

---

## IP Tunnel Command Reference

- Hardware Commands on page 493
- ISA Commands on page 493
- IPsec Commands on page 494
- Service Configuration Commands on page 497
  - IES Commands on page 497
  - VPRN Commands on page 500
- Auto-Update Commands on page 506
- Show Commands on page 507
- Debug Commands on page 507

---

## Configuration Commands

### Hardware Commands

```

config
  — card slot-number
     — mda mda-slot
        — mda-type isa-tunnel
        — no mda-type
  
```

### ISA Commands

```

config
  — isa
     — tunnel-group tunnel-group-id [create]
     — no tunnel-group tunnel-group-id
        — active-mda-number [1..16]
        — no active-mda-number
        — backup mda-id
        — no backup
        — description description-string
        — no description
        — [no] ipsec-responder-only
        — mda mda-id
        — [no] mda
        — multi-active
        — primary mda-id
        — no primary
        — reassembly [wait-msecs]
        — no reassembly
        — [no] shutdown
  
```

## IPSec Commands

```

config
  — ipsec
    — cert-profile profile-name [create]
    — no cert-profile profile-name
      — entry entry-id [create]
      — no entry entry-id
        — cert cert-filename
        — no cert
        — key key-filename
        — no key
        — [no] send-chain
          — [no] send-chain
        — [no] shutdown
    — trust-anchor-profile name [create]
    — no trust-anchor-profile
      — trust-anchor ca-profile-name
      — no trust-anchor
    — ts-list list-name [create]
    — no ts-list list-name
      — local
        — entry entry-id [create]
        — no entry entry-id
          — address prefix ip-prefix/ip-prefix-len
          — address from begin-ip-address to end-ip-address
          — no address

config
  — ipsec
    — ike-policy ike-policy-id [create]
    — no ike-policy ike-policy-id
      — auth-algorithm auth-algorithm
      — no auth-algorithm
      — auth-method {psk|plain-psk-xauth|cert-auth|psk-radius|cert-radius|eap|auto-eap-radius}
      — no auth-method
      — auto-eap-method {psk|cert|psk-or-cert}
      — auto-eap-own-method {psk|cert}
      — description description-string
      — no description
      — dh-group {1 | 2 | 5 | 14 | 15}
      — no dh-group
      — dpd [interval interval] [max-retries max-retries] [reply-only]
      — no dpd
      — encryption-algorithm {des | 3des | aes128 | aes192 | aes256}
      — no encryption-algorithm
      — ike-mode {main | aggressive}
      — no ike-mode
      — ike-version [1..2]
      — ipsec-lifetime ipsec-lifetime
      — no ipsec-lifetime
      — isakmp-lifetime isakmp-lifetime
      — no isakmp-lifetime
      — [no] match-peer-id-to-cert
      — nat-traversal [force] [keep-alive-interval keep-alive-interval] [force-keep-alive]

```

```

— no nat-traversal
— own-auth-method {psk | cert | eap-only}
— no own-auth-method
— pfs [dh-group {1 | 2 | 5 | 14 | 15}]
— no pfs
— relay-unsolicited-cfg-attribute
  — [no] internal-ip4-dns
  — [no] internal-ip4-netmask
  — [no] internal-ip6-dns

config
— ipsec
  — ipsec-transform transform-id [create]
  — no ipsec-transform transform-id
    — esp-auth-algorithm {null | md5 | sha1 | sha256 | sha384 | sha512 | aes-xcbc}
    — no esp-auth-algorithm
    — esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256}
    — no esp-encryption-algorithm

config
— ipsec
  — [no] static-sa sa-name
    — authentication auth-algorithm ascii-key ascii-string
    — authentication auth-algorithm hex-key hex-string [hash|hash2]
    — no authentication
    — description description-string
    — no description
    — direction ipsec-direction
    — no direction
    — protocol ipsec-protocol
    — no protocol
    — spi spi
    — no spi

config
— ipsec
  — tunnel-template ipsec template identifier [create]
  — no tunnel-template ipsec template identifier
    — [no] clear-df-bit
    — description description-string
    — no description
    — encapsulated-ip-mtu octets
    — no encapsulated-ip-mtu
    — icmp6-generation
      — packet-too-big number [10..1000] seconds [1..60]
      — packet-too-big
      — no packet-too-big
    — ip-mtu octets
    — no ip-mtu
    — replay-window {32 | 64 | 128 | 256 | 512}
    — no replay-window
    — [no] sp-reverse-route
    — transform transform-id [transform-id...(up to 4 max)]
    — no transform

```

```

config
  — ipsec
    — radius-accounting-policy name [create]
    — no radius-accounting-policy name
      — [no] include-radius-attribute
        — [no] called-station-id
        — [no] calling-station-id
        — [no] framed-ip-addr
        — [no] nas-identifier
        — [no] nas-ip-addr
        — [no] nas-port-id
      — radius-server-policy radius-server-policy-name
      — no radius-server-policy
      — update-interval minutes [jitter seconds]
      — no update-interval
    — radius-authentication-policy name [create]
    — no radius-authentication-policy name
      — [no] include-radius-attribute
        — [no] called-station-id
        — [no] calling-station-id
        — [no] nas-identifier
        — [no] nas-ip-addr
        — [no] nas-port-id
      — password password [hash|hash2]
      — no password
      — radius-server-policy radius-server-policy-name
      — no radius-server-policy
  
```

## Service Configuration Commands

### IES Commands

```

config
  — service
    — ies service-id [customer customer-id] [vpn vpn-id]
      — [no] interface ip-int-name [tunnel]
        — dynamic-tunnel-redundant-next-hop ip-address
        — no dynamic-tunnel-redundant-next-hop
        — static-tunnel-redundant-next-hop ip-address
        — no static-tunnel-redundant-next-hop
        — [no] sap sap-id [create]
          — ip-tunnel ip-tunnel-name [create]
            — backup-remote-ip ip-address
            — no backup-remote-ip
            — [no] clear-df-bit
            — delivery-service {service-id | svc-name}
            — no delivery-service
            — description description-string
            — no description
            — dscp dscp-name
            — no dscp
            — [no] dest-ip ip-address
            — gre-header
            — gre-header send-key send-key receive-key receive-key
            — no gre-header
            — ip-mtu octets
            — no ip-mtu
            — reassemble [wait-msecs]
            — no reassemble
            — remote-ip ip-address
            — no remote-ip
            — [no] shutdown
            — source ip-address
            — no source
          — [no] ipsec-gw
            — cert
              — cert filename
              — no cert
              — cert-profile profile
              — no cert-profile
              — key filename
              — no key
              — status-verify
                — default-result {revoked|good}
                — no default-result
                — primary {ocsp|crl}
                — no primary
                — secondary {ocsp|crl}
                — no secondary

```

- **trust-anchor** *ca-profile-name*
- **no trust-anchor**
- **trust-anchor-profile** *profile-name*
- **no trust-anchor-profile**
- **trust-anchor** *ca-profile-name*
- **no trust-anchor**
- **trust-anchor-profile** *profile-name*
- **no trust-anchor-profile**
- **default-secure-service** *service-id ipsec-interface ip-int-name*
- **no default-secure-service**
- **default-tunnel-template** *ipsec template identifier*
- **no default-tunnel-template**
- **[no] dhcp**
  - **gi-address** *ip-address*
  - **no gi-address**
  - **[no] send-release**
  - **server** *ip-address [ip-address...(upto 8 max)] router router-instance*
  - **server** *ip-address [ip-address...(upto 8 max)] service-name service-name*
  - **no server**
  - **[no] shutdown**
- **ike-policy** *ike-policy-id*
- **no ike-policy**
- **[no] local-address-assignment**
  - **ipv4**
    - **address-source router** *router-instance dhcp-server local-dhcp4-svr-name pool dhcp4-server-pool*
    - **address-source service-name** *service-name dhcp-server local-dhcp4-svr-name pool dhcp4-server-pool*
    - **no address-source**
  - **ipv6**
    - **address-source router** *router-instance dhcp-server local-dhcp6-svr-name pool dhcp6-server-pool*
    - **address-source service-name** *service-name dhcp-server local-dhcp6-svr-name pool dhcp6-server-pool*
    - **no address-source**
  - **[no] shutdown**
- **local-gateway-address** *ip-address*
- **no local-gateway-address**
- **local-id** {*ipv4 | fqnd | ipv6*} [*value [255 chars max]*]
- **no local-id**
- **pre-shared-key** *key*
- **no pre-shared-key**
- **radius-accounting-policy** *policy-name*
- **no radius-accounting-policy**
- **radius-accounting-policy** *name*
- **no radius-accounting-policy**
- **[no] shutdown**
- **ts-negotiation ts-list** *list-name*

— no **ts-negotiation**

## VPRN Commands

```

config
  — service
    — vprn service-id [customer customer-id]
    — no vprn service-id
      — ipsec
        — security-policy security-policy-id [create]
        — no security-policy security-policy-id
          — entry entry-id [create]
          — no entry entry-id
            — local-ip {ip-prefix/prefix-length | ip-prefix netmask |
              any}
            — local-v6-ip ipv6-prefix/prefix-length
            — local-v6-ip any
            — no local-v6-ip
            — remote-ip {ip-prefix/prefix-length | ip-prefix netmask |
              any}
            — remote-v6-ip any
            — remote-v6-ip ipv6-prefix/prefix-length
            — no remote-v6-ip
          — [no] interface ip-int-name
            — ipv6
              — address ipv6-address/prefix-length [eui-64] [preferred] [track-
                srrp srrp-instance]
              — no address ipv6-address/prefix-length
              — link-local-address ipv6-address [preferred]

config
  — service
    — vprn service-id [customer customer-id]
    — no vprn service-id
      — [no] interface ip-int-name [create] [tunnel]
        — dynamic-tunnel-redundant-next-hop ip-address
        — no dynamic-tunnel-redundant-next-hop
        — static-tunnel-redundant-next-hop ip-address
        — no static-tunnel-redundant-next-hop
        — [no] sap sap-id [create]
          — ip-tunnel ip-tunnel-name [create]
            — backup-remote-ip ip-address
            — no backup-remote-ip
            — [no] clear-df-bit
            — delivery-service {service-id | svc-name}
            — no delivery-service
            — description description-string
            — no description
            — dscp dscp-name
            — no dscp
            — [no] dest-ip ip-address
            — [no] gre-header
            — ip-mtu octets
            — no ip-mtu
            — reassembly [wait-msecs]
            — no reassembly
            — remote-ip ip-address
            — no remote-ip

```



- [no] **shutdown**
- **source** *ip-address*
- **no source**
- [no] **ipsec-gw**
  - **cert**
    - **cert** *filename*
    - **no cert**
    - **cert-profile** *profile*
    - **no cert-profile**
    - **key** *filename*
    - **no key**
    - **status-verify**
      - **default-result** {revoked|good}
      - **no default-result**
      - **primary** {ocsp|crl}
      - **no primary**
      - **secondary** {ocsp|crl}
      - **no secondary**
    - **trust-anchor** *ca-profile-name*
    - **no trust-anchor**
    - **trust-anchor-profile** *profile-name*
    - **no trust-anchor-profile**
  - **default-secure-service** *service-id ipsec-interface ip-int-name*
  - **no default-secure-service**
  - **default-tunnel-template** *ipsec template identifier*
  - **no default-tunnel-template**
  - [no] **dhcp**
    - **gi-address** *ip-address*
    - **no gi-address**
    - [no] **send-release**
    - **server** *ip-address [ip-address...(upto 8 max)] router router-instance*
    - **server** *ip-address [ip-address...(upto 8 max)] service-name service-name*
    - **no server**
    - [no] **shutdown**
  - **ike-policy** *ike-policy-id*
  - **no ike-policy**
  - [no] **local-address-assignment**
    - **ipv4**
      - **address-source** **router** *router-instance dhcp-server local-dhcp4-svr-name pool dhcp4-server-pool*
      - **address-source** **service-name** *service-name dhcp-server local-dhcp4-svr-name pool dhcp4-server-pool*
      - **no address-source**
    - **ipv6**
      - **address-source** **router** *router-instance dhcp-server local-dhcp6-svr-name pool dhcp6-server-pool*
      - **address-source** **service-name** *service-name dhcp-server local-dhcp6-svr-name pool dhcp6-server-pool*

- **no address-source**
- **[no] shutdown**
- **local-gateway-address** *ip-address*
- **no local-gateway-address**
- **local-id** {*ipv4* | *fqdn* | *ipv6*} [*value* [255 chars max]]
- **no local-id**
- **[no] shutdown**
- **ts-negotiation** **ts-list** *list-name*
- **no ts-negotiation**
- **ipsec-tunnel** *ipsec-tunnel-name* [**create**]
- **no ipsec-tunnel** *ipsec-tunnel-name*
  - **[no] bfd-designate**
  - **bfd-enable** **service** *service-id* **interface** *interface-name* **dst-ip** *ip-address*
  - **[no] clear-df-bit**
  - **description** *description-string*
  - **no description**
  - **[no] dest-ip** *ip-address*
  - **[no] dynamic-keying**
    - **[no] auto-establish**
    - **cert**
      - **cert** *filename*
      - **no cert**
      - **cert-profile** *profile*
      - **no cert-profile**
      - **key** *filename*
      - **no key**
      - **status-verify**
        - **default-result** {*revoked*|*good*}
        - **no default-result**
        - **primary** {*ocsp*|*crl*}
        - **no primary**
        - **secondary** {*ocsp*|*crl*}
        - **no secondary**
      - **trust-anchor** *ca-profile-name*
      - **no trust-anchor**
      - **trust-anchor-profile** *profile-name*
      - **no trust-anchor-profile**
    - **ike-policy** *ike-policy-id*
    - **no ike-policy**
    - **local-id** {*ipv4* | *fqdn* | *ipv6*} [*value* [255 chars max]]
    - **no local-id**
    - **pre-shared-key** *key*
    - **no pre-shared-key**
    - **transform** *transform-id* [*transform-id*...(up to 4 max)]
    - **no transform**
  - **encapsulated-ip-mtu** *octets*
  - **no encapsulated-ip-mtu**
  - **icmp6-generation**
    - **packet-too-big**
    - **packet-too-big** **number** [10..1000] *seconds* [1..60]
    - **no packet-too-big**

- **ip-mtu** *octets*
- **no ip-mtu**
- **local-gateway-address** *ip-address* **peer** *ip-address*  
**delivery-service** *service-id*
- **no local-gateway-address**
- **local-id** **type** *type* [**value** <[255 chars max]>]
- **no local-id**
- **[no] manual-keying**
  - **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**}
  - **replay-window** *replay-window-size*
  - **no replay-window**
  - **security-policy** *security-policy-id*
  - **no security-policy**

## IPSec Mastership Election Commands

```

configure
  — redundancy
    — multi-chassis
      — peer ip-address [create]
      — no peer ip-address
        — [no] mc-ipsec
          — [no] bfd-enable
          — discovery-interval interval-secs [boot interval-secs]
          — no discovery-interval
          — hold-on-neighbor-failure multiplier
          — no hold-on-neighbor-failure
          — keep-alive-interval interval
          — no keep-alive-interval
          — tunnel-group tunnel-group-id [create]
          — no tunnel-group tunnel-group-id
            — peer-group tunnel-group-id
            — no peer-group
            — priority priority
            — no priority
            — [no] shutdown
  
```

## Related Commands

```

config
  — router
    — policy-options
      — policy-statement
        — entry
          — from
            — protocol protocol [all | instance instance]
            — no protocol
            — state state
            — no state
config
  — redundancy
    — multi-chassis
      — peer
        — sync
          — [no] ipsec
          — tunnel-group tunnel-group-id sync-tag tag-name [create]
          — no tunnel-group tunnel-group-id
  
```

## CMPv2 Commands

```

config
  — system
    — security
      — pki
        — certificate-display-format {ascii|utf8}
        — ca-profile name [create]
        — no ca-profile name
          — cmpv2
            — [no] accept-unprotected-errormsg
            — [no] accept-unprotected-pkiconf
            — [no] always-set-sender-for-ir
            — http-response-timeout timeout
            — no http-response-timeout
            — http-version [1.0|1.1]
            — key-list
              — key password [hash|hash2] reference reference-number
              — no key reference reference-number
            — response-signing-cert filename
            — no response-signing-cert
            — [no] same-recipnonce-for-pollreq
            — url url-string [service-id service-id]
            — no url
          — revocation-check {crl | crl-optional}

admin
  — certificate
    — cmpv2
      — cert-request ca ca-profile-name current-key key-filename current-cert cert-filename
        [hash-alg hash-algorithm] newkey key-filename subject-dn subject-dn
        [domain-name <[255 chars max]>] [ip-addr <ip-address|ipv6-address>] save-as
        save-path-of-result-cert
      — clear-request ca ca-profile-name
      — initial-registration ca ca-profile-name key-to-certify key-filename protection-alg
        {password password reference ref-number | signature [cert cert-file-name [send-
        chain [with-ca ca-profile-name]]] [protection-key key-file-name] [hash-alg {md5 |
        sha1 | sha224 | sha256 | sha384 | sha512}]} subject-dn dn [domain-name <[255
        chars max]>] [ip-addr <ip-address|ipv6-address>] save-as save-path-of-result-cert
      — key-update ca ca-profile-name newkey key-filename oldkey key-filename oldcert
        cert-filename [hash-alg hash-algorithm] save-as save-path-of-result-cert
      — poll ca ca-profile-name
      — show-request [ca ca-profile-name]
  
```

## Auto-Update Commands

```

config
  — system
    — file-transmission-profile name [create]
    — no file-transmission-profile name
      — ipv4-source-address ip-address
      — no ipv4-source-address
      — ipv6-source-address ipv6-address
      — no ipv6-source-address
      — redirection [1..8]
      — no redirection
      — retry count
      — no retry
      — router router-instance
      — timeout seconds

config
  — system
    — security
      — pki
        — ca-profile name [create]
        — no ca-profile name
          — auto-crl-update [create]
          — no auto-crl-update
            — crl-urls
              — url-entry entry-id [create]
              — no url-entry entry-id
              — file-transmission-profile profile-name
              — no file-transmission-profile
              — url url
              — no url
            — periodic-update-interval [days days] [hrs hours]
              [min minutes] [sec seconds]
            — pre-update-time [days days] [hrs hours] [min min-
              utes] [sec seconds]
            — retry-interval seconds
            — no retry-interval
            — pre-update-time schedule-type
            — schedule-type schedult-type
            — [no] shutdown

admin
  — certificate
    — crl-update ca ca-profile-name

```

## Show Commands

```

show
  — ipsec
    — cert-profile name association
    — cert-profile [name]
    — cert-profile name entry [1..8]
    — certificate filename association
    — gateway name name
    — gateway [service service-id]
    — gateway tunnel [ip-address:port]
    — gateway name name tunnel ip-address:port
    — gateway name name tunnel
    — gateway [name name] tunnel state state
    — gateway [name name] tunnel idi-value idi-prefix
    — gateway tunnel count
    — ike-policy ike-policy-id
    — ike-policy
    — radius-accounting-policy [name]
    — radius-authentication-policy [name]
    — security-policy service-id [security-policy-id]
    — security-policy
    — static-sa
    — static-sa name sa-name
    — static-sa spi spi
    — transform [transform-id]
    — trust-anchor-profile trust-anchor-profile association
    — trust-anchor-profile [trust-anchor-profile ]
    — ts-list [list-name]
    — ts-list list-name association
    — ts-list list-name entry [1..32]
    — tunnel ipsec-tunnel-name
    — tunnel
    — tunnel-template [ipsec template identifier]
  — redundancy
    — multi-chassis
      — mc-ipsec peer ip-address tunnel-group tunnel-group-id
      — mc-ipsec peer ip-address

```

## Debug Commands

```

debug
  — ipsec
    — [no] gateway name name tunnel ip-address[:port] [nat-ip nat-ip[:port]] [detail]
    — tunnel ipsec-tunnel-name [detail]
    — no tunnel ipsec-tunnel-name
    — [no] certificate filename
  — cmpv2
    — [no] ca-profile profile-name
  — ocsp

```

## Tools Commands

```
tools
  — perform
    — redundancy
      — multi-chassis
        — mc-ipsec
          — force-switchover tunnel-group local-group-id [now][to
            {master|standby}]
```