# IPSec Configuration Commands

# Generic Commands

## description

**Syntax** **description** *description-string*

**Context** config>isa>ipsec-group
config>isa

**Description** This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

**Default** **none**

**Parameters** *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

## shutdown

**Syntax** [**no**] **shutdown**

**Context** config>isa
config>isa>aa-group
config>isa>tunnel-grp

**Description** This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

# Hardware Commands

## mda-type

**Syntax** **mda-type** *isa-tunnel*
**no mda-type**

**Context** config>card>mda

**Description** This command provisions or de-provisions an MDA to or from the device configuration for the slot.

**Parameters** *isa-tunnel* — Specifies the ISA tunnel.

# ISA Commands

## isa

**Syntax** **isa**

**Context** config

**Description** This command enables the context to configure Integrated Services Adapter (ISA) parameters.

## tunnel-group

**Syntax** **tunnel-group** *tunnel-group-id* [**create**]
**no tunnel-group** *tunnel-group-id*

**Context** config>isa

**Description** This command allows a tunnel group to be created or edited. A tunnel group is a set of one or more MS-ISAs that support the origination and termination of IPSec and IP/GRE tunnels. All of the MS-ISAs in a tunnel group must have isa-tunnel as their configured mda-type.

The **no** form of the command deletes the specified tunnel group from the configuration

**Parameters** *tunnel-group-id* — An integer value that uniquely identifies the tunnel-group.

**Values** 1—16

**create —** Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled/disabled in the **environment>create** context.

## active-mda-number

**Syntax** **active-mda-number** *number*
**no active-mda-number**

**Context** config>isa>tunnel-grp

**Description** This command specifies the number of active MS-ISA within all configured MS-ISA in the tunnel-group with multi-active enabled. IPsec traffic will be load balanced across all active MS-ISAs. If the number of configured MS-ISA is greater than the active-mda-number then the delta number of MS-ISA will be backup.

**Default** no

**Parameters** *number* — Specifies the number of active MDAs.

**Values** 1—16

## backup

**Syntax** **backup** *mda-id*
**no backup**

**Context** config>isa>tunnel-grp

**Description** This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup module provides the IPSec group with warm redundancy when the primary module in the group is configured. An IPSec group must always have a primary configured.

Primary and backup modules have equal operational status and when both modules are coming up, the one that becomes operational first becomes the active module. An IPSec module can serve as a backup for multiple IPSec groups but the backup can become active for only one ISA IPSec group at a time.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified module from the IPSec group.

**Default** no backup

**Parameters** *mda-id* — Specifies the card/slot identifying a provisioned module to be used as a backup module.

**Values** mda-id: *slot*/*mda*
slot 1 — up to 10 depending on chassis model
mda 1 — 2

## mda

**Syntax** **mda** *mda-id*
**[no] mda**

**Context** config>isa>tunnel-grp

**Description** This command specifies the MDA id of the MS-ISA as the member of tunnel-group with multi-active enabled. Up to 16 MDA could be configured under the same tunnel-group.

**Default** no

**Parameters** *mda-id* — Specifies the id of MS-ISA.

**Values** iom-slot-id/mda-slot-id

## multi-active

**Syntax** **multi-active**
**[no] multi-active**

**Context** config>isa>tunnel-grp

**Description** This command enables configuring multiple active MS-ISA in the tunnel-group. IPsec traffic will be load balanced to configured active MS-ISAs.

Note:

- A shutdown of group and removal of all existing configured tunnels of the tunnel-group are needed before provisioning command “multi-active”.
- If the tunnel-group is admin-up with “multi-active” configured then the configuration of “primary” and “backup” are not allowed.
- The active-mda-number must be =< total number of ISA configured.

  If active-mda-number is less than total number of ISA configured then the delta number of ISA will become backup ISA.

**Default** no

## primary

**Syntax** **primary** *mda-id*
**no primary**

**Context** config>isa>tunnel-grp

**Description** This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup ISA IPSec provides the IPSec group with warm redundancy when the primary ISA IPSec in the group is configured. Primary and backup ISA IPSec have equal operational status and when both MDAs are coming up, the one that becomes operational first becomes the active ISA IPSec.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified primary ID from the group’s configuration.

**Default** no primary

**Parameters** *mda-id* — Specifies the card/slot identifying a provisioned IPSec ISAA.

## reassembly

**Syntax** **reassembly** [*wait-msecs*]
**no reassembly**

**Context** config>isa>tunnel-group
config>service>ies>interface>sap>gre-tunnel
config>service>vprn>interface>sap>gre-tunnel

**Description** This command configures IP packet reassembly for IPSec and GRE tunnels supported by an MS-ISA. The reassembly command at the tunnel-group level configures IP packet reassembly for all IPSec and GRE tunnels associated with the tunnel-group. The reassembly command at the GRE tunnel level configures IP packet reassembly for that one specific GRE tunnel, overriding the tunnel-group configuration.

The **no** form of the command disables IP packet reassembly.

**Default** no reassembly (tunnel-group level)

reassembly (gre-tunnel level)

**Parameters** *wait* — Specifies the maximum number of milliseconds that the ISA tunnel application will wait to receive all fragments of a particular IPSec or GRE packet. If one or more fragments are still missing when this limit is reached the partially reassembled datagram is discarded and an ICMP time exceeded message is sent to the source host (if allowed by the ICMP configuration of the sending interface). Internally, the configured value is rounded up to the nearest multiple of 100 ms.

**Values** 100 — 5000

**Default** 2000 (tunnel-group level)

# Internet Key Exchange (IKE) Commands

## ipsec

**Syntax** **ipsec**

**Context** config

**Description** This command enables the context to configure Internet Protocol security (IPSec) parameters. IPSec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

## ike-policy

**Syntax** **ike-policy** *ike-policy-id* [**create**]
**no ike-policy** *ike-policy-id*

**Context** config>ipsec

**Description** This command enables the context to configured an IKE policy.

The **no** form of the command

**Parameters** *ike-policy-id* — Specifies a policy ID value to identify the IKE policy.

**Values** 1 — 2048

## auth-algorithm

**Syntax** **auth-algorithm** *auth-algorithm*
**no auth-algorithm**

**Context** config>ipsec>ike-policy

**Description** The command specifies which hashing algorithm to use for the IKE authentication function.

The **no** form of the command removes the parameter from the configuration.

**Parameters** **md5 —** Specifies the hmac-md5 algorithm for authentication.

**sha1 —** Specifies the hmac-sha1 algorithm for authentication.

**sha256 —** Specifies the sha256 algorithm for authentication.

**sha384 —** Specifies the sha384 algorithm for authentication.

**sha512 —** Specifies the sha512 algorithm for authentication.

## auth-method

**Syntax** **auth-method** {**psk**|**plain-psk-xauth**|**cert-auth**|**psk-radius**|**cert-radius**|**eap**}
**no auth-method**

**Context** config>ipsec>ike-policy

**Description** This command specifies the authentication method used with this IKE policy.

The **no** form of the command removes the parameter from the configuration.

**Default** no auth-method

**Parameters** **psk —** Both client and gateway authenticate each other by a hash derived from a pre-shared secret. Both client and gateway must have the PSK. This work with both IKEv1 and IKEv2

**plain-psk-xauth —** Both client and gateway authenticate each other by pre-shared key and RADIUS. This work with IKEv1 only.

## dh-group

**Syntax** **dh-group** {**1** | **2** | **5** | **14** | **15**}
**no dh-group**

**Context** config>ipsec>ike-policy

**Description** This command specifies which Diffie-Hellman group to calculate session keys. Three groups are supported with IKE-v1:

- Group 1: 768 bits
- Group 2: 1024 bits
- Group 5: 1536 bits
- Group 14: 2048 bits
- Group 15: 3072 bits

More bits provide a higher level of security, but require more processing.

**Default** 5

The **no** form of the command removes the Diffie-Hellman group specification.

## dpd

**Syntax** **dpd** [**interval** *interval*] [**max-retries** *max-retries*] [**reply-only**]
**no dpd**

**Context** config>ipsec>ike-policy

**Description** This command controls the dead peer detection mechanism.

The **no** form of the command removes the parameters from the configuration.

**Parameters** **interval** *interval* — Specifies the interval that will be used to test connectivity to the tunnel peer. If the peer initiates the connectivity check before the interval timer it will be reset.

**Values** 10 — 300 seconds

**Default** 30

**max-retries** *max-retries* **—** Specifies the maximum number of retries before the tunnel is removed.

**Values** 2 — 5

**Default** 3

**reply-only —** Specifies to only reply to DPD keepalives. Issuing the command without the reply-only keyword disables the behavior.

**Values** reply-only

## encryption-algorithm

**Syntax** **encryption-algorithm** {**des** | **3des** | **aes128** | **aes192** | **aes256**}
**no encryption-algorithm**

**Context** config>ipsec>ike-policy

**Description** This command specifies the encryption algorithm to use for the IKE session.

The **no** form of the command removes the encryption algorithm from the configuration.

**Default** aes128

**Parameters** **des —** This parameter configures the 56-bit **des** algorithm for encryption. This is an older algorithm, with relatively weak security. While better than nothing, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

**3des —** This parameter configures the **3-des** algorithm for encryption. This is a modified application of the **des** algorithm which uses multiple **des** operations for more security.

**aes128 —** This parameter configures the **aes** algorithm with a block size of 128 bits. This is the mandatory impelmentation size for **aes**.

**aes192 —** This parameter configures the **aes** algorithm with a block size of 192 bits. This is a stronger version of **aes**.

**aes256 —** This parameter configures the **aes** algorithm with a block size of 256 bits. This is the strongest available version of **aes**.

## ike-mode

**Syntax** **ike-mode** {**main** | **aggressive** }
**no ike-mode**

**Context** config>ipsec>ike-policy

**Description** This command specifies one of either two modes of operation. IKE version 1 can support main mode and aggressive mode. The difference lies in the number of messages used to establish the session.

The **no** form of the command removes the mode of operation from the configuration.

**Default** main

**Parameters** **main —** Specifies identity protection for the hosts initiating the IPSec session. This mode takes slightly longer to complete.

**aggresive —** Aggressive mode provides no identity protection but is faster.

## ike-version

**Syntax** **ike-version** [1..2]
**no ike-version**

**Context** config>ipsec>ike-policy

**Description** This command sets the IKE version (1 or 2) that the `ike-policy` will use.

**Default** 1

**Parameters** **1 | 2 —** The version of IKE protocol.

## ipsec-lifetime

**Syntax** **ipsec-lifetime** *ipsec-lifetime*
**no ipsec-lifetime**

**Context** config>ipsec>ike-policy

**Description** This parameter specifies the lifetime of a phase two SA.

The **no** form of the command reverts the *ipsec-lifetime* value to the default.

**Default** 3600 (1 hour)

**Parameters** *ipsec-lifetime* — specifies the lifetime of the phase two IKE key in seconds.

**Values** 60 — 4294967295

## isakmp-lifetime

**Syntax** **isakmp-lifetime** *isakmp-lifetime*
**no isakmp-lifetime**

**Context** config>ipsec>ike-policy

**Description** This command specifies the lifetime of a phase one SA. ISAKMP stands for Internet Security Association and Key Management Protocol

The **no** form of the command reverts the *isakmp-lifetime* value to the default.

**Default** 28800

**Parameters** — Specifies the lifetime of the phase one IKE key in seconds.

**Values** 60 — 4294967295

## match-peer-id-to-cert

**Syntax** [**no**] **match-peer-id-to-cert**

**Context** config>ipsec>ike-policy

**Description** This command enables checking the IKE peer's ID matches the peer's certificate when performing certificate authentication.

## nat-traversal

**Syntax** **nat-traversal** [**force**] [**keep-alive-interval** *keep-alive-interval*] [**force-keep-alive]**
**no nat-traversal**

**Context** config>ipsec>ike-policy

**Description** This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled or in forced mode.

The **no** form of the command reverts the parameters to the default.

**Default** none

**Parameters** **force —** Forces to enable NAT-T.

**keep-alive-interval** *keep-alive-interval* **—** Specifies the keep-alive interval.

**Values** 10 — 3600 seconds

**force-keep-alive —** When specified, the keep-alive does not expire.

## own-auth-method

**Syntax** **own-auth-method** {**psk** | **cert** | **eap-only**}
**no own-auth-method**

**Context** config>ipsec>ike-policy

**Description** This command configures the authentication method used with this IKE policy on its own side.

## pfs

**Syntax** **pfs** [**dh-group** {**1** | **2** | **5**}]
**no pfs**

**Context** config>ipsec>ike-policy

**Description** This command enables perfect forward secrecy on the IPSec tunnel using this policy. PFS provides for a new Diffie-hellman key exchange each time the SA key is renegotiated. After that SA expires, the key is forgotten and another key is generated (if the SA remains up). This means that an attacker who cracks part of the exchange can only read the part that used the key before the key changed. There is no advantage in cracking the other parts if they attacker has already cracked one.

The **no** form of the command disables PFS. If this it turned off during an active SA, when the SA expires and it is time to re-key the session, the original Diffie-hellman primes will be used to generate the new keys.

**Default** 5

**Parameters** **dh-group** {**1** | **2** | **5**} — Specifies which Diffie-hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1:

Group 1: 768 bits
Group 2: 1024 bits
Group 5: 1536 bits

## static-sa

**Syntax** [**no**] **static-sa** *sa-name*

**Context** config>ipsec

**Description** This command configures an IPSec static SA.

## direction

**Syntax** **direction** *ipsec-direction*
**no direction**

**Context** config>ipsec>static-sa

**Description** This command configures the direction for an IPSec manual SA.

The **no** form of the command reverts to the default value.

**Default** bidirectional

**Parameters** *ipsec-direction* — Identifies the direction to which this static SA entry can be applied.

**Values** inbound,outbound, bidirectional

## protocol

**Syntax** **protocol** *ipsec-protocol*
**no protocol**

**Context** config>ipsec>static-sa

**Description** This command configures the security protocol to use for an IPSec manual SA. The **no** statement resets to the default value.

**Parameters** *ipsec-protocol* — Identifies the IPSec protocol used with this static SA.

**Values** ah — Specifies the Authentication Header protocol.
esp — Specifies the Encapsulation Security Payload protocol.

**Default** esp

## authentication

**Syntax** **authentication** *auth-algorithm* **ascii-key** *ascii-string*
**authentication** *auth-algorithm* **hex-key** *hex-string* [**hash**|**hash2**]
**no authentication**

**Context** config>ipsec>static-sa

**Description** This command configures the authentication algorithm to use for an IPSec manual SA.

The **no** form of the command reverts to the default value.

**Default** sha1

**Parameters** *ascii-key* — Specifies an ASCII key.

*hex-key* — Specifies a HEX key.

## spi

**Syntax** **spi** *spi*
**no spi**

**Context** config>ipsec>static-sa

**Description** This command configures the SPI key value for an IPSec manual SA.

This command specifies the SPI (Security Parameter Index) used to lookup the instruction to verify and decrypt the incoming IPSec packets when the value of the **direction** command is **inbound**.

The SPI value specifies the SPI that will be used in the encoding of the outgoing packets when the when the value of the **direction** command is **outbound**. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

If **no spi** is selected, then this static SA cannot be used.

The **no** form of the command reverts to the default value.

**Default** none

**Parameters** *spi* — Specifies the security parameter index for this SA.

**Values** 256..16383

## ipsec-transform

**Syntax** **ipsec-transform** *transform-id* [**create**]

**Context** config>ipsec

**Description** This command enables the context to create an ipsec-transform policy. IPSec transforms policies can be shared. A change to the ipsec-transform is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

IPSec transform policy assignments to a tunnel require the tunnel to be shutdown.

The **no** form of the command removes the ID from the configuration.

**Parameters** *transform-id* — Specifies a policy ID value to identify the IPSec transform policy.

**Values** 1 — 2048

**create —** Keyword that

**create —** This keyword is mandatory when creating an ipsec-transform policy. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## esp-auth-algorithm

**Syntax** **esp-auth-algorithm** {**null** | **md5** | **sha1** | **sha256** | **sha384** | **sha512**}}
**no esp-auth-algorithm**

**Context** config>ipsec>transform

**Description** The command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a manually configured tunnel must share the same configuration parameters for the IPSec tunnel to enter the operational state.

The **no** form of the command disables the authentication.

**Parameters** **null —** This is a very fast algorithm specified in RFC 2410, which provides no authentication.

**md5 —** This parameter configures ESP to use the **hmac-md5** algorithm for authentication.

**sha1 —** This parameter configures ESP to use the **hmac-sha1** algorithm for authentication.

**sha256 —** This parameter configures ESP to use the sha256 algorithm for authentication.

**sha384 —** This parameter configures ESP to use the sha384 algorithm for authentication.

**sha512 —** This parameter configures ESP to use the sha512 algorithm for authentication.

## esp-encryption-algorithm

**Syntax** **esp-encryption-algorithm** {**null** | **des** | **3des** | **aes128** | **aes192** | **aes256**}
**no esp-encryption-algorithm**

**Context** config>ipsec>transform

**Description** This command specifies the encryption algorithm to use for the IPSec session. Encryption only applies to esp configurations. If encryption is not defined esp will not be used.

For IPSec tunnels to come up, both ends need to be configured with the same encryption algorithm.

The **no** form of the command removes the

**Default** aes128

**Parameters** **null —** This parameter configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.

**des —** This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

**3des —** This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make things more secure.

**aes128 —** This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory impelmentation size for aes. As of today, this is a very strong algorithm choice.

**aes192 —** This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

**aes256 —** This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

## tunnel-template

**Syntax** **tunnel-template** *ipsec template identifier* [**create**]
**no tunnel-template** *ipsec template identifier*

**Context** config>ipsec

**Description** This command creates a tunnel template. Up to 2,000 templates are allowed.

**Default** none

**Parameters** *ipsec template identifier* — Specifies the template identifier.

**Values** 1 — 2048

**create —** Mandatory keyword used when creating a tunnel-template in the IPSec context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## replay-window

**Syntax** **replay-window** {**32** | **64** | **128** | **256** | **512**}
**no replay-window**

**Context** config>ipsec>tnl-temp

**Description** This command sets the anti-replay window.

The **no** form of the command removes the parameter from the configuration.

**Default** no replay-window

**Parameters** {32 | 64 | 128 | 256 | 512} — Specifies the size of the anti-replay window.

## sp-reverse-route

**Syntax** [**no**] **sp-reverse-route**

**Context** config>ipsec>tnl-temp

**Description** This command specifies whether the node using this template will accept framed-routes sent by the RADIUS server and install them for the lifetime of the tunnel as managed routes.

The **no** form of the command disables sp-reverse-route.

**Default** no sp-reverse-route

## transform

**Syntax** **transform** *transform-id* [*transform-id*...(up to 4 max)]
**no transform**

**Context** config>ipsec>tnl-temp
config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command configures IPSec transform.

# IPSec Configuration Commands

## ipsec

**Syntax** **ipsec**

**Context** config>service>vprn>ipsec

**Description** This command enables the context to configure IPSec policies.

**Default** none

## security-policy

**security-policy** *security-policy-id* [**create**]
**no security-policy** *security-policy-id*

**Context** config>service>vprn>ipsec

**Description** This command configures a security policy to use for an IPSec tunnel.

**Default** none

**Parameters** *security-policy-id* — specifies a value to be assigned to a security policy.

**Values** 1 — 8192

**create —** Keyword used to create the security policy instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## entry

**Syntax** **entry** *entry-id* [**create**]
**no entry** *entry-id*

**Context** config>service>vprn>ipsec>sec-plcy

**Description** This command configures an IPSec security policy entry.

**Parameters** *entry-id* — Specifies the IPSec security policy entry.

**Values** 1 — 16

**create —** Keyword used to create the security policy entry instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## local-ip

**Syntax** **local-ip** {*ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

**Context** config>service>vprn>ipsec>sec-plcy>entry

**Description** This command configures the local (from the VPN ) IP prefix/mask for the policy parameter entry.

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

**Parameters** *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

**Values** a.b.c.d (host bits must be 0)
prefix-length 1 — 32

*netmask* — The subnet mask in dotted decimal notation.

**any —** keyword to specify that it can be any address.

## remote-ip

**Syntax** **remote-ip** *ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

**Context** config>service>vprn>ipsec>sec-plcy>entry

**Description** This command configures the remote (from the tunnel) IP prefix/mask for the policy parameter entry.

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

**Parameters** *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

**Values** a.b.c.d (host bits must be 0)
prefix-length 1 — 32

*netmask* — The subnet mask in dotted decimal notation.

**any —** keyword to specify that it can be any address.

## cert

**Syntax** **cert** *file-name*
**no cert**

**Context** config>service>ies>if>sap>ipsec-gateway>cert

**Description** This command configures cert with a local file URL used by this SAP IPSec gateway.

**Parameters** *file-name* — Specifies the local file to use in the cert. Specify a file name, 95 characters maximum.

## key

**Syntax** **key** *file-name*
**no cert**

**Context** config>service>ies>if>sap>ipsec-gateway>cert

**Description** This command configures a key with the CA profile used by this SAP IPSec gateway.

**Parameters** *file-name* — Specifies the file to use in the key. Specify a file name, 95 characters maximum.

## dynamic-tunnel-redundant-next-hop

**Syntax** **dynamic-tunnel-redundant-next-hop** *ip-address*
**no dynamic-tunnel-redundant-next-hop**

**Context** config>service>ies>if
config>service>vprn>if

**Description** This command configures the dynamic ISA tunnel redundant next-hop address.

**Default** no dynamic-tunnel-redundant-next-hop

**Parameters** *ip-address* — Specifies the IP address of the next hop.

## static-tunnel-redundant-next-hop

**Syntax** **static-tunnel-redundant-next-hop** *ip-address*
**no static-tunnel-redundant-next-hop**

**Context** config>service>ies>if
config>service>vprn>if

**Description** This command specifies redundant next-hop address on public or private IPSec interface (with public or private tunnel-sap) for static IPSec tunnel. The specified next-hop address will be used by standby node to shunt IPSec traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

**Default** no static-tunnel-redundant-next-hop

**Parameters** *ip-address* — Specifies the IP address of the next hop.

## interface

**Syntax** **interface** *ip-int-name* [**create**] [**tunnel**]
**no interface** *ip-int-name*

**Context** config>service>vprn

**Description** This command creates a logical IP routing interface for a Virtual Private Routed Network (VPRN). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within VPRN service IDs. The **interface** command can be executed in the context of an VPRN service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for subscriber internet access.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for **config router interface** and **config service vprn interface**. Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

The available IP address space for local subnets and routes is controlled with the **config router service-prefix** command. The **service-prefix** command administers the allowed subnets that can be defined on service IP interfaces. It also controls the prefixes that may be learned or statically defined with the service IP interface as the egress interface. This allows segmenting the IP address space into **config router** and **config service** domains.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All VPRN IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The **no** form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the **no interface** command.

For VPRN services, the IP interface must be shutdown before the SAP on that interface may be removed. VPRN services do not have the **shutdown** command in the SAP CLI context. VPRN service SAPs rely on the interface status to enable and disable them.

**Parameters** *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Values** 1 — 32 characters maximum

**tunnel —** Specifies that the interface is configured as tunnel interface, which could be used to terminate IPSec or GRE tunnels in the private service.

**create —** Keyword used to create the IPSec interface instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## sap

**Syntax** **sap** *sap-id* [**create**]
**no sap** *sap-id*

**Context** config>service>ies>if
config>service>vprn>if

**Description** This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.
Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.
A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command. Channelized TDM ports are always access ports.
If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.

**Default** No SAPs are defined.

**Special Cases** **sap tunnel**-*id*.**private** | **public**:*tag* — This parameter associates a tunnel group SAP with this interface.

This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The "tag" will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 — 4094.

**Parameters** *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Appendix A: Common CLI Command Descriptions on page 811 for command syntax.

*port-id* — Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 61/2/3 specifies port 3 on MDA 2 in slot 61.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

**create —** Keyword used to create a SAP instance.

## ipsec-tunnel

**Syntax** **ipsec-tunnel** *ipsec-tunnel-name* [**create**]
**no ipsec-tunnel** *ipsec-tunnel-name*

**Context** config>service>vprn>if>sap

**Description** This command specifies an IPSec tunnel name. An IPSec client sets up the encrypted tunnel across public network. The 7750-SR IPSec MDA acts as a concentrator gathering, and terminating these IPSec tunnels into an IES or VPRN service. This mechanism allows as service provider to offer a global VPRN service even if node of the VPRN are on an uncontrolled or insecure portion of the network.

**Default** none

**Parameters** *ipsec-tunnel-name* — Specifies an IPSec tunnel name up to 32 characters in length.

**create —** Keyword used to create the IPSec tunnel instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

## bfd-designate

**Syntax** [**no**] **bfd-designate**

**Context** config>service>vprn>if>sap>ipsec-tunnel

**Description** This command specifies whether this IPSec tunnel is the BFD designated tunnel.

**Default** none

## bfd-enable

**Syntax** [**no**] **bfd-enable service** *service-id* **interface** *interface-name* **dst-ip** *ip-address*

**Context** config>service>vprn>if>tunnel

**Description** This command assign a BFD session provide heart-beat mechanism for given IPSec tunnel. There can be only one BFD session assigned to any given IPSec tunnel, but there can be multiple IPSec tunnels using same BFD session. BFD control the state of the associated tunnel, if BFD session goes down, system will also bring down the associated non-designated IPSec tunnel.

**Default** none

**Parameters** **service** *service-id* **—** Specifies where the service-id that the BFD session resides.

**interface** *interface-name* **—** Specifies the name of the interface used by the BFD session.

**dst-ip** *ip-address* **—** Specifies the destination address to be used for the BFD session.

## dynamic-keying

**Syntax** [**no**] **dynamic-keying**

**Context** config>service>vprn>if>tunnel

**Description** This command enables dynamic keying for the IPSec tunnel.

**Default** none

## auto-establish

**Syntax** [**no**] **auto-establish**

**Context** config>service>vprn>if>tunnel

**Description** This command specifies whether to attempt to establish a phase 1 exchange automatically.

The **no** form of the command disables the automatic attempts to establish a phase 1 exchange.

**Default** no auto-establish

## transform

**Syntax** **transform** *transform-id* [*transform-id*...(up to 4 max)]
**no transform**

**Context** config>service>vprn>if>tunnel>dynamic-keying

**Description** This command associates the IPSec transform sets allowed for this tunnel. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).

**Default** none

**Parameters** *transform-id* — Specifies the value used for transforms for dynamic keying.

**Values** 1 — 2048

## local-gateway-address

**Syntax** **local-gateway-address** *ip-address* **peer** *ip-address* **delivery-service** *service-id*
**no local-gateway-address**

**Context** config>service>vprn>if>tunnel

**Description** This command specifies the local gateway address used for the tunnel and the address of the remote security gateway at the other end of the tunnelremote peer IP address to use.

**Default** The base routing context is used if the delivery-router option is not specified.

**Parameters** *ip-address* — IP address of the local end of the tunnel.

**delivery-service** *service-id* — The ID of the IES or VPRN (front-door) delivery service of this tunnel. Use this service-id to find the VPRN used for delivery.

**Values** *service-id*: 1 — 2147483648
*svc-name:* Specifies an existing service name up to 64 characters in length.

## manual-keying

**Syntax** **[no] manual-keying**

**Context** config>service>vprn>if>tunnel
config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command configures Security Association (SA) for manual keying. When enabled, the command specifies whether this SA entry is created manually by the user or dynamically by the IPSec sub-system.

**Default** none

## security-association

**Syntax** **security-association** *security-entry-id* **authentication-key** *authentication-key* **encryption-key** *encryption-key* **spi** *spi* **transform** *transform-id* **direction** {**inbound** | **outbound**}
**no security-association** *security-entry-id* **direction** {**inbound** | **outbound**}

**Context** config>service>vprn>if>tunnel>manual-keying
config>service>ies>if>sap>ipsec-gateway>manual-keying
config>service>vprn>if>sap>ipsec-gateway>manual-keying

**Description** This command configures the information required for manual keying SA creation.

**Default** none

**Parameters** *security-entry-id* — Specifies the ID of an SA entry.

**Values** 1 — 16

**encryption-key** *encryption-key* — specifies the key used for the encryption algorithm.

**Values** none or 0x0..0xFFFFFFFF...(max 64 hex nibbles)

**authentication-key** *authentication-key* —

**Values** none or 0x0..0xFFFFFFFF...(max 40 hex nibbles)

**spi** *spi* — Specifies the SPI (Security Parameter Index) used to look up the instruction to verify and decrypt the incoming IPSec packets when the direction is inbound. When the direction is outbound, the SPI that will be used in the encoding of the outgoing packets. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

**Values** 256 — 16383

**transform** *transform-id* — specifies the transform entry that will be used by this SA entry. This object should be specified for all the entries created which are manual SAs. If the value is dynamic, then this value is irrelevant and will be zero.

**Values** 1 — 2048

**direction** {**inbound** | **outbound**} — Specifies the direction of an IPSec tunnel.

## replay-window

**Syntax** **replay-window** {**32** | **64** | **128** | **256** | **512**}
**no replay-window**

**Context** config>service>vprn>if>tunnel>manual keying

**Description** This command specifies the size of the anti-replay window. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet.

**Default** none

**Parameters** {**32** | **64** | **128** | **256** | **512**} — Specifies the size of the SA anti-replay window.

## security-policy

**Syntax** **security-policy** *security-policy-id*
**no security-policy**

**Context** config>service>vprn>ipsec-if>tunnel

**Description** This command configures an IPSec security policy. The policy may then be associated with tunnels defined in the same context.

**Default** none

**Parameters** *security-policy-id* — Specifies the IPSec security policy entry that the tunnel will use.

**Values** 1 — 8192

# Interface SAP Tunnel Commands

## ip-tunnel

**Syntax** **ip-tunnel** *ip-tunnel-name* **[create]**
**no ip-tunnel** *ip-tunnel-name*

**Context** config>service>ies>sap
config>service>vprn>sap

**Description** This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service.

The **no** form of the command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the **no ip-tunnel** command.

**Default** no IP tunnels are defined.

**Parameters** *ip-tunnel-name* — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

## source

**Syntax** **source** *ip-address*
**no source**

**Context** config>service>interface>ies>sap
config>service>interface>vprn>sap>gre-tunnel

**Description** This command sets the source IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. It must be an address in the subnet of the associated public tunnel SAP interface. The GRE tunnel does not come up until a valid source address is configured.

The **no** form of the command deletes the source address from the GRE tunnel configuration. The tunnel must be administratively shutdown before issuing the **no source** command.

**Parameters** *ip-address* — Specifies the source IPv4 address of the GRE tunnel.

**Values** 1.0.0.0 — 223.255.255.255

## remote-ip

**Syntax** **remote-ip** *ip-address*
**no remote-ip**

**Context** config>service>interface>ies>sap

config>service>interface>vprn>sap>gre-tunnel

**Description** This command sets the primary destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The **no** form of the command deletes the destination address from the GRE tunnel configuration.

**Parameters** *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

**Values** 1.0.0.0 — 223.255.255.255

## backup-remote-ip

**Syntax** **backup-remote-ip** *ip-address*
**no backup-remote-ip**

**Context** config>service>interface>ies>sap>gre-tunnel
config>service>interface>vprn>sap>gre-tunnel

**Description** This command sets the backup destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If the primary destination address is not reachable in the delivery service (there is no route) or not defined then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The **no** form of the command deletes the backup-destination address from the GRE tunnel configuration.

**Parameters** *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

**Values** 1.0.0.0 — 223.255.255.255

## clear-df-bit

**Syntax** [**no**] **clear-df-bit**

**Context** config>service>vprn>interface>sap>ipsec-tunnel
config>service>vprn>interface>sap>gre-tunnel
config>service>ies>interface>sap>gre-tunnel

**Description** This command instructs the MS-ISA to reset the DF bit to 0 in all payload IP packets associated with the GRE or IPSec tunnel, before any potential fragmentation resulting from the **ip-mtu** command. (This will require a modification of the header checksum.) The no clear-df-bit command, corresponding to the default behavior, leaves the DF bit unchanged.

The **no** form of the command disables the DF bit reset.

**Default** none

## delivery-service

**Syntax** **delivery-service** {*service-id* | *svc-name*}
**no delivery-service**

**Context** config>service>interface>ies>sap>delivery-service
config>service>interface>vprn>sap>gre-tunnel

**Description** This command sets the delivery service for GRE encapsulated packets associated with a particular GRE tunnel. This is the IES or VPRN service where the GRE encapsulated packets are injected and terminated. The delivery service may be the same service that owns the private tunnel SAP associated with the GRE tunnel. The GRE tunnel does not come up until a valid delivery service is configured.

The **no** form of the command deletes the delivery-service from the GRE tunnel configuration.

**Parameters** *service-id* — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

**Values** 1—2147483648

*svc-name* — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

**Values** 1—64 characters

## dscp

**Syntax** **dscp** *dscp-name*
**no dscp**

**Context** config>service>interface>ies>sap
config>service>interface>vprn>sap>gre-tunnel

**Description** This command sets the DSCP code-point in the outer IP header of GRE encapsulated packets associated with a particular GRE tunnel. The default, set using the no form of the command, is to copy the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.

**Default** no dscp

**Parameters** *dscp* — Specifies the DSCP code-point to be used.

**Values** be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

## dest-ip

**Syntax** **dest-ip** *ip-address*

**Context** config>service>ies>sap>ip-tunnel
config>service>vprn>sap>ip-tunnel

**Description** This command configures the private address of the remote tunnel endpoint. The configuration of this address is mandatory in the configuration of every IP-IP or IP-GRE tunnel.

**Note:** Unnumbered interfaces are not supported.

**Default** No default

**Parameters** *ip-address* — Specifies the private IP address of the remote IP tunnel endpoint. If this remote IP address is not within the subnet of the IP interface associated with the tunnel then the tunnel will not come up.

## gre-header

**Syntax** **[no] gre-header**

**Context** config>service>ies>sap>ip-tunnel
config>service>vprn>sap>ip-tunnel

**Description** This command configures the type of the IP tunnel. If the gre-header command is configured then the tunnel is a GRE tunnel with a GRE header inserted between the outer and inner IP headers. If the **no** form of the command is configured then the tunnel is a simple IP-IP tunnel.

**Default** no gre-header

## ip-mtu

**Syntax** **ip-mtu** *octets*
**no ip-mtu**

**Context** config>service>ies>if>sap>gre-tunnel
config>service>vprn>if>sap>gre-tunnel
config>service>vprn>if>sap>ipsec-tunnel

**Description** This command configures the IP maximum transmit unit (packet) for this interface.

Note that because this connects a Layer 2 to a Layer 3 service, this parameter can be adjusted under the IES interface.

The MTU that is advertized from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for ethernet network interface) if no ip-mtu is configured it is (1568 - 14) = 1554.

The **ip-mtu** command instructs the MS-ISA to perform IP packet fragmentation, prior to IPSec encryption and encapsulation, based on the configured MTU value. In particular:

- If the length of a payload IP packet (including its header) exceeds the configured MTU value and the DF flag is clear (due to the presence of the clear-df-bit command or because the original DF value was 0) then the MS-ISA fragments the payload packet as efficiently as possible (i.e. it creates the minimum number of fragments each less than or equal to the configured MTU size); in each created fragment the DF bit shall be 0.

If the length of a payload IP packet (including its header) exceeds the configured MTU value and the

DF flag is set (because the original DF value was 1 and the tunnel has no clear-df-bit in its configuration) then the MS-ISA discards the payload packet without sending an ICMP type 3/code 4 message back to the packet's source address.

The **no ip-mtu** command, corresponding to the default behavior, disables fragmentation of IP packets by the MS-ISA; all IP packets, regardless of size or DF bit setting, are allowed into the tunnel.

Note that the effective MTU for packets entering a tunnel is the minimum of the private tunnel SAP interface IP MTU value (used by the IOM) and the tunnel IP MTU value (configured using the above command and used by the MS-ISA). So if it desired to fragment IP packets larger than X bytes with DF set, rather than discarding them, the tunnel IP MTU should be set to X and the private tunnel SAP interface IP MTU should be set to a value larger than X.

**Default** no ip-mtu

## reassembly

**Syntax** **reassembly** [*wait-msecs*]
**no reassembly**

**Context** config>service>ies>if>sap

**Description** This command configures the reassembly wait time.

# IPSec Gateway Commands

## ipsec-gw

**Syntax** [**no**] **ipsec-gw**

**Context** config>service>ies>if>sap
config>service>vprn>if>sap

**Description** This command configures an IPSec gateway.

## default-secure-service

**Syntax** **default-secure-service** *service-id* **ipsec-interface** *ip-int-name*
**no default-secure-service**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command specifies a service ID or service name of the default security service used by this SAP IPSec gateway.

**Parameters** *service-id* — Specifies a default secure service.

**Values** *service-id*: 1 — 2147483648
*svc-name:* An existing service name up to 64 characters in length.

## default-tunnel-template

**Syntax** **default-tunnel-template** *ipsec template identifier*
**no default-tunnel-template**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command configures a default tunnel policy template for the gateway.

## ike-policy

**Syntax** **ike-policy** *ike-policy-id*
**no ike-policy**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command configures IKE policy for the gateway.

**Parameters** *ike-policy-id* — Specifies the IKE policy ID.

**Values** 1 — 2048

## local-gateway-address

**Syntax** **local-gateway-address** *ip-address*
**no local-gateway-address**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command configures an ipsec-gateway local address.

## local-id

**Syntax** **local-id type** {**ipv4** | **fqdn**} [**value** [*255 chars max*]]
**no local-id**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway
service>vprn>if>sap>ipsec-tunnel

**Description** This command specifies the local ID for 7750 SRs used for IDi or IDr for IKEv2 tunnels.

The **no** form of the command removes the parameters from the configuration.

**Default** Depends on local-auth-method like following:

- Psk:local tunnel ip address
- Cert-auth: subject of the local certificate

**Parameters** **type —** Specifies the type of local ID payload, it could be ipv4 address/FQDN domain name, distinguish name of subject in X.509 certificate.

**ipv4 —** Specifies to use ipv4 as the local ID type, the default value is the local tunnel end-point address.

*value* — Specifies to use FQDN as the local ID type. The value must be configured.

## pre-shared-key

**Syntax** **pre-shared-key** *key*
**no pre-shared-key**

**Context** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

**Description** This command specifies the shared secret between the two peers forming the tunnel.

**Parameters** *key* — Specifies a pre-shared-key for dynamic-keying.

## cert

**Syntax** **cert**

**Context** config>service>ies>if>sap>ipsec-tunnel

**Description** This command configures cert parameters used by this SAP IPSec gateway.

## cert

**Syntax** [**no**] **cert local-file-url**

**Default** config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-tun>dynamic-keying>cert
config>svc>vprn>if>sap>ipsec-gw>cert>

**Description** This command specifies the certificate that 7750 used to identify itself in case peer need it. 7750 will load (reload) the certificate from the configured URL when the ipsec-tunnel/ipsec-gw is "no shutdown".

When system is loading the certificate, it will check if it is a valid X.509v3 certificate by performing following:

- **key** file must be already configured
- Configured cert file must be a DER formatted X.509v3 certificate file
- All non-optional fields defined in section 4.1 of RFC5280 must exist in the cert-file and conform to the RFC5280 defined format.
- The version field to see if its value is 0x2
- The Validity field to see that if the certificate is still in validity period.
- If Key Usage extension exists, then At least digitalSignature and keyEncipherment shall be set;
- The public key of the certificate can match with the public key in the configured key file.

If any of above checks fails, then the "no shutdown" command will fails

Configured certificate file url can only be changed or removed when tunnel or gw is shutdown.

Same certificate could be used for multiple ipsec-tunnels or ipsec-gws, however for each certificate file, there is only one memory instance, if a certificate file has been updated, "no shutdown" in any of tunnel that use the certificate file will cause the memory instance updated, which will not impact the current up and running tunnels that use the certificate file, but the new authentication afterwards will use the updated memory instance.

**Default** None

**Parameters** *local-file-url* — URL for input file, this url is local CF card URL.

## key

**Syntax** [**no**] **key local-file-url**

**Context** config>service>vprn>if>sap>ipsec-tun>dynamic-keying>cert
config>svc>vprn>if>sap>ipsec-gw>cert
config>service>ies>if>sap>ipsec-gateway>cert

**Description** This command specifies the key pair file 7750 will use for X.509 certificate authentication. System will load the key file when the ipsec-tunnel/gw is "no shutdown"

When system is loading the key file, it will check if it is a valid 7750 formatted key file.

Key file url can only be changed or removed when tunnel or gw is shutdown.

Same key could be used for multiple ipsec-tunnels or ipsec-gws, however for each key file, there is only one memory instance, if a key file has been updated, "no shutdown" in any of tunnel that use the key file will cause the memory instance updated, which will not impact the current up and running tunnels that use the key file, but the new authentication afterwards will use the updated memory instance.

**Default** None

**Parameters** *local-file-url* — URL for input file, this url is local CF card URL.

## status-verify

**Syntax** **status-verify**

**Context** config>service>ies>if>sap>ipsec-gw>cert
config>service>vprn>if>sap>ipsec-gw>cert
config>service>vprn>if>sap>ipsec-tun>dyn>cert

**Description** This command enables the context to configure certificate recovation status verification parameters.

**Default** none

## default-result

**Syntax** **default-result** {**revoked**|**good**}
**no default-result**

**Context** config>service>ies>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-tun>dyn>cert>>cert-status-verify

**Description** This command specifies the default result when both primary and secondary method failed to provide an answer.

**Default** default-result revoked

**Parameters** **good —** Specifies thatthe certificate is considered as good.

**revoked —** Specifies that the certificate is considered as revoked.

## primary

**Syntax** **primary** {**ocsp**|**crl**}
**no primary**

**Context** config>service>ies>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-tun>dyn>cert>cert-status-verify

**Description** This command specifies the primary method that used to verify revocation status of the peer's certificate; could be either CRL or OCSP

OCSP or CRL will use the corresponding configuration in the ca-profile of the issuer of the certificate in question.

**Default** primary crl

**Parameters** **ocsp —** Specifies to use the OCSP protocol. The OCSP server is configured in the corresponding ca-profile.

**crl —** Specifies to use the local CRL file The CRL file is configured in the corresponding ca-profile

## secondary

**Syntax** **secondary** {**ocsp**|**crl**}
**no secondary**

**Context** config>service>ies>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-gw>cert>cert-status-verify
config>service>vprn>if>sap>ipsec-tun>dyn>cert>cert-status-verify

**Description** This command specifies the secondary method that used to verify revocation status of the peer's certificate; could be either CRL or OCSP.

OCSP or CRL will use the corresponding configuration in the ca-profile of the issuer of the certificate in question.

secondary method will only be used when the primary method failed to provide an answer:

- OCSP — unreachable / any answer other than "good" or "revoked" / ocsp is NOT configured in ca-profile/ OCSP response is not signed/Invalid nextUpdate
- CRL: CRL expired

**Default** no secondary

**Parameters** **ocsp —** Specifies to use the OCSP protocol, the OCSP server is configured in the corresponding ca-profile.

**crl —** Specifies to use the local CRL file, the CRL file is configured in the corresponding ca-profile

## auto-establish

**Syntax** [**no**] **auto-establish**

**Context** config>service>vprn>if>sap>ipsec-tun>dynamic-keyig

**Description** The system will automatically establish phase 1 SA as soon as the tunnel is provisioned and enabled (**no shutdown**). This option should only be configured on one side of the tunnel.

Note that any associated static routes will remain up as long as the tunnel could be up, even though it may actually be Oper down according to the CLI.

**Default** None

## trust-anchor

**Syntax** **trust-anchor** *ca-profile-name*
**no trust-anchor**

**Context** config>service>ies>if>sap>ipsec-gateway>cert

**Description** This command configures trust anchor with a CA profile used by this SAP IPSec gateway.

**Parameters** *ca-profile-name* — Specifies the CA profile to use in the trust anchor. Specify a file name, 95 characters maximum.

# IPSec Mastership Election Commands

## multi-chassis

**Syntax** **multi-chassis**

**Context** config>redundancy

**Description** Thiis command enables the context to configure multi-chassis parameters.

## peer

**Syntax** **peer** *ip-address* [**create**]
**no peer** *ip-address*

**Context** config>redundancy

**Description** This command configures a multi-chassis redundancy peer.

**Parameters** *ip-address* — Specifies the peer address.

**create —** Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled/disabled in the **environment>create** context.

## mc-ipsec

**Syntax** [**no**] **mc-ipsec**

**Context** config>redundancy>multi-chassis>peer

**Description** This command enables the context to configure multi-chassis peer parameters.

## bfd-enable

**Syntax** [**no**] **bfd-enable**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec

**Description** This command enables tracking a central BFD session, if the BFD session goes down, then system consider the peer is down and change the mc-ipsec status of configured tunnel-group accordingly.

The BFD session uses specified the loopback interface (in the specified service) address as the source address and uses specified dst-ip as the destination address. Other BFD parameters are configured with the **bfd** command on the specified interface.

**Default** 300

## discovery-interval

**Syntax** **discovery-interval** *interval-secs* [**boot** *interval-secs*]
**no discovery-interval**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec

**Description** This command specifies the time interval of tunnel-group stays in "Discovery" state. Interval-1 is used as discovery-interval when a new tunnel-group is added to multi-chassis redundancy (mp-ipsec); interval-2 is used as discovery-interval when system boot-up, it is optional, when it is not specified, the interval-1 will be used.

**Default** 300

**Parameters** *interval-secs* — Specifies the maximum duration, in seconds, of the discovery interval during which a newly activated multi- chassis IPsec tunnel-group will remain dormant while trying to contact its redundant peer. Groups held dormant in this manner will neither pass traffic nor negotiate security keys. This interval ends when either the redundant peer is contacted and a master election occurs, or when the maximum duration expires.

**Values** 1 — 1800

**boot** *interval-secs* **—** Specifies the maximum duration of an interval immediately following system boot up. When the normal discovery interval for a group would expire while the post-boot discovery interval is still active, then the group's discovery interval is extended until the post-boot discovery interval expires. This allows an extension to the normal discovery stage of groups following a chassis reboot, to account for the larger variance in routing

## hold-on-neighbor-failure

**Syntax** **hold-on-neighbor-failure** *multiplier*
**no hold-on-neighbor-failure**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec

**Description** This command specifies the number of keep-alive failure before consider the peer is down.

The **no** form of the command reverts to the default.

**Default** 3

**Parameters** *multiplier* — Specifies the hold time applied on neighbor failure

**Values** 2 — 25

## keep-alive-interval

**Syntax** **keep-alive-interval** *interval*
**no keep-alive-interval**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec

**Description** This command specifies the time interval of mastership election protocol sending keep-alive packet.

The **no** form of the command reverts to the default.

**Default** 10

**Parameters** *interval* — Specifies the keep alive interval in tenths of seconds.

**Values** 5 — 500

## tunnel-group

**Syntax** **tunnel-group** *tunnel-group-id* [**create**]
**no tunnel-group** *tunnel-group-id*

**Context** config>redundancy>multi-chassis>peer>mc-ipsec

**Description** This command enables multi-chassis redundancy for specified tunnel-group; or enters an already configured tunnel-group context. The configured tunnel-group could failover independently.

The **no** form of the command removes the tunnel group ID from the configuration.

**Default** none

**Parameters** *tunnel-group-id* — Specifies the tunnel-group identifier.

**Values** 1 — 16

## peer-group

**Syntax** **peer-group** *tunnel-group-id*
**no peer-group**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group

**Description** This command specifies the corresponding tunnel-group id on peer node. The peer tunnel-group id does not necessary equals to local tunnel-group id.

The **no** form of the command removes the tunnel group ID from the configuration.

**Default** none

**Parameters** *tunnel-group-id* — Specifies the tunnel-group identifier.

**Values** 1 — 16

## priority

**Syntax** **priority** *priority*
**no priority**

**Context** config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group

**Description** This command specifies the local priority of the tunnel-group, this is used to elect master, higher number win. If priority are same, then the peer has more active ISA win; and priority and the number of active ISA are same, then the peer with higher IP address win.

The **no** form of the command removes the priority value from the configuration.

**Default** 100

**Parameters** *priority* — Specifies the priority of this tunnel-group.

**Values** 0 — 255

## protocol

**Syntax** **protocol** {*protocol*} [**all** | **instance** *instance*]
**no protocol**

**Context** config>router>policy-options>policy-statement>entry>to

**Description** This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending how it is used.

When the **ipsec** is specified this means IPSecroutes.

If no protocol criterion is specified, any protocol is considered a match.

The **no** form of the command removes the protocol match criterion.

**Default** **no protocol** — Matches any protocol.

**Parameters** **protocol —** The protocol name to match on.

**Values** direct, static, bgp, isis, ospf, rip, aggregate, bgp-vpn, igmp, pim, ospf3, ldp, sub-mgmt, mld, managed, vpn-leak, tms, nat, periodic, **ipsec**, mpls

**instance —** The OSPF or IS-IS instance.

**Values** 1 — 31

**all —** OSPF- or ISIS-only keyword.

## state

**Syntax** **state** *state*
**no state**

**Context** config>router>policy-options>policy-statement>entry>from

**Description** This command will configure a match criteria on the state attribute. The state attribute carries the state of an SRRP instance and it can be applied to:

- subscriber-interface routes
- subscriber-management routes (/32 IPv4 and IPv6 PD wan-host)
- managed-routes (applicable only to IPv4).

Based on the state attribute of the route we can manipulate the route advertisement into the network.

We can enable or disable (in case there is no SRRP running) tracking of SRRP state by routes.

This is done on a per subscriber-interface route basis, where a subscriber-interface route is tracking a single SRRP instance state (SRRP instance might be in a Fate Sharing Group).

For subscriber-management and managed-routes, tracking is enabled per group interface under which SRRP is enabled.

**Default** **none**

**Description** This command specifies a multicast data source address as a match criterion for this entry.

**Parameters** **srrp-master —** Track routes with the state attribute carrying srrp-master state.

**srrp-non-master —** Track routes with the state attribute carrying srrp-non-master state.

**ipsec-master-with-peer —** Track routes with the state attribute carrying ipsec-master-with-peer state.

**ipsec-non-master —** Track routes with the state attribute carrying ipsec-non-master state.

**ipsec-master-without-peer —** Track routes with the state attribute carrying ipsec-master-without-peer state.

## tunnel-group

**Syntax** **tunnel-group** *tunnel-group-id* **sync-tag** *tag-name* [**create**]
**no tunnel-group**

**Context** config>redundancy>multi-chassis>peer>sync

**Description** This command enables multi-chassis synchronization of IPsec states of specified tunnel-group with peer. sync-tag is used to match corresponding tunnel-group on both peers. IPsec states will be synchronized between tunnel-group with same sync-tag.

**Default** no

**Parameters** *tunnel-group-id* — Specifies the id of the tunnel-group

*tag-name* — Specifies the name of the sync-tag.

## ipsec

**Syntax** [**no**] **ipsec**

**Context** config>redundancy>multi-chassis>peer>sync

**Description** This command enables multi-chassis synchronization of IPsec states on system level.

**Default** no

## ipsec-responder-only

**Syntax** [**no**] **ipsec-responder-only**

**Context** config>isa>tunnel-group

**Description** With this command configured, system will only act as IKE responder except for the automatic CHILD_SA rekey upon MC-IPsec switchover.

**Default** no

# Show Commands

## gateway

**Syntax** **gateway name** *name*
**gateway** [**service** *service-id*]
**gateway tunnel** [*ip-address:port*]
**gateway name** *name* **tunnel** *ip-address:port*
**gateway name** *name* **tunnel**
**gateway tunnel count**

**Context** show>ipsec

**Description** This command displays IPSec gateway information.

**Parameters** **name** *name* **—** Specifies an IPSec gateway name.

**service** *service-id* **—** specifies the service ID of the default security service used by the IPSec gateway.

**Values** 1 — 214748364
svc-name: 64 char max

**tunnel** *ip-address:port* **—** Specifies to display the IP address and UDP port of the SAP IPSec gateway to the tunnel.

**Values** port: 0— 65535

**count —** Specifies to display the number of IPSec gateway tunnels with the **ike-policy>auth-method** command set to **psk**.

## tunnel

**Syntax** **tunnel** [*gre-tunnel-name*]

**Context** show>gre

**Description** This command displays information about a particular GRE tunnel or all GRE tunnels.

**Parameters** *gre-tunnel-name* — Specifies the name of a GRE tunnel.

The following table lists the information displayed for each GRE tunnel.

| Label | Description |
|---|---|
| TunnelName (Tunnel Name) | The name of the GRE tunnel. |
| SvcID (Service ID) | The service ID of the IES or VPRN service that owns the GRE tunnel. |
| SapId (Sap ID) | The ID of the private tunnel SAP that owns the GRE tunnel. |

| Label | Description (Continued) |
|---|---|
| Description | The description for the GRE tunnel. |
| LocalAddress (Source Address) | The source address of the GRE tunnel (public/outer IP) |
| RemoteAddress (Remote Address) | The destination address of the GRE tunnel (public/outer IP) |
| Bkup RemAddr (Backup Address) | The backup destination address of the GRE tunnel (public/outer IP) |
| To (Target Address) | The remote address of the GRE tunnel (private/inner IP). This is the peer's IP address to the GRE tunnel. This comes from the tunnel configuration. |
| DlvrySvcId (Delivery Service) | The service ID of the IES or VPRN service that handles the GRE encapsulated packets belonging to the tunnel. |
| DSCP | The forced DSCP codepoint in the outer IP healer of GRE encapsulated packets belonging to the tunnel. |
| Admn (Admin State) | Admin state of the tunnel (up/down). |
| Oper (Operational State) | Operational state of the tunnel (up/down). |
| Oper Rem Addr (Oper Remote Addr) | The destination address of the GRE tunnel (public/outer IP) that is currently being used. |
| Pkts Rx | Number of GRE packts received belonging to the tunnel. |
| Pkts Tx | Number of GRE packets transmitted belonging to the tunnel. |
| Bytes Rx | Number of bytes in received GRE packets associated with the tunnel. |
| Bytes Tx | Number of bytes in transmitted GRE packets associated with the tunnel. |
| Key Ignored Rx | Incremented every time a GRE packet is received with a GRE key field. |
| Too Big Tx | Incremented every time an IP packet with DF=1 is to be forwarded into the GRE tunnel and its size exceeds the interface IP MTU. |
| Seq Ignored Rx | Incremented every time a GRE packet is received with a sequence number. |
| Vers Unsup. Rx | Incremented every time a GRE packet is dropped because the GRE version is unsupported. |

| Label | Description (Continued) |
|---|---|
| Invalid Chksum Rx | Incremented every time a GRE packet is dropped because the checksum is invalid. |
| Loops Rx | Incremented eery time a GRE packet is dropped because the destination IP address of the un-encapsulated packet would cause it be re-encapsulated into the same tunnel. |

### Sample Output

```
dut-A# show gre tunnel
===============================================================================
GRE Tunnels
===============================================================================
TunnelName                       LocalAddress     SvcId       Admn
 SapId                            RemoteAddress    DlvrySvcId  Oper
  To                               Bkup RemAddr     DSCP        Oper Rem Addr
-------------------------------------------------------------------------------
toce2                            50.1.1.7         500         Up
 tunnel-1.private:1               30.1.1.3         500         Up
  20.1.1.2                         30.1.2.7         None        30.1.1.3
toce2_backup                     50.1.2.3         502         Up
 tunnel-1.private:3               30.1.1.3         502         Up
  20.1.2.2                         0.0.0.0          None        30.1.1.3
-------------------------------------------------------------------------------
GRE Tunnels: 2
===============================================================================

A:Dut-A# show gre tunnel "toce2"

===============================================================================
GRE Tunnel Configuration Detail
===============================================================================
Service Id       : 500                  Sap Id           : tunnel-1.private:1
Tunnel Name      : toce2
Description      : None
Target Address   : 20.1.1.2             Delivery Service : 500
Admin State      : Up                   Oper State       : Up
Source Address   : 50.1.1.7             Oper Remote Addr : 30.1.1.3
Remote Address   : 30.1.1.3             Backup Address   : 30.1.2.7
DSCP             : None
Oper Flags       : None

===============================================================================
GRE Tunnel Statistics: toce2
===============================================================================
Errors Rx        : 0                    Errors Tx        : 0
Pkts Rx          : 165342804            Pkts Tx          : 605753463
Bytes Rx         : 84986201256          Bytes Tx         : 296819196870
Key Ignored Rx   : 0                    Too Big Tx       : 0
Seq Ignored Rx   : 0
Vers Unsup. Rx   : 0
Invalid Chksum Rx: 0
Loops Rx         : 0
===============================================================================
===============================================================================
```

```
A:Dut-A# show gre tunnel count
-------------------------------------------------------------------------------
GRE Tunnels: 2
-------------------------------------------------------------------------------
```

## ike-policy

**Syntax** **ike-policy** *ike-policy-id*
**ike-policy**

**Context** show>ipsec

**Description** This command displays

**Parameters** *ike-policy-id* — Specifies the ID of an IKE policy entry.

**Values** 1 — 2048

**Sample Output**

```
*A:ALA-48# show ipsec ike-policy 10
===============================================================================
IPsec IKE policy Configuration Detail
===============================================================================
Policy Id        : 10                  IKE Mode         : main
DH Group         : Group2              Auth Method      : psk
PFS              : False               PFS DH Group     : Group2
Auth Algorithm   : Sha1                Encr Algorithm   : Aes128
ISAKMP Lifetime  : 86400               IPsec Lifetime   : 3600
NAT Traversal    : Disabled
NAT-T Keep Alive : 0                   Behind NAT Only  : True
DPD              : Disabled
DPD Interval     : 30                  DPD Max Retries  : 3
Description      : (Not Specified)
===============================================================================
*A:ALA-48#
```

## security-policy

**Syntax** **security-policy** *service-id* [*security-policy-id*]
**security-policy**

**Context** show>ipsec

**Description** This command displays

**Parameters** *service-id* — Specifies the service-id of the tunnel delivery service.

**Values** 1 — 214748364
svc-name: 64 char max

*security-policy-id* — Specifies the IPSec security policy entry that this tunnel will use.

**Values** 1 — 8192

**Sample Output**

```
*A:ALA-48>show>ipsec# security-policy 1
===============================================================================
Security Policy Param Entries
===============================================================================
SvcId      Security   Policy     LocalIp            RemoteIp
           PlcyId     ParamsId
-------------------------------------------------------------------------------
1          1          1          0.0.0.0/0          0.0.0.0/0
-------------------------------------------------------------------------------
No. of IPsec Security Policy Param Entries: 1
===============================================================================
*A:ALA-48>show>ipsec#
```

## static-sa

**Syntax** **static-sa**
**static-sa name** *sa-name*
**static-sa spi** *spi*

**Context** show>ipsec

**Description** This command displays IPSec static-SA information.

**Parameters** *sa-name* — Specifies the SA name.

**Values** 32 chars max

*spi* — Specifies the spi.

**Values** 256..16383

## transform

**Syntax** **transform** [*transform-id*]

**Context** show>ipsec

**Description** This command displays IPSec transforms.

**Parameters** *transform-id* — Specifies an IPSec transform entry.

**Values** 1 — 2048

**Sample Output**

```
*A:ALA-48>config>ipsec# show ipsec transform 1
===============================================================
IPsec Transforms
===============================================================
TransformId    EspAuthAlgorithm    EspEncryptionAlgorithm
---------------------------------------------------------------
1              Sha1                Aes128
```

```
-------------------------------------------------------------
No. of IPsec Transforms: 1
=============================================================
*A:ALA-48>config>ipsec#
```

## tunnel

**Syntax** **tunnel** *ipsec-tunnel-name*
**tunnel**

**Context** show>ipsec

**Description** This command displays

**Parameters** *ipsec-tunnel-name* — Specifies the name of the tunnel up to 32 characters in length.

## tunnel-template

**Syntax** **tunnel-template** *[ipsec template identifier]*

**Context** show>ipsec

**Description** This command displays

**Parameters** *ipsec template identifier* — Displays an existing IPSec tunnel template ID.

**Values** 1 — 2048

**Sample Output**

```
*A:ALA-48>config>ipsec# show ipsec tunnel-template 1
===============================================================================
IPSec Tunnel Template
===============================================================================
Id      Trnsfrm1  Trnsfrm2  Trnsfrm3  Trnsfrm4  ReverseRoute      ReplayWnd
-------------------------------------------------------------------------------
1       1         none      none      none      useSecurityPolicy 128
-------------------------------------------------------------------------------
Number of templates: 1
===============================================================================
*A:ALA-48>config>ipsec#
```

## mc-ipsec

**Syntax** **mc-ipsec peer** *ip-address* **tunnel-group** *tunnel-group-id*
**mc-ipsec peer** *ip-address*

**Context** show>redundancy>multi-chassis

**Description** This command displays the IPSec multi-chassis states. Optionally, only state of specified tunnel-group will be displayed.

**Parameters** *ip-address* — Specifies the peer address.

*tunnel-group-id* — Specifies the tunnel-group.

**Output** **Show MC-IPSec Peer Command Output —** The following table describes show redundancy multi-chassis mc-ipsec output fields.

| Label | Description |
|---|---|
| Admin State | Displays the admin state of mc-ipsec. |
| Mastership/Master State | Displays the current MIMP state. |
| Protection Status | Displays **nominal** or **notReady**.<br>**notReady** means the system is not ready for a switchover. There could be major traffic impact if switchover happens in case of notReady.<br>**nominal** means the tunnel-group is in a better situation to switchover than notReady. However there still might be traffic impact. |
| Installed | Displays the number of tunnels that has been successfully installed on MS-ISA |
| Installing | Displays the number of tunnels that are being installed on MS-ISA. |
| Awaiting Config | Displays the number of synced tunnels that do not have corresponding configuration ready |
| Failed | Displays the number of tunnels that have been failed to installed on MS-ISA. |

### Sample Output

```
show redundancy multi-chassis mc-ipsec peer 2.2.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 2.2.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Disable
Last update     : 09/27/2012 00:44:23

=========================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
=========================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------
1              2              100       Up             standby
-------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
=========================================================================


show redundancy multi-chassis mc-ipsec peer 2.2.2.2 tunnel-group 1
===============================================================================
```

```
Multi-Chassis MC-IPsec Multi Active Tunnel-Group: 1
===============================================================================
Peer Ex Tnl Grp : 2                  Priority             : 100
Master State    : standby            Protection Status    : nominal
Admin State     : Up                 Oper State           : Up
===============================================================================
===============================================================================
Multi-Chassis Tunnel Statistics
===============================================================================
                              Static              Dynamic
-------------------------------------------------------------------------------
Installed                     1                   0
Installing                    0                   0
Awaiting Config               0                   0
Failed                        0                   0
===============================================================================
```

# Debug Commands

## gateway

**Syntax** [**no**] **gateway name** *name* **tunnel** *ip-address*[:*port*]

**Context** debug>ipsec

**Description** This command enables debugging for specified IPSec tunnel terminated on specified ipsec-gw.

Note that only one IPSec tunnel is allowed to enable debugging at a time.

**Parameters** **name** *name* **—** Specifies the name of ipsec-gw.

**tunnel** *ip-address* **—** The tunnel IP address of remote peer.

*port* — The remote UDP port of IKE.

## tunnel

**Syntax** **tunnel** *ipsec-tunnel-name* [**detail**]
**no tunnel** *ipsec-tunnel-name*

**Context** debug>ipsec

**Description** This command enables debugging for specified IPSec tunnel.

Note that only one IPSec tunnel is allowed to enable debugging at a time.

**Parameters** *ipsec-tunnel-name* — Specifies the name of ipsec-tunnel.

**detail —** Displays detailed debug information.

# Tools Commands

## mc-ipsec

**Syntax** **mc-ipsec**

**Context** tools>perform>redundancy>multi-chassis>

**Description** This command enables the mc-ipsec context.

## force-switchover

**Syntax** **force-switchover tunnel-group** *local-group-id* [**now**] [**to** {**master**|**standby**}]

**Context** tools>perform>redundancy>multi-chassis>mc-ipsec

**Description** This command manually switchover mc-ipsec mastership of specified tunnel-group.

**Parameters** *local-group-id* — Specifies the local tunnel-group id configured in the config>redundancy>multi-chassis>peer>mc-ipsec context.

**now —** This optional parameter removes the prompt of confirmation.

**to** {**master**|**standby**} **—** specifies the desired mastership state to be achieved following a forced switch between this tunnel group and its redundant peer. If the target state matches the current state when the switch is attempted, then no switch will occur.