

Caution!

Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of debug messages on a production system.

1.20.4 Examples

```
[local]Redback#debug ike config
```

1.21 debug ipsec card

debug ipsec card ***slot-id/asp-id message-type*** {**trace**|**log**} {**console**|**external**|**trace buffer**} [**level** ***level***]

1.21.1 Command Mode

exec

1.21.2 Syntax Description

card ***slot-id***

Chassis slot number where the ASE card is installed. The range of values depends on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

ID of the ASP on the ASE card. Possible values are 1 and 2.

message-type

Type of debug message to forward:

- **all**
- **infra** — IPsec infrastructure messages
- **packet**—Packet messages
- **sad**—SAD messages
- **spd** — SPD messages
- **tunnel**—Tunnel messages

trace

Enables generation of trace messages.

log

Enables generation of log messages.

trace-buffer

Sends debug information to the circular buffer on the controller card.

console

Sends debug information to the console.

`external`	Sends debug information to an external system.
`level` *`level`*	Optional. Specifies the debug logging level, where *`level`* is one of the following (in descending severity order): • `0`—Only emergency events. • `1`—Alert and more severe events. • `2`—Critical and more severe events. • `3`—Error and more severe events. • `4`—Warning and more severe events. • `5`—Notice and more severe events. • `6`—Informational and more severe events. • `7`–All events, including debug events.

1.21.3 Usage Guidelines

Enables the generation of debug messages for the IPsec configuration of a specific ASP on a specific ASE card.

Caution!

Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of debug messages on a production system.

1.21.4 Examples

The following example shows how to enable the generation of packet debug messages for the IPsec configuration on the ASP:

```
[local]Redback#debug ipsec card 1/1 packet log console level warning
```

1.22 debug ipsec config

`debug ipsec config`

1.22.1 Command Mode

exec

1.22.2 Syntax Description

This command has no keywords or arguments.

1.22.3 Usage Guidelines

Enables the generation of debug messages for the IPsec configuration.

Caution!

Risk of performance loss. Enabling the generation of debug messages can severely affect system performance. To reduce the risk, exercise caution when enabling the generation of debug messages on a production system.

1.22.4 Examples

```
[local]Redback#debug ipsec config
```

1.23 description (IPsec)

```
description string
```

```
no description
```

1.23.1 Command Mode

IKE policy configuration

IKE proposal configuration

IKEv2 policy configuration

IKEv2 proposal configuration

IPsec Access Control List (ACL) configuration

IPsec policy configuration

IPsec proposal configuration

IPsec security association configuration

1.23.2 Syntax Description

string	Descriptive text; up to 255 characters.

1.23.3 Default

No description is configured.

1.23.4 Usage Guidelines

Specifies the description of the IKE policy, IKE proposal, IPsec ACL, IPsec policy, IPsec proposal, or IPsec SA.

1.23.5 Examples

```
[local]Redback(config-ipsec-proposal)#description IPsec-Proposal-1
```

1.24 df-bit

df-bit {**propagate**|**set**|**clear**}

no df-bit

1.24.1 Command Mode

tunnel configuration

IPsec profile configuration

1.24.2 Syntax Description

propagate	Propagate DF bit from inner IP to outer IP header.
set	Set the DF bit in the outer IP header
clear	Clear the DF bit from the outer IP header

1.24.3 Default

Propagate

1.24.4 Usage Guidelines

Specifies how to configure the Don't Fragment (DF) bit for the IP header. The default value, **propagate**, copies to the DF bit setting used in the inner IP heading to the outer IP heading. Using the **no** form of the command resets the configuration to the default.

1.24.5 Examples

```
[local]Redback(config-tunnel)#df-bit clear
```

1.25 dh-group

dh-group *dh-group*

no dh-group

1.25.1 Command Mode

IKE proposal configuration

IKEv2 proposal configuration

1.25.2 Syntax Description

dh-group *dh-group*	The Diffie-Hellman group to use: 1, 2, 5, or 14

1.25.3 Default

1

1.25.4 Usage Guidelines

Specifies the Diffie-Hellman group for IKE key exchanges in an IKE proposal. Using the **no** form of the command resets the configuration to the default.

1.25.5 Examples

```
[local]Redback(config-ike-proposal)#dh-group 2
```

1.26 encryption algorithm

encryption algorithm {**aes-128-cbc**|**aes-192-cbc**|**aes-256-cbc**|**des-cbc**|**3des-cbc**}

no encryption algorithm

1.26.1 Command Mode

IKE proposal configuration

IKEv2 proposal configuration

1.26.2 Syntax Description

`aes-128-cbc`	aes-128-cbc protocol.
`aes-192-cbc`	aes-192-cbc protocol
`aes-256-cbc`	aes-256-cbc protocol
`des-cbc`	des-cbc protocol
`3des-cbc`	3des-cbc protocol

1.26.3 Default

aes-128-cbc

1.26.4 Usage Guidelines

Specifies the encryption algorithm for an IKE proposal. Using the **no** form of the command resets the configuration to the default.

1.26.5 Examples

```
[local]Redback(config-ike-proposal)#encryption algorithm aes-192-cbc
```

1.27 esp authentication

esp authentication {**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcbc**}

no esp authentication

1.27.1 Command Mode

IPsec proposal configuration

1.27.2 Syntax Description

`hmac-md5-96`	hmac-md5-96 algorithm
`hmac-sha1-96`	hmac-sha1-96 algorithm
`hmac-aes-xcbc`	hmac-aes-xcbc algorithm

1.27.3 Default

hmac-sha1-96

1.27.4 Usage Guidelines

Specifies the ESP authentication algorithm of an IPsec proposal.

If ESP authentication is configured without ESP encryption, the ESP encryption is set to null.

When neither ESP or AH authentication is configured, using the **no** form of the command sets the ESP authentication (and ESP encryption) to the default. If either ESP or AH authentication is configured, using the **no** form of the command removes the ESP authentication configuration.

1.27.5 Examples

```
[local]Redback(config-ipsec-proposal)#esp authentication hmac-aes-xcbc
```

1.28 esp authentication key

esp authentication [**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcbc**] **key** {**hex** ***hex-number***|***ASCII-value***}

no esp authentication [**hmac-md5-96**|**hmac-sha1-96**|**hmac-aes-xcb c**] **key** {**hex** ***hex-number***|***ASCII-value***}

1.28.1 Command Mode

IPsec SA SPI configuration

1.28.2 Syntax Description

hmac-md5-96	hmac-md5-96 algorithm
hmac-sha1-96	hmac-sha1-96 algorithm
hmac-aes-xcbc	hmac-aes-xcbc algorithm
hex ***hex-number***	Hexadecimal number. The length of the value is specified inTable 2.
ASCII-value	ASCII value. The length of the value is specified in Table 2

1.28.3 Default

hmac-sha1-96

1.28.4 Usage Guidelines

Specifies the ESP authentication algorithm and the manual key for encrypting inbound, outbound, or bidirectional traffic SAs. The **no** form of the command removes the ESP authentication algorithm from the configuration.

If ESP encryption is configured without ESP authentication, only encryption is done. If ESP authentication is configured without ESP encryption, the encryption is set to null.

Table 2 lists the valid key lengths for each of the supported authentication algorithms.

Table 2 Valid Key Length Values for ESP Authentication Algorithms

Keyword	ASCII Text Key Length	Hexadecimal Number Key Length
hmac-md5-96,	16	32
hmac-sha1-96	20	40
hmac-aes-xcbc	16	32

1.28.5 Examples

```
[local]Redback(config-ipsec-sa-spi)#esp authentication
hmac-aes-xcbc key 1234123412341234
```

1.29 esp encryption

```
esp encryption {aes-128-cbc|aes-192-cbc|aes-256-cbc|aes-128-ctr|aes-192-ctr|aes-256-ctr|des-cbc|3des-cbc|null}
```

```
no esp encryption
```

1.29.1 Command Mode

IPsec proposal configuration

1.29.2 Syntax Description

`aes-128-cbc`	aes-128-cbc algorithm
`aes-192-cbc`	aes-192-cbc algorithm
`aes-256-cbc`	aes-256-cbc algorithm
`aes-128-ctr`	aes-128-ctr algorithm
`aes-192-ctr`	aes-192-ctr algorithm
`aes-256-ctr`	aes-256-ctr algorithm
`des-cbc`	des-cbc algorithm
`3des-cbc`	3des-cbc algorithm
`null`	null encryption algorithm

1.29.3 Default

aes-128-cbc

1.29.4 Usage Guidelines

Specifies the ESP encryption algorithm of an IPsec proposal.

When neither ESP nor AH authentication is specified, the default is the ESP encryption **aes-128-cbc** with ESP authentication **hmac-sha1-96**. If ESP authentication is configured without ESP encryption, the ESP encryption is set to null.

If AH authentication is configured, using the **no** form of the command removes the encryption. If neither ESP authentication or AH is specified, using the **no** form of the command resets the configuration to the default.

1.29.5 Examples

```
[local]Redback(config-ipsec-proposal)#esp encryption aes-256-cbc
```

1.30 esp encryption key

esp encryption [**aes-128-cbc**|**aes-192-cbc**|**aes-256-cbc**|**aes-128-ctr**|**aes-192-ctr**|**aes-256-ctr**|**des-cbc**|**3des-cbc**] **key** {**hex** ***hex-number***|***ASCII-value***}

no esp encryption [**aes-128-cbc**|**aes-192-cbc**|**aes-256-cbc**|**aes-128-ctr**|**aes-192-ctr**|**aes-256-ctr**|**des-cbc**|**3des-cbc**] **key** {**hex** ***hex-number***|***ASCII-value***}

1.30.1 Command Mode

IPsec SA SPI configuration (manual key mode)

1.30.2 Syntax Description

aes-128-cbc	aes-128-cbc algorithm
aes-192-cbc	aes-192-cbc algorithm
aes-256-cbc	aes-256-cbc algorithm
aes-128-ctr	aes-128-ctr algorithm
aes-192-ctr	aes-192-ctr algorithm
aes-256-ctr	aes-256-ctr algorithm
des-cbc	des-cbc algorithm
3des-cbc	3des-cbc algorithm
hex ***hex-number***	Hexadecimal number. The length of the value is specified in Table 3.
ASCII-value	ASCII value. The length of the value is specified in Table 3

1.30.3 Default

aes-128-cbc

1.30.4 Usage Guidelines

Specifies the ESP encryption algorithm and the manual key for encrypting inbound, outbound, or bidirectional traffic SAs. If no encryption algorithm is specified, the default algorithm (aes-128-cbc) is used.

If ESP is configured without ESP authentication, only encryption is done. If ESP authentication is configured without ESP encryption, the encryption is set to null.

Table 3 lists the valid key length values for each of the supported ESP encryption algorithms.

Table 3 Valid Key Length Values for Different ESP Encryption Algorithms

Keyword	ASCII Text Key Length	Hexadecimal Number Key Length
des-cbc	8	16
3des-cbc	24	48
aes-128-cbc (default)	16	32
aes-192-cbc	24	48
aes-256-cbc	32	64
aes-128-ctr	16	32
aes-192-ctr	24	48
aes-256-ctr	32	64

1.30.5 Examples

```
[local]Redback(config-ipsec-sa-spi)#esp encryption des-cbc key 12345678
```

1.31 esp spi

```
esp spi spi-value
```

```
no esp spi spi-value
```

1.31.1 Command Mode

IPsec SA SPI configuration

1.31.2 Syntax Description

spi-value	256-0x1ffff: in, both; 1-0xffffffff: out

1.31.3 Default

No SPI value is configured.

1.31.4 Usage Guidelines

Specifies the ESP SPI value for the inbound traffic, outbound traffic, or bidirectional traffic SAs.

1.31.5 Examples

```
[local]Redback(config-ipsec-sa-spi)#esp spi 65535
```

1.32 identity local

identity local {*value*|**fqdn** *fqdn-string*}

no identity local

1.32.1 Command Mode

IKE policy configuration

IKEv2 policy configuration

1.32.2 Syntax Description

value	IP address
fqdn *fqdn-string*	Fully qualified domain name

1.32.3 Default

No local identity is configured.

1.32.4 Usage Guidelines

Specifies the identity of the local IPsec tunnel endpoint in an IKE policy to use when negotiating IKE requests with a remote peer. Use the IP address or FQDN of the loopback interface defined to provide the identity of the gateway for IPsec tunnels configured on this SmartEdge router as the value. When IKE sessions are negotiated, the local identity configured in the IKE policy on one peer must match the remote ID configured in the IPsec tunnel endpoint on the other peer. Only one local identity is allowed for each policy. The same local identity can appear in multiple policies. Using the **no** form of the command will remove the configuration.

1.32.5 Examples

```
[local]Redback(config-ike-policy)#identity local 30.0.1.3
```

```
[local]Redback(config-ike-policy)#identity local fqdn peer1.redback.com
```

1.33 ike keepalive

```
ike keepalive
```

```
no ike keepalive
```

1.33.1 Command Mode

context configuration

1.33.2 Syntax Description

This command has no keywords or arguments.

1.33.3 Default

Disabled.

1.33.4 Usage Guidelines

Enables the sending of Dead Peer Detection (DPD) messages to IKE peers. When enabled, a DPD message is sent to the remote peer when there is traffic to be sent to the remote peer, but there has been no traffic received from the remote peer for 10 seconds. If a response is received, no further messages are sent unless the previous condition is met. If no response is received from the remote peer, the keepalive is retried three times at an interval of 10 seconds. If there is no response from the remote peer, the tunnel is brought down. Using the **no** form of the command disables the sending of DPD messages (the default setting).

1.33.5 Examples

The following example shows how to enable the sending of DPD messages to IKE peers:

```
[local]Redback(config-ctx)#ike keepalive
```

1.34 ike policy

ike policy ***ike-policy-name***

no ike policy ***ike-policy-name***

1.34.1 Command Mode

context configuration

tunnel configuration

1.34.2 Syntax Description

ike-policy-name	In context configuration mode, name of the IKEv1 policy, which must be unique; up to 39 characters. In tunnel configuration mode, name of a previously created IKEv1 policy.

1.34.3 Default

No IKEv1 policy is configured in a context by default. No IKEv1 policy is specified for an IPsec tunnel by default.

1.34.4 Usage Guidelines

In context configuration mode, creates (with default attributes), or selects an IKEv1 policy and enters IKE policy configuration mode. Using the **no** form of the command removes the IKE policy.

In tunnel configuration mode, specifies the IKEv1 policy used by the IPsec tunnel. Using the **no** form of the command removes the IKEv1 policy from the IPsec tunnel configuration. When a tunnel configuration specifies an IKEv1 policy, the IKEv1 protocol is used for all IKE exchanges for that tunnel.

1.34.5 Examples

The following example shows how to configure the **IKE_Pol1** IKE policy in the local context:

```
[local]Redback(config-ctx)#ike policy IKE_Pol1
```

The following example shows how to associate the **IKE_Pol1** IKE policy to the **rec_2_1** tunnel in the local context.

```
[local]Redback(config)#tunnel ipsec rec_2_1
```

```
[local]Redback(config-tunnel)#ike-policy IKE_Pol1
```

1.35 ike2 policy

ike2 policy ***ike2-policy-name***

no ike2 policy ***ike2-policy-name***

1.35.1 Command Mode

context configuration

tunnel configuration

1.35.2 Syntax Description

ike2-policy-name	In context configuration mode, name of the IKEv2 policy, which must be unique; up to 39 characters. In tunnel configuration mode, name of a previously created IKEv2 policy.

1.35.3 Default

No IKEv2 policy is configured in a context by default. No IKEv2 policy is specified for an IPsec tunnel by default.

1.35.4 Usage Guidelines

In context configuration mode, creates (with default attributes), or selects an IKEv2 policy and enters IKEv2 policy configuration mode. Using the **no** form of the command removes the IKEv2 policy.

In tunnel configuration mode, specifies the IKEv2 policy used by the IPsec tunnel. Using the **no** form of the command removes the IKEv2 policy from the IPsec tunnel configuration. . When a tunnel configuration specifies an IKEv2 policy, the IKEv2 protocol is used for all IKE exchanges for that tunnel.

1.35.5 Examples

The following example shows how to configure the **IKE2_Pol1** IKE policy in the local context:

```
[local]Redback(config-ctx)#ike2 policy IKE2_Pol1
```

The following example shows how to associate the **IKE2_Pol1** IKE policy to the **rec_2_1** tunnel in the local context.

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#ike2-policy IKE2_Pol1
```

1.36 ike proposal

ike proposal ***ike-proposal-name***

no ike proposal ***ike-proposal-name***

1.36.1 Command Mode

global configuration

1.36.2 Syntax Description

ike-proposal-name	Name of an IKE proposal, which must be unique; up to 39 characters.

1.36.3 Default

No IKE proposal is configured.

1.36.4 Usage Guidelines

Creates (with default attributes) or selects an IKEv1 proposal and enters IKE proposal configuration mode. Using the **no** form of the command removes the IKEv1 proposal.

1.36.5 Examples

```
[local]Redback(context)#ike proposal IKE_Prop1
```

1.37 ike2 proposal

ike2 proposal ***ike2-proposal-name***

no ike2 proposal ***ike2-proposal-name***

1.37.1 Command Mode

global configuration

1.37.2 Syntax Description

ike2-proposal-name	Name of an IKEv2 proposal, which must be unique; up to 39 characters.

1.37.3 Default

No IKEV2 proposal is configured.

1.37.4 Usage Guidelines

Creates (with default attributes) or selects an IKEv2 proposal and enters IKEv2 proposal configuration mode. Using the **no** form of the command removes the IKE proposal.

1.37.5 Examples

```
[local]Redback(context)#ike2 proposal IKE2_Prop1
```

1.38 import pki certificate

import pki certificate {**self rsa key-pair** ***key-pair-name***|**trusted rsa**} **file** ***file-name***

1.38.1 Command Mode

exec

1.38.2 Syntax Description

key-pair ***key-pair-name***	Unique name for the key pair; up to 39 characters.
file ***file-name***	Full path to the location of the file (in PEM format) from which the private key is to be imported.

1.38.3 Default

No certificate is imported.

1.38.4 Usage Guidelines

This command imports either a self certificate or a trusted certificate generated by a CA from a file in PEM format into the SmartEdge router configuration. The certificate is encrypted using the RSA algorithm. When you specify a self certificate, you must provide both the name of the public-private key-pair used to generate the certificate and the full path and name of the file containing the certificate. When you specify a trusted certificate you must provide the full path and name of the file containing the certificate.

1.38.5 Examples

The following example imports the self certificate generated by the CA with the key pair `first_key_pair` from the file `selfcert1.cert` in the CF partition into the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#import pki certificate self rsa key-pair first_
key_pair file /flash/selfcert1.cert
```

The following example imports the trusted certificate generated by the CA from file `trustcert1.cert` in the CF partition into the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#import pki certificate trusted rsa file
/flash/selfcert1.cert
```

1.39 import pki key pair

import pki key-pair ***key-pair-name*** **file** ***file-name***

1.39.1 Command Mode

exec

1.39.2 Syntax Description

key-pair ***key-pair-name***	Unique name for the key pair; up to 39 characters.
file ***file-name***	Full path to the location of the file (in PEM format) from which the private key is to be imported.

1.39.3 Default

No key pair is imported.

1.39.4 Usage Guidelines

This command allows a private key generated on a CA to be imported into the SmartEdge router configuration.

1.39.5 Examples

The following example imports the key pair `first_key_pair` from file `key1.key` in the CF partition into the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#import pki key-pair first_key_pair file /flash/key1.key
```

1.40 in

in

no in

1.40.1 Command Mode

IPsec SA configuration

1.40.2 Syntax Description

This command has no keywords or arguments.

1.40.3 Default

None.

1.40.4 Usage Guidelines

Enters IPsec SA SPI configuration mode for configuring the SA attributes for inbound traffic. Using the **no** form of the command removes the inbound traffic configuration.

This command cannot be used with the **both** command. If the **both** command is configured, neither inbound nor outbound SA traffic attributes can be configured separately. To configure the same SA attributes for inbound and outbound traffic, see the **both** command.

1.40.5 Examples

```
[local]Redback(config-ipsec-sa)#in
```

1.41 interface (context)

`interface` *`if-name`* [**`bridge`**|**`intercontext`** *`if-type grp-num`*|**`ipsec`** [**`multibind`**]|**`loopback`**|**`multibind`** [**`lastresort`**]|**`p2p`**]

`no interface` *`if-name`*[**`bridge`**|**`intercontext`** *`if-type grp-num`*|**`ipsec`**[**`multibind`**]|**`loopback`**|**`multibind`** [**`lastresort`**]|**`p2p`**]

1.41.1 Purpose

Creates a new interface, or selects an existing one for modification, and enters interface configuration mode.

1.41.2 Command Mode

context configuration

1.41.3 Syntax Description

`if-name`	Name of the interface; an alphanumeric string with up to 127 characters.
`bridge`	Optional. Specifies that the interface is a bridged interface.
`intercontext`	Optional. Specifies that the interface is to link two or more contexts. Use an intercontext interface only for: • Intermediate System-to-Intermediate System (IS-IS) routing • Intercontext static routes • Interfacing to the default Multicast Domain Tree (MDT) group in multicast VPNs. If you provide an IP address to an intercontext interface, the netmask 255.255.255.255 is not allowed.
`if-type`	Optional. Type of intercontext interface, according to the following keywords: • **`lan`**—Specifies a point-to-multipoint (LAN) interface. • **`p2p`**—Specifies a point-to-point interface.
`grp-num`	Optional. Intercontext group number; the range of values is 1 to 1,023.

ipsec	Optional. Specifies that the interface is an IPsec interface.
loopback	Optional. Specifies that the interface is a loopback interface.
multibind	Optional. Enables the interface to have multiple circuits bound to it.
lastresort	Optional. Specifies that this multibind interface, called a last-resort interface, is used for any subscriber circuit that attempts to come up and cannot bind to any other interface.
p2p	Optional. When binding to a LAN circuit, indicates to routing protocols, such as IS-IS or Open Shortest Path First (OSPF), that the circuit should be treated as a point-to-point interface from an Interior Gateway Protocol (IGP) perspective.

1.41.4 Default

None

1.41.5 Usage Guidelines

Use the **interface** command to create a new interface, or select an existing one for modification, and enter interface configuration mode. Optionally, you can specify the interface as an intercontext interface or a loopback interface, or enable the interface to have multiple circuits bound to it.

You must bind a port or circuit to an interface (other than a bridged or loopback interface) for data to flow across the interface.

For an IPsec multibind interface, the interface is always unnumbered. Most of the operations listed for the **interface** command are not supported when you configure **interface ipsec multibind**. If a routing protocol is enabled over an IPsec multibind interface, then all tunnels bound to a multibind interface will run the same routing protocol. Static routes cannot be configured to use the IPsec multibind interface.

When there are only two routers over the LAN media, you can configure the interface as a point-to-point interface from a routing protocol perspective by using the **p2p** keyword. For more detailed information, see the Internet Draft, `draft-ietf-isis-igp-p2p-over-lan-03.txt`.

Use the **bind interface** command (in link configuration mode) to bind a port or circuit to a previously created interface in the specified context. Both the interface and the specified context must exist before you enter the **bind interface** command. If either is missing, an error message displays. For more information about this command, see the *Command List*.

Use the **bridge** command (in interface configuration mode) to associates the bridge with the interface or subscriber. For more information on this command, see the *Command List*.

Use the **no** form of this command to delete the interface.

Caution!

Risk of data loss. Deleting an interface removes all bindings to the interface. To reduce the risk, do not delete an interface, unless you are certain it is no longer needed.

Note: To enable OSPF routing on an interface, see *Configuring OSPF* .

1.41.6 Examples

The following example configures an interface, **enet1:**

```
[local]Redback(config-ctx)#interface enet1

[local]Redback(config-if)#ip address 10.1.1.1 255.255.255.0
```

The following example configures a loopback interface, **local-loopback**, for the local context:

```
[local]Redback(config-ctx)#interface local-loopback loopback

[local]Redback(config-if)#ip address 10.1.1.1/32
```

The following example configures three intercontext interfaces in three different contexts all with group **10:**

```
[local]Redback(config-config)#context isp1

[local]Redback(config-ctx)#interface isp1-lan intercontext lan 10

[local]Redback(config-if)#ip address 10.1.1.1/24

[local]Redback(config-if)#exit

[local]Redback(config-ctx)#exit

!Configure the second interface

[local]Redback(config-config)#context isp2

[local]Redback(config-ctx)#interface isp2-lan intercontext lan 10

[local]Redback(config-if)#ip address 10.1.1.2/24

[local]Redback(config-if)#exit

[local]Redback(config-ctx)#exit

!Configure the third interface

[local]Redback(config-config)#context isp3

[local]Redback(config-ctx)#interface isp3-lan intercontext lan 10

[local]Redback(config-if)#ip address 10.1.1.3/24

[local]Redback(config-if)#exit

[local]Redback(config-ctx)#exit
```

The following example deletes the **atm3** interface:

```
[local]Redback(config-ctx)#no interface atm3
```

The following example configures a last-resort interface and borrows an IP address for it from the **enet1** interface:

```
[local]Redback(config-ctx)#interfacelast multibind lastresort

[local]Redback(config-if)#ip unnumbered enet1
```

The following example configures a bridged interface and binds it to an existing bridge group, **isp1:**

```
[local]Redback(config-config)#context bridge
[local]Redback(config-ctx)#interfaceif-isp1 bridge
[local]Redback(config-if)#bridge name isp1
```

The following example configures an IPsec multibind interface:

```
[local]ipsec-se1(config)#context ctx-1
[local]ipsec-se1(config-ctx)#interface ipsec_mb_se_1 ipsec multibind
```

1.42 ip-comp

ip-comp

no ip-comp

1.42.1 Command Mode

IPsec proposal configuration

IPsec security association configuration

1.42.2 Syntax Description

This command has no keywords or arguments.

1.42.3 Default

Disabled

1.42.4 Usage Guidelines

Enables IP compression using the IP Compression (IPComp) protocol. Using the **no** form of the command disables IP compression.

1.42.5 Examples

```
[local]Redback(config-ipsec-proposal)#ip-comp
```

1.43 ip route traffic-selector-guided

ip route traffic-selector-guided [**cost** *route cost* |**distance** *route distance*]

no ip route traffic-selector-guided [**cost** *route cost*|**distance** *route distance*]

1.43.1 Command Mode

tunnel configuration

1.43.2 Syntax Description

cost*route cost*	Optional. The cost of reaching a destination router. User-defined numeric value. The default is 255.
distance *route distance*	Optional. The value used to rank the routes between the source and destination routers. User-defined numeric value. The default is 0.

1.43.3 Default

Traffic selectors

1.43.4 Usage Guidelines

Enables traffic-selector guided route addition in a static or on-demand auto key IPsec tunnel configuration. Traffic-selector guided route addition uses the traffic selectors negotiated as part of the IKE negotiations used to establish the IPsec SAs to add routes from the local endpoint to the network protected by the remote peer. The command accepts cost and distance associated with a router, as parameters. The IPSec routes are redistributed using the following protocols:

- BGP

  For more information on IPSec redistribution, refer section redistribute (BGP, IPv4) in Commands: r, Reference [4].

- IS-IS

  For more information on IPSec redistribution, refer section redistribute (IS-IS, IPv4) in Commands: r, Reference [4].

- OSPF

For more information on IPSec redistribution, refer section redistribute (OSPF) in Commands: r, Reference [4].

- RIP

  For more information on IPSec redistribution, refer section redistribute (RIP) in Commands: r, Reference [4].

Traffic selectors specify the IP address, protocol, or ports secured by each IPsec SA, and exist in pairs: source traffic selector and destination traffic selector. When enabled, traffic-selector guided route addition automatically adds and deletes IP routes dynamically that point to the IPsec tunnel as the tunnel comes up or goes down. If it is not enabled, you must explicitly add static IP routes to point to the IPsec tunnel or run dynamic routing protocols over the tunnel. Using the **no** form of the command disables traffic-selector guided route addition.

1.43.5 Examples

The following example enables traffic-selector guided route addition in the static or on-demand auto key IPsec tunnel configuration currently being configured.

```
[local]Redback(config-tunnel)#ip route traffic-selector-g
uided distance 50 cost 105
```

1.44 ipsec access-list

ipsec access-list ***ipsec-acl-name***

no ipsec access-list ***ipsec-acl-name***

1.44.1 Command Mode

context configuration

1.44.2 Syntax Description

ipsec-acl-name	Name of an IPsec access list, which must be unique; up to 39 characters

1.44.3 Default

No IPsec access list is configured.

1.44.4 Usage Guidelines

Creates (with default attributes) or selects an IPsec access list and enters IPsec ACL configuration mode. Using the **no** form of the command will remove an existing configuration.

1.44.5 Examples

```
[local]Redback(config-ctx)#ipsec access-list ipsec_ACL1
```

1.45 ipsec alarms holddown

ipsec alarms holddown *seconds*

no ipsec alarms holddown *seconds*

1.45.1 Command Mode

global configuration

1.45.2 Syntax Description

seconds	Number of seconds before tunnel alarms are generated; from 0 to 120 seconds.

1.45.3 Default

30 seconds.

1.45.4 Usage Guidelines

Sets the delay between when the tunnnel state changes and the tunnel state alarm is generated. Does not apply to tunnel status change alarm triggered by DPD failure.

1.45.5 Example

```
[local]Redback(config)#ipsec alarms holddown 60
```

1.46 ipsec policy

ipsec policy *ipsec-policy-name*

```
no ipsec policy ipsec-policy-name
```

1.46.1 Command Mode

global configuration

1.46.2 Syntax Description

ipsec-policy-name	Name of an IPsec policy, which must be unique; up to 39characters.

1.46.3 Default

No IPsec policy is configured.

1.46.4 Usage Guidelines

Creates (with default attributes) or selects an IPsec policy and enters IPsec policy configuration mode. Using the **no** form of the command will remove an existing configuration.

1.46.5 Examples

```
[local]Redback(context)#ipsec policy ipsec_Pol1
```

1.47 ipsec profile

```
ipsec profile profile-name
```

```
no ipsec profile profile-name
```

1.47.1 Command Mode

context configuration

1.47.2 Syntax Description

profile-name	Name of the IPsec profile. Must match the name of the on-demand IPsec tunnel created with the **tunnel ipsec** ***name*** **on-demand** command in global configuration mode.

1.47.3 Default

None.

1.47.4 Usage Guidelines

Creates an IPsec profile, which specifies how traffic in the on-demand IPsec tunnel should be handled. The IPsec profile must be created in the same context as the multibind interface to which the on-demand IPsec tunnel is bound.

1.47.5 Examples

```
[local]Redback(config)#context ctx-1
[local]Redback(config-ctx)#ipsec profile profile_se_1
[local]Redback(cfg-ipsec-profile)#
```

1.48 ipsec proposal

ipsec proposal ***ipsec-proposal-name***

no ipsec proposal ***ipsec-proposal-name***

1.48.1 Command Mode

global configuration

1.48.2 Syntax Description

ipsec-proposal-name	Name of the IPsec proposal, which must be unique; up to 39 characters.

1.48.3 Default

No IPsec proposal configuration.

1.48.4 Usage Guidelines

Creates (with default attributes) or selects an IPsec proposal and enters IPsec proposal configuration mode. Using the **no** form of the command will remove an existing configuration.

1.48.5 Examples

```
[local]Redback(context)#ipsec proposal ipsec_Prop1
```

1.49 ipsec qos policy pq

ipsec qos policy ***name*** **pq**

no ipsec qos policy ***name*** **pq**

1.49.1 Command Mode

global configuration

1.49.2 Syntax Description

This command has no keywords or arguments.

ipsec qos policy ***name***	Unique name of the IPsec QoS policy

1.49.3 Default

No IPsec Quality of Service (QoS) policies are configured.

1.49.4 Usage Guidelines

This command configures an IPsec QoS policy for priority queuing and enters IPsec QoS policy configuration mode. Using the **no** form of the command removes the IPsec QoS policy

1.49.5 Examples

```
[local]Redback(config)#ipsec qos policy ipsec-qos-pq-3 pq
```

1.50 ipsec security-association

ipsec security-association ***sa-name***

no ipsec security-association ***sa-name***

1.50.1 Command Mode

global configuration

1.50.2 Syntax Description

sa-name	Name of an IPsec security association, which must be unique; up to 39 characters.

1.50.3 Default

No IPsec security association configuration.

1.50.4 Usage Guidelines

Creates or selects an IPsec security association and enters IPsec security association configuration mode. Using the **no** form of the command will remove an existing configuration.

1.50.5 Examples

```
[local]Redback(context)#ipsec security-association ipsec_sa_1
```

1.51 lifetime seconds

lifetime seconds ***seconds***

no lifetime seconds

1.51.1 Command Mode

IKE2 policy configuration

IKE proposal configuration

IPsec proposal configuration

1.51.2 Syntax Description

seconds	300 to 99999999

1.51.3 Default

86400 (one day)

1.51.4 Usage Guidelines

Specifies the lifetime for IKE SAs in seconds for an IKEv2 policy, IKE proposal or IPsec proposal. Specify 0 seconds for no timeout; any number of seconds from 1 to 299 is rejected. Using the **no** form of the command resets the configuration to the default.

1.51.5 Examples

```
[local]Redback(config-ike-proposal)#lifetime seconds 43200
```

1.52 lifetime kbytes

lifetime kbytes ***kbytes***

no lifetime

1.52.1 Command Mode

IPsec proposal configuration

1.52.2 Syntax Description

kbytes	128 to 2147483647

1.52.3 Default

0 kbytes

1.52.4 Usage Guidelines

Specifies the lifetime for IPsec SAs in kbytes for an IPsec proposal. Specify 0 kbytes for no timeout. The lifetime is expected to be tied to the strength of the encryption and authentication algorithms configured. Using the **no** form of the command resets the configuration to the default.

1.52.5 Examples

```
[local]Redback(config-ipsec-proposal)#lifetime kbytes 256
```

1.53 max-tunnels

max-tunnels ***value***

no max-tunnels

1.53.1 Command Mode

tunnel configuration

1.53.2 Syntax Description

value	Maximum number of tunnels per IPsec profile for the on-demand IPsec tunnel being configured. 1 to 1024.

1.53.3 Default

8 tunnels per IPsec profile

1.53.4 Usage Guidelines

Specifies the maximum number of tunnels per profile in this on-demand tunnel.

1.53.5 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#max-tunnels 50
```

1.54 mode

mode {**main**|**aggressive**}

no mode

1.54.1 Command Mode

IKE policy configuration

1.54.2 Syntax Description

`main`	The slower, but more secure, negotiation mode. Six messages are exchanged. Endpoint IDs are exchanged after a secure channel has been set up.
`aggressive`	The faster, but less secure, negotiation mode. Only three messages are exchanged; however, because endpoint IDs are exchanged in clear text, it is less secure.

1.54.3 Default

main

1.54.4 Usage Guidelines

Specifies the negotiation mode to use for key exchanges. The IKE policy can accept multiple IKE proposals in main mode regardless of connection type, and in aggressive mode only if the connection type is set to responder-only. The **no** form of the command resets the mode to the default.

1.54.5 Examples

The following example shows how to set the mode for key exchange to aggressive.

```
[local]Redback(config-ike-policy)#mode aggressive
```

1.55 mtu

mtu ***size***

no mtu

1.55.1 Command Mode

IPsec profile configuration

tunnel configuration

1.55.2 Syntax Description

size	MTU size in bytes. Range: 256 to 16,384.

1.55.3 Default

Maximum Transmission Unit (MTU) size for the interface to which the IPsec tunnel is bound

1.55.4 Usage Guidelines

Sets the MTU for packets sent into an IPsec tunnel. The MTU is used by the ASP for pre-encryption fragmentation. The MTU for a manual key IPsec tunnel or a static auto key IPsec tunnel is set in tunnel configuration mode when the IPsec tunnel is configured; for an on-demand IPsec tunnel it is set in IPsec profile configuration mode when the IPsec profile associated with the tunnel is configured. If a packet exceeds the MTU, the ASP fragments that packet.

A tunnel uses the MTU for the interface to which you have bound it (using the bind interface command in tunnel configuration mode), unless you explicitly configure the MTU using this command. After you configure an MTU for the tunnel, the system determines the effective MTU by comparing the configured MTU with the interface MTU and selecting the lesser of the two values.

Post-encryption fragmentation can also occur on the outgoing line card based on the MTU of the outgoing interface.

Use the **no** form of this command to set the MTU to the default value.

1.55.5 Examples

The following example shows how to specify the MTU in an IPsec profile for an on-demand IPsec tunnel:

```
[local]Redback(config-ctx)#ipsec profile profile_se_1
[local]Redback(cfg-ipsec-profile)#mtu 256
```

The following example shows how to specify the MTU in an IPsec tunnel for a static auto key IPsec tunnel:

```
[local]Redback(config)#tunnel ipsec ipsec-tun-1
[local]Redback(config-tunnel)#mtu 256
```

1.56 num-queues

num-queues ***num***

no num-queues

1.56.1 Command Mode

IPsec QoS policy for priority queuing configuration

1.56.2 Syntax Description

num-queues *num*	The number of priority queues to instantiate in each SA when a tunnel becomes operational.

1.56.3 Default

By default no priority queues are instantiated.

1.56.4 Usage Guidelines

This command configures the number of priority queues to instantiate for each SA when a tunnel becomes operational. Using the **no** form of the command removes the configuration. When the number of queues is not specified, all data traffic is processed by a single queue.

1.56.5 Examples

The following example shows the number of queues set to 3 for the IPsec QoS policy for priority queuing `ipsec-qos-pq-3`.

```
[local]Redback(config)#ipsec qos policy ipsec-qos-pq-3 pq
[local]Redback(config-ipsec-policy-pq)#num-queues 3
```

1.57 out

out

no out

1.57.1 Command Mode

IPsec SA configuration

1.57.2 Syntax Description

This command has no keywords or arguments.

1.57.3 Default

No SA values for traffic are configured.

1.57.4 Usage Guidelines

Enters IPsec SA SPI configuration mode for configuring the SA attributes for outbound traffic. Using the **no** form of the command removes the outbound traffic configuration.

This command cannot be used with the **both** command. If the **both** command is configured, neither inbound nor outbound SA traffic attributes can be configured separately. To configure the same SA attributes for inbound and outbound traffic, see the **both** command.

1.57.5 Examples

```
[local]Redback(config-ipsec-sa)#out
```

1.58 peer-end-point

peer-end-point local ***loc-ip-addr*** [**remote** ***rem-ip-addr***] [**context** ***ctx-name***]

no peer-end-point

1.58.1 Command Mode

tunnel configuration

1.58.2 Syntax Description

local ***loc-ip-addr***	IP address of the local end of the tunnel. The format is ***A.B.C.D***.
remote ***rem-ip-addr***	Optional. IP address of the remote end of the tunnel. Required except when you have created an overlay tunnel for which you have specified that the system assign the remote IP address. The format is ***A.B.C.D***.
context ***ctx-name***	Optional. Name of the context that contains the interface to the local end of the tunnel. If no context is specified, the interface to the local end of the tunnel is assumed to be in the **local** context.

1.58.3 Default

None

1.58.4 Usage Guidelines

Use the **peer-end-point** command to assign IP addresses to the tunnel endpoints. This command creates the tunnel between the two endpoints.

Note: IP-in-IP and overlay tunnels support a single tunnel circuit in each tunnel; GRE tunnels can support multiple tunnel circuits with the use of keys. For information about GRE tunnel circuits, see *Configuring GRE Tunnels*.

The remote IP address at one end of the tunnel is the same as the local IP address at the other end of the tunnel. If the remote IP address is not adjacent to the local IP address, and the remote site cannot be reached with a routing protocol, you must also enter the **ip route** command in context configuration mode.

If you create an overlay tunnel using the **tunnel** command with the **ipv6v4-auto** keyword, the system assigns an IP address to the remote endpoint. In this case, you do not include the **remote** ***rem-ip-addr*** construct when you enter this command.

The **local** ***loc-ip-addr*** construct must match the IP address of an interface.

If you are creating more than one tunnel, you can use the same IP address for the local endpoint (the IP address assigned to the interface) as long as the remote IP addresses are all different.

To use an interface and its local IP address for more than one tunnel, you must specify the **loopback** keyword with the **interface** command (in context configuration mode) when you create the interface for the tunnels. The **loopback** keyword allows you to reuse the IP address for more than one tunnel.

Use the **no** form of this command to delete this tunnel and any associated parameters that have been specified in tunnel configuration mode. The keywords are not available for the **no** form of this command.

1.58.5 Examples

The following example shows how to create an interface, **toDenver**, with a public IP address of **172.16.1.1**; then it creates an overlay tunnel, **DenverTnl**, with a remote IP address of **172.16.1.2** and a local IP address of **172.16.1.1:**

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface toDenver
[local]Redback(config-if)#ip address 172.16.1.1/30
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#tunnel ipv6v4-manual DenverTnl
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.16.1.2
```

The following example shows how to create two overlay tunnels each using an interface, **LocalEnd**. Both tunnels use the same local IP address; it is assumed that the remote IP address for **Tun2** can be reached with a routing protocol, so the **ip route** command in context configuration mode is not needed:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface LocalEnd loopback
[local]Redback(config-if)#ip address 172.16.1.1/32
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#tunnel Tunl
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.16.1.2
[local]Redback(config-tunnel)#no shutdown
[local]Redback(config-tunnel)#exit
[local]Redback(config-ctx)#tunnel Tun2
[local]Redback(config-tunnel)#peer-end-point local 172.16.1.1 remote 172.20.1.2
[local]Redback(config-tunnel-peer)#no shutdown
[local]Redback(config-tunnel-peer)#end
```

1.59 perfect-forward-secrecy dh-group

perfect-forward-secrecy dh-group ***dh-group***

no perfect-forward-secrecy dh-group

1.59.1 Command Mode

IPsec policy configuration

1.59.2 Syntax Description

dh-group	1, 2, or 5

1.59.3 Default

No DH group is configured.

1.59.4 Usage Guidelines

This command configures the Diffie-Hellman group for Perfect Forward Secrecy (PFS) in an IPsec policy. Using the **no** form of the command resets the configuration to the default.

1.59.5 Examples

```
[local]Redback(config-ipsec-policy)#perfect-forward-secrecy dh-group 5
```

1.60 pki alarms certificate

pki alarms certificate {**self** |**trusted**} {**expiry** ***days*** | **missing**}

no pki alarms certificate {**self** |**trusted**} {**expiry** | **missing**}

1.60.1 Command Mode

global configuration

1.60.2 Syntax Description

self	Specifies the certificate type as RSA self-certificate.
trusted	Specifies the certificate type as RSA trusted-certificate.
expiry ***days***	Sets the alarm warning period in days. The alarm is triggered a certain number of days before the certificate is due to expire. Range 1 to 30. Default setting is 7 days.
missing	Sends the alarm when there are no valid certificates of the specified certificate type found in a context.

1.60.3 Default

By default, no certificate expiration warning is generated.

By default, no certificate missing alarm is generated.

1.60.4 Usage Guidelines

When the **expiry** keyword is used, this command generates an RSA certificate expiry warning alarm. The alarm is triggered in a configurable number of days before the expiration date of the RSA certifcate. When the **missing** keyword is used, this command generates an alarm when there are no valid certificates of the specified certificate type found in a context.

1.60.5 Example

```
[local]Redback(config)#pki alarms certificate self expiry 5
[local]Redback(config)#pki alarms certificate trusted missing
```

1.61 pre-shared-key

pre-shared-key {**hex** ***hex-value***|***ASCII-value***|**use-aaa**}

no pre-shared-key

1.61.1 Command Mode

IKE policy configuration

IKEv2 policy configuration

1.61.2 Syntax Description

hex ***hex-value***	Hexadecimal number (24 to 98 characters).
ASCII-value	ASCII value (12 to 49 characters).
use-aaa	Specifies that the pre-shared key is configured on the AAA server. The format expected by the node is: **ike pre-shared-key {hex** ***hex-value***|***ASCII-value*****}** Applies only to on-demand IPsec tunnels. Can only be specified for an IKE policy configured to use aggressive mode for key exchange.

1.61.3 Default

No pre-shared key is configured.

1.61.4 Usage Guidelines

Specifies the local pre-shared key in an IKE policy. Using the **no** form of the command will remove the configuration.

1.61.5 Examples

```
[local]Redback(config-ike-policy)#pre-shared-key 0x4d79
486578506135357730726 4
```

1.62 pseudo-random-function

pseudo-random-function [**hmac-md5**|**hmac-sha1**|**aes-128-xcbc**]

no pseudo-random-function

1.62.1 Command Mode

IKEv2 proposal configuration

1.62.2 Syntax Description

hmac-md5	hmac-md5 algorithm
hmac-sha1	hmac-sha1 algorithm
aes-i28-xcbc	aes-128-xcbc algorithm

1.62.3 Default

hmac-sha1

1.62.4 Usage Guidelines

This command configures the prf algorithm for an IKEcv2 proposal. Using the **no** form of the command removes the pseudo random function configuration.

1.62.5 Examples

```
[local]Redback(context)#pseudo-random-function aes-128-xcbc
```

1.63 qos policy queuing

qos policy queuing ***policy-name***

```
no qos policy queuing policy-name
```

1.63.1 Command Mode

tunnel configuration

1.63.2 Syntax Description

`qos policy queuing` *`name`*	Unique name of the IPsec QoS policy for priority queuing associated with the tunnel

1.63.3 Default

No IPsec QoS policy is specified for the tunnel.

1.63.4 Usage Guidelines

This command configures the IPsec QoS policy for priority queuing used by the tunnel. Using the **`no`** form of the command removes the IPsec QoS policy for priority queuing from the tunnel configuration.

1.63.5 Examples

The following example configures the IPsec QoS policy for priority queuing `ipsec-qos-pq-3` for use with the tunnel currently being configured.

```
[local]Redback(config-tunnel)#qos policy queuing ipsec-qos-pq-3
```

1.64 remote-id

```
remote-id remote_id
```

1.64.1 Command Mode

tunnel configuration

1.64.2 Syntax Description

`remote_id`	IP address or FQDN.

1.64.3 Default

No remote ID is specified for an IPsec tunnel.

1.64.4 Usage Guidelines

Specifies the identity of the remote IPsec tunnel endpoint. This value is used when negotiating IKE requests with a remote peer. When IKE sessions are negotiated, the remote ID in the IPsec tunnel endpoint configured on one peer must match the local identity configured in the IKE policy on the other peer.

1.64.5 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#remote-id 72.0.0.1
```

1.65 remove pki

remove pki {all|certificate handle *handle*|certificate request *request-name*|key-pair *key-pair-name*|unused}

1.65.1 Command Mode

exec

1.65.2 Syntax Description

certificate handle *handle*

certificate request *request-name*

key-pair *key-pair-name* Unique name for the key pair; up to 39 characters.

1.65.3 Default

No PKI object is removed from the configuration.

1.65.4 Usage Guidelines

This command removes specified PKI objects from the configuration. The **all** keyword removes all PKI objects. The **certificate handle** keyword removes the certificate specified by the handle value. The **certificate request** keyword removes the specified certificate request. The **key pair** keyword removes the specified key pair. The **unused** keyword removes unused PKI objects.

1.65.5 Examples

The following example removes the key pair `first_key_pair` from the context `vpn1`.

```
[local]Redback#context vpn1
[vpn1]Redback#remove pki key-pair first_key_pair
```

1.66 seq (IPsec)

seq *sequence-number* [*protocol*] {*source-network-prefix*/*source-prefix-length*|**any** } {**eq** *source-port* } [*dest-network-prefix*/*dest-prefix-length*|**any**] [**eq** *dest-port*]

no seq *sequence-number*

1.66.1 Command Mode

IPsec ACL configuration

IPsec profile configuration

1.66.2 Syntax Description

sequence-number	Sequence number for the statement. Range: 1 to 429496729.
protocol	Optional. Number indicating a protocol as specified in RFC 1700, *Assigned Numbers*. Range: 0 to 255or one of the keywords listed in Table 4.
source-network-prefix	Source IP address to be included in the criteria.
source-prefix-length	Number of prefix bits for the source IP address. Range: 0 to 32.
dest-network-prefix	Optional. Destination IP address to be included in the criteria.
dest-prefix-length	Optional. Number of prefix bits for the destination IP address. Range: 0 to 32.

`any`	Optional. Indicates that IP traffic from all IP addresses is to be included in the criteria. Used instead of specifying the *`network-prefix`* and *`prefix-length`*.
`eq`	Optional. Specifies that values must be equal to those specified by the *`source-port`* or *`dest-port`* argument.
`source-port`	Optional. Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port. This argument is available only if you specify TCP or UDP as the protocol. Range: 1 to 65535 or one of the keywords listed in Table 5 and Table 6.
`dest-port`	Optional. TCP or UDP destination port. This argument is available only if you specify TCP or UDP as the protocol. Range: 1 to 65535 or one of the keywords listed in Table 5 and Table 6.

1.66.3 Default

No ACLs are configured.

1.66.4 Usage Guidelines

Creates an ACL rule to allow packets that meet the specified criteria. Up to 32 rules can be specified in an IPsec ACL.

Note: There is an implicit **`deny any any`** statement at the end of every ACL.

Table 4 lists the valid keyword substitutions for the *`protocol`* argument.

Table 4 Valid Keyword Substitutions for the protocol Argument

Keyword	Definition
`ah`	Authentication Header
`esp`	Encapsulation Security Payload
`gre`	Generic Routing Encapsulation (GRE)
`host`	Host source address
`icmp`	Internet Control Message Protocol (ICMP)
`igmp`	Internet Group Management Protocol (IGMP)
`ip`	Internet Protocol v4
`ipinip`	IP-in-IP tunneling

Keyword	Definition
`ospf`	Open Shortest Path First (OSPF)
`pcp`	Payload Compression Protocol (PCP)
`pim`	Protocol Independent Multicast (PIM)
`tcp`	Transmission Control Protocol (TCP)
`udp`	User Datagram Protocol (UDP)

Table 5 lists the valid keyword substitutions for the ***source-port*** and ***dest-port*** argument when they are used to specify a TCP port.

Table 5 Valid Keyword Substitutions for the source-port and dest-port Arguments (TCP Port)

Keyword	Definition	Corresponding Port Number
`bgp`	Border Gateway Protocol (BGP)	179
`chargen`	Character generator	19
`cmd`	Remote commands (rcmd)	514
`daytime`	Daytime	13
`discard`	Discard	9
`domain`	Domain Name System (DNS)	53
`echo`	Echo	7
`exec`	Exec (rsh)	512
`finger`	Finger	79
`ftp`	File Transfer Protocol (FTP)	21
`ftp-data`	FTP data connections (used infrequently)	20
`gopher`	Gopher	70
`hostname`	Network Interface Card (NIC) hostname server	101
`ident`	Identification protocol	113
`irc`	Internet Relay Chat	194
`klogin`	Kerberos login	543
`kshell`	Kerberos Shell	544
`login`	Login (rlogin)	513
`lpd`	Printer service	515
`nntp`	Network News Transport Protocol (NNTP)	119

Table 5 Valid Keyword Substitutions for the source-port and dest-port Arguments (TCP Port)

Keyword	Definition	Corresponding Port Number
`pim-auto-rp`	Protocol Independent Multicast Auto-RP	496
`pop2`	Post Office Protocol Version 2 (POP2)	109
`pop3`	Post Office Protocol Version 3 (POP3)	110
`shell`	Remote command shell	514
`smtp`	Simple Mail Transport Protocol (SMTP)	25
`ssh`	Secure Shell (SSH)	22
`sunrpc`	Sun Remote Procedure Call	111
`syslog`	System logger	514
`tacacs`	Terminal Access Controller Access Control System (TACACS)	49
`talk`	talk	517
`telnet`	Telnet	23
`time`	Time	37
`uucp`	UNIX-to-UNIX Copy Program	540
`whois`	Nickname	43
`www`	World Wide Web (HTTP)	80

Table 6 lists the valid keyword substitutions for the *`source-port`* and *`dest-port`* arguments when they are used to specify a UDP port.

Table 6 Valid Keyword Substitutions for the source-port and dest-port Arguments (UDP Port)

Keyword	Definition	Corresponding Port Number
`biff`	Biff (Mail Notification, Comsat)	512
`bootpc`	Bootstrap Protocol client	68
`bootps`	Bootstrap Protocol server	67
`discard`	Discard	9
`dnsix`	DNSIX Security Protocol Auditing	195
`domain`	Domain Name System (DNS)	53
`echo`	Echo	7

Table 6 Valid Keyword Substitutions for the source-port and dest-port Arguments (UDP Port)

Keyword	Definition	Corresponding Port Number
isakmp	Internet Security Association and Key Management Protocol (ISAKMP)	500
mobile-ip	Mobile IP Registration	434
nameserver	IEN116 Name Service (obsolete)	42
netbios-dgm	NetBIOS Datagram Service	138
netbios-ns	NetBIOS Name Service	137
netbios-ss	NetBIOS Session Service	139
ntp	Network Time Protocol (NTP)	123
pim-auto-rp	Protocol Independent Multicast Auto-RP	496
rip	Router Information Protocol (RIP)	520
snmp	Simple Network Management Protocol (SNMP)	161
snmptrap	SNMP Traps	162
sunrpc	Sun Remote Procedure Call	111
syslog	System logger	514
tacacs	Terminal Access Controller Access Control System	49
talk	Talk	517
tfpt	Trivial File Transfer Protocol (TFPT)	69
time	Time	37
who	Who Service (rwho)	513
xdmcp	X Display Manager Control Protocol	177

1.66.5 Examples

```
[local]Redback(config-ipsec-acl)#seq 10 tcp 1.1.1.0/24 eq 20000
[local]Redback(config-ipsec-acl)#seq 20 1.1.1.0/24 2.2.2.0/24
[local]Redback(config-ipsec-acl)#seq 30 any any
```

1.67 seq ipsec-policy

seq *id* **ipsec-policy** *ipsec-pol-name* [**access-group** *ipsec-acl-name*]

no seq *id* **ipsec-policy** *ipsec-policy-name* [**access-group** *ipsec-acl-name*

1.67.1 Command Mode

tunnel configuration

IPsec profile configuration

1.67.2 Syntax Description

id	Sequence number for the statement. Range: 1 to 429496729.You can configure up to eight sequenced entries for each tunnel.
ipsec-policy *ipsec-policy-name*	Name of a previously created IPsec policy.
access-group *ipsec-acl-name*	Optional. Name of a previously created IPsec ACL.

1.67.3 Default

No IPsec policies are configured for a IPsec tunnel using IKE.

1.67.4 Usage Guidelines

This command applies only to IPsec tunnels using IKE. It specifies up to eight sequenced IPsec policies, each optionally with an IPsec ACL. When no IPsec ACL is specified, a wildcard selector is added by default. Using the **no** form of the command will remove the configuration.

1.67.5 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#seq 10 ipsec-policy ipsec_Pol1 access-group ipsec_ACL1
[local]Redback(config-tunnel)#seq 20 ipsec-policy ipsec_Pol2 access-group ipsec_ACL2
```

1.68 seq proposal

seq *sequence-number* **proposal** *ike-proposal-name*

1.68.1 Command Mode

IKE policy configuration

IKEv2 policy configuration

IPsec policy configuration

1.68.2 Syntax Description

`sequence-number`	1 to 429496729.
`proposal` *`ike-proposal-name`*	Name of a previously created IKE proposal (in IKE policy or IKEv2 policy configuration mode) or IPsec policy proposal (in IPsec policy configuration mode).

1.68.3 Default

No IKE proposals are configured for an IKE policy. No IPsec proposals are configured for an IPsec policy.

1.68.4 Usage Guidelines

When configuring an IKE policy, specifies the IKE proposals used by the IKE policy. When configuring an IPsec policy, specifies the IPsec proposals used by the IPsec policy. Up to 16 sequenced proposals can be specified for each policy. Using the **`no`** form of the command will remove the configuration.

1.68.5 Examples

The following example shows how to add a reference to the **`IKE_Prop1`** IKE proposal to the IKE policy:

```
[local]Redback(config-ike-policy)#seq 10 IKE_Prop1
```

The following example shows how to add a reference to the **`IPsec_Prop1`** IPsec proposal to the IPsec policy:

```
[local]Redback(config-ipsec-policy)#seq 10 IPsec_Prop1
```

1.69 seq security-association

`seq` *`id`* **`security-association`** *`sa-name`* [**`access-group`** *`ipsec-acl-name`*]

no seq *id* **security-association** *sa-name* [**access-group** *ipsec-acl-name*]

1.69.1 Command Mode

tunnel configuration

1.69.2 Syntax Description

id	Sequence number for the statement. Range: 1 to 429496729.You can configure up to 8 sequenced entries per tunnel.
security-association *sa-name*	Name of a previously created IPsec SA.
access-group *ipsec-acl-name*	Name of a previously created IPsec ACL.

1.69.3 Default

No security associations with manual keys are configured for a manual mode IPsec tunnel.

1.69.4 Usage Guidelines

This command applies only to manual mode IPsec tunnels. It specifies up to eight sequenced manual-keyed SAs, each optionally with an IPsec ACL, for a manual mode IPsec tunnel. When no IPsec ACL is specified, a wildcard selector is added by default. Using the **no** form of the command will remove the configuration.

1.69.5 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
[local]Redback(config-tunnel)#seq 10 security association ipsec_sa_1 access-group ipsec_ACL1
[local]Redback(config-tunnel)#seq 20 security association ipsec_sa_2 access-group ipsec_ACL2
```

1.70 show configuration ike

show configuration ike [**all-contexts**] [**verbose**]

1.70.1 Command Mode

all modes

1.70.2 Syntax Description

all-contexts Optional. Displays the configuration for IKE in all contexts.

verbose Optional. Displays all defaulted parameters.

1.70.3 Usage Guidelines

Displays configuration information for IKE in the current context, or all contexts if the optional **all-contexts** keyword is specified. The optional **verbose** keyword list all defaulted parameters.

1.70.4 Examples

```
[local]Redback#show configuration ike
Building configuration...

Current configuration:

context local
!
! ** End Context **
ike proposal ikeProp1
 authentication algorithm hmac-sha1-96
 encryption algorithm des-cbc
 dh-group 1
 lifetime seconds 3600
!
ike proposal simple-ike-proposal
 authentication algorithm hmac-sha1-96
 encryption algorithm des-cbc
 dh-group 1
 lifetime seconds 3600
!
!
end
```

1.71 show configuration ipsec

show configuration ipsec [**all-contexts**] [**verbose**]

1.71.1 Command Mode

all modes

1.71.2 Syntax Description

all-contexts	Optional. Displays the configuration for IKE in all contexts.
verbose	Optional. Displays all defaulted parameters.

1.71.3 Usage Guidelines

Displays configuration information for IPsec in the current context, or all contexts if the optional **all-contexts** keyword is specified. The optional **verbose** keyword list all defaulted parameters.

1.71.4 Examples

```
[local]subzero#show configuration ipsec
Building configuration...

Current configuration:

context local
!
! ** End Context **
ipsec proposal ipsecProp1
 esp encryption des-cbc
 esp authentication hmac-sha1-96
 ip-comp
 lifetime seconds 1800
!
ipsec proposal simple-ipsec-proposal
 esp encryption des-cbc
 esp authentication hmac-sha1-96
 ip-comp
 lifetime seconds 1800
!
ipsec policy ipsecPol1
 anti-replay-window 64
 seq 1 proposal ipsecProp1
!
ipsec policy simple-ipsec-policy
 anti-replay-window 64
 seq 1 proposal simple-ipsec-proposal
!
!
end
```

1.72 show configuration tunnel

show configuration tunnel [**all-contexts**] [**verbose**]

1.72.1 Command Mode

all modes

1.72.2 Syntax Description

all-contexts	Optional. Displays the configuration for IKE in all contexts.
verbose	Optional. Displays all defaulted parameters.

1.72.3 Usage Guidelines

Displays configuration information for tunnels in the current context, or all contexts if the optional **all-contexts** keyword is specified. The optional **verbose** keyword list all defaulted parameters.

1.72.4 Examples

```
[local]Redback#show configuration tunnel
Building configuration...

Current configuration:

context local
!
! ** End Context **
tunnel ipsec rec_1_2_m manual
 peer-end-point local 1.1.1.1 remote 2.1.1.1 context vpn1
 bind interface tunnel_ipsec_1 vpn1
 seq 10 security-association sa1_2 access-group acl1_2
!
!
end
```

1.73 show ike policy

show ike [**card** ***slot-id/asp-id***] [**policy** ***policy-name***

1.73.1 Command Mode

all modes

1.73.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. The range of values depends on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

policy ***policy-name***

Optional. Name of a previously created IKE policy.

1.73.3 Usage Guidelines

Displays configuration information for IKE policies in the current context. If no IKE policy is specified, one line of configuration information for each IKE policy with the name, local ID, and mode is displayed. If an IKE policy is specified, all attributes, including defaults, are displayed for the specified policy. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.73.4 Examples

```
[local]Redback#show ike policy
Name                  Local-ID        Mode
ike-policy1           1.1.1.1         aggressive
```

```
[local]Redback#show ike policy ike-policy1
IKE Policy:       ike-policy1
Description:      IKE policy for aggressive mode
Mode:             aggressive
Connection Type:  both
Local Identity:   1.1.1.1
Remote Identity:  2.2.2.2   3.3.3.3   4.4.4.4   5.5.5.5
Pre-shared Key:   0x12345678910123456789 0
// For the administrators
Pre-shared Key:   **********
// For the operators
seq 10  proposal IKE-Prop1
seq 20  proposal IKE-Prop2
```

1.74 show ike proposal

show ike [**card** ***slot-id*****/*****asp-id***] [**proposal** ***proposal-name***]

1.74.1 Command Mode

all modes

1.74.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

proposal ***proposal-name***

Optional. Name of a previously created IKE proposal.

1.74.3 Usage Guidelines

Displays configuration information for IKE proposals. If no IKE proposal is specified, one line of configuration information for each IKE proposal with the name, encryption algorithm, authentication algorithm, and Diffie-Hellman group is displayed. If an IKE proposal is specified, all attributes, including defaults, are displayed for the specified proposal. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.74.4 Examples

```
[local]Redback#show ike proposal
               Encryption    Authentication   DH-Group
IKE-Prop1      des-cbc       hmac-md5-96      1
IKE-Prop2      3des-cbc      hmac-sha1-96     2


[local]Redback#show ike card 2/1 proposal IKE-Prop1
IKE Proposal     : IKE-Prop11
Encryption Algorithm          : 3des-cbc
Authentication Algorithm      : hmac-md5-96
DH Group                      : 1
Lifetime                      : 86400 seconds
```

1.75 show ike statistics global

show ike [**card** ***slot-id/asp-id***] **statistics global** {**ike1**|**ike2**}

1.75.1 Command Mode

all modes

1.75.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

ike1|**ike2**

Specify either IKEv1 or IKE v2 protocol counters be shown.

1.75.3 Usage Guidelines

Displays ASP level IKE statistics. You must specify whether you want to show either IKEv1 or IKEv2 protocol counters.

1.75.4 Examples

```
[local]Redback#show card 2/1 statistics global ike1
# Main Mode 1st messages sent                         : 28
# Main Mode 1st messages received                     : 27
# Main Mode 2nd messages sent                         : 27
# Main Mode 2nd messages received                     : 27
# Main Mode 3rd messages sent                         : 27
# Main Mode 3rd messages received                     : 27
# Main Mode 4th messages sent                         : 27
# Main Mode 4th messages received                     : 27
# Main Mode 5th messages sent                         : 27
# Main Mode 5th messages received                     : 27
# Main Mode 6th messages sent                         : 27
# Main Mode 6th messages received                     : 27
# Aggressive Mode 1st messages sent                   : 0
# Aggressive Mode 1st messages received               : 0
# Aggressive Mode 2nd messages sent                   : 0
# Aggressive Mode 2nd messages received               : 0
# Aggressive Mode 3rd messages sent                   : 0
# Aggressive Mode 3rd messages received               : 0
# Xauth request messages sent                         : 0
# Xauth request messages received                     : 0
# Xauth reply messages sent                           : 0
# Xauth reply messages received                       : 0
# Xauth status messages sent                          : 0
# Xauth status messages received                      : 0
# Xauth ack messages sent                             : 0
# XAUTH ack messages received                         : 0
# New Group Mode 1st messages sent                    : 0
# New Group Mode 1st messages received                : 0
# New Group Mode 2nd messages sent                    : 0
# New Group Mode 2nd messages received                : 0
# Mode Config request messages sent                   : 0
# Mode Config request messages received               : 0
# Mode Config reply messages sent                     : 0
# Mode Config reply messages received                 : 0
# Mode Config set messages sent                       : 0
# Mode Config set messages received                   : 0
# Mode Config ack messages sent                       : 0
# Mode Config ack messages received                   : 0
# Quick Mode 1st messages sent                        : 9079
# Quick Mode 1st messages received                    : 36183
# Quick Mode 2nd messages sent                        : 40
# Quick Mode 2nd messages received                    : 40
# Quick Mode 3rd messages sent                        : 40
# Quick Mode 3rd messages received                    : 40
# DPD R_U_THERE messages sent                         : 0
# DPD R_U_THERE messages received                     : 0
# DPD R_U_THERE_ACK messages sent                     : 0
# DPD R_U_THERE_ACK messages received                 : 0
# DPTD PING messages sent                             : 0
# DPTD PING messages received                         : 0
# DPTD PONG messages sent                             : 0
# DPTD PONG messages received                         : 0
# Ike Delete notifications sent                       : 48
# Ike Delete notifications for received               : 4
# IPsec Delete notifications sent                     : 58
# IPsec Delete notifications received                 : 58
# QM Connect notifications  received                  : 0
# Responder Life Time notifications sent              : 0
# Responder Life Time notifications received          : 0
# Reply Status notifications sent                     : 0
# Reply Status notifications received                 : 0
# Initial Contact messages sent                       : 18
# Initial Contact messages received                   : 18
# Other Notifications sent                            : 17
# Other Notifications received                        : 17
# Informational Exchanges sent                        : 123
# Informational Exchanges received                    : 79
# retries done                                        : 27109
# IKE SAs matured                                     : 54
# Phase-1 negotiations dropped due to rate-limit      : 0
# Phase-2 negotiations dropped due to rate-limit      : 0
# negotiation requests dropped from IPsec
  when IKE SA is responder and not matured            : 0
# XAUTH changes failed due to auth failures           : 0
# negotiation requests dropped from IPsec
  when VSG status disabled                            : 0
# messages dropped from peer when VSG status disabled : 0
# negotiation requests dropped from IPsec
  when Ike policy not found                                     : 0
# Messages dropped from peer due to invalid Isakmp header length: 0
# Messages dropped from peer due to
  SA life time KB value getting exeeded                       : 0
# Messages dropped from peer due to
  Ike policy configured as initiator only                     : 0
# negotiation requests dropped from IPsec
  Ike policy configured as responder only                     : 0
# QM 1st messages dropped from peer due to received
  peer Id is not matching with IPsec policy peer Id           : 0
# Messages dropped from peer due to
  more number of certificate requests(>=8) exist              : 0
# Current phase-1 negotiations                                : 0
# Current phase-2 negotiations                                : 1
# Queued QMs in IKE SA for which phase-2 not started      : 0
# Phase-1 negotiations dropped due to rate-limit          : 0
# Phase-2 negotiations dropped due to rate-limit          : 0
# Dropped negotiation requests from IPsec                 : 0
# Create SA negotiation requests from IPsec               : 18004
# Renew SA negotiation requests from IPsec                : 38


[local]Redback#show ike asp 2/1 statistics global ike2
# IKE packets sent:      0     # IKE packets received:  159787
# SAs Created: 31486           # SAs Active:  0        # SAs Matured:    0

# Remote User's ID Verify Failures   : 31459
# Cookie Verify Failures             : 0
# MessageID Check Failures           : 0
# Local Informational Exchg attempts : 9
# Remote Informational Exchg attempts: 0
# Invalid Major Version Errors       : 0
# Payload Errors                     : 18
# Non_Matured SAs Deleted            : 31486
# Retries                            : 9
# Duplicate SA_INIT responses        : 0
# Cookie Notify messages Sent        : 0
# Cookie Notify messages Received    : 0
# Invalid KE Payloads Sent           : 0
# Invalid KE Payloads Received       : 0
# CP Payload Requests Sent           : 0
# CP Payload Requests Received       : 0
# CP Payload Reply Msgs Sent         : 0
# CP Payload Reply Msgs Received     : 0
```

1.76 show ipsec access-list

show ipsec [**card** ***slot-id/asp-id***] [**access-list** ***ipsec-acl-name***]

1.76.1 Command Mode

all modes

1.76.2 Syntax Description

card *slot-id*	Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis: • SmartEdge 600 : 1 to 6 • SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14 • SmartEdge 400: 1 to 4
asp-id	Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.
access-list [*ipsec-acl-name*	Optional. Name of a previously created IPsec ACL.

1.76.3 Usage Guidelines

Displays configuration information for IPsec ACLs configured in the current context. If no ACL is specified, one line of configuration information for each ACL with the name and description is displayed. If an ACL is specified, all attributes, including defaults, are displayed for the specified proposal. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.76.4 Examples

```
[local]Redback#show ipsec access-list

Name                                    Description
Ipsec-ACL1                              IPsec Access List #1


[local]Redback#show ipsec access-list Ipsec-ACL1
IPsec Access-List: Ipsec-ACL1
Description:    IPsec Access List #1
Seq 1 tcp 1.1.1.0/24 eq 200000 2.2.2.0/24 eq 200000
Seq 2 1.1.1.0/24 2.2.2.0/24
Seq 3 any any
```

1.77 show ipsec profile

show ipsec [**card** *slot*/*asp-id*] [**profile** *profile-name*]

1.77.1 Command Mode

all modes

1.77.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

profile ***profile-name***

Optional. Name of an IPsec profile.

1.77.3 Usage Guidelines

Displays configuration information for IPsec profiles configured in the current context. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.77.4 Examples

```
[vpn1]l4l7-1#show ipsec profile
IPsec Profile: rec1_1
 DF Bit: 0
 MTU: 1480
 1 IPsec Policy: ipsec_policy1 Access List: acl1_1
```

1.78 show ipsec policy

show ipsec [**card** ***slot-id***/***asp-id***] [**policy** ***policy-name***]

1.78.1 Command Mode

all modes

1.78.2 Syntax Description

card *slot-id*

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

policy *policy-name*

Name of a previously created IPsec policy.

1.78.3 Usage Guidelines

Displays configuration information for IPsec policies in the current context. If no IPsec policy is specified, one line of configuration information for each IPsec policy with the name and Diffie-Hellman group is displayed. If an IKE policy is specified, all attributes, including defaults, are displayed for the specified policy. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.78.4 Examples

```
[local]Redback#show ipsec policy
Name                                       PFS
Ipsec-Policy1                              dh-group 2
```

```
[local]Redback#show ipsec policy Ipsec-Policy1
IPsec Policy: ipsec-Pol1
Perfect-forward-secrecy:  dh-group 2
Anti-replay-window:       64
seq 10 ipsec-Prop1
seq 20 ipsec-Prop2
```

1.79 show ipsec proposal

show ipsec [**card** *slot-id*/*asp-id*] **proposal** *proposal-name*

1.79.1 Command Mode

all modes

1.79.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

proposal ***proposal-name***

Name of a previously created IPsec proposal.

1.79.3 Usage Guidelines

Displays configuration information for IPsec proposals. If no IPsec proposal is specified, one line of configuration information for each IPsec proposal with the name, encryption algorithm, authentication algorithm, and ip-comp flag is displayed. If an IKE proposal is specified, all attributes, including defaults, are displayed for the specified proposal. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.79.4 Examples

```
[local]Redback#show ipsec proposal
Name          Encryption     Authentication    IP-Comp
ipsec-Prop1     des-cbc         hmac-md5-96        Enabled
ipsec-Prop2     3des-cbc        hmac-sha1-96       Disabled
```

```
[local]Redback#show ipsec proposal ipsec-Prop1
IPsec Proposal: ipsec-Prop1
Description: IPsec Proposal 1
ESP:          encryption: aes-128-ctr
              authentication: hmac-sha1-96
AH:           authentication: hmac-md5-96
IP-Comp:      Enabled
Lifetime:     86400 seconds, 50000 KBytes
```

1.80 show ipsec security-association

show ipsec [**card** ***slot-id*/*asp-id***] [**security-association** ***sa-name***]

1.80.1 Command Mode

all modes

1.80.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

security-association ***sa-name***

Name of a previously created IPsec SA.

1.80.3 Usage Guidelines

Displays configuration information for IPsec SAs configured in the current context. If no SA is specified, one line of configuration information for each SA with the name and description is displayed. If an SA is specified, all attributes, including defaults, are displayed for the specified proposal. If no ASP is specified, the information is retrieved from the SmartEdge controller card; otherwise, it is retrieved from the specified ASP.

1.80.4 Examples

```
[local]Redback#show ipsec security-association

Name                      Description
ipsec-sa1                 IPsec Security Association #1
```

```
[local]Redback#show ipsec security-association IPsec-SA1

IPsec Security-Association: ipsec-sa1
Description:    IPsec Security Association #1
Anti Replay Window Size: 64
Ip-Compression: Enable
Security Association: both
   esp spi 0x00001111
       encryption 3des-cbc
         key 0x010203040506070809
// For the administrators
         key **********
// For the operators
       authentication hmac-sha1-96
         key 0x010203040506070809
// For the administrators
         key **********
// For the operators
   ah spi 0x00002222 hmac-md5-96
         key 0x0102030405060708
```

1.81 show ipsec alarms statistics

show ipsec alarms statistics

1.81.1 Command Mode

Global

1.81.2 Usage Guidelines

Shows the statistics including number of raised and number of cleared alarms for tunnel-state change events.

1.82 show ipsec statistics global context

show ipsec card ***slot-id/asp-id*** **statistics global context** ***context-name***

1.82.1 Command Mode

all modes

1.82.2 Syntax Description

card ***slot-id***

Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis:

- SmartEdge 600 : 1 to 6
- SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14
- SmartEdge 400: 1 to 4

asp-id

Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.

global context ***context-name***

Name of a previously created context.

1.82.3 Usage Guidelines

Displays IPsec statistics for the specified context.

1.82.4 Examples

The following example shows the global IPsec statistics for the context `vpn1`.

```
[local]Redback#show ipsec card 2/1 statistics global context vpn1
----------------------------------------------------------------------
   IPsec4 Global Packet Processing Stats::
----------------------------------------------------------------------
# Packets Received for Inbound Processing  : 0
# Packets Processed by Inbound Processing   : 0
# Packets Received for Outbound Processing  : 0
# Packets Processed by Outbound Processing   : 0
# Inbound Secured Packets Received  : 0
# Inbound Secured Packets Processed  : 0
# Outbound Packets Received to Apply Security  : 0
# Outbound Packets Security has Applied  : 0
# Inbound UDP Encapsulated Packets  : 0
(Errors)
# Inbound Packet has Dropped, Because of SA is Deleted or not Complete SA  : 0
# Inbound ICMP Error Packets  : 0
# Unable to Find Subscriber Network ID  : 0
# Can't Handle ICMP Error Messages  : 0
# Invalid IP Header Length  : 0
# Can't Allow this ICMP Error Message Type and Code to Process   : 0
# Updated Out SA PMTU Value with Received ICMP MTU Error Message Value  : 0
# SPD Policy has Modified, Pkt Selectors not matched with Policy Selectors : 0
# Packet Length is less than Minimum ESP Header Length  : 0
# Packet Length is less than Minimum AH Header Length  : 0
# Unable to Allocate memory for SA Info  : 0
# Unable to Allocate memory for Packet Queue Node  : 0
# Can't Process the Packet, Because of Delete Mark Set in SA  : 0
# Unable to Allocate memory for IKE request Info Node  : 0
# Updating of NAT IP and Port Change of Ihappi Reg Function returns Failure  : 0
# Unable to Allocate Memory for HA Data Node  : 0
# Unable to Allocate Memory for New buffer(igwbuf)  : 0
# Dropping the Packet, Invalid Sequence Number Recieved  : 0
# Dropping the Packet, Late Packets Received  : 0
# Dropping the Packet, Duplicate Packets Received  : 0
# Dropping the Packet, Invalid Buffer Length  : 0
# Inbound Packet IP Comp Header Flag field is not Zero : 0
# Inbound Packet AH Header Reserved field is not Zero : 0
# Wrong AH Header Payload length of Inbound Packet  : 0
# Dropping the Packet, IP Header Placement Error  : 0
# Dropping the Packet, Decompression of Inbound packet Failure  : 0
# Dropping the Packet, Authentication of Inbound packet Failure  : 0
# Possibly Decryption is done with wrong key  : 0
# Received in Transport mode, but Expected to Tunnel mode packet  : 0
# Received in Tunnel mode, but Expected to Transport mode packet  : 0
# Inbound Packet has Dropped, SA Hard Life Time KB is Expired  : 0
# Pkts Recieved with IPv6 selector and IPv6 Engine has not been Registered  : 0
# Matching SA Selectors with Packet Selectors Failed  : 0
# Inner IP Header has IPv6, Submit to IPv6 Engine  : 0
# Unable to Allocate Memory for Tasklet Group Node  : 0
# Unable to Allocate Memory for Tasklet Data Node  : 0
# Unable to Schedule the Tasklet  : 0
# Packet has Bypassed, Subscriber Network Id has disabled  : 0
# Unable to Allocate memory for IP Selector Node  : 0
# Dropping the Pkts, Apply Policy Configured for Received ICMP Error Message: 0
# Dropping the Pkts, Discard Policy Matched for Outbound ICMP Error Message: 0
# Dropping the Pkts, Discard Policy Matched for Inbound ICMP Error Message:  0
# Unable to Find Matching Selector Set from Packet Selectors  : 0
# No policy or Non Bypass policy found for ICMP Error Massage Inner Payload  : 0
# Unable to Allocate Memory for FW VPN Info Node  : 0
# Dropping the Packet, Apply Policy Configured for Received Plain Packet  : 0
# Dropping the Packet, Discard Policy Matched for Outbound Packet  : 0
# Dropping the Packet, Discard Policy Matched for Inbound Packet  : 0
# Dropping the Packet, No Matching Policy Found for Outbound Packet  : 0
# Dropping the Packet, No Matching Policy Found for Inbound Packet  : 0
# Matching Policy Found for Outbound Packet, but Mark has Delete Policy  : 0
# Unable to Find Another Policy for Non Initial Fragments  : 0
# Matching Policy for Non Initial Fragments is not Apply Policy  : 0
# Starting of SA Negotiations must not be with ICMP Error Message  : 0
# Dropping the packet, Negotiations would be under process   : 0
# Packet DSCP Value Doesn't Fall Under Policy DSCP Ranges  : 0
# Unable to Get the SPI and Create Redundant SA  : 0
# Unable to Find the Created Redundant SA  : 0
# Preparing Negotiation Request Information to IKE Failure  : 0
# Queuing of Request Information to IKE Failure  : 0
# Unable to Allocate Memory for Negotiating Response Info Node  : 0
# Unable to Create Manual SA, No Local and Remote Gateway in Policy  : 0
# Unable to Create Manual SA, More than One Attribute in Proposal  : 0
# Unable to Create Manual SA, More than One Proposal in Manual Policy  : 0
# Unable to Create Manual SA, Conversion of Selector to TS Info Failure  : 0
# Manual SA Creation Failures  : 0
# Dropping the Packet, SA is not in Complete State or Backup SA  : 0
# Dropping the Packet, Time to Live is Zero  : 0
# Formation of Chain of Fragments for Fragmentation before Encap Failures : 0
# Packet Submit to IPv6 Engine for Outbound Processing : 0
# Dropping the Packet, Packet Size more than SA Path MTU size  : 0
# Invalid SA IP Compression Information  : 0
# Dropping the Outbound Packet, Sequence Number Overflow  : 0
# Applying Crypto Operation or Compression on Plain Packet Failures  : 0
# Outbound Packet has Dropped, SA Hard Life Time KB Expired  : 0
# Addition of Encapsulated UDP Header on Packet Failure  : 0
# Dropping the packet, Request send to IKE for SA Negotiations : 0
# Dropping the packet, Request send for Manual Outbound SA Creation  : 0
# Mismatch SA Selectors IP Version, Inner IP is IPv4,SA Selector is IPv6  : 0
# Invalid ESP header Pad Length Field value of Inbound Packet  : 0
# Packets dropped since tunnel is in unbind/unoperational/disable state  : 0
# Packets dropped since SA backlogQ threshold cnt reached  : 0
# Packets dropped due to bDeleteSAMatched, no kick to IKE   : 0
```

1.83 show pki alarms statistics

show pki alarms statistics

1.83.1 Command Mode

Global

1.83.2 Usage Guidelines

Shows the statistics including number of raised and number of cleared alarms for certificate-expiry warning and certificate-missing events. Applies to RSA trusted and self certificates.

1.84 show pki certificate rsa

```
show pki [asp slot-id/asp-id] certificate {trusted|self} rsa
[identity identity|handle handle]
```

1.84.1 Command Mode

all modes

1.84.2 Syntax Description

asp *slot-id*	Optional. Number of the chassis slot where the card is installed. Possible values are 1 to 14. The actual slots that can contain an ASE card depend on the chassis: • SmartEdge 600 : 1 to 6 • SmartEdge 800, 1200, or 1200H: 1 to 6 and 9 to 14 • SmartEdge 400: 1 to 4
asp-id	Optional. ID of the ASP on the ASE card. Possible values are 1 and 2.
trusted	Displays information about trusted certificates.
self	Displays information about self certificates.
handle *handle*	The handle of a specific certificate.
identity *identity*	The identity of a specific certificate.

1.84.2.1 Usage Guidelines

This command displays information about the trusted or self certificate specified, either trusted or self. If the certificate identity or handle is specified, information about the specified certificate is shown. Use the **handle** keyword to specify a specific imported certificate. The value for handle is a unique number assigned to each certificate when it is imported and is never reused; the value for handle assigned to the first imported certificate is 0, and the value increments each time a new certificate is imported. The value for the **identity** keyword is the subject name of the certificate. If you do not know the value for the **handle** or **identity** keywords, you must first show all the self or trusted certificates.

1.84.2.2 Examples

The following example displays information about the key pair `first_key_pair` in the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#show pki key-pair first_key_pair
```

1.85 show pki key-pair

show pki key-pair[*key-pair-name*

1.85.1 Command Mode

all modes

1.85.2 Syntax Description

key-pair	Unique name for the key pair; up to 39 characters.

1.85.3 Usage Guidelines

This command displays a minimal amount of information about the keys, and does not display the actual keys.

1.85.4 Examples

The following example displays information about the key pair `first_key_pair` in the `vpn1` context.

```
[local]Redback#context vpn1
[vpn1]Redback#show pki key-pair first_key_pair
```

1.86 show tunnel ipsec

show tunnel ipsec [[**name** *tunnel-name*|**remote** *ip-address*] [**detail**]]|[[**name** *tunnel-name*] **on-demand**]

1.86.1 Command Mode

all modes

1.86.2 Syntax Description

`name` ***`tunnel-name`***	Optional. Name of a previously created IPsec tunnel.
`remote` ***`ip-address`***	Optional. IP address of the remote endpoint.
`detail`	Optional. Displays detailed configuration information.
`tunnel-name`	Optional. Tunnel name.
`on-demand`	Optional. Displays information about on-demand IPsec tunnels.

1.86.3 Usage Guidelines

Displays configuration information for IPsec tunnels. If no IPsec tunnel is specified, generic information about all IPsec tunnels is displayed. You can specify a single IPsec tunnel by name. Specify IPsec tunnels that share the same remote endpoint by specifying the IP address of the remote endpoint. All generic attributes, including the name, endpoints, ASP slot/ID, state, bound interface, circuit ID, and circuit handle are displayed. If you use the optional **`detail`** keyword in addition to specifying the tunnel or remote endpoint, IPsec-specific attributes, including encryption algorithms, authentication algorithms, active SAs, and the operational status are also displayed. Use the **`on-demand`** keyword to display on-demand tunnel names and count; use the on-demand tunnel name to list information for the specified on-demand tunnel.

1.86.4 Examples

```
[local]Redback#show tunnel ipsec

:::: Tunnel : rec_2_1
   Key        : -
   Remote IP : 77.0.0.1    Local IP    : 77.0.0.2
   Tnl Type  : IPsec       ASP Slot/Id : 2/1
   State     : Up          Bound to    : tunnel_ipsec2@ipsec_context2
   Circuit ID: 18          Internal Hdl: 255/28:1023:63/0/1/18

:::: Tunnel : rec_1_2
   Key        : -
   Remote IP : 77.0.0.2    Local IP    : 77.0.0.1
   Tnl Type  : IPsec       ASP Slot/Id : 2/1
   State     : Up          Bound to    : tunnel_ipsec2@ipsec_context
   Circuit ID: 17          Internal Hdl: 255/28:1023:63/0/1/17


[local]Redback#show tunnel ipsec name rec_2_1
 :::: Tunnel : rec_2_1
    Key        : -
    Remote IP : 77.0.0.1    Local IP    : 77.0.0.2
    Tnl Type  : IPsec       ASP Slot/Id : 2/1
    State     : Up          Bound to    : tunnel_ipsec2@ipsec_context2
    Circuit ID: 18          Internal Hdl: 255/28:1023:63/0/1/18


[local]Redback#show tunnel ipsec remote 77.0.0.2 detail


:::: Tunnel : rec_1_2_d
   Key        : -
   Remote IP : 77.0.0.2    Local IP    : 77.0.0.1
   Tnl Type  : IPsec       ASP Slot/Id : 2/1
   State     : Up          Bound to    : tunnel_ipsec2@vpn1
   Circuit ID: 3           Internal Hdl: 255/28:1023:63/0/1/3

[local]router# show tunnel ipsec name rec_1_2_d detail

:::: Tunnel : rec_1_2_d
   Key        : -
   Remote IP : 77.0.0.2    Local IP    : 77.0.0.1
   Tnl Type  : IPsec       ASP Slot/Id : 2/1
   State     : Up          Bound to    : tunnel_ipsec2@vpn1
   Circuit ID: 3           Internal Hdl: 255/28:1023:63/0/1/3

   Tunnel is User Configured
   local-ip 77.0.0.1, context-for-local-ip: vpn1
   mtu 1480
   log-state-changes no
```

```
  clear-df no
   destination UP on nhop resolved in valid intf
   resolved on to_ipsec_peer2 grid 0x10000003
   Tunnel ID: ipsec 3
   Circuit ID Internal: 255/28:1023:63/0/1/3

# of IKE SAs   :    1
# of IPsec SAs :    4

IKE Policy: ike_pol1

               ************ IKE SA's ***************
-------------------------------------------------------------------------
SA Number : 1      Initiator State: (SA_MATURE)
-------------------------------------------------------------------------
Policy Name: ike_pol1
Authentication Mode: Pre-shared Key  Peer Address: 77.0.0.2
Remote Id Type: IPV4_ADDR  RemoteId: 77.0.0.2
Initiator Cookie : 0x2d154957844f95ca
Responder Cookie : 0xb83c7d1dd8cb26d5
Life Time in Sec: 86291  Life Time In Bytes: 0
Negotiated Life Time in Sec  : 86400
Negotiated Life Time In Bytes: 0
Authentication Algorithm   : HMAC-MD5-96
Encryption Algorithm       : 3DES-CBC
DH Group: 1
SA Status : Active

seq 10 ipsec-policy pol1 access-group acl1_2

               ************ IPSEC SA's ***************
-------------------------------------------------------------------------
 SA #1: Outbound ESP
--------------------
   SPI : 0x2005d9
   Encr: 3des-cbc
   Auth: hmac-md5-96
   Selector: IP 55.0.0.0/16 -> 60.0.0.0/16
             Proto tcp port [0 - 0] -> [0 - 0]
   Path MTU: 1388
   Negotiated Lifetime in Seconds: 86400
   Negotiated Lifetime in Bytes  : 0
   (Soft / Hard) Lifetime in Seconds: 11639 / 11873
   (Soft / Hard) Lifetime in Bytes  : 0 / 0
   Packets processed: 0
   Bytes processed  : 0
   IP Compression Status: Disabled

 SA #2: Inbound ESP
--------------------
   SPI : 0x2005c9
   Encr: 3des-cbc
   Auth: hmac-md5-96
   Selector: IP 60.0.0.0/16 -> 55.0.0.0/16
             Proto tcp port [0 - 0] -> [0 - 0]
   Negotiated Lifetime in Seconds: 86400
   Negotiated Lifetime in Bytes  : 0
   (Soft / Hard) Lifetime in Seconds: 11637 / 11873
   (Soft / Hard) Lifetime in Bytes  : 0 / 0
   Packets processed: 0
   Bytes processed  : 0
   IP Compression Status: Disabled

 SA #3: Outbound AH
--------------------
   SPI : 0x2005df
   Auth: hmac-md5-96
   Selector: IP 55.0.0.0/16 -> 60.0.0.0/16
             Proto tcp port [0 - 0] -> [0 - 0]
Path MTU: 1388
   Negotiated Lifetime in Seconds: 86400
   Negotiated Lifetime in Bytes  : 0
   (Soft / Hard) Lifetime in Seconds: 11727 / 11873
   (Soft / Hard) Lifetime in Bytes  : 0 / 0
   Packets processed: 0
   Bytes processed  : 0
   IP Compression Status: Disabled

 SA #4: Inbound AH
--------------------
   SPI : 0x2005cf
   Auth: hmac-md5-96
   Selector: IP 60.0.0.0/16 -> 55.0.0.0/16
             Proto tcp port [0 - 0] -> [0 - 0]
   Negotiated Lifetime in Seconds: 86400
   Negotiated Lifetime in Bytes  : 0
   (Soft / Hard) Lifetime in Seconds: 11357 / 11873
   (Soft / Hard) Lifetime in Bytes  : 0 / 0
   Packets processed: 0
   Bytes processed  : 0
   IP Compression Status: Disabled
```

```
[local]l417-1#show tunnel ipsec rec1_1 on-demand
IKE Policy         : ike_policy1_1
Local IP           : 1.1.1.1
Bind Interface     : tunnel_ipsec_multibind_1_1
Bind Context       : vpn1
AAA Authentication : Disabled
Maximum Tunnels    : 1
Number of Tunnels  : 1
Number of Active Tunnels: 1
Local IP: 1.1.1.1
Remote-IP     ASP   Tunnel-Name                Bind                       Context   Creation Time
2.1.1.1       2/1  _*DynTun*_23000001_00310000 tunnel_ipsec_multibind_1_1 vpn1          Today

[local]l417-1#show tunnel ipsec on-demand
Tunnel                  Count
rec1_1                   1
```

1.87 show tunnel ipsec statistics

show tunnel ipsec name ***tunnel-name*** [**on-demand**] **statistics** [**detail**]

1.87.1 Command Mode

all modes

1.87.2 Syntax Description

name ***tunnel-name***	Name of a previously created IPsec tunnel.
on-demand	Optional. Displays statistics at the tunnel profile level.
detail	Optional. Displays basic cumulative statistics for the tunnel and the statistics for each SA.

1.87.3 Usage Guidelines

Displays the IPsec statistics associated with the specified tunnel. Identify only the tunnel to show basic cumulative statistics for the tunnel. Use the **detail** keyword to show basic cumulative statistics for the tunnel and the statistics for each SA. Use the **on-demand** keyword to show statistics for the on-demand tunnel at the tunnel profile level.

1.87.4 Examples

The following example shows the results following a ping test in which 215 packets were sent.

```
[local]Redback#show tunnel ipsec name rec_2_1 statistics

IPsec Decryption Errors                                 : 0
IPsec Authentication Errors                             : 0
IPsec Policy Errors                                     : 0
IPsec Padding Errors                                    : 0
Anti-Replay Errors in IPsec                             : 0
Other Errors in IPsec                                   : 0
Number of IN IPsec packets                              : 215
IPsec IN packets HO value                               : 0
Number of OUT IPsec packets                             : 215
IPsec OUT packets HO value                              : 0
Send OUT IPsec pkts Errors                              : 0
Total IN Bytes Processed By IPsec                       : 15480
IN Bytes Processed HO value                             : 0
Total OUT Bytes Processed By IPsec                      : 15480
OUT Bytes Processed HO value                            : 0
```

1.88 show tunnel ipsec name statistics ike

show tunnel ipsec name ***tunnel-name*** **statistics ike** [**detail**]

1.88.1 Command Mode

all modes

1.88.2 Syntax Description

name ***tunnel-name***	Name of a previously created IPsec tunnel.
detail	Optional. Displays detailed IKE SA statistics for the tunnel.

1.88.3 Usage Guidelines

Displays the IKE SA statistics associated with the specified tunnel. Identify only the tunnel to show basic cumulative IKE SA statistics for the tunnel.

Use the **detail** keyword to show detailed IKE SA statistics for the tunnel.

1.88.4 Examples

The following example shows the basic cumulative statistics for the tunnel `rec_1_2_d`.

```
[local]Redback#show tunnel ipsec name rec_1_2_d statistics ike

**************IKEv2 Policy Statistics ******************
Number of local IKE SA renewal attempt:                       0
Number of IKE SA renewal messages received:                   0
Number of IPSec SA create or renewal messages sent:           1
Number of IPSec SA create or renewal messages received:       0
Number of local IKE SA exchange attempts:                     1
Number of local IKE SA exchange attempt failures:             0
Number of remote IKE SA exchange attempts:                    0
Number of remote IKE SA exchange attempt failures:            0
Number of authentication failures:                            0
Number of ID verification failures:                           0
Number of EAP authentication failures:                        0
Number of certificate verification failures:                  0
Number of local IKE SA renewal attempts failures:             0
Number of remote IKE SA renewal attempts failures:            0
Number of IPsec SA create or renewal messages sent failed:    0
Number of IPsec SA create or renewal messages received failed: 0
Number of IKE proposal mismatches:                            0
Number of IPsec proposal mismatches:                          0
Number of traffic selector mismatches:                        0
Number of certificate unavailable errors:                     0

**************IKEv2 Policy SA Statistics ******************
IKE_SA_INIT request sent:          1
IKE_SA_INIT request received:      0
IKE_SA_INIT response sent:         0
IKE_SA_INIT response received:     1
IKE_AUTH request sent:             1
IKE_AUTH request received:         0
IKE_AUTH response sent:            0
IKE_AUTH response received:        1
CREATE_CHILD_SA request sent:      0
CREATE_CHILD_SA request received:  0
CREATE_CHILD_SA response sent:     0
CREATE_CHILD_SA response received: 0
INFORMATIONAL request sent:        0
INFORMATIONAL request received:    0
INFORMATIONAL response sent:       0
INFORMATIONAL response received:   0
IKE Invalid message exchanges:     0
CHILD_SAs rekeyed:                 0
```

The following example shows the detailed IKE statistics for the `tunnel rec_1_2_d`.

```
[local]Redback#show tunnel ipsec name rec_1_2_d statistics ike detail

Tunnel name: rec_1_2_d
IKE policy : ike_pol1
                ************ IKE SA's Statistics*******
-------------------------------------------------------------------------
SA Number : 1
Peer Address: 77.0.0.2
Initiator Cookie : 0x7e297db914b66772
Responder Cookie : 0xdaa84093bef72c32
-------------------------------------------------------------------------
IKEv1 SA Stats:
# IN Pkts:            2291            # OUT Pkts:           3
# IN Bytes:         430600            # OUT Bytes:          364

# Phase1 Request Dropped Awaiting Auth Response:                            0
# Phase2 Local Attempts:          0     # Phase2 Remote Attempts:           2288
# Phase2 Local Attempts Failed:   0     # Phase2 Remote Attempts Failed:    2288
(Errors)
# Invalid Protocol Id:   0          # Invalid SPI:               0
# Invalid TransformId:   0          # Invalid PayloadType:       0
# Invalid PayloadFmt:    0          # Invalid KeyInfo:           0
# Invalid IdInfo:        0

                ************ IKEv1 Policy Statistics*******
# IKE Local Attempts:               10    # IKE Remote Attempts:                5
# IKE Local Attempts Failed:         0    # IKE Remote Attempts Failed:         0
# Phase2 SA created as Initiator: 23    # Phase2 SA created as responder:   6
# IKE local Phase2 attempts:    15
# IKE remote Phase2 attempts: 2518
# IKE local Phase2 attempts failed: 0
# IKE remote Phase2 attempts failed: 2504

(Errors)
# Phase2 Proposal mismatch:       0    # Phase2 Traffic Selector mismatch:  2430
# Invalid IKE Cookie:             0
# Invalid Major Version in IKE:   0    # Invalid Minor Version in IKE:     0
# Invalid IKE Exchange Type:      0    # Invalid Flags:                    0
# Invalid IKE Message ID:         0    # Invalid Protocol ID:              0
# Invalid SPI:                    0    # Invalid Transform ID:             0
# Invalid Payload  Type:          0    # Invalid Payload  Type  format:    0
# Invalid Key Info: 0                  # Invalid ID Info:                  0
# Invalid Encoding in cert payload:  0 # Invalid Encoding in cert data:    0
# Invalid CA data in CERT_REQ payload:                                     0
# Invalid hash data in hash payload: 0 # Invalid signature:                0
# Authentication Failed:             0 # Phase1 proposal mismatch:         0
# Bad Proposal syntax:               0 # payload lengths mismatched:       0
# Certificate requested is unavailable:  0
# Lack of support for DOI in SA payload: 0
# Lack of protection for the situation:  0
# Lack of matching attribute:            0
# The Certificate type is not supported: 0
# Mismatch in Exchange Type is detected: 0

                ************ IKEv2 Policy Statistics*******
# Local IKE Renewal Attempts:  0     # Remote IKE Renewal Attempts: 0
# Local IPsec Create Or Renewal Attempts:     0
# Remote IPsec Create Or Renewal Attempts:    0
# Local IKE Exchg Attempts:   0      # Local IKE Exchg Attempt Failures:   0
# Remote IKE ExchgAttempts:   0      # Remote IKE Exchg Attempt Failures:  0
# Local IKE Renewal Attempt Failures:              0
# Remote IKE Renewal Attempt Failures:             0
# Local IPsec Create Or Renewal Attempt Failures:  0
# Remote IPsec Create Or Renewal Attempt Failures: 0
# Auth Failures:        0            # ID Verify Failures:   0
# EAP Auth Failures:    0            # Cert Verify Failures: 0
# IKE Proposal mismatches: 0        # IPsec Proposal mismatches: 0
# Traffic Selector mismatches: 0     # Certs Unavailable: 0
```

1.89 tunnel ipsec

tunnel ipsec ***name*** **[manual|on-demand] [economical]**

```
no tunnel ipsec name
```

1.89.1 Command Mode

global configuration

1.89.2 Syntax Description

name	Unique name for the IPsec tunnel; up to 50 characters. Do not use the reserved prefix _*DynTun*_.
manual	Optional. The tunnel must be configured with manually configured SAs.
on-demand	Optional. Creates the remote tunnel endpoint on demand during connection.
economical	Optional. Creates the tunnel in economical mode, which routes data traffic directly to the ASE card for encryption and does not consume a circuit on a traffic card. An economical mode tunnel bypasses the circuit-based services on the traffic cards. The number of tunnels is not limited by the capacity of the traffic card.

1.89.3 Default

No IPsec tunnels are configured.

1.89.4 Usage Guidelines

Creates (with default attributes) or selects an IPsec tunnel, and enters tunnel configuration mode. Use the **economical** keyword to create an IPsec tunnel that does not require any traffic card services and whose traffic can be routed directly to the SE card for encryption. Use the **manual** keyword to create an IPsec tunnel that uses SAs manually configured with the **ipsec security-association** command. Otherwise, the IPsec tunnel uses SAs negotiated using IKE. Once an IPsec tunnel is created, you cannot change its mode. Using the **no** form of the command will remove an existing configuration.

On a SmartEdge router, each ASE card can support any combination of up to 8,000 IKE and IPsec tunnel sessions, up to a total of 32,000 sessions for the SmartEdge router.

1.89.5 Examples

```
[local]Redback(config)#tunnel ipsec rec_2_1
```

```
[local]Redback(config)#tunnel ipsec rec_3_2 on-demand
```

1.90 validate-certificate-identity

validate-certificate-identity

1.90.1 Command Mode

IKEv1 policy configuration

IKEv2 policy configuration

1.90.2 Syntax Description

This command has no keywords or arguments.

1.90.3 Default

Checking of the IKE remote ID provided by the peer in the identification payload against the contents of the certificate provided by the peer is not enabled.

1.90.4 Usage Guidelines

This command enables checking of the IKE remote ID provided by the peer in the identification payload against the contents of the certificate provided by the peer. Using the **no** form of the command disables checking.

1.90.5 Examples

```
[local]Redback(config-ctx)#ike policy ike_pol1
[local]Redback(config-ike-policy)#validate-certificate-identity
```

Glossary

ACL
Access Control List

AH
Authentication Header

ASE
Advanced Services Engine

ASP
Advanced Services Processor

BGP
Border Gateway Protocol

CA
Certificate Authority

DF
Don't Fragment

DNS
Domain Name System

DoS
Denial of Service

DPD
Dead Peer Detection

ESP
Encapsulating Security Payload

FTP
File Transfer Protocol

GRE
Generic Routing Encapsulation

ICMP
Internet Control Message Protocol

IGMP
Internet Group Management Protocol

IGP
Interior Gateway Protocol

IKEv1
Internet Key Exchange version 1

IKEv2
Internet Key Exchange version 2

IPComp
IP Compression

IPsec
Internet Protocol Security

IPsec
Specified Internet Protocol Security

IS-IS
Intermediate System-to-Intermediate System

MTU
Maximum Transmission Unit

NIC
Network Interface Card

NNTP
Network News Transport Protocol

NTP
Network Time Protocol

OSPF
Open Shortest Path First

PCP
Payload Compression Protocol

PFS
Perfect Forward Secrecy

PIM
Protocol Independent Multicast

PKI
Public Key Infrastructure

POP2
Post Office Protocol Version 2

POP3
Post Office Protocol Version 3

QoS
Quality of Service

RIP
Router Information Protocol

SA
Security Association

SA
Service Association

SMTP
Simple Mail Transport Protocol

SNMP
Simple Network Management Protocol

SPI
Security Parameter Index

TACACS
Terminal Access Controller Access Control System

TCP
Transmission Control Protocol

TFPT
Trivial File Transfer Protocol

UDP
User Datagram Protocol

VPN
Virtual Private Network

Reference List

Ericsson

[1] *IPsec VPN Overview*, 2/221 02-CRA 119 1170/1-V1

[2] *IPsec VPN Configuration and Operation Using the SmartEdge OS CLI*, 1/1543-CRA 119 1170/1-V1

[3] *Command List*, 1/19077-CRA 119 1170/1-V1

[4] *Commands: r*, 15/190 82-CRA 119 1170/1