# Contents

# IPsec commands

The following matrix shows the feature and hardware compatibility:

| Hardware series | Model | IPsec compatibility |
|---|---|---|
| WX1800H series | WX1804H<br>WX1810H<br>WX1820H | Yes |
| WX2500H series | WX2510H<br>WX2540H<br>WX2560H | Yes |
| WX3000H series | WX3010H | Yes |
| | WX3010H-L | No |
| | WX3010H-X | Yes |
| | WX3024H | Yes |
| | WX3024H-L | No |
| WX3500H series | WX3508H<br>WX3510H<br>WX3520H<br>WX3540H | Yes |
| WX5500E series | WX5510E<br>WX5540E | Yes |
| WX5500H series | WX5540H<br>WX5560H<br>WX5580H | Yes |
| Access controller modules | EWPXM1MAC0F<br>EWPXM1WCME0<br>EWPXM2WCMD0F<br>LSQM1WCMX20<br>LSQM1WCMX40<br>LSUM1WCME0<br>LSUM1WCMX20RT<br>LSUM1WCMX40RT | Yes |

## ah authentication-algorithm

Use **ah authentication-algorithm** to specify authentication algorithms for the AH protocol.

Use **undo ah authentication-algorithm** to remove all specified authentication algorithms for the AH protocols.

### Syntax

**ah authentication-algorithm** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

**undo ah authentication-algorithm**

### Default

AH does not use an authentication algorithm.

### Views

IPsec transform set view

### Predefined user roles

network-admin

### Parameters

**aes-xcbc-mac**: Uses the HMAC-AES-XCBC-MAC algorithm, which uses a 128-bit key.

**md5**: Uses the HMAC-MD5 algorithm, which uses a 128-bit key.

**sha1**: Uses the HMAC-SHA1 algorithm, which uses a 160-bit key.

**sha256**: Uses the HMAC-SHA256 algorithm, which uses a 256-bit key.

**sha384**: Uses the HMAC-SHA384 algorithm, which uses a 384-bit key.

**sha512**: Uses the HMAC-SHA512 algorithm, which uses a 512-bit key.

### Usage guidelines

You can specify multiple AH authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified AH authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first AH authentication algorithm.

### Examples

# Create an IPsec transform set, and specify the AH authentication algorithm for the transform set as HMAC-SHA1.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] ah authentication-algorithm sha1
```

## description

Use **description** to configure description for an IPsec policy or IPsec policy template.

Use **undo description** to restore the default.

### Syntax

**description** *text*

**undo description**

### Default

No description is defined.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*text*: Specifies the description content, a case-sensitive string of 1 to 80 characters.

### Usage guidelines

If the system has multiple IPsec policies or IPsec policy templates, you can use this command to configure different descriptions for them to distinguish them.

### Examples

# Configure description for IPsec policy 1 as **CenterToA**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] description CenterToA
```

## display ipsec { ipv6-policy | policy }

Use **display ipsec** { **ipv6-policy | policy** } to display information about IPsec policies.

### Syntax

**display ipsec** { **ipv6-policy | policy** } [ *policy-name* [ *seq-number* ] ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**ipv6-policy**: Displays information about IPv6 IPsec policies.

**policy**: Displays information about IPv4 IPsec policies.

*policy-name*: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies an IPsec policy entry by its sequence number in the range of 1 to 65535.

### Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec policies.

If you specify an IPsec policy name and a sequence number, this command displays information about the specified IPsec policy entry. If you specify an IPsec policy name without any sequence number, this command displays information about all IPsec policy entries with the specified name.

### Examples

# Display information about all IPv4 IPsec policies.

```
<Sysname> display ipsec policy
-------------------------------------------
IPsec Policy: mypolicy
-------------------------------------------

  -----------------------------
  Sequence number: 1
  Mode: Manual
  -----------------------------
  The policy configuration is incomplete:
           ACL not specified
           Incomplete transform-set configuration
  Description: This is my first IPv4 manual policy
  Security data flow:
  Remote address: 2.5.2.1
  Transform set: transform

  Inbound AH setting:
    AH SPI: 1200 (0x000004b0)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1400 (0x00000578)
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 1300 (0x00000514)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 1500 (0x000005dc)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  -----------------------------
  Sequence number: 2
  Mode: ISAKMP
  -----------------------------
  The policy configuration is incomplete:
           Remote-address not set
           ACL not specified
           Transform-set not set
  Description: This is my first IPv4 Isakmp policy
  Traffic Flow Confidentiality: Enabled
  Security data flow:
  Selector mode: standard
  Local address:
  Remote address:
  Transform set:
  IKE profile:
  IKEv2 profile:
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
-------------------------------------------
IPsec Policy: mycompletepolicy
Interface: LoopBack2
-------------------------------------------

  -----------------------------
  Sequence number: 1
  Mode: Manual
  -----------------------------
  Description: This is my complete policy
  Security data flow: 3100
  Remote address: 2.2.2.2
  Transform set: completetransform

  Inbound AH setting:
    AH SPI: 5000 (0x00001388)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 7000 (0x00001b58)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 6000 (0x00001770)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 8000 (0x00001f40)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  -----------------------------
  Sequence number: 2
  Mode: ISAKMP
  -----------------------------
  Description: This is my complete policy
  Traffic Flow Confidentiality: Enabled
  Security data flow: 3200
  Selector mode: standard
  Local address:
  Remote address: 5.3.6.9
  Transform set:  completetransform
  IKE profile:
  IKEv2 profile:
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
```

# Display information about all IPv6 IPsec policies.

```
<Sysname> display ipsec ipv6-policy
-------------------------------------------
IPsec Policy: mypolicy
-------------------------------------------

  -----------------------------
  Sequence number: 1
  Mode: Manual
  -----------------------------
  Description: This is my first IPv6 policy
  Security data flow: 3600
  Remote address: 1000::2
  Transform set: mytransform

  Inbound AH setting:
    AH SPI: 1235 (0x000004d3)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1236 (0x000004d4)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 1237 (0x000004d5)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 1238 (0x000004d6)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:
```

**Table 1 Command output**

| Field | Description |
|---|---|
| IPsec Policy | IPsec policy name. |
| Interface | Interface applied with the IPsec policy. |
| Sequence number | Sequence number of the IPsec policy entry. |

| Field | Description |
|---|---|
| Mode | Negotiation mode of the IPsec policy:<br>- **Manual**—Manual mode.<br>- **ISAKMP**—IKE negotiation mode.<br>- **Template**—IPsec policy template mode. |
| The policy configuration is incomplete | IPsec policy configuration incomplete. Possible causes include:<br>- The ACL is not configured.<br>- The IPsec transform set is not configured.<br>- The ACL does not have any **permit** statements.<br>- The IPsec transform set configuration is not complete.<br>- The peer IP address of the IPsec tunnel is not specified.<br>- The SPI and key of the IPsec SA do not match the IPsec policy. |
| Description | Description of the IPsec policy. |
| Traffic Flow Confidentiality | Whether Traffic Flow Confidentiality (TFC) padding is enabled. |
| Security data flow | ACL used by the IPsec policy. |
| Selector mode | Data flow protection mode of the IPsec policy:<br>- standard<br>- aggregation<br>- per-host |
| Local address | Local end IP address of the IPsec tunnel (available only for the IPsec policy using IKE negotiation). |
| Remote address | Remote end IP address or host name of the IPsec tunnel. |
| Transform set | Transform set used by the IPsec policy. |
| IKE profile | IKE profile used by the IPsec policy. |
| IKEv2 profile | IKEv2 profile used by the IPsec policy. |
| SA duration(time based) | Time-based IPsec SA lifetime, in seconds. |
| SA duration(traffic based) | Traffic-based IPsec SA lifetime, in kilobytes. |
| SA idle time | Idle timeout of the IPsec SA, in seconds. |
| AH string-key | AH string key (****** is displayed if the key is configured). |
| AH authentication hex key | AH authentication hex key (****** is displayed if the key is configured). |
| ESP string-key | ESP string key (****** is displayed if the key is configured). |
| ESP encryption hex key | ESP encryption hex key (****** is displayed if the key is configured). |
| ESP authentication hex key | ESP authentication hex key (****** is displayed if the key is configured). |

### Related commands

**ipsec** { **ipv6-policy** | **policy** }

# display ipsec { ipv6-policy-template | policy-template }

Use **display ipsec** { **ipv6-policy-template** | **policy-template** } to display information about IPsec policy templates.

## Syntax

**display ipsec** { **ipv6-policy-template** | **policy-template** } [ *template-name* [ *seq-number* ] ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**ipv6-policy-template**: Displays information about IPv6 IPsec policy templates.

**policy-template**: Displays information about IPv4 IPsec policy templates.

*template-name*: Specifies an IPsec policy template by its name, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies an IPsec policy template entry by its sequence number in the range of 1 to 65535.

## Usage guidelines

- If you do not specify any parameters, this command displays information about all IPsec policy templates.
- If you specify an IPsec policy template name and a sequence number, this command displays information about the specified IPsec policy template entry. If you specify an IPsec policy template name without any sequence number, this command displays information about all IPsec policy template entries with the specified name.

## Examples

# Display information about all IPv4 IPsec policy templates.

```
<Sysname> display ipsec policy-template
-----------------------------------------------
IPsec Policy Template: template
-----------------------------------------------

  ---------------------------------
  Sequence number: 1
  ---------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 162.105.10.2
Transform set:  testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

# Display information about all IPv6 IPsec policy templates.

```
<Sysname> display ipsec ipv6-policy-template
```

```
-----------------------------------------------
IPsec Policy Template: template6
-----------------------------------------------

  ---------------------------------
  Sequence number: 1
  ---------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 200::1/64
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

**Table 2 Command output**

| Field | Description |
|---|---|
| IPsec Policy Template | IPsec policy template name. |
| Sequence number | Sequence number of the IPsec policy template entry. |
| Description | Description of the IPsec policy template. |
| Traffic Flow Confidentiality | Whether Traffic Flow Confidentiality (TFC) padding is enabled. |
| Security data flow | ACL used by the IPsec policy template. |
| Selector mode | Data flow protection mode of the IPsec policy template:<br>• standard<br>• aggregation<br>• per-host |
| Local address | Local end IP address of the IPsec tunnel. |
| IKE profile | IKE profile used by the IPsec policy template. |
| IKEv2 profile | IKEv2 profile used by the IPsec policy template. |
| Remote address | Remote end IP address of the IPsec tunnel. |
| Transform set | Transform set used by the IPsec policy template. |
| IPsec SA local duration(time based) | Time-based IPsec SA lifetime, in seconds. |
| IPsec SA local duration(traffic based) | Traffic-based IPsec SA lifetime, in kilobytes. |
| SA idle time | Idle timeout of the IPsec SA, in seconds. |

## Related commands

**ipsec** { **ipv6-policy** | **policy** } **isakmp template**

# display ipsec sa

Use **display ipsec sa** to display information about IPsec SAs.

## Syntax

**display ipsec sa** [ **brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [ *seq-number* ] | **remote** [ **ipv6** ] *ip-address* ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

**brief**: Displays brief information about all IPsec SAs.

**count**: Displays the number of IPsec SAs.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

**ipv6-policy**: Displays detailed information about IPsec SAs created by using a specified IPv6 IPsec policy.

**policy**: Displays detailed information about IPsec SAs created by using a specified IPv4 IPsec policy.

*policy-name*: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies an IPsec policy by its sequence number. The value range is 1 to 65535.

**remote** *ip-address*: Specifies an IPsec SA by its remote end IP address.

**ipv6**: Specifies an IPsec SA by its remote end IPv6 address. If this keyword is not specified, the specified remote end IP address is an IPv4 address.

## Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec SAs.

## Examples

# Display brief information about IPsec SAs.

```
<Sysname> display ipsec sa brief
-----------------------------------------------------------------------
Interface/Global             Dst Address      SPI         Protocol  Status
-----------------------------------------------------------------------
Vlan-interface100            10.1.1.1         400         ESP       Active
Vlan-interface100            255.255.255.255  4294967295  ESP       Active
Vlan-interface100            100::1/64        500         AH        Active
Global                       --               600         ESP       Active
```

**Table 3 Command output**

| Field | Description |
|---|---|
| Interface/Global | Interface where the IPsec SA belongs to. |
| Dst Address | Remote end IP address of the IPsec tunnel. |
| SPI | IPsec SA SPI. |

| Field | Description |
|---|---|
| Protocol | Security protocol used by IPsec. |
| Status | Status of the IPsec SA: **Active** or **Standby**.<br>In a VSRP scenario, this field displays either **Active** or **Standby**.<br>In standalone mode, this field always displays **Active**. |

# Display the number of IPsec SAs.

```
<Sysname> display ipsec sa count
Total IPsec SAs count: 4
```

# Display information about all IPsec SAs.

```
<Sysname> display ipsec sa
-------------------------------
Interface: Vlan-interface100
-------------------------------

  -----------------------------
  IPsec policy: r2
  Sequence number: 1
  Mode: ISAKMP
  Flow table status: Active
  -----------------------------
    Tunnel id: 3
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
Inside VRF: vp1
    Extended Sequence Number enable: Y
Traffic Flow Confidentiality enable: N
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.2.2
        remote address: 1.1.1.2
    Flow:
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3564837569 (0xd47b1ac1)
      Connection ID: 1
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max received sequence-number: 5
      Anti-replay check enable: Y
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
      Status: Active
    [Outbound ESP SAs]
      SPI: 801701189 (0x2fc8fd45)
      Connection ID: 2
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max sent sequence-number: 6
      UDP encapsulation used for NAT traversal: N
      Status: Active
-------------------------------
Global IPsec SA
-------------------------------

  -----------------------------
  IPsec profile: profile
  Mode: Manual
  -----------------------------
    Encapsulation mode: transport
    [Inbound AH SAs]
      SPI: 1234563 (0x0012d683)
      Connection ID: 9
      Transform set: AH-SHA1
      No duration limit for this SA
    [Outbound AH SAs]
      SPI: 1234563 (0x002d683)
      Connection ID: 10
      Transform set: AH-SHA1
      No duration limit for this SA
```

**Table 4 Command output**

| Field | Description |
|---|---|
| Interface | Interface where the IPsec SA belongs. |
| IPsec policy | Name of the used IPsec policy. |
| IPsec profile | Name of the used IPsec profile.<br>This field is not supported in the current software version. |
| Sequence number | Sequence number of the IPsec policy entry. |
| Mode | Negotiation mode used by the IPsec policy:<br>• Manual<br>• ISAKMP<br>• Template |
| Flow table status | Status of the flow entries deployed by IPsec: **Active** or **Inactive**. |
| Tunnel id | IPsec tunnel ID. |
| Encapsulation mode | Encapsulation mode, transport or tunnel. |

| Field | Description |
|---|---|
| Perfect Forward Secrecy | Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation:<br>• 768-bit Diffie-Hellman group (**dh-group1**)<br>• 1024-bit Diffie-Hellman group (**dh-group2**)<br>• 1536-bit Diffie-Hellman group (**dh-group5**)<br>• 2048-bit Diffie-Hellman group (**dh-group14**)<br>• 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**)<br>• 256-bit ECP Diffie-Hellman group (**dh-group19**)<br>• 384-bit ECP Diffie-Hellman group (**dh-group20**) |
| Extended Sequence Number enable | Whether Extended Sequence Number (ESN) is enabled. |
| Traffic Flow Confidentiality enable | Whether Traffic Flow Confidentiality (TFC) padding is enabled. |
| Inside VRF | VPN instance to which the protected data flow belongs.<br>The device does not support this field in the current software version. |
| Path MTU | Path MTU of the IPsec SA. |
| Tunnel | Local and remote addresses of the IPsec tunnel. |
| local address | Local end IP address of the IPsec tunnel. |
| remote address | Remote end IP address of the IPsec tunnel. |
| Flow | Information about the data flow protected by the IPsec tunnel. |
| sour addr | Source IP address of the data flow. |
| dest addr | Destination IP address of the data flow. |
| port | Port number. |
| protocol | Protocol type:<br>• **ip**—IPv4.<br>• **ipv6**—IPv6. |
| SPI | SPI of the IPsec SA. |
| Connection ID | Identifier of the IPsec SA. |
| Transform set | Security protocol and algorithms used by the IPsec transform set. |
| SA duration (kilobytes/sec) | IPsec SA lifetime, in kilobytes or seconds. |
| SA remaining duration (kilobytes/sec) | Remaining IPsec SA lifetime, in kilobytes or seconds. |
| Max received sequence-number | Max sequence number in the received packets. |
| Max sent sequence-number | Max sequence number in the sent packets. |
| Anti-replay check enable | Whether any-replay checking is enabled. |
| UDP encapsulation used for NAT traversal | Whether NAT traversal is used by the IPsec SA. |

| Field | Description |
|---|---|
| Status | Status of the IPsec SA: **Active** or **Standby**.<br>In a VSRP scenario, this field displays either **Active** or **Standby**.<br>In standalone mode, this field always displays **Active**. |
| No duration limit for this SA | The manual IPsec SAs do not have lifetime. |

### Related commands

- **ipsec sa global-duration**
- **reset ipsec sa**

# display ipsec statistics

Use **display ipsec statistics** to display IPsec packet statistics.

### Syntax

**display ipsec statistics** [ **tunnel-id** *tunnel-id* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**tunnel-id** *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967295. You can use the **display ipsec tunnel brief** command to view the IDs of established IPsec tunnels.

### Usage guidelines

If you do not specify any parameters, this command displays statistics for all IPsec packets.

### Examples

# Display statistics for all IPsec packets.

```
<Sysname> display ipsec statistics
  IPsec packet statistics:
    Received/sent packets: 47/64
    Received/sent bytes: 3948/5208
    Dropped packets (received/sent): 0/45

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 45
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

# Display statistics for the packets of IPsec tunnel 1.

```
<Sysname> display ipsec statistics tunnel-id 1
  IPsec packet statistics:
    Received/sent packets: 5124/8231
    Received/sent bytes: 52348/64356
    Dropped packets (received/sent): 0/0

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 0
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

**Table 5 Command output**

| Field | Description |
|---|---|
| Received/sent packets | Number of received/sent IPsec-protected packets. |
| Received/sent bytes | Number of bytes of received/sent IPsec-protected packets. |
| Dropped packets (received/sent) | Number of dropped IPsec-protected packets (received/sent). |
| No available SA | Number of packets dropped due to lack of available IPsec SA. |
| Wrong SA | Number of packets dropped due to wrong IPsec SA. |
| Invalid length | Number of packets dropped due to invalid packet length. |
| Authentication failure | Number of packets dropped due to authentication failure. |
| Encapsulation failure | Number of packets dropped due to encapsulation failure. |
| Decapsulation failure | Number of packets dropped due to decapsulation failure. |
| Replayed packets | Number of dropped replayed packets. |
| ACL check failure | Number of packets dropped due to ACL check failure. |
| MTU check failure | Number of packets dropped due to MTU check failure. |
| Loopback limit exceeded | Number of packets dropped due to loopback limit exceeded. |
| Crypto speed limit exceeded | Number of packets dropped due to crypto speed limit exceeded. |

## Related commands

**reset ipsec statistics**

# display ipsec transform-set

Use **display ipsec transform-set** to display information about IPsec transform sets.

## Syntax

**display ipsec transform-set** [ *transform-set-name* ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Parameters

*transform-set-name*: Specifies an IPsec transform set by its name, a case-insensitive string of 1 to 63 characters.

## Usage guidelines

If you do not specify an IPsec transform set, this command displays information about all IPsec transform sets.

## Examples

# Display information about all IPsec transform sets.

```
<Sysname> display ipsec transform-set
IPsec transform set: mytransform
  State: incomplete
  Encapsulation mode: tunnel
  ESN: Enabled
  PFS:
  Transform: ESP

IPsec transform set: completeTransform
  State: complete
  Encapsulation mode: transport
  ESN: Enabled
  PFS:
  Transform: AH-ESP
  AH protocol:
    Integrity: SHA1
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128
```

**Table 6 Command output**

| Field | Description |
|---|---|
| IPsec transform set | Name of the IPsec transform set. |
| State | Whether the IPsec transform set is complete. |
| Encapsulation mode | Encapsulation mode used by the IPsec transform set: transport or tunnel. |
| ESN | Whether Extended Sequence Number (ESN) is enabled. |

| Field | Description |
|---|---|
| PFS | Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation:<br>• 768-bit Diffie-Hellman group (**dh-group1**)<br>• 1024-bit Diffie-Hellman group (**dh-group2**)<br>• 1536-bit Diffie-Hellman group (**dh-group5**)<br>• 2048-bit Diffie-Hellman group (**dh-group14**)<br>• 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**)<br>• 256-bit ECP Diffie-Hellman group (**dh-group19**)<br>• 384-bit ECP Diffie-Hellman group (**dh-group20**) |
| Transform | Security protocols used by the IPsec transform set: AH, ESP, or both. If both protocols are configured, IPsec uses ESP before AH. |
| AH protocol | AH settings. |
| ESP protocol | ESP settings. |
| Integrity | Authentication algorithm used by the security protocol. |
| Encryption | Encryption algorithm used by the security protocol. |

### Related commands

**ipsec transform-set**

# display ipsec tunnel

Use **display ipsec tunnel** to display information about IPsec tunnels.

### Syntax

**display ipsec tunnel** { **brief** | **count** | **tunnel-id** *tunnel-id* }

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**brief**: Displays brief information about IPsec tunnels.

**count**: Displays the number of IPsec tunnels.

**tunnel-id** *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967295.

### Usage guidelines

IPsec is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

### Examples

# Display brief information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel brief
----------------------------------------------------------------------------
Tunn-id   Src Address     Dst Address     Inbound SPI   Outbound SPI  Status
----------------------------------------------------------------------------
```

```
0         --              --              1000          2000          Active
                                          3000          4000
1         1.2.3.1         2.2.2.2         5000          6000          Active
                                          7000          8000
```

**Table 7 Command output**

| Field | Description |
|---|---|
| Src Address | Source IP address of the IPsec tunnel. |
| Dst Address | Destination IP address of the IPsec tunnel. |
| Inbound SPI | Valid SPI in the inbound direction of the IPsec tunnel.<br>If the tunnel uses two security protocols, two SPIs in the inbound direction are displayed in two lines. |
| Outbound SPI | Valid SPI in the outbound direction of the IPsec tunnel.<br>If the tunnel uses two security protocols, two SPIs in the outbound direction are displayed in two lines. |
| Status | Status of the IPsec SA: **Active** or **Standby**.<br>In a VSRP scenario, this field displays either **Active** or **Standby**.<br>In standalone mode, this field always displays **Active**. |

# Display the number of IPsec tunnels.

```
<Sysname> display ipsec tunnel count
Total IPsec Tunnel Count: 2
```

# Display information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel
Tunnel ID: 0
Status: active
Perfect forward secrecy:
SA's SPI:
    outbound:  2000        (0x000007d0)   [AH]
    inbound:   1000        (0x000003e8)   [AH]
    outbound:  4000        (0x00000fa0)   [ESP]
    inbound:   3000        (0x00000bb8)   [ESP]
Tunnel:
    local  address:
    remote address:
Flow:

Tunnel ID: 1
Status: Active
Perfect forward secrecy:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
Flow:
    as defined in ACL3100
```

# Display information about IPsec tunnel 1.

```
<Sysname> display ipsec tunnel tunnel-id 1
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
Flow:
    as defined in ACL 3100
```

**Table 8 Command output**

| Field | Description |
|---|---|
| Tunnel ID | IPsec ID, used to uniquely identify an IPsec tunnel. |
| Status | IPsec tunnel status: **Active** or **Standby**.<br>In a VSRP scenario, this field displays either **Active** or **Standby**.<br>In standalone mode, this field always displays **Active**. |
| Perfect Forward Secrecy | Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation:<br>• 768-bit Diffie-Hellman group (**dh-group1**)<br>• 1024-bit Diffie-Hellman group (**dh-group2**)<br>• 1536-bit Diffie-Hellman group (**dh-group5**)<br>• 2048-bit Diffie-Hellman group (**dh-group14**)<br>• 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**)<br>• 256-bit ECP Diffie-Hellman group (**dh-group19**)<br>• 384-bit ECP Diffie-Hellman group (**dh-group20**) |
| SA's SPI | SPIs of the inbound and outbound SAs. |
| Tunnel | Local and remote addresses of the IPsec tunnel. |
| local  address | Local end IP address of the IPsec tunnel. |
| remote address | Remote end IP address of the IPsec tunnel. |
| Flow | Information about the data flow protected by the IPsec tunnel, including source IP address, destination IP address, source port, destination port and protocol. |
| as defined in ACL 3001 | Range of data flow protected by the IPsec tunnel that is established manually. This information shows that the IPsec tunnel protects all data flows defined by ACL 3001. |

# encapsulation-mode

Use **encapsulation-mode** to set the encapsulation mode that the security protocol uses to encapsulate IP packets.

Use **undo encapsulation-mode** to restore the default.

## Syntax

**encapsulation-mode** { **transport** | **tunnel** }

**undo encapsulation-mode**

## Default

IP packets are encapsulated in tunnel mode.

## Views

IPsec transform set view

## Predefined user roles

network-admin

## Parameters

**transport**: Uses the transport mode for IP packet encapsulation.

**tunnel**: Uses the tunnel mode for IP packet encapsulation.

## Usage guidelines

IPsec supports the following encapsulation modes:

- **Transport mode**—The security protocols protect the upper layer data of an IP packet. Only the transport layer data is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are placed after the original IP header. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications.
- **Tunnel mode**—The security protocols protect the entire IP packet. The entire IP packet is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are encapsulated in a new IP packet. In this mode, the encapsulated packet has two IP headers. The inner IP header is the original IP header. The outer IP header is added by the network device that provides the IPsec service. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications.

The IPsec transform sets at both ends of the IPsec tunnel must have the same encapsulation mode.

## Examples

# Configure the IPsec transform set **tran1** to use the transport mode for IP packet encapsulation.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] encapsulation-mode transport
```

## Related commands

**ipsec transform-set**

# esn enable

Use **esn enable** to enable the Extended Sequence Number (ESN) feature.

Use **undo esn enable** to disable the ESN feature.

### Syntax

**esn enable** [ **both** ]

**undo esn enable**

### Default

ESN is disabled.

### Views

IPsec transform set view

### Predefined user roles

network-admin

### Parameters

**both**: Specifies IPsec to support both extended sequence number and traditional sequence number. If you do not specify this keyword, IPsec only supports extended sequence number.

### Usage guidelines

The ESN feature extends the sequence number length from 32 bits to 64 bits. This feature prevents the sequence number space from being exhausted when large volumes of data are transmitted at high speeds over an IPsec SA. If the sequence number space is not exhausted, the IPsec SA does not need to be renegotiated.

This feature must be enabled at both the initiator and the responder.

### Examples

# Enable the ESN feature in the IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esn enable
```

### Related commands

**display ipsec transform-set**

# esp authentication-algorithm

Use **esp authentication-algorithm** to specify an authentication algorithm for ESP.

Use **undo esp authentication-algorithm** to restore the default.

### Syntax

**esp authentication-algorithm** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

**undo esp authentication-algorithm**

### Default

ESP does not use an authentication algorithm.

### Views

IPsec transform set view

### Predefined user roles

network-admin

### Parameters

**aes-xcbc-mac**: Uses the HMAC-AES-XCBC-MAC algorithm, which uses a 128-bit key.

**md5**: Uses the HMAC-MD5 algorithm, which uses a 128-bit key.

**sha1**: Uses the HMAC-SHA1 algorithm, which uses a 160-bit key.

**sha256**: Uses the HMAC-SHA256 algorithm, which uses a 256-bit key.

**sha384**: Uses the HMAC-SHA384 algorithm, which uses a 384-bit key.

**sha512**: Uses the HMAC-SHA512 algorithm, which uses a 512-bit key.

### Usage guidelines

You can specify multiple ESP authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP authentication algorithm.

### Examples

# Configure IPsec transform set **tran1** to use HMAC-SHA1 algorithm as the ESP authentication algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

### Related commands

**ipsec transform-set**

## esp encryption-algorithm

Use **esp encryption-algorithm** to specify encryption algorithms for ESP.

Use **undo esp encryption-algorithm** to remove all encryption algorithms specified for ESP.

### Syntax

**esp encryption-algorithm** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** | **null** } *

**undo esp encryption-algorithm**

### Default

ESP does not use any encryption algorithms.

### Views

IPsec transform set view

### Predefined user roles

network-admin

### Parameters

**3des-cbc**: Uses the 3DES algorithm in CBC mode, which uses a 168-bit key.

**aes-cbc-128**: Uses the AES algorithm in CBC mode, which uses a 128-bit key.

**aes-cbc-192**: Uses the AES algorithm in CBC mode, which uses a 192-bit key.

**aes-cbc-256**: Uses the AES algorithm in CBC mode, which uses a 256-bit key.

**aes-ctr-128**: Uses the AES algorithm in CTR mode, which uses a 128-bit key. This keyword is available only for IKEv2.

**aes-ctr-192**: Uses the AES algorithm in CTR mode, which uses a 192-bit key. This keyword is available only for IKEv2.

**aes-ctr-256**: Uses the AES algorithm in CTR mode, which uses a 256-bit key. This keyword is available only for IKEv2.

**camellia-cbc-128**: Uses the Camellia algorithm in CBC mode, which uses a 128-bit key. This keyword is available only for IKEv2.

**camellia-cbc-192**: Uses the Camellia algorithm in CBC mode, which uses a 192-bit key. This keyword is available only for IKEv2.

**camellia-cbc-256**: Uses the Camellia algorithm in CBC mode, which uses a 256-bit key. This keyword is available only for IKEv2.

**des-cbc**: Uses the DES algorithm in CBC mode, which uses a 64-bit key.

**gmac-128**: Uses the GMAC algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

**gmac-192**: Uses the GMAC algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

**gmac-256**: Uses the GMAC algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

**gcm-128**: Uses the GCM algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

**gcm-192**: Uses the GCM algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

**gcm-256**: Uses the GCM algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

**null**: Uses the NULL algorithm, which means encryption is not performed.

## Usage guidelines

You can specify multiple ESP encryption algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP encryption algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP encryption algorithm.

GCM and GMAC algorithms are combined mode algorithms. GCM algorithms provide encryption and authentication services. GMAC algorithms only provide authentication service. Combined mode algorithms can be used only when ESP is used alone without AH. Combined mode algorithms cannot be used together with ordinary ESP authentication algorithms.

## Examples

# Configure IPsec transform set **tran1** to use **aes-cbc-128** as the ESP encryption algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

## Related commands

**ipsec transform-set**

# ike-profile

Use **ike-profile** to specify an IKE profile for an IPsec policy or IPsec policy template.

Use **undo ike-profile** to restore the default.

### Syntax

**ike-profile** *profile-name*

**undo ike-profile**

### Default

No IKE profile is specified. The IPsec policy or IPsec policy template uses the global IKE settings for negotiation.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*profile-name*: Specifies an IKE profile by its name, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

If no IKE profile is specified for an IPsec policy or IPsec policy template, the device selects an IKE profile configured in system view for negotiation. If no IKE profile is configured, the globally configured IKE settings are used for negotiation.

The IKE profile specified for an IPsec policy or IPsec policy template defines the parameters used for IKE negotiation.

You can specify only one IKE profile for an IPsec policy or IPsec policy template.

### Examples

# Specify the IKE profile **profile1** for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-profile profile1
```

### Related commands

**ike profile**

# ikev2-profile

Use **ikev2-profile** to specify an IKEv2 profile for an IPsec policy or IPsec policy template.

Use **undo ikev2-profile** to restore the default.

### Syntax

**ikev2-profile** *profile-name*

**undo ikev2-profile**

### Default

No IKEv2 profile is specified for an IPsec policy or IPsec policy template.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*profile-name*: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

The IKEv2 profile specified for an IPsec policy or IPsec policy template defines the parameters used for IKEv2 negotiation.

You can specify only one IKEv2 profile for an IPsec policy or IPsec policy template.

On the initiator, you must specify an IKEv2 profile for the IPsec policy. On the responder, an IKEv2 profile is optional for the IPsec policy or IPsec policy template. If you do not specify an IKEv2 profile, the responder can use any IKEv2 profile for negotiation.

### Examples

# Specify the IKEv2 profile **profile1** for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

### Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**
- **ikev2 profile**

## ipsec { ipv6-policy | policy }

Use **ipsec** { **ipv6-policy** | **policy** } to create an IPsec policy entry and enter its view, or enter the view of an existing IPsec policy entry.

Use **undo ipsec** { **ipv6-policy | policy** } to delete the specified IPsec policy.

### Syntax

**ipsec** { **ipv6-policy | policy** } *policy-name seq-number* [ **isakmp | manual** ]

**undo ipsec** { **ipv6-policy | policy** } *policy-name* [ *seq-number* ]

### Default

No IPsec policy is created.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**ipv6-policy**: Specifies an IPv6 IPsec policy.

**policy**: Specifies an IPv4 IPsec policy.

*policy-name*: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies a sequence number for the IPsec policy entry, in the range of 1 to 65535.

**isakmp**: Establishes IPsec SAs through IKE negotiation.

**manual**: Establishes IPsec SAs manually.

### Usage guidelines

When you create an IPsec policy, you must specify the SA setup mode (**isakmp** or **manual**). When you enter the view of an existing IPsec policy, you do not need to specify the SA setup mode.

You cannot change the SA setup mode of an existing IPsec policy.

An IPsec policy is a set of IPsec policy entries that have the same name but different sequence numbers. In the same IPsec policy, an IPsec policy entry with a smaller sequence number has a higher priority.

If you specify the *seq-number* argument, the **undo** command deletes the specified IPsec policy entry. If you do not specify this argument, the **undo** command deletes all entries of the specified IPsec policy.

An IPv4 IPsec policy and IPv6 IPsec policy can have the same name.

### Examples

# Create an IKE-based IPsec policy entry with the name **policy1** and sequence number 100, and enter the IPsec policy view.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

# Create a manual IPsec policy entry with the name **policy1** and sequence number 101, and enter the IPsec policy view.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 101 manual
[Sysname-ipsec-policy-manual-policy1-101]
```

### Related commands

- **display ipsec** { **ipv6-policy** | **policy** }
- **ipsec apply**

## ipsec { ipv6-policy | policy } isakmp template

Use **ipsec** { **ipv6-policy** | **policy** } **isakmp template** to create an IKE-based IPsec policy by using an IPsec policy template.

Use **undo ipsec** { **ipv6-policy** | **policy** } to delete the specified IPsec policy.

### Syntax

**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp template** *template-name*

**undo ipsec** { **ipv6-policy** | **policy** } *policy-name* [ *seq-number* ]

### Default

No IPsec policy is created.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**ipv6-policy**: Specifies an IPv6 IPsec policy.

**policy**: Specifies an IPv4 IPsec policy.

*policy-name*: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies a sequence number for the IPsec policy, in the range of 1 to 65535. A smaller number indicates a higher priority.

**isakmp template** *template-name*: Specifies an IPsec policy template by its name, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

If you do not specify the *seq-number* argument, the **undo** command deletes all entries of the specified IPsec policy.

An interface applied with an IPsec policy that is configured by using an IPsec policy template cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. When the remote end's information (such as the IP address) is unknown, this method allows the remote end to initiate negotiations with the local end.

### Examples

# Create an IPsec policy entry by using the IPsec policy template **temp1**, and specify the IPsec policy name as **policy2** and the sequence number as 200.

```
<Sysname> system-view
[Sysname] ipsec policy policy2 200 isakmp template temp1
```

### Related commands

- **display ipsec** { **ipv6-policy** | **policy** }
- **ipsec** { **ipv6-policy-template** | **policy-template** }

# ipsec { ipv6-policy | policy } local-address

Use **ipsec** { **ipv6-policy** | **policy** } **local-address** to bind an IPsec policy to a source interface.

Use **undo ipsec** { **ipv6-policy** | **policy** } **local-address** to remove the bindings of IPsec policies and source interfaces.

### Syntax

**ipsec** { **ipv6-policy** | **policy** } *policy-name* **local-address** *interface-type interface-number*

**undo ipsec** { **ipv6-policy** | **policy** } *policy-name* **local-address**

### Default

No IPsec policy is bound to a source interface.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**ipv6-policy**: Specifies an IPv6 IPsec policy.

**policy**: Specifies an IPv4 IPsec policy.

*policy-name*: Name of an IPsec policy, a case-insensitive string of 1 to 63 characters.

**local-address** *interface-type interface-number*: Specifies the shared source interface by its type and number.

### Usage guidelines

For high availability, two interfaces can operate in backup or load sharing mode. After an IPsec policy is applied to the two interfaces, they negotiate with their peers to establish IPsec SAs respectively. When one interface fails and a link failover occurs, the other interface needs to take some time to renegotiate SAs, resulting in service interruption.

To solve these problems, bind a source interface to an IPsec policy and apply the policy to both interfaces. This enables the two physical interfaces to use the same source interface to negotiate IPsec SAs. As long as the source interface is up, the negotiated IPsec SAs will not be removed and will keep working, regardless of link failover.

After an IPsec policy is applied to a service interface and IPsec SAs have been established, if you bind the IPsec policy to a source interface, the existing IPsec SAs are deleted.

Only the IKE-based IPsec policies can be bound to a source interface.

An IPsec policy can be bound to only one source interface. If you execute this command multiple times for the same IPsec policy, the most recent configuration takes effect.

A source interface can be bound to multiple IPsec policies.

H3C recommends that you use a stable interface, such as a Loopback interface, as a source interface.

### Examples

# Bind the IPsec policy **map** to source interface Loopback 11.

```
<Sysname> system-view
[Sysname] ipsec policy map local-address loopback 11
```

### Related commands

**ipsec** { **ipv6-policy** | **policy** }

# ipsec { ipv6-policy-template | policy-template }

Use **ipsec** { **ipv6-policy-template** | **policy-template** } to create an IPsec policy template entry and enter its view, or enter the view of an existing IPsec policy template entry.

Use **undo ipsec** { **ipv6-policy-template** | **policy-template** } to delete the specified IPsec policy template.

### Syntax

**ipsec** { **ipv6-policy-template** | **policy-template** } *template-name seq-number*

**undo ipsec** { **ipv6-policy-template** | **policy-template** } *template-name* [ *seq-number* ]

### Default

No IPsec policy templates exist.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**ipv6-policy-template**: Specifies an IPv6 IPsec policy template.

**policy-template**: Specifies an IPv4 IPsec policy template.

*template-name*: Specifies a name for the IPsec policy template, a case-insensitive string of 1 to 63 characters.

*seq-number*: Specifies a sequence number for the IPsec policy template, in the range of 1 to 65535. A smaller number indicates a higher priority.

### Usage guidelines

The configurable parameters for an IPsec policy template are similar to the parameters that you use when you configure an IKE-based IPsec policy. However, all parameters except for the IPsec transform sets and the IKE peer are optional for an IPsec policy template.

An IPsec policy template is a set of IPsec policy template entries that have the same name but different sequence numbers.

With the *seq-number* argument specified, the **undo** command deletes an IPsec policy template entry.

An IPv4 IPsec policy template and an IPv6 IPsec policy template can have the same name.

### Examples

# Create an IPsec policy template entry with the name **template1** and sequence number 100, and enter the IPsec policy template view.

```
<Sysname> system-view
[Sysname] ipsec policy-template template1 100
[Sysname-ipsec-policy-template-template1-100]
```

### Related commands

- **display ipsec** { **ipv6-policy-template | policy-template** }
- **ipsec** { **ipv6-policy | policy** }
- **ipsec** { **ipv6-policy | policy** } **isakmp template**

## ipsec anti-replay check

Use **ipsec anti-replay check** to enable IPsec anti-replay checking.

Use **undo ipsec anti-replay check** to disable IPsec anti-replay checking.

### Syntax

**ipsec anti-replay check**

**undo ipsec anti-replay check**

### Default

IPsec anti-replay checking is enabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets is not necessary but consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some situations, service data packets are received in a different order than their original order. The IPsec anti-replay feature drops them as replayed packets, which impacts communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

IPsec anti-replay checking does not affect manually created IPsec SAs. According to the IPsec protocol, only IPsec SAs negotiated by IKE support anti-replay checking.

### Examples

# Enable IPsec anti-replay checking.

```
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

### Related commands

**ipsec anti-replay window**

## ipsec anti-replay window

Use **ipsec anti-replay window** to set the anti-replay window size.

Use **undo ipsec anti-replay window** to restore the default.

### Syntax

**ipsec anti-replay window** *width*

**undo ipsec anti-replay window**

### Default

The anti-replay window size is 64.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*width*: Specifies the size for the anti-replay window. It can be 64, 128, 256, 512, or 1024 packets.

### Usage guidelines

Changing the anti-replay window size affects only the IPsec SAs negotiated later.

In some cases, some service data packets might be received in a very different order than their original order, and the IPsec anti-replay feature might drop them as replayed packets, affecting normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

### Examples

# Set the size of the anti-replay window to 128.

```
<Sysname> system-view
[Sysname] ipsec anti-replay window 128
```

### Related commands

**ipsec anti-replay check**

## ipsec apply

Use **ipsec apply** to apply an IPsec policy to an interface.

Use **undo ipsec apply** to remove the application.

### Syntax

**ipsec apply** { **ipv6-policy** | **policy** } *policy-name*

**undo ipsec apply** { **ipv6-policy** | **policy** }

### Default

No IPsec policy is applied to an interface.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

**ipv6-policy**: Specifies an IPv6 IPsec policy.

**policy**: Specifies an IPv4 IPsec policy.

*policy-name*: Name of an IPsec policy, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

You can apply only one IPsec policy on an interface.

An IKE-based IPsec policy can be applied to multiple interfaces. A manual IPsec policy can be applied to only one interface.

### Examples

# Apply the IPsec policy **policy1** to interface VLAN-interface 200.

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] ipsec apply policy policy1
```

### Related commands

- **display ipsec** { **ipv6-policy** | **policy** }
- **ipsec** { **ipv6-policy** | **policy** }

## ipsec decrypt-check enable

Use **ipsec decrypt-check enable** to enable ACL checking for de-encapsulated IPsec packets.

Use **undo ipsec decrypt-check** to disable ACL checking for de-encapsulated IPsec packets.

### Syntax

**ipsec decrypt-check enable**

**undo ipsec decrypt-check enable**

### Default

ACL checking for de-encapsulated IPsec packets is enabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

In tunnel mode, the IP packet encapsulated in an inbound IPsec packet might not be under the protection of the ACL specified in the IPsec policy. After being de-encapsulated, such packets bring threats to the network security. In this scenario, you can enable ACL checking for de-encapsulated IPsec packets. All packets failing the checking are discarded, improving the network security.

### Examples

# Enable ACL checking for de-encapsulated IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec decrypt-check enable
```

## ipsec df-bit

Use **ipsec df-bit** to configure the DF bit for the outer IP header of IPsec packets on an interface.

Use **undo ipsec df-bit** to restore the default.

### Syntax

**ipsec df-bit** { **clear** | **copy** | **set** }

**undo ipsec df-bit**

### Default

The DF bit is not configured for the outer IP header of IPsec packets on an interface. The global DF bit setting is used.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

**clear**: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

**copy**: Copies the DF bit setting of the original IP header to the outer IP header.

**set**: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

### Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

If multiple interfaces use an IPsec policy that is bound to a source interface, you must use the same DF bit setting on these interfaces.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent the IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. If you cannot make sure of this, H3C recommends that you clear the DF bit.

### Examples

# Set the DF bit in the outer IP header of IPsec packets on VLAN-interface 200.

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] ipsec df-bit set
```

### Related commands

**ipsec global-df-bit**

## ipsec fragmentation

Use **ipsec fragmentation** to configure the IPsec fragmentation feature.

Use **undo ipsec fragmentation** to restore the default.

### Syntax

**ipsec fragmentation** { **after-encryption** | **before-encryption** }

**undo ipsec fragmentation**

### Default

The device fragments packets before IPsec encapsulation.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**after-encryption**: Fragments packets after IPsec encapsulation.

**before-encryption**: Fragments packets before IPsec encapsulation.

### Usage guidelines

If you configure the device to fragment packets before IPsec encapsulation, the device predetermines the encapsulated packet size before the actual encapsulation. If the encapsulated packet size exceeds the MTU of the output interface, the device fragments the packets before encapsulation. If a packet's DF bit is set, the device drops the packet and sends an ICMP error message.

If you configure the device to fragment packets after IPsec encapsulation, the device directly encapsulates the packets and fragments the encapsulated packets in subsequent service modules.

### Examples

# Configure the device to fragment packets after IPsec encapsulation.

```
<Sysname>system-view
[Sysname] ipsec fragmentation after-encryption
```

## ipsec global-df-bit

Use **ipsec global-df-bit** to configure the DF bit for the outer IP header of IPsec packets on all interfaces.

Use **undo ipsec global-df-bit** to restore the default.

### Syntax

**ipsec global-df-bit** { **clear** | **copy** | **set** }

**undo ipsec global-df-bit**

### Default

The DF bit setting of the original IP header is copied to the outer IP header for IPsec packets.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**clear**: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

**copy**: Copies the DF bit setting of the original IP header to the outer IP header.

**set**: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

### Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. If you cannot make sure of this, H3C recommends that you clear the DF bit.

### Examples

# Set the DF bit in the outer IP header of IPsec packets on all interfaces.

```
<Sysname> system-view
[Sysname] ipsec global-df-bit set
```

### Related commands

**ipsec df-bit**

## ipsec limit max-tunnel

Use **ipsec limit max-tunnel** to set the maximum number of IPsec tunnels that can be established.

Use **undo ipsec limit max-tunnel** to restore the default.

### Syntax

**ipsec limit max-tunnel** *tunnel-limit*

**undo ipsec limit max-tunnel**

### Default

The number of IPsec tunnels is not limited.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*tunnel-limit*: Specifies the maximum number of IPsec tunnels, in the range of 1 to 4294967295.

### Usage guidelines

To maximize concurrent performance of IPsec when memory is sufficient, increase the maximum number of IPsec tunnels. To ensure service availability when memory is insufficient, decrease the maximum number of IPsec tunnels.

### Examples

# Set the maximum number of IPsec tunnels that can be established to 5000.

```
<Sysname> system-view
[Sysname] ipsec limit max-tunnel 5000
```

### Related commands

**ike limit**

# ipsec logging negotiation enable

Use **ipsec logging negotiation enable** to enable logging for IPsec negotiation.

Use **undo ipsec logging negotiation packet enable** to disable logging for IPsec negotiation.

### Syntax

**ipsec logging negotiation enable**

**undo ipsec logging negotiation enable**

### Default

Logging for IPsec negotiation is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

This command enables the device to output logs for the IPsec negotiation process.

### Examples

# Enable logging for IPsec negotiation.

```
<Sysname> system-view
[Sysname] ipsec logging negotiation enable
```

# ipsec logging packet enable

Use **ipsec logging packet enable** to enable logging for IPsec packets.

Use **undo ipsec logging packet enable** to disable logging for IPsec packets.

### Syntax

**ipsec logging packet enable**

**undo ipsec logging packet enable**

### Default

Logging for IPsec packets is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

After logging for IPsec packets is enabled, the device outputs a log when an IPsec packet is discarded. IPsec packets might be discarded due to lack of inbound SA, AH/ESP authentication failure, or ESP encryption failure. A log contains the source and destination IP addresses, SPI, and sequence number of the packet, and the reason it was discarded.

### Examples

# Enable logging for IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec logging packet enable
```

## ipsec redundancy enable

Use **ipsec redundancy enable** to enable IPsec redundancy.

Use **undo ipsec redundancy enable** to disable IPsec redundancy.

### Syntax

**ipsec redundancy enable**

**undo ipsec redundancy enable**

### Default

IPsec redundancy is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

With IPsec redundancy enabled, the system synchronizes the following information from the active device to the standby device at configurable intervals:

- Lower bound values of the IPsec anti-replay window for inbound packets.
- IPsec anti-replay sequence numbers for outbound packets.

The synchronization ensures uninterrupted IPsec traffic forwarding and anti-replay protection when the active device fails.

To configure synchronization intervals, use the **redundancy replay-interval** command.

### Examples

# Enable IPsec redundancy.

```
<Sysname> system-view
[Sysname] ipsec redundancy enable
```

### Related commands

**redundancy replay-interval**

## ipsec sa global-duration

Use **ipsec sa global-duration** to configure the global IPsec SA lifetime.

Use **undo ipsec sa global-duration** to restore the default.

## Syntax

**ipsec sa global-duration** { **time-based** *seconds* **|** **traffic-based** *kilobytes* }

**undo ipsec sa global-duration** { **time-based | traffic-based** }

## Default

The time-based global lifetime is 3600 seconds, and the traffic-based global lifetime is 1843200 kilobytes.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**time-based** *seconds*: Specifies the time-based global lifetime for IPsec SAs, in the range of 180 to 604800 seconds.

**traffic-based** *kilobytes*: Specifies the traffic-based global lifetime for IPsec SAs, in the range of 2560 to 4294967295 kilobytes. When traffic on an SA reaches this value, the SA expires.

## Usage guidelines

You can also configure IPsec SA lifetimes in IPsec policy view or IPsec policy template view. The device prefers the IPsec SA lifetimes configured in IPsec policy view or IPsec policy template view over the global IPsec SA lifetimes.

When IKE negotiates IPsec SAs, it uses the local lifetime settings or those proposed by the peer, whichever are smaller.

An IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires. Before the IPsec SA expires, IKE negotiates a new IPsec SA, which takes over immediately after its creation.

## Examples

# Configure the global IPsec SA lifetime as 7200 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

# Configure the global IPsec SA lifetime as 10240 kilobytes.

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

## Related commands

- **display ipsec sa**
- **sa duration**

# ipsec sa idle-time

Use **ipsec sa idle-time** to enable the global IPsec SA idle timeout feature and set the idle timeout. If no traffic matches an IPsec SA within the idle timeout interval, the IPsec SA is deleted.

Use **undo ipsec sa idle-time** to disable the global IPsec SA idle timeout feature.

## Syntax

**ipsec sa idle-time** *seconds*

**undo ipsec sa idle-time**

### Default

The global IPsec SA idle timeout feature is disabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the IPsec SA idle timeout in the range of 60 to 86400 seconds.

### Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE.

The IPsec SA idle timeout can also be configured in IPsec policy view or IPsec policy template view, which takes precedence over the global IPsec SA timeout.

### Examples

# Set the IPsec SA idle timeout to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa idle-time 600
```

### Related commands

- **display ipsec sa**
- **sa idle-time**

## ipsec transform-set

Use **ipsec transform-set** to create an IPsec transform set and enter its view, or enter the view of an existing IPsec transform set.

Use **undo ipsec transform-set** to delete an IPsec transform set.

### Syntax

**ipsec transform-set** *transform-set-name*

**undo ipsec transform-set** *transform-set-name*

### Default

No IPsec transform sets exist.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*transform-set-name*: Specifies a name for the IPsec transform set, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, and authentication algorithms.

## Examples

# Create an IPsec transform set named **tran1** and enter its view.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-transform-set-tran1]
```

## Related commands

**display ipsec transform-set**

# local-address

Use **local-address** to configure the local IP address for the IPsec tunnel.

Use **undo local-address** to restore the default.

## Syntax

**local-address** { *ipv4-address* | **ipv6** *ipv6-address* }

**undo local-address**

## Default

The primary IPv4 address of the interface to which the IPsec policy is applied is used as the local IPv4 address. The first IPv6 address of the interface to which the IPsec policy is applied is used as the local IPv6 address.

## Views

IPsec policy view

IPsec policy template view

## Predefined user roles

network-admin

## Parameters

*ipv4-address*: Specifies the local IPv4 address for the IPsec tunnel.

**ipv6** *ipv6-address*: Specifies the local IPv6 address for the IPsec tunnel.

## Usage guidelines

The remote IP address on the IKE negotiation initiator must be the same as the local address on the IKE negotiation responder.

In a VRRP network, the local IP address must be the virtual IP address of the VRRP group to which the IPsec-applied interface belongs.

## Examples

# Configure the local address 1.1.1.1 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy map 1 isakmp
[Sysname-ipsec-policy-isakmp-map-1] local-address 1.1.1.1
```

## Related commands

**remote-address**

# pfs

Use **pfs** to enable the Perfect Forward Secrecy (PFS) feature for an IPsec transform set, used for IKE negotiation.

Use **undo pfs** to restore the default.

## Syntax

**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group24** | **dh-group19** | **dh-group20** }

**undo pfs**

## Default

The PFS feature is disabled for the IPsec transform set.

## Views

IPsec transform set view

## Predefined user roles

network-admin

## Parameters

**dh-group1**: Uses 768-bit Diffie-Hellman group.

**dh-group2**: Uses 1024-bit Diffie-Hellman group.

**dh-group5**: Uses 1536-bit Diffie-Hellman group.

**dh-group14**: Uses 2048-bit Diffie-Hellman group.

**dh-group24**: Uses 2048-bit and 256-bit subgroup Diffie-Hellman group.

**dh-group19**: Uses 256-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

**dh-group20**: Uses 384-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

## Usage guidelines

In terms of security and necessary calculation time, the following groups are in descending order: 384-bit ECP Diffie-Hellman group (**dh-group20**), 256-bit ECP Diffie-Hellman group (**dh-group19**), 2048-bit and 256-bit subgroup Diffie-Hellman group (**dh-group24**), 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), 1024-bit Diffie-Hellman group (**dh-group2**), and 768-bit Diffie-Hellman group (**dh-group1**).

The security level of the Diffie-Hellman group of the initiator must be higher than or equal to that of the responder.

The end without the PFS feature performs IKE negotiation according to the PFS requirements of the peer end.

## Examples

# Enable PFS using 2048-bit Diffie-Hellman group for IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] pfs dh-group14
```

# protocol

Use **protocol** to specify a security protocol for an IPsec transform set.

Use **undo protocol** to restore the default.

### Syntax

**protocol** { **ah** | **ah-esp** | **esp** }

**undo protocol**

### Default

The IPsec transform set uses the ESP protocol.

### Views

IPsec transform set view

### Predefined user roles

network-admin

### Parameters

**ah**: Specifies the AH protocol.

**ah-esp**: Specifies using the ESP protocol first and then using the AH protocol.

**ah**: Specifies the AH protocol.

### Usage guidelines

The two tunnel ends must use the same security protocol in the IPsec transform set.

### Examples

# Specify the AH protocol for the IPsec transform set.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] protocol ah
```

## qos pre-classify

Use **qos pre-classify** to enable the QoS pre-classify feature.

Use **undo qos pre-classify** to disable the QoS pre-classify feature.

### Syntax

**qos pre-classify**

**undo qos pre-classify**

### Default

The QoS pre-classify feature is disabled. QoS uses the new IP header of IPsec packets to perform traffic classification.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Usage guidelines

The QoS pre-classify feature enables QoS to classify packets by using the IP header of the original IP packets.

### Examples

# Enable the QoS pre-classify feature.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] qos pre-classify
```

# redundancy replay-interval

Use **redundancy replay-interval** to set the anti-replay window lower bound value synchronization interval for inbound packets and the sequence number synchronization interval for outbound packets.

Use **undo redundancy replay-interval** to restore the default.

## Syntax

**redundancy replay-interval inbound** *inbound-interval* **outbound** *outbound-interval*

**undo redundancy replay-interval**

## Default

The active device synchronizes the anti-replay window lower bound value every time it receives 1000 packets and synchronizes the sequence number every time it sends 100000 packets.

## Views

IPsec policy view

IPsec policy template view

## Predefined user roles

network-admin

## Parameters

**inbound** *inbound-interval*: Sets the interval at which the active device synchronizes the lower bound value of the IPsec anti-replay window to the standby device. This interval is expressed in the number of received packets, in the range of 0 to 1000. If you set the value to 0, the lower bound value of the anti-replay window will not be synchronized.

**outbound** *outbound-interval*: Sets the interval at which the active device synchronizes the IPsec anti-replay sequence number to the standby device. This interval is expressed in the number of sent packets, in the range of 1000 to 100000.

## Usage guidelines

The intervals take effect only after you enable IPsec redundancy by using the **ipsec redundancy enable** command.

A short interval improves the anti-replay information consistency between the active device and the standby device, but it sacrifices the forwarding performance of the devices.

## Examples

# Set the anti-replay window lower bound value synchronization interval for inbound packets to 800. Set the sequence number synchronization interval for outbound packets to 50000.

```
<Sysname> system-view
[Sysname] ipsec policy test 1 manual
[sysname-ipsec-policy-manual-test-1] redundancy replay-interval inbound 800 outbound
50000
```

## Related commands

- **ipsec anti-replay check**
- **ipsec anti-replay window**
- **ipsec redundancy enable**

# remote-address

Use **remote-address** to configure the remote IP address for the IPsec tunnel.

Use **undo remote-address** to restore the default.

## Syntax

**remote-address** { [ **ipv6** ] *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* }

**undo remote-address** { [ **ipv6** ] *host-name* **|** *ipv4-address* **|** **ipv6** *ipv6-address* }

## Default

No remote IP address is specified for the IPsec tunnel.

## Views

IPsec policy view

IPsec policy template view

## Predefined user roles

network-admin

## Parameters

**ipv6**: Specifies a remote IPv6 address. If you do not specify this keyword, you specify an IPv4 address or host name.

*hostname*: Specifies the remote host name, a case-insensitive string of 1 to 253 characters. The host name can be resolved to an IP address by the DNS server.

*ipv4-address*: Specifies a remote IPv4 address.

*ipv6-address*: Specifies a remote IPv6 address.

## Usage guidelines

This remote IP address configuration is required on the IKE negotiation initiator and optional on the responder if the responder uses an IPsec policy template.

A manual IPsec policy does not support DNS. Therefore, you must specify a remote IP address rather than a remote host name for the manual IPsec policy.

If you configure a remote host name, make sure the local end can always resolve the host name into the latest IP address of the remote end.

- If a DNS server is used for resolution, the local end queries the remote IP address again from the DNS server after the previously cached remote IP address expires. This mechanism ensures that the local end can always obtain the latest remote IP address.
- If a static DNS entry is used for resolution, you must reconfigure the **remote-address** command whenever the remote IP address changes. Without the reconfiguration, the local end cannot obtain the latest remote IP address.

For example, the local end has a static DNS entry which maps the host name **test** to the IP address 1.1.1.1. Configure the following commands:

# Configure the remote host name to **test** for the IPsec tunnel in the IPsec policy **policy1**.

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] remote-address test
```

# Change the IP address for the host **test** to 2.2.2.2.

```
[Sysname] ip host test 2.2.2.2
```

In this case, you must reconfigure the remote host name for the IPsec policy **policy1** so that the local end can obtain the latest IP address of the remote host.

# Reconfigure the remote host name to **test** for the IPsec tunnel in the IPsec policy **policy1**.

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname -ipsec-policy-isakmp-policy1-1] remote-address test
```

### Examples

# Specify the remote IP address 10.1.1.2 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-manual-policy1-10] remote-address 10.1.1.2
```

### Related commands

- **ip host** (see *Layer 3—IP Services Commands Reference*)
- **local-address**

## reset ipsec sa

Use **reset ipsec sa** to clear IPsec SAs.

### Syntax

**reset ipsec sa** [ { **ipv6-policy** | **policy** } *policy-name* [ *seq-number* ] | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } | **spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num* ]

### Views

User view

### Predefined user roles

network-admin

### Parameters

{ **ipv6-policy** | **policy** } *policy-name* [ *seq-number* ]: Clears IPsec SAs for the specified IPsec policy.

- **ipv6-policy**: Specifies an IPv6 IPsec policy.
- **policy**: Specifies an IPv4 IPsec policy.
- *policy-name*: Specifies the name of the IPsec policy, a case-insensitive string of 1 to 63 characters.
- *seq-number*: Specifies the sequence number of an IPsec policy entry, in the range of 1 to 65535. If you do not specify this argument, all the entries in the IPsec policy are specified.

**remote**: Clears IPsec SAs for the specified remote address.

- *ipv4-address*: Specifies a remote IPv4 address.
- **ipv6** *ipv6-address*: Specifies a remote IPv6 address.

**spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num* ]: Clears IPsec SAs matching the specified SA triplet: the remote address, the security protocol, and the SPI.

- *ipv4-address*: Specifies a remote IPv4 address.
- **ipv6** *ipv6-address*: Specifies a remote IPv6 address.
- **ah**: Specifies the AH protocol.
- **esp**: Specifies the ESP protocol.
- *spi-num*: Specifies the security parameter index in the range of 256 to 4294967295.

### Usage guidelines

If you do not specify any parameters, this command clears all IPsec SAs.

If you specify an SA triplet, this command clears the IPsec SA matching the triplet, and all the other IPsec SAs that were established during the same negotiation process, including the corresponding IPsec SA in the other direction, and the inbound and outbound IPSec SAs using the other security protocol (AH or ESP).

An outbound SA is uniquely identified by an SA triplet and an inbound SA is uniquely identified by an SPI. To clear IPsec SAs by specifying a triplet in the outbound direction, you should provide the remote IP address, the security protocol, and the SPI. To clear IPsec SAs by specifying a triplet in the inbound direction, you should provide the SPI and use any valid values for the other two parameters.

After a manual IPsec SA is cleared, the system automatically creates a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system creates new SAs only when IKE negotiation is triggered by packets.

### Examples

# Clear all IPsec SAs.

```
<Sysname> reset ipsec sa
```

# Clear the inbound and outbound IPsec SAs for the triplet of SPI 256, remote IP address 10.1.1.2, and security protocol AH.

```
<Sysname> reset ipsec sa spi 10.1.1.2 ah 256
```

# Clear all IPsec SAs for the remote IP address 10.1.1.2.

```
<Sysname> reset ipsec sa remote 10.1.1.2
```

# Clear all IPsec SAs for the entry 10 of the IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1 10
```

# Clear all IPsec SAs for the IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1
```

### Related commands

**display ipsec sa**

## reset ipsec statistics

Use **reset ipsec statistics** to clear IPsec packet statistics.

### Syntax

**reset ipsec statistics**[ **tunnel-id** *tunnel-id* ]

### Views

User view

### Predefined user roles

network-admin

### Parameters

**tunnel-id** *tunnel-id*: Clears IPsec packet statistics for the specified IPsec tunnel. The value range for the *tunnel-id* argument is 0 to 4294967295. If you do not specify this option, the command clears all IPsec packet statistics.

### Examples

# Clear IPsec packet statistics.

```
<Sysname> reset ipsec statistics
```

### Related commands

**display ipsec statistics**

# reverse-route dynamic

Use **reverse-route dynamic** to enable the IPsec reverse route inject (RRI) feature.

Use **undo reverse-route dynamic** to disable IPsec RRI.

## Syntax

**reverse-route dynamic**

**undo reverse-route dynamic**

## Default

IPsec RRI is disabled.

## Views

IPsec policy view

IPsec policy template view

## Predefined user roles

network-admin

## Usage guidelines

IPsec RRI is usually used on a gateway device at the headquarters side in an IPsec VPN.

After IPsec RRI is enabled for an IPsec policy or an IPsec policy template on a gateway device, the gateway device automatically creates a static route upon IPsec SA creation according to this IPsec policy or IPsec policy template.

In the static route, the destination IP address is the protected peer private network, and the next hop is the IP address of the remote tunnel interface.

When you enable or disable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs that are created according to this IPsec policy, and the associated static routes.

To display the static routes created by RRI, use the **display ip routing-table** command.

## Examples

# Enable IPsec RRI to create a static route according to the IPsec SA negotiated by the specified IPsec policy. The destination IP address is the protected peer private network 3.0.0.0/24, and the next hop is the IP address (1.1.1.2) of the remote tunnel interface.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

# Display the routing table. You can see a created static route. (Other information is not shown.)

```
[Sysname] display ip routing-table
…
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan-interface100
```

## Related commands

- **display ip routing-table** (*Layer 3—IP Routing Command Reference)*
- **ipsec policy**
- **ipsec policy-template**

# reverse-route preference

Use **reverse-route preference** to change the preference of the static routes created by IPsec RRI.

Use **undo reverse-route preference** to restore the default.

## Syntax

**reverse-route preference** *number*

**undo reverse-route preference**

## Default

The preference for the static routes created by IPsec RRI is 60.

## Views

IPsec policy view

IPsec policy template view

## Predefined user roles

network-admin

## Parameters

*number*: Sets a preference value. The value range is 1 to 255. A smaller value represents a higher preference.

## Usage guidelines

When you change this preference in an IPsec policy, the device deletes all IPsec SAs created according to this IPsec policy, and the associated static routes.

## Examples

# Change the preference to 100 for static routes created by IPsec RRI.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route preference 100
```

## Related commands

- **ipsec policy**
- **ipsec policy-template**

# reverse-route tag

Use **reverse-route tag** to set a route tag for the static routes created by IPsec RRI.

Use **undo reverse-route tag** to restore the default.

## Syntax

**reverse-route tag** *tag-value*

**undo reverse-route tag**

## Default

The tag value is 0 for the static routes created by IPsec RRI.

## Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*tag-value*: Sets a tag value. The value range is 1 to 4294967295.

### Usage guidelines

The tag value set by this command helps in implementing flexible route control through routing policies. When you change this tag value in an IPsec policy, the device deletes all IPsec SAs created by this IPsec policy, and all associated static routes.

### Examples

# Set the tag value to 50 for the static routes created by IPsec RRI.

```
<Sysname>system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route tag 50
```

### Related commands

- **ipsec policy**
- **ipsec policy-template**

## sa duration

Use **sa duration** to set an SA lifetime for an IPsec policy or IPsec policy template.

Use **undo sa duration** to remove the specified type of SA lifetime.

### Syntax

**sa duration** { **time-based** *seconds* **|** **traffic-based** *kilobytes* }

**undo sa duration** { **time-based | traffic-based** }

### Default

The SA lifetime of an IPsec policy or IPsec policy template is the current global SA lifetime.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

**time-based** *seconds*: Sets the time-based SA lifetime in the range of 180 to 604800 seconds.

**traffic-based** *kilobytes*: Sets the traffic-based SA lifetime in the range of 2560 to 4294967295 kilobytes.

### Usage guidelines

IKE prefers the SA lifetime of the IPsec policy or IPsec policy template over the global SA lifetime configured by the **ipsec sa global-duration** command. If the IPsec policy or IPsec policy template is not configured with the SA lifetime, IKE uses the global SA lifetime for SA negotiation.

During SA negotiation, IKE selects the shorter SA lifetime between the local SA lifetime and the remote SA lifetime.

### Examples

# Set the SA lifetime for the IPsec policy **policy1** to 7200 seconds.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

# Set the SA lifetime for the IPsec policy **policy1** to 20 MB. The IPsec SA expires after transmitting 20480 bytes.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

### Related commands

- **display ipsec sa**
- **ipsec sa global-duration**

## sa hex-key authentication

Use **sa hex-key authentication** to configure a hexadecimal authentication key for manual IPsec SAs.

Use **undo sa hex-key authentication** to remove the hexadecimal authentication key.

### Syntax

**sa hex-key authentication** { **inbound** | **outbound** } { **ah** | **esp** } { **cipher** | **simple** } *string*

**undo sa hex-key authentication** { **inbound** | **outbound** } { **ah** | **esp** }

### Default

No authentication key is configured for manual IPsec SAs.

### Views

IPsec policy view

### Predefined user roles

network-admin

### Parameters

**inbound**: Specifies a hexadecimal authentication key for inbound SAs.

**outbound**: Specifies a hexadecimal authentication key for outbound SAs.

**ah**: Uses AH.

**esp**: Uses ESP.

**cipher**: Specifies a key in encrypted form.

**simple**: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

*string*: Specifies the key. Its plaintext form is case insensitive and must be a 16-byte hexadecimal string for HMAC-MD5, a 20-byte hexadecimal string for HMAC-SHA1, and a 32-byte hexadecimal string for HMAC-SM3. Its encrypted form is a case-sensitive string of 1 to 85 characters.

### Usage guidelines

This command applies only to manual IPsec policies.

You must set an authentication key for both the inbound and outbound SAs.

The local inbound SA must use the same authentication key as the remote outbound SA, and the local outbound SA must use the same authentication key as the remote inbound SA.

If you execute this command multiple times, the most recent configuration takes effect.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

### Examples

# Configure plaintext authentication keys **0x112233445566778899aabbccddeeff00** and **0xaabbccddeeff001100aabbccddeeff00** for the inbound and outbound SAs that use AH.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication inbound ah simple
112233445566778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication outbound ah simple
aabbccddeeff001100aabbccddeeff00
```

### Related commands

- **display ipsec sa**
- **sa string-key**

## sa hex-key encryption

Use **sa encryption-hex** to configure a hexadecimal encryption key for manual IPsec SAs.

Use **undo sa encryption-hex** to remove the hexadecimal encryption key.

### Syntax

**sa hex-key encryption** { **inbound | outbound** } **esp** { **cipher | simple** } *string*

**undo sa hex-key encryption** { **inbound | outbound** } **esp**

### Default

No encryption key is configured for manual IPsec SAs.

### Views

IPsec policy view

### Predefined user roles

network-admin

### Parameters

**inbound**: Specifies a hexadecimal encryption key for inbound SAs.

**outbound**: Specifies a hexadecimal encryption key for outbound SAs.

**esp**: Uses ESP.

**cipher**: Specifies a key in encrypted form.

**simple**: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

*string*: Specifies the key. Its encrypted form is a case-sensitive string of 1 to 117 characters. Its plaintext form is a case-insensitive hexadecimal string and the key length varies by algorithm.

The following matrix shows the key length for the algorithms:

| Algorithm | Key length (bytes) |
|---|---|
| DES-CBC | 8 |
| 3DES-CBC | 24 |
| AES128-CBC | 16 |
| AES192-CBC | 24 |
| AES256-CBC | 32 |
| SM1128-CBC | 16 |
| SM1192-CBC | 24 |
| SM1256-CBC | 32 |

### Usage guidelines

This command applies only to manual IPsec policies.

You must set an encryption key for both the inbound and outbound SAs.

The local inbound SA must use the same encryption key as the remote outbound SA, and the local outbound SA must use the same encryption key as the remote inbound SA.

If you execute this command multiple times, the most recent configuration takes effect.

The keys for the IPsec SAs at the two tunnel ends must be configured in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

### Examples

# Configure plaintext encryption keys **0x1234567890abcdef** and **0xabcdefabcdef1234** for the inbound and outbound IPsec SAs that use ESP.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption inbound esp simple
1234567890abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption outbound esp simple
abcdefabcdef1234
```

### Related commands

- **display ipsec sa**
- **sa string-key**

## sa idle-time

Use **sa idle-time** to set the IPsec SA idle timeout for an IPsec policy or IPsec policy template. If no traffic matches an IPsec SA within the idle timeout interval, the IPsec SA is deleted.

Use **undo sa idle-time** to restore the default.

### Syntax

**sa idle-time** *seconds*

**undo sa idle-time**

### Default

An IPsec policy or IPsec policy template uses the global IPsec SA idle timeout.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the IPsec SA idle timeout in the range of 60 to 86400 seconds.

### Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE and takes effect when the **ipsec sa idle-time** command has been configured.

The IPsec SA idle timeout configured by this command takes precedence over the global IPsec SA timeout configured by the **ipsec sa idle-time** command.

### Examples

# Set the IPsec SA idle timeout to 600 seconds for the IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy map 100 isakmp
[Sysname-ipsec-policy-isakmp-map-100] sa idle-time 600
```

### Related commands

- **display ipsec sa**
- **ipsec sa idle-time**

## sa spi

Use **sa spi** to configure an SPI for IPsec SAs.

Use **undo sa spi** to remove the SPI.

### Syntax

**sa spi** { **inbound | outbound** } { **ah | esp** } *spi-number*

**undo sa spi** { **inbound | outbound** } { **ah | esp** }

### Default

No SPI is configured for IPsec SAs.

### Views

IPsec policy view

### Predefined user roles

network-admin

### Parameters

**inbound**: Specifies an SPI for inbound SAs.

**outbound**: Specifies an SPI for outbound SAs.

**ah**: Uses AH.

**esp**: Uses ESP.

*spi-number*: Specifies a security parameters index (SPI) in the range of 256 to 4294967295.

### Usage guidelines

This command applies only to manual IPsec policies.

You must configure an SPI for both inbound and outbound SAs, and make sure the SAs in each direction are unique: For an outbound SA, make sure its triplet (remote IP address, security protocol, and SPI) is unique. For an inbound SA, make sure its SPI is unique.

The local inbound SA must use the same SPI as the remote outbound SA, and the local outbound SA must use the same SPI as the remote inbound SA.

### Examples

# Set the SPI for the inbound SA to 10000 and the SPI for the outbound SA to 20000 in a manual IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

### Related commands

**display ipsec sa**

## sa string-key

Use **sa string-key** to set a key string (a key in character format) for manual IPsec SAs.

Use **undo sa string-key** to remove the key string.

### Syntax

**sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } [ **cipher** | **simple** ] *string*

**undo sa string-key** { **inbound** | **outbound** } { **ah** | **esp** }

### Default

No key string is configured for manual IPsec SAs.

### Views

IPsec policy view

### Predefined user roles

network-admin

### Parameters

**inbound**: Sets a key string for inbound IPsec SAs.

**outbound**: Sets a key string for outbound IPsec SAs.

**ah**: Uses AH.

**esp**: Uses ESP.

**cipher**: Specifies a key string in encrypted form.

**simple**: Specifies a key string in plaintext form. For security purposes, the key string specified in plaintext form will be stored in encrypted form.

*string*: Specifies the key string. Its encrypted form is a case-sensitive string of 1 to 373 characters. Its plaintext form is a case-sensitive string of 1 to 255 characters. Using the key string, the system automatically generates keys that meet the algorithm requirements. When the protocol is ESP, the system automatically generates keys for the authentication algorithm and encryption algorithm.

### Usage guidelines

This command applies only to manual IPsec policies.

You must set a key for both inbound and outbound SAs.

The local inbound SA must use the same key as the remote outbound SA, and the local outbound SA must use the same key as the remote inbound SA.

If you execute this command multiple times, the most recent configuration takes effect.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

### Examples

# Configure the inbound and outbound SAs that use AH to use the plaintext keys **abcdef** and **efcdab**, respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key outbound ah simple efcdab
```

### Related commands

- **display ipsec sa**
- **sa hex-key**

## security acl

Use **security acl** to specify an ACL for an IPsec policy or IPsec policy template.

Use **undo security acl** to restore the default.

### Syntax

**security acl** [ **ipv6** ] { *acl-number* **| name** *acl-name* } [ **aggregation | per-host** ]

**undo security acl**

### Default

An IPsec policy or IPsec policy template does not use an ACL.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

**ipv6**: Specifies an IPv6 ACL.

*acl-number*: Specifies an ACL by its number in the range of 3000 to 3999.

**name** *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

**aggregation**: Specifies the data protection mode as aggregation. The device does not support protecting IPv6 data flows in aggregation mode.

**per-host**: Specifies the data protection mode as per-host.

### Usage guidelines

An IKE-based IPsec policy supports the following data flow protection modes:

- **Standard mode**—One IPsec tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one IPsec tunnel that is established solely for it. The standard mode is used if you do not specify the aggregation or the per-host mode.
- **Aggregation mode**—One IPsec tunnel protects all data flows permitted by all the rules of an ACL. This mode is only used to communicate with old-version devices.
- **Per-host mode**—One IPsec tunnel protects one host-to-host data flow. One host-to-host data flow is identified by one ACL rule and protected by one IPsec tunnel established solely for it. This mode consumes more system resources when multiple data flows exist between two subnets to be protected.

A manual IPsec policy supports only the aggregation mode.

### Examples

# Specify IPv4 advanced ACL 3001 for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

# Specify IPv4 advanced ACL 3002 for the IPsec policy **policy2** and specify the data protection mode as aggregation.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination
10.1.2.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] rule 1 permit ip source 10.1.3.1 0.0.0.255 destination
10.1.3.2 0.0.0.255
[Sysname] ipsec policy policy2 1 isakmp
[Sysname-ipsec-policy-isakmp-policy2-1] security acl 3002 aggregation
```

### Related commands

- **display ipsec sa**
- **display ipsec tunnel**

# snmp-agent trap enable ipsec

Use **snmp-agent  trap enable ipsec** command to enable SNMP notifications for IPsec.

Use **undo snmp-agent trap enable ipsec** command to disable SNMP notifications for IPsec.

### Syntax

**snmp-agent trap enable ipsec** [ **auth-failure** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** **tunnel-start** | **tunnel-stop**] *

**undo snmp-agent trap enable ipsec** [ **auth-failure** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** **tunnel-start** | **tunnel-stop**] *

### Default

All SNMP notifications for IPsec are disabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**auth-failure**: Specifies SNMP notifications for authentication failures.

**decrypt-failure**: Specifies SNMP notifications for decryption failures.

**encrypt-failure**: Specifies SNMP notifications for encryption failures.

**global**: Specifies SNMP notifications globally.

**invalid-sa-failure**: Specifies SNMP notifications for invalid-SA failures.

**no-sa-failure**: Specifies SNMP notifications for SA-not-found failures.

**policy-add**: Specifies SNMP notifications for events of adding IPsec policies.

**policy-attach**: Specifies SNMP notifications for events of applying IPsec policies to interfaces.

**policy-delete**: Specifies SNMP notifications for events of deleting IPsec policies.

**policy-detach**: Specifies SNMP notifications for events of removing IPsec policies from interfaces.

**tunnel-start**: Specifies SNMP notifications for events of creating IPsec tunnels.

**tunnel-stop**: Specifies SNMP notifications for events of deleting IPsec tunnels.

### Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IPsec.

To generate and output SNMP notifications for a specific IPsec failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IPsec globally.
2. Enable SNMP notifications for the failure type or event type.

### Examples

# Enable SNMP notifications for IPsec globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ipsec global
```

# Enable SNMP notifications for events of creating IPsec tunnels.

```
[Sysname] snmp-agent trap enable ipsec tunnel-start
```

## tfc enable

Use **tfc enable** to enable the Traffic Flow Confidentiality (TFC) padding feature.

Use **undo tfc enable** to disable TFC padding.

### Syntax

**tfc enable**

**undo tfc enable**

### Default

TFC padding is disabled.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Usage guidelines

The TFC padding feature can hide the length of the original packet, and might affect the packet encapsulation and de-encapsulation performance. This feature takes effect on UDP packets encapsulated by ESP in transport mode and on original IP packets encapsulated by ESP in tunnel mode.

### Examples

# Enable TFC padding for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

### Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**

## transform-set

Use **transform-set** to specify an IPsec transform set for an IPsec policy or IPsec policy template.

Use **undo transform-set** to remove the IPsec transform set specified for an IPsec policy or IPsec policy template.

### Syntax

**transform-set** *transform-set-name*&<1-6>

**undo transform-set** [ *transform-set-name* ]

### Default

No IPsec transform set is specified for an IPsec policy or IPsec policy template.

### Views

IPsec policy view

IPsec policy template view

### Predefined user roles

network-admin

### Parameters

*transform-set-name*&<1-6>: Specifies a space-separated list of up to six IPsec transform sets by their names, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

A manual IPsec policy can use only one IPsec transform set. If you specify an IPsec transform set for the manual IPsec policy multiple times, the most recent configuration takes effect.

An IKE-based IPsec policy can use a maximum of six IPsec transform sets. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.

If you do not specify the *transform-set-name* argument, the **undo transform-set** command removes all IPsec transform sets specified for the IPsec policy or IPsec policy template.

## Examples

# Specify the IPsec transform set **prop1** for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set prop1
[Sysname-ipsec-transform-set-prop1] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] transform-set prop1
```

## Related commands

- **ipsec** { **ipv6-policy** | **policy** }
- **ipsec transform-set**

# IKE commands

The following matrix shows the feature and hardware compatibility:

| Hardware series | Model | IKE compatibility |
|---|---|---|
| WX1800H series | WX1804H<br>WX1810H<br>WX1820H | Yes |
| WX2500H series | WX2510H<br>WX2540H<br>WX2560H | Yes |
| WX3000H series | WX3010H | Yes |
| | WX3010H-L | No |
| | WX3010H-X | Yes |
| | WX3024H | Yes |
| | WX3024H-L | No |
| WX3500H series | WX3508H<br>WX3510H<br>WX3520H<br>WX3540H | Yes |
| WX5500E series | WX5510E<br>WX5540E | Yes |
| WX5500H series | WX5540H<br>WX5560H<br>WX5580H | Yes |
| Access controller modules | EWPXM1MAC0F<br>EWPXM1WCME0<br>EWPXM2WCMD0F<br>LSQM1WCMX20<br>LSQM1WCMX40<br>LSUM1WCME0<br>LSUM1WCMX20RT<br>LSUM1WCMX40RT | Yes |

## aaa authorization

Use **aaa authorization** to enable IKE AAA authorization.

Use **undo aaa authorization** to disable IKE AAA authorization.

### Syntax

**aaa authorization domain** *domain-name* **username** *user-name*

**undo aaa authorization**

### Default

IKE AAA authorization is disabled.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**domain** *domain-name*: Specifies the ISP domain used for requesting authorization attributes. The ISP domain name is a case-insensitive string of 1 to 255 characters and must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

**username** *user-name*: Specifies the username used for requesting authorization attributes. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain the domain name.
- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

### Usage guidelines

The AAA authorization feature enables IKE to request authorization attributes, such as the IKE IPv4 address pool, from AAA.

IKE uses the ISP domain and username to request authorization attributes. AAA uses the authorization settings in the ISP domain to request the user's authorization attributes from the remote AAA server or the local user database. After IKE passes the username authentication, it obtains the authorization attributes.

This feature is applicable when AAA is used to centrally manage and deploy authorization attributes.

### Examples

# Create the IKE profile **profile1**.

```
<Sysname> system-view
[Sysname] ike profile profile1
```

# Enable AAA authorization. Specify the ISP domain **abc** and the username **test**.

```
[Sysname-ike-profile-profile1] aaa authorization domain abc username test
```

## authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for an IKE proposal.

Use **undo authentication-algorithm** to restore the default.

### Syntax

**authentication-algorithm** { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

**undo authentication-algorithm**

### Default

The IKE proposal uses the HMAC-SHA1 authentication algorithm.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

**md5**: Specifies HMAC-MD5 as the authentication algorithm.

**sha**: Specifies HMAC-SHA1 as the authentication algorithm.

**sha256**: Specifies HMAC-SHA256 as the authentication algorithm.

**sha384**: Specifies HMAC-SHA384 as the authentication algorithm.

**sha512**: Specifies HMAC-SHA512 as the authentication algorithm.

### Examples

# Specify HMAC-SHA1 as the authentication algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-algorithm sha
```

### Related commands

**display ike proposal**

## authentication-method

Use **authentication-method** to specify an authentication method to be used in an IKE proposal.

Use **undo authentication-method** to restore the default.

### Syntax

**authentication-method** { **dsa-signature** | **pre-share** | **rsa-signature** }

**undo authentication-method**

### Default

The IKE proposal uses the pre-shared key as the authentication method.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

**dsa-signature**: Specifies the DSA signatures as the authentication method.

**pre-share**: Specifies the pre-shared key as the authentication method.

**rsa-signature**: Specifies the RSA signatures as the authentication method.

### Usage guidelines

Pre-shared key authentication does not require certificates as signature authentication does, and it is usually used in a simple network. Signature authentication provides higher security, and it is usually deployed in a large-scale network, such as a network with many branches.

Authentication methods configured on both IKE ends must match.

If you specify RSA or DSA signatures, you must configure the IKE peer to obtain certificates from a CA.

If you specify pre-shared keys, you must configure these pre-shared keys on both IKE ends.

### Examples

# Specify pre-shared key authentication to be used in IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-method pre-share
```

### Related commands

- **display ike proposal**
- **ike keychain**
- **pre-shared-key**

## certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication.

Use **undo certificate domain** to remove a PKI domain for signature authentication.

### Syntax

**certificate domain** *domain-name*

**undo certificate domain** *domain-name*

### Default

No PKI domains are specified for signature authentication.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

*domain-name*: Specifies the name of a PKI domain, a case-insensitive string of 1 to 31 characters. If you do not specify this argument, all PKI domains configured on the device are used for enrollment, authentication, certificate issuing, validation, and signature.

### Usage guidelines

You can specify a maximum of six PKI domains for an IKE profile.

IKE uses the specified PKI domains for enrollment, authentication, certificate issuing, validation, and signature. If you do not specify any PKI domains, IKE uses all PKI domains configured on the device.

Follow these restrictions and guidelines for the device to obtain the CA certificate during IKE negotiation:

- On the initiator:
  - If the IKE profile has a PKI domain and the automatic certificate request mode is configured for the PKI domain, the initiator automatically obtains the CA certificate.
  - If the IKE profile has no PKI domain, you must manually obtain the CA certificate.
- On the responder:

- If main mode is used in IKE phase 1, the responder does not automatically obtain the CA certificate. You must manually obtain the CA certificate.
- If aggressive mode is used in IKE phase 1, the responder automatically obtains the CA certificate if the following conditions are met:
  - A matching IKE profile is found.
  - An PKI domain is specified in the IKE profile.
  - The automatic certificate request mode is configured for the PKI domain.

  If the conditions are not met, you must manually obtain the CA certificate.

IKE first automatically obtains the CA certificate, and then requests a local certificate. If the CA certificate already exists locally, IKE automatically requests a local certificate.

### Examples

# Specify the PKI domain **abc** for IKE profile 1.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] certificate domain abc
```

### Related commands

- **authentication-method**
- **pki domain**

## client-authentication

Use **client-authentication** to enable client authentication.

Use **undo client-authentication** to disable client authentication.

### Syntax

**client-authentication xauth**

**undo client-authentication**

### Default

Client authentication is disabled.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**xauth**: Uses Extended Authentication within ISAKMP/Oakley (XAUTH) for authentication.

### Usage guidelines

The client authentication feature provides additional authentication in IKE negotiation for secure remote access to an IPsec VPN.

When networking an IPsec VPN for remote access, enable client authentication on the IPsec gateway. During the IKE negotiation, the IPsec gateway uses a RADIUS server to authenticate the remote users. Remote users that provide the correct username and password pass the authentication and continue with the negotiation. This feature simplifies the configuration on the IPsec gateway and ensures the validity of the remote users. If you do not use this feature, you must configure an IPsec policy and an authentication password for each remote user, which is time-consuming and hard to maintain.

### Examples

# Enable XAUTH client authentication.

```
<Sysname> system-view
[Sysname] ike profile test
[Sysname-ike-profile-test] client-authentication xauth
```

### Related commands

**local-user**

## description

Use **description** to configure a description for an IKE proposal.

Use **undo description** to restore the default.

### Syntax

**description** *text*

**undo description**

### Default

An IKE proposal does not have a description.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

*text*: Specifies the description, a case-sensitive string of 1 to 80 characters.

### Usage guidelines

You can configure different descriptions for IKE proposals to distinguish them.

### Examples

# Configure a description of **test** for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] description test
```

## dh

Use **dh** to specify the DH group to be used in key negotiation phase 1 for an IKE proposal.

Use **undo dh** to restore the default.

### Syntax

**dh** { **group1** | **group14** | **group2** | **group24** | **group5** }

**undo dh**

### Default

An IKE proposal uses **group1**, the 768-bit Diffie-Hellman group.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

**group1**: Uses the 768-bit Diffie-Hellman group.

**group14**: Uses the 2048-bit Diffie-Hellman group.

**group2**: Uses the 1024-bit Diffie-Hellman group.

**group24**: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

**group5**: Uses the 1536-bit Diffie-Hellman group.

### Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose a proper Diffie-Hellman group for your network.

### Examples

# Specify the 2048-bit Diffie-Hellman group **group1** to be used in key negotiation phase 1 for an IKE proposal.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] dh group14
```

### Related commands

**display ike proposal**

## display ike proposal

Use **display ike proposal** to display configuration information about all IKE proposals.

### Syntax

**display ike proposal**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Usage guidelines

This command displays the configuration information about all IKE proposals in descending order of proposal priorities. If no IKE proposal is configured, this command displays the default IKE proposal.

### Examples

# Display the configuration information about all IKE proposals.

```
<Sysname> display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
----------------------------------------------------------------------------
```

```
1        RSA-SIG            SHA1        DES-CBC     Group 1        5000
11       PRE-SHARED-KEY     SHA1        DES-CBC     Group 1        50000
default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```

**Table 9 Command output**

| Field | Description |
|---|---|
| Priority | Priority of the IKE proposal |
| Authentication method | Authentication method used by the IKE proposal. |
| Authentication algorithm | Authentication algorithm used in the IKE proposal:<br>• **MD5**—HMAC-MD5 algorithm.<br>• **SHA1**—HMAC-SHA1 algorithm.<br>• **SHA256**—HMAC-SHA256 algorithm.<br>• **SHA384**—HMAC-SHA384 algorithm.<br>• **SHA512**—HMAC-SHA512 algorithm. |
| Encryption algorithm | Encryption algorithm used by the IKE proposal:<br>• **3DES-CBC**—168-bit 3DES algorithm in CBC mode.<br>• **AES-CBC-128**—128-bit AES algorithm in CBC mode.<br>• **AES-CBC-192**—192-bit AES algorithm in CBC mode.<br>• **AES-CBC-256**—256-bit AES algorithm in CBC mode.<br>• **DES-CBC**—56-bit DES algorithm in CBC mode. |
| Diffie-Hellman group | DH group used in IKE negotiation phase 1. |
| Duration (seconds) | IKE SA lifetime (in seconds) of the IKE proposal |

### Related commands

**ike proposal**

# display ike sa

Use **display ike sa** to display information about the current IKE SAs.

### Syntax

**display ike sa** [ **verbose** [ **connection-id** *connection-id* | **remote-address** [ **ipv6** ] *remote-address* ] ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**verbose**: Displays detailed information.

**connection-id** *connection-id*: Displays detailed information about IKE SAs by connection ID in the range of 1 to 2000000000.

**remote-address**: Displays detailed information about IKE SAs with the specified remote address.

**ipv6**: Specifies an IPv6 address.

*remote-address*: Remote IP address.

## Usage guidelines

If you do not specify any parameters, this command displays a summary about all IKE SAs.

## Examples

# Display information about the current IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote          Flag        DOI
  ----------------------------------------------------------
      1            202.38.0.2      RD          IPSEC
Flags:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING
```

**Table 10 Command output**

| Field | Description |
|---|---|
| Connection-ID | Identifier of the IKE SA. |
| Remote | Remote IP address of the SA. |
| Flags | Status of the SA:<br>• **RD (READY)**—The SA has been established.<br>• **ST (STAYALIVE)**—This end is the initiator of the tunnel negotiation.<br>• **RL (REPLACED)**—The SA has been replaced by a new one and will be deleted later.<br>• **FD (FADING)**—The SA is in use, but it is about to expire and will be deleted soon.<br>• **RK (REKEY)**—The SA is a Rekey SA.<br>• **Unknown**—The SA status is unknown. |
| DOI | Interpretation domain to which the SA belongs.<br>• **IPSEC**—The SA belongs to an IPsec DOI.<br>• **Group**—The SA belongs to a GDOI. The device does not support GDOI in the current software version. |

# Display detailed information about the current IKE SAs.

```
<Sysname> display ike sa verbose
    ---------------------------------------------
    Connection ID: 2
    Outside VPN: 1
    Inside VPN: 1
    Profile: prof1
    Transmitting entity: Initiator
    ---------------------------------------------
    Local IP: 4.4.4.4
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP: 4.4.4.5
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected
    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
```

# Display detailed information about the IKE SA with the remote address of 4.4.4.5.

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
    -----------------------------------------------
    Connection ID: 2
    Outside VPN: 1
    Inside VPN: 1
    Profile: prof1
    Transmitting entity: Initiator
    -----------------------------------------------
    Local IP: 4.4.4.4
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP: 4.4.4.5
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected
    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
```

**Table 11 Command output**

| Field | Description |
|---|---|
| Connection ID | Identifier of the IKE SA. |
| Outside VPN | Name of the VPN instance to which the receiving interface belongs.<br>The device does not support this field in the current software version. |
| Inside VPN | Name of the VPN instance to which the protected data belongs.<br>The device does not support this field in the current software version. |
| Profile | Name of the matching IKE profile found in the IKE SA negotiation.<br>If no matching profile is found, this field displays nothing. |

| Field | Description |
|---|---|
| Transmitting entity | Role of the IKE negotiation entity: Initiator or Responder. |
| Local IP | IP address of the local gateway. |
| Local ID type | Identifier type of the local gateway. |
| Local ID | Identifier of the local gateway. |
| Remote IP | IP address of the remote gateway. |
| Remote ID type | Identifier type of the remote gateway. |
| Remote ID | Identifier of the remote security gateway. |
| Authentication-method | Authentication method used by the IKE proposal. |
| Authentication-algorithm | Authentication algorithm used by the IKE proposal:<br>• **MD5**—HMAC-MD5 algorithm.<br>• **SHA1**—HMAC-SHA1 algorithm.<br>• **SHA256**—HMAC-SHA256 algorithm.<br>• **SHA384**—HMAC-SHA384 algorithm.<br>• **SHA512**—HMAC-SHA512 algorithm. |
| Encryption-algorithm | Encryption algorithm used by the IKE proposal:<br>• **3DES-CBC**—168-bit 3DES algorithm in CBC mode.<br>• **AES-CBC-128**—128-bit AES algorithm in CBC mode.<br>• **AES-CBC-192**—192-bit AES algorithm in CBC mode.<br>• **AES-CBC-256**—256-bit AES algorithm in CBC mode.<br>• **DES-CBC**—56-bit DES algorithm in CBC mode. |
| Life duration(sec) | Lifetime of the IKE SA in seconds. |
| Remaining key duration(sec) | Remaining lifetime of the IKE SA in seconds. |
| Exchange-mode | IKE negotiation mode in phase 1: main mode or aggressive mode. |
| Diffie-Hellman group | DH group used for key negotiation in IKE phase 1. |
| NAT traversal | Whether NAT traversal is detected. |
| Extend authentication | Whether extended authentication for clients is enabled. |
| Assigned IP address | IP address assigned to the remote peer.<br>This field is not displayed if no IP address is assigned. |

# display ike statistics

Use **display ike statistics** to display IKE statistics.

## Syntax

**display ike statistics**

## Views

Any view

## Predefined user roles

network-admin

network-operator

### Examples

# Display IKE statistics.

```
<Sysname> display ike statistics
  No matching proposal: 0
  Invalid ID information: 0
  Unavailable certificate: 0
  Unsupported DOI: 0
  Unsupported situation: 0
  Invalid proposal syntax: 0
  Invalid SPI: 0
  Invalid protocol ID: 0
  Invalid certificate: 0
  Authentication failure: 0
  Invalid flags: 0
  Invalid message id: 0
  Invalid cookie: 0
  Invalid transform ID: 0
  Malformed payload: 0
  Invalid key information: 0
  Invalid hash information: 0
  Unsupported attribute: 0
  Unsupported certificate type: 0
  Invalid certificate authority: 0
  Invalid signature: 0
  Unsupported exchage type: 0
  No available SA: 1
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
```

### Related commands

**reset ike statistics**

## dpd

Use **dpd** to enable the device to send DPD messages.

Use **undo dpd** to disable the IKE DPD feature.

### Syntax

**dpd interval** *interval* [ **retry** *seconds* ] { **on-demand** | **periodic** }

**undo dpd interval**

### Default

IKE DPD is disabled.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**interval** *interval*: Specifies a period of time in seconds. The value range is from 1 to 300.

- If the **on-demand** keyword is specified, this parameter specifies the number of seconds during which no IPsec packet is received before DPD is triggered if the local end has IPsec traffic to send.
- If the **periodic** keyword is specified, this parameter specifies a DPD triggering interval.

**retry** *seconds*: Specifies the number of seconds between DPD retries if the DPD message fails. The value for the *second* argument is from 1 to 60 seconds, and it defaults to 5 seconds.

**on-demand**: Sends DPD messages on demand.

**periodic**: Sends DPD messages at regular intervals.

### Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

### Examples

# Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] dpd interval 10 retry 5 on-demand
```

### Related commands

**ike dpd**

## encryption-algorithm

Use **encryption-algorithm** to specify an encryption algorithm for an IKE proposal.

Use **undo encryption-algorithm** to restore the default.

### Syntax

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

**undo encryption-algorithm**

### Default

An IKE proposal uses the 56-bit DES encryption algorithm in CBC mode.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

**3des-cbc**: Uses the 3DES algorithm in CBC mode as the encryption algorithm. The 3DES algorithm uses a 168-bit key for encryption.

**aes-cbc-128**: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses a 128-bit key for encryption.

**aes-cbc-192**: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses a 192-bit key for encryption.

**aes-cbc-256**: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses a 256-bit key for encryption.

**des-cbc**: Uses the DES algorithm in CBC mode as the encryption algorithm. The DES algorithm uses a 56-bit key for encryption.

### Usage guidelines

Different algorithms provide different levels of protection. Generally, an algorithm with a longer key is stronger. A stronger algorithm provides more resistance to decryption but uses more resources. The algorithm strength from low to high is **des-cbc**, **3des-cbc**, **aes-cbc-128**, **aes-cbc-192**, and **aes-cbc-256**.

### Examples

# Use the 128-bit AES in CBC mode as the encryption algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] encryption-algorithm aes-cbc-128
```

### Related commands

**display ike proposal**

## exchange-mode

Use **exchange-mode** to select an IKE negotiation mode for phase 1.

Use **undo exchange-mode** to restore the default.

### Syntax

**exchange-mode** { **aggressive** | **main** }

**undo exchange-mode**

### Default

Main mode is used for phase 1.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**aggressive**: Specifies the aggressive mode.

**main**: Specifies the main mode.

### Usage guidelines

When a user at the local end of an IPsec tunnel obtains an IP address automatically and pre-shared key authentication is used, H3C recommends specifying the **aggressive** mode at the local end.

### Examples

# Specify that IKE negotiation operates in main mode.

```
<Sysname> system-view
```

```
[Sysname] ike profile 1
[Sysname-ike-profile-1] exchange-mode main
```

### Related commands

**display ike proposal**

## ike address-group

Use i**ke address-group** to configure an IKE IPv4 address pool for assigning IPv4 addresses to remote peers.

Use **undo** i**ke address-group** to delete an IKE IPv4 address pool.

### Syntax

i**ke address-group** *group-name start-ipv4-address end-ipv4-address* [ *mask* **|** *mask-length* ]

**undo** i**ke address-group** *group-name*

### Default

No IKE IPv4 address pools exist.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*group-name*: Specifies a name for the IKE IPv4 address pool, a case-insensitive string of 1 to 63 characters.

*start-ipv4-address end-ipv4-address*: Specifies an IPv4 address range. The *start-ipv4-address* argument specifies the start IPv4 address. The *end-ipv4-address* argument specifies the end IPv4 address.

*mask*: Specifies the IPv4 address mask.

*mask-length*: Specifies the length of the IPv4 address mask.

### Usage guidelines

An IKE IPv4 address pool can contain a maximum of 8192 IPv4 addresses.

To modify or delete an address pool, you must delete all IKE SAs and IPsec SAs. Otherwise, the assigned IPv4 addresses might not be reclaimed.

### Examples

# Configure an IKE IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask 255.255.255.0.

```
<Sysname> system-view
[Sysname] ike address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

# Configure an IKE IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask length 32.

```
<Sysname> system-view
[Sysname] ike address-group ipv4group 1.1.1.1 1.1.1.2 32
```

### Related commands

**aaa authorization**

# ike dpd

Use **ike dpd** to enable sending DPD messages.

Use **undo ike dpd** to disable the DPD feature.

## Syntax

**ike dpd interval** *interval* [ **retry** *seconds* ] { **on-demand** | **periodic** }

**undo ike dpd interval**

## Default

IKE DPD is disabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**interval** *interval*: Specifies a period of time in seconds. The value range is from 1 to 300.

- If the **on-demand** keyword is specified, this parameter specifies the number of seconds during which no IPsec packet is received before DPD is triggered if the local end has IPsec traffic to send.
- If the **periodic** keyword is specified, this parameter specifies a DPD triggering interval.

**retry** *seconds*: Specifies the number of seconds between DPD retries if the DPD message fails. The value for the *second* argument is from 1 to 60 seconds, and it defaults to 5 seconds.

**on-demand**: Sends DPD messages on demand.

**periodic**: Sends DPD messages at regular intervals.

## Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodical triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

## Examples

# Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike dpd interval 10 retry 5 on-demand
```

## Related commands

**dpd**

# ike identity

Use **ike identity** to specify the global identity used by the local end during IKE negotiations.

Use **undo ike identity** to restore the default.

### Syntax

**ike identity** { **address** { *ipv4-address* **| ipv6** *ipv6-address* } **| dn | fqdn** [ *fqdn-name* ] **| user-fqdn** [ *user-fqdn-name* ] }

**undo ike identity**

### Default

The IP address of the interface where the IPsec policy applies is used as the IKE identity.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**address** { *ipv4-address* **| ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the identity.

**dn**: Uses the DN in the digital signature as the identity.

**fqdn** *fqdn-name*: Uses the FQDN name as the identity. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

**user-fqdn** *user-fqdn-name*: Uses the user FQDN name as the identity. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, abc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

### Usage guidelines

The global identity can be used by the device for all IKE SA negotiations. The local identity (set by the **local-identity** command) can be used only by the device that uses the IKE profile.

In pre-shared key authentication, you cannot set the DN as the identity.

When you specify the global identity for signature authentication, follow these restrictions and guidelines:

- You can set any type of identity information.
- The **ike signature-identity from-certificate** command sets the local device to always use the identity information obtained from the local certificate.
- If the **ike signature-identity from-certificate** command is not set, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

### Examples

# Set the IP address 2.2.2.2 as the identity.

```
<sysname> system-view
[sysname] ike identity address 2.2.2.2
```

### Related commands

- **local-identity**
- **ike signature-identity from-certificate**

# ike invalid-spi-recovery enable

Use **ike invalid-spi-recovery enable** to enable invalid security parameter index (SPI) recovery.

Use **undo ike invalid-spi-recovery enable** to disable invalid SPI recovery.

### Syntax

**ike invalid-spi-recovery enable**

**undo ike invalid-spi-recovery enable**

### Default

Invalid SPI recovery is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

IPsec "black hole" occurs when one IPsec peer fails (for example, a peer can fail if a reboot occurs). One peer fails and loses its SAs with the other peer. When an IPsec peer receives a data packet for which it cannot find an SA, an invalid SPI is encountered. The peer drops the data packet and tries to send an SPI invalid notification to the data originator. This notification is sent by using the IKE SA. When no IKE SA is available, the notification is not sent. The originating peer continues sending the data by using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic.

The invalid SPI recovery feature enables the receiving peer to set up an IKE SA with the originator so that an SPI invalid notification can be sent. Upon receiving the notification, the originating peer deletes the IPsec SA that has the invalid SPI. If the originator has data to send, new SAs will be set up.

Use caution when you enable the invalid SPI recovery feature, because using this feature can result in a DoS attack. Attackers can make a great number of invalid SPI notifications to the same peer.

### Examples

# Enable invalid SPI recovery.

```
<Sysname> system-view
[Sysname] ike invalid-spi-recovery enable
```

## ike keepalive interval

Use **ike keepalive interval** to enable sending IKE keepalives and set the sending interval.

Use **undo ike keepalive interval** to restore the default.

### Syntax

**ike keepalive interval** *interval*

**undo ike keepalive interval**

### Default

No IKE keepalives are sent.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*interval*: Sets the number of seconds between IKE keepalives, in the range of 20 to 28800.

### Usage guidelines

To detect the status of the peer, configure IKE DPD instead of the IKE keepalive feature, unless IKE DPD is not supported on the peer.

The keepalive timeout time configured at the local must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout timer to three times as long as the keepalive interval.

### Examples

# Set the keepalive interval to 200 seconds

```
<Sysname> system-view
[Sysname] ike keepalive interval 200
```

### Related commands

**ike keepalive timeout**

## ike keepalive timeout

Use **ike keepalive timeout** to set the IKE keepalive timeout time.

Use **undo ike keepalive timeout** to restore the default.

### Syntax

**ike keepalive timeout** *seconds*

**undo ike keepalive timeout**

### Default

The IKE keepalive timeout time is not set.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the number of seconds between IKE keepalives. The value is in the range of 20 to 28800.

### Usage guidelines

If the local end receives no keepalive packets from the peer during the timeout time, the IKE SA is deleted along with the IPsec SAs it negotiated.

The keepalive timeout time configured at the local end must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout timer to three times as long as the keepalive interval.

### Examples

# Set the keepalive timeout time to 20 seconds.

```
<Sysname> system-view
[Sysname] ike keepalive timeout 20
```

### Related commands

**ike keepalive interval**

# ike keychain

Use **ike keychain** to create an IKE keychain and enter its view, or enter the view of an existing IKE keychain.

Use **undo ike keychain** to delete an IKE keychain.

## Syntax

**ike keychain** *keychain-name*

**undo ike keychain** *keychain-name*

## Default

No IKE keychains exist.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*keychain-name*: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

## Usage guidelines

To use pre-shared key authentication, you must create and specify an IKE keychain for the IKE profile.

## Examples

# Create IKE keychain **key1** and enter its view.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1]
```

## Related commands

- **authentication-method**
- **pre-shared-key**

# ike limit

Use **ike limit** to set the maximum number of half-open IKE SAs and the maximum number of established IKE SAs.

Use **undo ike limit** to restore the default.

## Syntax

**ike limit** { **max-negotiating-sa** *negotiation-limit* **|** **max-sa** *sa-limit* }

**undo ike limit** { **max-negotiating-sa | max-sa** }

## Default

There is no limit to the maximum number of IKE SAs.

## Views

System view

### Predefined user roles

network-admin

### Parameters

**max-negotiating-sa** *negotiation-limit*: Sets the maximum number of half-open IKE SAs and IPsec SAs. The value range for the *negotiation-limit* argument is 1 to 99999.

**max-sa** *sa-limit*: Sets the maximum number of established IKE SAs. The value range for the *sa-limit* argument is 1 to 99999.

### Usage guidelines

The supported maximum number of half-open IKE SAs depends on the device's processing capability. Adjust the maximum number of half-open IKE SAs to make full use of the device's processing capability without affecting the IKE SA negotiation efficiency.

The supported maximum number of established IKE SAs depends on the device's memory space. Adjust the maximum number of established IKE SAs to make full use of the device's memory space without affecting other applications in the system.

### Examples

# Set the maximum number of half-open IKE SAs and IPsec SAs to 200.

```
<Sysname> system-view
[Sysname] ike limit max-negotiating-sa 200
```

# Set the maximum number of established IKE SAs to 5000.

```
<Sysname> system-view
[Sysname] ike limit max-sa 5000
```

## ike logging negotiation enable

Use **ike logging negotiation enable** to enable logging for IKE negotiation.

Use **undo ike logging negotiation packet enable** to disable logging for IKE negotiation.

### Syntax

**ike logging negotiation enable**

**undo ike logging negotiation enable**

### Default

Logging for IKE negotiation is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

This command enables the device to output logs for the IKE negotiation process.

### Examples

# Enable logging for IKE negotiation.

```
<Sysname> system-view
[Sysname] ike logging negotiation enable
```

# ike nat-keepalive

Use **ike nat-keepalive** to set the NAT keepalive interval.

Use **undo ike nat-keepalive** to restore the default.

## Syntax

**ike nat-keepalive** *seconds*

**undo ike nat-keepalive**

## Default

The NAT keepalive interval is 20 seconds.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*seconds*: Sets the NAT keepalive interval in seconds, in the range of 5 to 300.

## Usage guidelines

This command takes effect only for a device behind a NAT server. When the device resides behind a NAT server, the IKE gateway behind the NAT server needs to send NAT keepalive packets to its peer IKE gateway to keep the NAT session alive. For information about how to display the lifetime of NAT entries, see *Layer 3–IP Services Command Reference*.

## Examples

# Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ike nat-keepalive 5
```

# ike profile

Use **ike profile** to create an IKE profile and enter its view, or enter the view of an existing IKE profile.

Use **undo ike profile** to delete an IKE profile.

## Syntax

**ike profile** *profile-name*

**undo ike profile** *profile-name*

## Default

No IKE profiles exist.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*profile-name*: Specifies an IKE profile name, a case-insensitive string of 1 to 63 characters.

### Examples

# Create IKE profile 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1]
```

## ike proposal

Use **ike proposal** to create an IKE proposal and enter its view, or enter the view of an existing IKE proposal.

Use **undo ike proposal** to delete an IKE proposal.

### Syntax

**ike proposal** proposal-number

**undo ike proposal** *proposal-number*

### Default

The system has an IKE proposal that is used as the default IKE proposal. This proposal has the lowest priority and uses the following settings:

- **Encryption algorithm**—DES-CBC.
- **Authentication method**—HMAC-SHA1.
- **Authentication algorithm**—Pre-shared key authentication.
- **DH group**—Group 1.
- **IKE SA lifetime**—86400 seconds.

You cannot change the settings of the default IKE proposal.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*proposal-number*: Specifies an IKE proposal number in the range of 1 to 65535. The lower the number, the higher the priority of the IKE proposal.

### Usage guidelines

During IKE negotiation:

- The initiator sends its IKE proposals to the peer.
  - If the initiator is using an IPsec policy with an IKE profile, the initiator sends all IKE proposals specified for the IKE profile to the peer. An IKE proposal specified earlier for the IKE profile has a higher priority.
  - If the initiator is using an IPsec policy with no IKE profile, the initiator sends all its IKE proposals to the peer. An IKE proposal with a smaller number has a higher priority.
- The peer searches its own IKE proposals for a match. The search starts from the IKE proposal with the highest priority and proceeds in descending order of priority until a match is found. The matching IKE proposals are used to establish the IKE SA. If all user-defined IKE proposals are mismatched, the two peers use their default IKE proposals to establish the IKE SA.

### Examples

# Create IKE proposal 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1]
```

### Related commands

**display ike proposal**

# ike signature-identity from-certificate

Use **ike signature-identity from-certificate** to configure the local device to obtain identity information from the local certificate for signature authentication.

Use **undo ike signature-identity from-certificate** to restore the default.

### Syntax

**ike signature-identity from-certificate**

**undo ike signature-identity from-certificate**

### Default

The local end uses identity information specified by **local-identity** or **ike identity** for signature authentication.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

This command requires the local device to always use the identity information in the local certificate for signature authentication, regardless of the **local-identity** or **ike identity** configuration.

Configure this command when the aggressive mode and signature authentication are used and the device interconnects with a Comware 5-based peer device. Comware 5 supports only DN for signature authentication.

If the **ike signature-identity from-certificate** command is not configured, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

### Examples

# Configure the local device to always obtain the identity information from the local certificate for signature authentication.

```
<Sysname> system-view
[sysname] ike signature-identity from-certificate
```

### Related commands

- **local-identity**
- **ike identity**

# keychain

Use **keychain** to specify an IKE keychain for pre-shared key authentication.

Use **undo keychain** to remove an IKE keychain.

### Syntax

**keychain** *keychain-name*

**undo keychain** *keychain-name*

### Default

No IKE keychain is specified for pre-shared key authentication.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

*keychain-name*: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority.

### Examples

# Specify IKE profile **1** for IKE keychain **abc**.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] keychain abc
```

### Related commands

**ike keychain**

## local-identity

Use **local-identity** to configure the local ID, the ID that the device uses to identify itself to the peer during IKE negotiation.

Use **undo local-identity** to restore the default.

### Syntax

**local-identity** { **address** { *ipv4-address* **| ipv6** *ipv6-address* } **| dn | fqdn** [ *fqdn-name* ] **| user-fqdn** [ *user-fqdn-name* ] }

**undo local-identity**

### Default

No local ID is configured for an IKE profile. An IKE profile uses the local ID configured in system view by using the **ike identity** command. If the local ID is not configured in system view, the IKE profile uses the IP address of the interface to which the IPsec policy is applied as the local ID.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**address** { *ipv4-address* **| ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

**dn**: Uses the DN in the local certificate as the local ID.

**fqdn** *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

**user-fqdn** *user-fqdn-name*: Uses a user FQDN as the local ID. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

### Usage guidelines

An IKE profile can have only one local ID.

For digital signature authentication, the device can use any type of ID. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses its FQDN (the device name configured by using the **sysname** command) instead.

For pre-shared key authentication, the device can use any type of ID other than the DN.

An IKE profile with no local ID specified uses the local ID configured by using the **ike identity** command in system view.

### Examples

# Set the local ID to IP address **2.2.2.2**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] local-identity address 2.2.2.2
```

### Related commands

- **match remote**
- **ike identity**

## match local address (IKE keychain view)

Use **match local address** to specify a local interface or IP address to which an IKE keychain can be applied.

Use **undo match local address** to restore the default.

### Syntax

**match local address** { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

**undo match local address**

### Default

An IKE keychain can be applied to any local interface or IP address.

### Views

IKE keychain view

### Predefined user roles

network-admin

### Parameters

*interface-type interface-number*: Specifies a local interface. It can be any Layer 3 interface.

*ipv4-address*: Specifies the IPv4 address of a local interface.

**ipv6** *ipv6-address*: Specifies the IPv6 address of a local interface.

### Usage guidelines

Use this command to specify which address or interface can use the IKE keychain for IKE negotiation.

Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority. To give an IKE keychain a higher priority, you can configure this command for the keychain. For example, suppose you specified IKE keychain A before specifying IKE keychain B, and you configured the peer ID 2.2.0.0/16 for IKE keychain A and the peer ID 2.2.2.0/24 for IKE keychain B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE keychain A is preferred because IKE keychain A was specified earlier. To use IKE keychain B, you can use this command to restrict the application scope of IKE keychain B to address 3.3.3.3.

### Examples

# Create IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

# Apply the IKE keychain **key1** to the interface with the IP address **2.2.2.2**.

```
[sysname-ike-keychain-key1] match local address 2.2.2.2
```

## match local address (IKE profile view)

Use **match local address** to specify a local interface or IP address to which an IKE profile can be applied.

Use **undo match local address** to restore the default.

### Syntax

**match local address** { *interface-type interface-number* | { *ipv4-address* **|** **ipv6** *ipv6-address* } }

**undo match local address**

### Default

An IKE profile can be applied to any local interface or IP address.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

*interface-type interface-number*: Specifies a local interface. It can be any Layer 3 interface.

*ipv4-address*: Specifies the IPv4 address of a local interface.

**ipv6** *ipv6-address*: Specifies the IPv6 address of a local interface.

### Usage guidelines

Use this command to specify which address or interface can use the IKE profile for IKE negotiation.

Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

An IKE profile configured earlier has a higher priority. To give an IKE profile that is configured later a higher priority, you can configure this command for the profile. For example, suppose you configured IKE profile A before configuring IKE profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKE profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKE profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE profile A is preferred because IKE profile A was configured earlier. To use IKE profile B, you can use this command to restrict the application scope of IKE profile B to address 3.3.3.3.

### Examples

# Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

# Apply the IKE profile **prof1** to the interface with the IP address **2.2.2.2**.

```
[sysname-ike-profile-prof1] match local address 2.2.2.2
```

## match remote

Use **match remote** to configure a peer ID for IKE profile matching.

Use **undo match remote** to delete a peer ID.

### Syntax

**match remote** { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [ *mask* **|** *mask-length* ] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [ *prefix-length* ] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **user-fqdn** *user-fqdn-name* } }

**undo match remote** { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [ *mask* **|** *mask-length* ] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [ *prefix-length* ] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **user-fqdn** *user-fqdn-name* } }

### Default

No peer ID is configured for IKE profile matching.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**certificate** *policy-name*: Uses the DN in the peer's digital certificate as the peer ID for IKE profile matching. The *policy-name* argument is a string of 1 to 31 characters.

**identity**: Uses the specified information as the peer ID for IKE profile matching. The specified information is configured on the peer by using the **local-identity** command.

- **address** *ipv4-address* [ *mask* **|** *mask-length* ]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKE profile matching. The *mask-length* argument is in the range of 0 to 32.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [ *prefix-length* ] : Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKE profile matching. The *prefix-length* argument is in the range of 0 to 128.
- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.

- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKE profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **user-fqdn** *user-fqdn-name*: Uses the peer's user FQDN as the peer ID for IKE profile matching. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com.

### Usage guidelines

When an end needs to select an IKE profile, it compares the peer's ID received with the peer IDs of its local IKE profiles. If a match is found, it uses the IKE profile with the matching peer ID for IKE negotiation.

Each IKE profile must have at least one peer ID configured.

To make sure only one IKE profile is matched for a peer, do not configure the same peer ID for two or more IKE profiles. If you configure the same peer ID for two or more IKE profiles, which IKE profile is selected for IKE negotiation is unpredictable.

For an IKE profile, you can configure multiple peer IDs. A peer ID configured earlier has a higher priority.

### Examples

# Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

# Configure a peer ID with the identity type of FQDN and the value of **www.test.com**.

```
 [Sysname-ike-profile-prof1] match remote identity fqdn www.test.com
```

# Configure a peer ID with the identity type of IP address and the value of **10.1.1.1**.

```
[Sysname-ike-profile-prof1] match remote identity address 10.1.1.1
```

### Related commands

**local-identity**

## pre-shared-key

Use **pre-shared-key** to configure a pre-shared key.

Use **undo pre-shared-key** to remove a pre-shared key.

### Syntax

**pre-shared-key** { **address** { *ipv4-address* [ *mask* **|** *mask-length* ] **|** **ipv6** *ipv6-address* [ *prefix-length* ] } **|** **hostname** *host-name* } **key** { **cipher** **|** **simple** } *string*

**undo pre-shared-key** { **address** { *ipv4-address* [ *mask* **|** *mask-length* ] **|** **ipv6** *ipv6-address* [ *prefix-length* ] } **|** **hostname** *host-name* }

### Default

No pre-shared key is configured.

### Views

IKE keychain view

### Predefined user roles

network-admin

### Parameters

**address**: Specifies a peer by its address.

*ipv4-address*: Specifies the IPv4 address of the peer.

*mask*: Specifies the mask in dotted decimal notation. The default mask is 255.255.255.255.

*mask-length*: Specifies the mask length in the range of 0 to 32. The default mask length is 32.

**ipv6**: Specifies an IPv6 peer.

*ipv6-address*: Specifies the IPv6 address of the peer.

*prefix-length*: Specifies the prefix length in the range of 0 to 128. The default prefix length is 128.

**hostname** *host-name*: Specifies a peer by its hostname, a case-sensitive string of 1 to 255 characters.

**key**: Specifies a pre-shared key.

**cipher**: Specifies a pre-shared key in encrypted form.

**simple**: Specifies a pre-shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

*string*: Specifies the pre-shared key. The key is case sensitive. Its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters.

### Usage guidelines

The address option or the hostname option specifies the peer with which the device can use the pre-shared key to perform IKE negotiation.

Two peers must be configured with the same pre-shared key to pass pre-shared key authentication.

### Examples

# Create IKE keychain **key1** and enter IKE keychain view.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

# Set the pre-shared key to be used for IKE negotiation with peer 1.1.1.2 to **123456TESTplat&!**.

```
[Sysname-ike-keychain-key1] pre-shared-key address 1.1.1.2 255.255.255.255 key simple
123456TESTplat&!
```

### Related commands

- **authentication-method**
- **keychain**

## priority (IKE keychain view)

Use **priority** to specify a priority for an IKE keychain.

Use **undo priority** to restore the default.

### Syntax

**priority** *priority*

**undo priority**

### Default

The priority of an IKE keychain is 100.

### Views

IKE keychain view

### Predefined user roles

network-admin

### Parameters

**priority** *priority*: Specifies a priority number in the range of 1 to 65535. The lower the priority number, the higher the priority.

### Usage guidelines

To determine the priority of an IKE keychain, the device examines the existence of the **match local address** command before examining the priority number. An IKE keychain with the **match local address** command configured has a higher priority than an IKE keychain that does not have the **match local address** command configured.

### Examples

# Set the priority to **10** for IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1] priority 10
```

## priority (IKE profile view)

Use **priority** to specify a priority for an IKE profile.

Use **undo priority** to restore the default.

### Syntax

**priority** *priority*

**undo priority**

### Default

The priority of an IKE profile is 100.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

**priority** *priority*: Specifies a priority number in the range of 1 to 65535. The smaller the priority number, the higher the priority.

### Usage guidelines

To determine the priority of an IKE profile, the device examines the existence of the **match local address** command before examining the priority number. An IKE profile with the **match local address** command configured has a higher priority than an IKE profile that does not have the **match local address** command configured.

### Examples

# Set the priority to **10** for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] priority 10
```

## proposal

Use **proposal** to specify IKE proposals for an IKE profile.

Use **undo proposal** to restore the default.

### Syntax

**proposal** *proposal-number*&<1-6>

**undo proposal**

### Default

No IKE proposals are specified for an IKE profile and the IKE proposals configured in system view are used for IKE negotiation.

### Views

IKE profile view

### Predefined user roles

network-admin

### Parameters

*proposal-number*&<1-6>: Specifies a space-separated list of up to six IKE proposals by their numbers in the range of 1 to 65535. An IKE proposal specified earlier has a higher priority.

### Usage guidelines

When acting as the initiator, the device sends the specified IKE proposals to its peer for IKE negotiation. When acting as the responder, the device uses the IKE proposals configured in system view to match the IKE proposals received from the initiator.

### Examples

# Specify IKE proposal **10** for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] proposal 10
```

### Related commands

**ike proposal**

## reset ike sa

Use **reset ike sa** to delete IKE SAs.

### Syntax

**reset ike sa** [ **connection-id** *connection-id* ]

### Views

User view

### Predefined user roles

network-admin

### Parameters

**connection-id** *connection-id*: Specifies the connection ID of the IKE SA to be cleared, in the range of 1 to 2000000000.

### Usage guidelines

When you delete an IKE SA, the device automatically sends a notification to the peer.

### Examples

# Display the current IKE SAs.

```
<Sysname> display ike sa
    Total IKE SAs:  2
    Connection-ID  Remote            Flag        DOI
  ----------------------------------------------------------
      1            202.38.0.2      RD|ST       IPSEC
      2            202.38.0.3      RD|ST       IPSEC
Flags:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

# Delete the IKE SA with the connection ID **2**.

```
<Sysname> reset ike sa connection-id 2
```

# Display the current IKE SAs.

```
<Sysname> display ike sa

Total IKE SAs:  1
    Connection-ID  Remote            Flag        DOI
  ----------------------------------------------------------
      1            202.38.0.2      RD|ST       IPSEC
Flags:
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

# reset ike statistics

Use **reset ike statistics** command to clear IKE MIB statistics.

## Syntax

**reset ike statistics**

## Views

User view

## Predefined user roles

network-admin

## Examples

# Clears IKE MIB statistics.

```
<Sysname> reset ike statistics
```

## Related commands

**snmp-agent trap enable ike**

# sa duration

Use **sa duration** to set the IKE SA lifetime for an IKE proposal.

Use **undo sa duration** to restore the default.

## Syntax

**sa duration** *seconds*

**undo sa duration**

## Default

The IKE SA lifetime is 86400 seconds.

### Views

IKE proposal view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the IKE SA lifetime in seconds, in the range of 60 to 604800.

### Usage guidelines

If the communicating peers are configured with different IKE SA lifetime settings, the smaller setting takes effect.

Before an IKE SA expires, IKE negotiates a new SA. The new SA takes effect immediately after it is negotiated. The old IKE SA will be cleared when it expires.

### Examples

# Set the IKE SA lifetime to **600** seconds for IKE proposal **1**.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] sa duration 600
```

### Related commands

**display ike proposal**

## snmp-agent trap enable ike

Use **snmp-agent trap enable ike** command to enable SNMP notifications for IKE.

Use **undo snmp-agent trap enable ike** to disable SNMP notifications for IKE.

### Syntax

**snmp-agent trap enable ike** [ **attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type** ] *

**undo snmp-agent trap enable ike** [ **attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type** ] *

### Default

All SNMP notifications for IKE are enabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**attr-not-support**: Specifies SNMP notifications for attribute-unsupported failures.

**auth-failure**: Specifies SNMP notifications for authentication failures.

**cert-type-unsupport**: Specifies SNMP notifications for certificate-type-unsupported failures.

**cert-unavailable**: Specifies SNMP notifications for certificate-unavailable failures.

**decrypt-failure**: Specifies SNMP notifications for decryption failures.

**encrypt-failure**: Specifies SNMP notifications for encryption failures.

**global**: Specifies SNMP notifications globally.

**invalid-cert-auth**: Specifies SNMP notifications for invalid-certificate-authentication failures.

**invalid-cookie**: Specifies SNMP notifications for invalid-cookie failures.

**invalid-id**: Specifies SNMP notifications for invalid-ID failures.

**invalid-proposal**: Specifies SNMP notifications for invalid-IKE-proposal failures.

**invalid-protocol**: Specifies SNMP notifications for invalid-protocol failures.

**invalid-sign**: Specifies SNMP notifications for invalid-signature failures.

**no-sa-failure**: Specifies SNMP notifications for SA-not-found failures.

**proposal-add**: Specifies SNMP notifications for events of adding IKE proposals.

**proposal-delete**: Specifies SNMP notifications for events of deleting IKE proposals.

**tunnel-start**: Specifies SNMP notifications for events of creating IKE tunnels.

**tunnel-stop**: Specifies SNMP notifications for events of deleting IKE tunnels.

**unsupport-exch-type**: Specifies SNMP notifications for negotiation-type-unsupported failures.

### Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IKE.

To generate and output SNMP notifications for a specific IKE failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IKE globally.
2. Enable SNMP notifications for the failure type or event type.

### Examples

# Enable SNMP notifications for IKE globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ike global
```

# Enable SNMP notifications for events of creating IKE tunnels.

```
[Sysname] snmp-agent trap enable ike tunnel-start
```

# IKEv2 commands

The following matrix shows the feature and hardware compatibility:

| Hardware series | Model | IKEv2 compatibility |
|---|---|---|
| WX1800H series | WX1804H<br>WX1810H<br>WX1820H | Yes |
| WX2500H series | WX2510H<br>WX2540H<br>WX2560H | Yes |
| WX3000H series | WX3010H | Yes |
| | WX3010H-L | No |
| | WX3010H-X | Yes |
| | WX3024H | Yes |
| | WX3024H-L | No |
| WX3500H series | WX3508H<br>WX3510H<br>WX3520H<br>WX3540H | Yes |
| WX5500E series | WX5510E<br>WX5540E | Yes |
| WX5500H series | WX5540H<br>WX5560H<br>WX5580H | Yes |
| Access controller modules | EWPXM1MAC0F<br>EWPXM1WCME0<br>EWPXM2WCMD0F<br>LSQM1WCMX20<br>LSQM1WCMX40<br>LSUM1WCME0<br>LSUM1WCMX20RT<br>LSUM1WCMX40RT | Yes |

## aaa authorization

Use **aaa authorization** to enable IKEv2 AAA authorization.

Use **undo aaa authorization** to disable IKEv2 AAA authorization.

### Syntax

**aaa authorization domain** *domain-name* **username** *user-name*

**undo aaa authorization**

### Default

IKEv2 AAA authorization is disabled.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**domain** *domain-name*: Specifies the ISP domain used for requesting authorization attributes. The ISP domain name is a case-insensitive string of 1 to 255 characters and must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

**username** *user-name*: Specifies the username used for requesting authorization attributes. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain the domain name.
- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

### Usage guidelines

The AAA authorization feature enables IKEv2 to request authorization attributes, such as the IKEv2 IPv4 address pool, from AAA.

IKEv2 uses the ISP domain and username to request authorization attributes. AAA uses the authorization settings in the ISP domain to request the user's authorization attributes from the remote AAA server or the local user database. After IKEv2 passes the username authentication, it obtains the authorization attributes.

This feature is applicable when AAA is used to centrally manage and deploy authorization attributes.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Enable AAA authorization. Specify the ISP domain name **abc** and the username **test**.

```
[Sysname-ikev2-profile-profile1] aaa authorization domain abc username test
```

### Related commands

**display ikev2 profile**

## address

Use **address** to specify the IP address or IP address range of the IKEv2 peer.

Use **undo address** to restore the default.

### Syntax

**address** { *ipv4-address* [ *mask* | *mask-length* ] | **ipv6** *ipv6-address* [ *prefix-length* ] }

**undo address**

### Default

The IKEv2 peer's IP address or IP address range is not specified.

### Views

IKEv2 peer view

### Predefined user roles

network-admin

### Parameters

*ipv4-address*: Specifies the IPv4 address of the IKEv2 peer.

*Mask*: Specifies the subnet mask of the IPv4 address.

*mask-length*: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

**ipv6** *ipv6-address*: Specifies the IPv6 address of the IKEv2 peer.

*prefix-length*: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

### Usage guidelines

Both the initiator and the responder can look up an IKEv2 peer by IP address in IKEv2 negotiation.

The IP addresses of different IKEv2 peers in the same IKEv2 keychain cannot be the same.

### Examples

# Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

# Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

# Specify the IKEv2 peer's IP address 3.3.3.3 with the subnet mask 255.255.255.0.

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

### Related commands

- **ikev2 keychain**
- **peer**

## authentication-method

Use **authentication-method** to specify the local or remote identity authentication method.

Use **undo authentication-method** to remove the local or remote identity authentication method.

### Syntax

**authentication-method** { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

**undo authentication-method local**

**undo authentication-method remote** { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

### Default

No local or remote identity authentication method is specified.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**local**: Specifies the local identity authentication method.

**remote**: Specifies the remote identity authentication method.

**dsa-signature**: Specifies the DSA signatures as the identity authentication method.

**ecdsa-signature**: Specifies the ECDSA signatures as the identity authentication method.

**pre-share**: Specifies the pre-shared key as the identity authentication method.

**rsa-signature**: Specifies the RSA signatures as the identity authentication method.

### Usage guidelines

The local and remote identity authentication methods must both be specified and they can be different.

You can specify only one local identity authentication method. You can specify multiple remote identity authentication methods by executing this command multiple times when there are multiple remote ends whose authentication methods are unknown.

If you use RSA, DSA, or ECDSA signature authentication, you must specify PKI domains for obtaining certificates. You can specify PKI domains by using the **certificate domain** command in IKEv2 profile view or by using the **pki domain** command in system view. PKI domains specified in IKEv2 profile view take precedence over those specified in system view.

If you specify the pre-shared key method, you must specify a pre-shared key for the IKEv2 peer in the keychain used by the IKEv2 profile.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Specify the pre-shared key and RSA signatures as the local and remote authentication methods, respectively.

```
[Sysname-ikev2-profile-profile1] authentication local pre-share
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
```

# Specify the PKI domain **genl** as the PKI domain for obtaining certificates.

```
[Sysname-ikev2-profile-profile1] certificate domain genl
```

# Specify the keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

### Related commands

- **display ikev2 profile**
- **certificate domain** (IKEv2 profile view)
- **keychain** (IKEv2 profile view)

## certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication in IKEv2 negotiation.

Use **undo certificate domain** to remove a PKI domain for signature authentication in IKEv2 negotiation.

### Syntax

**certificate domain** *domain-name* [ **sign** | **verify** ]

**undo certificate domain** *domain-name*

### Default

PKI domains specified in system view are used.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

*domain-name*: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

**sign**: Uses the local certificate in the PKI domain to generate a signature.

**verify**: Uses the CA certificate in the PKI domain to verify the remote end's certificate.

### Usage guidelines

You can specify a PKI domain for each purpose (**sign** or **verify**). If you specify the same PKI domain for both purposes, the later configuration takes effect. For example, if you execute **certificate domain abc sign** and **certificate domain abc verify** successively, the PKI domain **abc** will be used only for verification. To use the same PKI domain for both purposes, specify the PKI domain without specifying the **sign** or **verify** keyword.

If the local end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for signature generation. If the remote end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for verifying the remote end's certificate. If you do not specify PKI domains, the PKI domains specified in system view will be used.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Specify the PKI domain **abc** for signature. Specify the PKI domain **def** for verification.

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

### Related commands

- **authentication-method**
- **pki domain**

## config-exchange

Use **config-exchange** to enable the configuration exchange feature.

Use **undo config-exchange** to disable the configuration exchange feature.

### Syntax

**config-exchange** { **request | set** { **accept | send** } }

**undo config-exchange** { **request | set** { **accept | send** } }

### Default

Configuration exchange is disabled.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**request**: Enables the device to send request messages carrying the configuration request payload during the IKE_AUTH exchange.

**set**: Specifies the configuration set payload exchange.

**accept**: Enables the device to accept the configuration set payload carried in Info messages.

**send**: Enables the device to send Info messages carrying the configuration set payload.

### Usage guidelines

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response. The enterprise center can push IP addresses to branches. The branches can request IP addresses, but the requested IP addresses cannot be used.

You can specify both **request** and **set** for the device.

If you specify **request** for the local end, the remote end will respond if it can obtain the requested data through AAA authorization.

If you specify **set send** for the local end, you must specify **set accept** for the remote end.

The device with **set send** specified pushes an IP address after the IKEv2 SA is set up if it does not receive any configuration request from the peer.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Enable the local end to add the configuration request payload to the request message of IKE_AUTH exchange.

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

### Related commands

- **aaa authorization**
- **configuration policy**
- **display ikev2 profile**

## dh

Use **dh** to specify DH groups to be used in IKEv2 key negotiation for an IKEv2 proposal.

Use **undo group** to restore the default.

### Syntax

**dh** { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } *

**undo dh**

### Default

No DH group is specified for an IKEv2 proposal.

### Views

IKEv2 proposal view

### Predefined user roles

network-admin

### Parameters

**group1**: Uses the 768-bit Diffie-Hellman group.

**group2**: Uses the 1024-bit Diffie-Hellman group.

**group5**: Uses the 1536-bit Diffie-Hellman group.

**group14**: Uses the 2048-bit Diffie-Hellman group.

**group24**: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

**group19**: Uses 256-bit ECP Diffie-Hellman group.

**group20**: Uses 384-bit ECP Diffie-Hellman group.

### Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose proper DH groups for your network.

You must specify a minimum of one DH group for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple DH groups for an IKEv2 proposal. A group specified earlier has a higher priority.

### Examples

# Specify DH groups 1 for the IKEv2 proposal 1.

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

### Related commands

**ikev2 proposal**

## display ikev2 policy

Use **display ikev2 policy** to display the IKEv2 policy configuration.

### Syntax

**display ikev2 policy** [ *policy-name* **|** **default** ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

*policy-name*: Specifies an IKEv2 policy by its name, a case-insensitive string of 1 to 63 characters.

**default**: Specifies the default IKEv2 policy.

### Usage guidelines

If you do not specify any parameters, this command displays the configuration of all IKEv2 policies.

### Examples

# Display the configuration of all IKEv2 policies.

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1:1::1:1
  Match VRF: vpn1
  Proposal: 1
  Proposal: 2
IKEv2 policy: default
  Match local address: Any
  Match VRF: Any
  Proposal: default
```

**Table 12 Command output**

| Field | Description |
|---|---|
| IKEv2 policy | Name of the IKEv2 policy. |
| Priority | Priority of the IKEv2 policy. |
| Match local address | IPv4 address to which the IKEv2 policy can be applied. |
| Match local address ipv6 | IPv6 address to which the IKEv2 policy can be applied. |
| Match VRF | VPN instance to which the IKEv2 policy can be applied.<br>The device does not support this field in the current software version. |
| Proposal | IKEv2 proposal that the IKEv2 policy uses. |

### Related commands

**ikev2 policy**

## display ikev2 profile

Use **display ikev2 profile** to display the IKEv2 profile configuration.

### Syntax

**display ikev2 profile** [ *profile-name* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

## Parameters

*profile-name*: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify any parameters, this command displays the configuration of all IKEv2 profiles.

## Examples

# Display the configuration of all IKEv2 profiles.

```
<Sysname> display ikev2 profile
IKEv2 profile: 1
  Priority: 100
  Match criteria:
    Local address 1.1.1.1
    Local address Vlan-interface100
    Local address 1:1::1:1
    Remote identity address 3.3.3.3/32
    VRF vrf1
  Inside-vrf:
  Local identity: address 1.1.1.1
  Local authentication method: pre-share
  Remote authentication methods: pre-share
  Keychain: Keychain1
  Sign certificate domain:
     Domain1
     abc
  Verify certificate domain:
     Domain2
     yy
  SA duration: 500 seconds
  DPD: Interval 32 secs, retry-interval 23 secs, periodic
  Config exchange: request, set accept, set send
  NAT keepalive: 10 seconds
  AAA authorization: Domain domain1, username ikev2
```

**Table 13 Command output**

| Field | Description |
|---|---|
| IKEv2 profile | Name of the IKEv2 profile. |
| Priority | Priority of the IKEv2 profile. |
| Match criteria | Criteria for looking up the IKEv2 profile. |
| Inside vrf | Inside VPN instance.<br>The device does not support this field in the current software version. |
| Local identity | ID of the local end. |
| Local authentication method | Method that the local end uses for authentication. |
| Remote authentication methods | Methods that the remote end uses for authentication. |
| Keychain | IKEv2 keychain that the IKEv2 profile uses. |
| Sign certificate domain | PKI domain used for signature generation. |

| Field | Description |
|---|---|
| Verify certificate domain | PKI domain used for verifying the remote end's certificate. |
| SA duration | Lifetime of the IKEv2 SA. |
| DPD | DPD settings:<br>• Detection interval in seconds.<br>• Retry interval in seconds.<br>• Detection mode, on demand or periodically.<br>If DPD is disabled, this field displays **Disabled**. |
| Config exchange | Configuration exchange settings:<br>• **request**—The local end sends request messages carrying the configuration request payload during the IKE_AUTH exchange.<br>• **set accept**—The local end accepts the configuration set payload carried in Info messages.<br>• **set send**—The local end sends Info messages carrying the configuration set payload. |
| NAT keepalive | NAT keepalive interval in seconds. |
| AAA authorization | AAA authorization settings:<br>• ISP domain name.<br>• Username. |

### Related commands

**ikev2 profile**

# display ikev2 proposal

Use **display ikev2 proposal** to display the IKEv2 proposal configuration.

### Syntax

**display ikev2 proposal** [ *name* | **default** ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

*name*: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

**default**: Specifies the default IKEv2 proposal.

### Usage guidelines

This command displays IKEv2 proposals in descending order of priorities.

If you do not specify any parameters, this command displays the configuration of all IKEv2 proposals.

### Examples

# Display the configuration of all IKEv2 proposals.

```
<Sysname> display ikev2 proposal
```

```
IKEv2 proposal: 1
  Encryption: 3DES-CBC, AES-CBC-128, AES-CTR-192, CAMELLIA-CBC-128
  Integrity: MD5, SHA256, AES-XCBC
  PRF: MD5, SHA256, AES-XCBC
  DH group: MODP1024/Group 2, MODP1536/Group 5

IKEv2 proposal: default
  Encryption: AES-CBC-128, 3DES-CBC
  Integrity: SHA1, MD5
  PRF: SHA1, MD5
  DH group: MODP1536/Group 5, MODP1024/Group 2
```

**Table 14 Command output**

| Field | Description |
|---|---|
| IKEv2 proposal | Name of the IKEv2 proposal. |
| Encryption | Encryption algorithms that the IKEv2 proposal uses. |
| Integrity | Integrity protection algorithms that the IKEv2 proposal uses. |
| PRF | PRF algorithms that the IKEv2 proposal uses. |
| DH group | DH groups that the IKEv2 proposal uses. |

### Related commands

**ikev2 proposal**

# display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

### Syntax

**display ikev2 sa** [ **count** | [ { **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } ] [ **verbose** [ **tunnel** *tunnel-id* ] ] ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Parameters

**count**: Displays the number of IKEv2 SAs.

**local**: Displays IKEv2 SA information for a local IP address.

**remote**: Displays IKEv2 SA information for a remote IP address.

*ipv4-address*: Specifies a local or remote IPv4 address.

**ipv6** *ipv6-address*: Specifies a local or remote IPv6 address.

**verbose**: Displays detailed information. If you do not specify this keyword, the command displays the summary information.

**tunnel** *tunnel-id*: Displays detailed IKEv2 SA information for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

## Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKEv2 SAs.

## Examples

# Display summary information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  --------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

# Display summary IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2
     Tunnel ID          Local             Remote             Status
  --------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

**Table 15 Command output**

| Field | Description |
|---|---|
| Tunnel ID | ID of the IPsec tunnel to which the IKEv2 SA belongs. |
| Local | Local IP address of the IKEv2 SA. |
| Remote | Remote IP address of the IKEv2 SA. |
| Status | Status of the IKEv2 SA:<br>• **IN-NEGO** (**Negotiating**)—The IKEv2 SA is under negotiation.<br>• **EST** (**Established**)—The IKEv2 SA has been set up.<br>• **DEL** (**Deleting**)—The IKEv2 SA is about to be deleted. |

# Display detailed information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: device_a
  Remote ID type: FQDN
  Remote ID: device_b
  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 20 secs, retry interval 2 secs
  Transmitting entity: Initiator

  Local window: 1
  Remote window: 1
  Local request message ID: 2
  Remote request message ID:2
  Local next message ID: 0
  Remote next message ID: 0

  Pushed IP address: 192.168.1.5
  Assigned IP address: 192.168.2.24
```

# Display detailed IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2 verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: device_a
  Remote ID type: FQDN
  Remote ID: device_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
```

```
NAT traversal: Not detected
DPD: Interval 30 secs, retry 10 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24
```

**Table 16 Command output**

| Field | Description |
|---|---|
| Tunnel ID | ID of the IPsec tunnel to which the IKEv2 SA belongs. |
| Local IP/Port | IP address and port number of the local security gateway. |
| Remote IP/Port | IP address and port number of the remote security gateway. |
| Outside VRF | Name of the VPN instance to which the protected outbound data flow belongs.<br>If the protected outbound data flow belongs to the public network, this field displays a hyphen (**-**).<br>The device does not support this field in the current software version. |
| Inside VRF | Name of the VPN instance to which the protected inbound data flow belongs.<br>If the protected inbound data flow belongs to the public network, this field displays a hyphen (**-**).<br>The device does not support this field in the current software version. |
| Local SPI | SPI that the local end uses. |
| Remote SPI | SPI that the remote end uses. |
| Local ID type | ID type of the local security gateway. |
| Local ID | ID of the local security gateway. |
| Remote ID type | ID type of the remote security gateway. |
| Remote ID | ID of the remote security gateway. |
| Auth sign method | Signature method that the IKEv2 proposal uses in authentication. |
| Auth verify method | Verification method that the IKEv2 proposal uses in authentication. |
| Integrity algorithm | Integrity protection algorithms that the IKEv2 proposal uses. |
| PRF algorithm | PRF algorithms that the IKEv2 proposal uses. |
| Encryption algorithm | Encryption algorithms that the IKEv2 proposal uses. |
| Life duration | Lifetime of the IKEv2 SA, in seconds. |

| Field | Description |
|---|---|
| Remaining key duration | Remaining lifetime of the IKEv2 SA, in seconds. |
| Diffie-Hellman group | DH groups used in IKEv2 key negotiation. |
| NAT traversal | Whether a NAT gateway is detected between the local and remote ends. |
| DPD | DPD settings:<br>• Detection interval in seconds.<br>• Retry interval in seconds.<br>If DPD is disabled, this field displays **Disabled**. |
| Transmitting entity | Role of the local end in IKEv2 negotiation, initiator or responder. |
| Local window | Window size that the local end uses. |
| Remote window | Window size that the remote end uses. |
| Local request message ID | ID of the request message that the local end is about to send. |
| Remote request message ID | ID of the request message that the remote end is about to send. |
| Local next message ID | ID of the message that the local end expects to receive. |
| Remote next message ID | ID of the message that the remote end expects to receive. |
| Pushed IP address | IP address pushed to the local end by the remote end. |
| Assigned IP address | IP address assigned to the remote end by the local end . |

# Display the number of IKEv2 SAs.

```
[Sysname] display ikev2 sa count
IKEv2 SAs count: 0
```

# display ikev2 statistics

Use **display ikev2 statistics** to display IKEv2 statistics.

## Syntax

**display ikev2 statistics**

## Views

Any view

## Predefined user roles

network-admin

network-operator

## Examples

# Display IKEv2 statistics.

```
<Sysname> display ikev2 statistics
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
  Invalid syntax: 0
  Invalid message ID: 0
  Invalid SPI: 0
  No proposal chosen: 0
  Invalid KE payload: 0
  Authentication failed: 0
  Single pair required: 0
  TS unacceptable: 0
  Invalid selectors: 0
  Tempture failure: 0
  No child SA: 0
  Unknown other notify: 0
  No enough resource: 0
  Enqueue error: 0
  No IKEv2 SA: 0
  Packet error: 0
  Other error: 0
  Retransmit timeout: 0
  DPD detect error: 0
  Del child for IPsec message: 1
  Del child for deleting IKEv2 SA: 1
  Del child for receiving delete message: 0
```

### Related commands

**reset ikev2 statistics**

# dpd

Use **dpd** to configure the IKEv2 DPD feature.

Use **undo dpd** to disable the IKEv2 DPD feature.

### Syntax

**dpd interval** *interval* [ **retry** *seconds* ] { **on-demand** | **periodic** }

**undo dpd interval**

### Default

IKEv2 DPD is disabled. The global IKEv2 DPD settings are used.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**interval** *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

- If the **on-demand** keyword is specified, the device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.
- If the **periodic** keyword is specified, the device triggers DPD at the specified intervals.

**retry** *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

**on-demand**: Triggers DPD on demand.

**periodic**: Triggers DPD at regular intervals.

### Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, but it consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

### Examples

# Configure on-demand IKEv2 DPD. Set the DPD triggering interval to 10 seconds and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

### Related commands

**ikev2 dpd**

## encryption

Use **encryption** to specify encryption algorithms for an IKEv2 proposal.

Use **undo encryption** to restore the default.

### Syntax

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

**undo encryption**

### Default

No encryption algorithm is specified for an IKEv2 proposal.

### Views

IKEv2 proposal view

### Predefined user roles

network-admin

### Parameters

**3des-cbc**: Uses the 3DES algorithm in CBC mode, which uses a 168-bit key.

**aes-cbc-128**: Uses the AES algorithm in CBC mode, which uses a 128-bit key.

**aes-cbc-192**: Uses the AES algorithm in CBC mode, which uses a 192-bit key.

**aes-cbc-256**: Uses the AES algorithm in CBC mode, which uses a 256-bit key.

**aes-ctr-128**: Uses the AES algorithm in CTR mode, which uses a 128-bit key.

**aes-ctr-192**: Uses the AES algorithm in CTR mode, which uses a 192-bit key.

**aes-ctr-256**: Uses the AES algorithm in CTR mode, which uses a 256-bit key.

**camellia-cbc-128**: Uses the Camellia algorithm in CBC mode, which uses a 128-bit key.

**camellia-cbc-192**: Uses the Camellia algorithm in CBC mode, which uses a 192-bit key.

**camellia-cbc-256**: Uses the Camellia algorithm in CBC mode, which uses a 256-bit key.

**des-cbc**: Uses the DES algorithm in CBC mode, which uses a 56-bit key.

### Usage guidelines

You must specify a minimum of one encryption algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple encryption algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

### Examples

# Specify the 168-bit 3DES algorithm in CBC mode as the encryption algorithm for IKE proposal **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

### Related commands

**ikev2 proposal**

# hostname

Use **hostname** to specify the host name of the IKEv2 peer.

Use **undo hostname** to restore the default.

### Syntax

**hostname** *name*

**undo hostname**

### Default

The IKEv2 peer's host name is not specified.

### Views

IKEv2 peer view

### Predefined user roles

network-admin

### Parameters

*name*: Specifies the host name of the IKEv2 peer, a case-insensitive string of 1 to 253 characters.

### Usage guidelines

Only the initiator can look up an IKEv2 peer by host name in IKEv2 negotiation.

### Examples

# Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

# Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

# Specify the host name **test** of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

### Related commands

- **ikev2 keychain**
- **peer**

# identity

Use **identity** to specify the ID of the IKEv2 peer.

Use **undo identity** to restore the default.

## Syntax

**identity** { **address** { *ipv4-address* **| ipv6** { *ipv6-address* } } **| fqdn** *fqdn-name* **| email** *email-string* **| key-id** *key-id-string* }

**undo identity**

## Default

The IKEv2 peer's ID is not specified.

## Views

IKEv2 peer view

## Predefined user roles

network-admin

## Parameters

*ipv4-address*: Specifies the IPv4 address of the peer.

**ipv6** *ipv6-address*: Specifies the IPv6 address of the peer.

**fqdn** *fqdn-name*: Specifies the FQDN of the peer. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

**email** *email-string*: Specifies the email address of the peer. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as esec@test.com.

**key-id** *key-id*: Specifies the remote gateway's key ID. The *key-id* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

## Usage guidelines

Only the responder can look up an IKEv2 peer by ID in IKEv2 negotiation. The initiator does not know the peer ID when initiating the IKEv2 negotiation, so it cannot use an ID for IKEv2 peer lookup.

## Examples

# Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

# Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

# Specify the peer IPv4 address 1.1.1.2 as the ID of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

## Related commands

- **ikev2 keychain**
- **peer**

# identity local

Use **identity local** to configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation.

Use **undo identity local** to restore the default.

## Syntax

**identity local** { **address** { *ipv4-address* **|** i**pv6** *ipv6-address* } **| dn | email** *email-string* **| fqdn** *fqdn-name* **| key-id** *key-id-string* }

**undo identity local**

## Default

No local ID is specified. The IP address of the interface to which the IPsec policy is applied is used as the local ID.

## Views

IKEv2 profile view

## Predefined user roles

network-admin

## Parameters

**address** { *ipv4-address* **| ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

**dn**: Uses the DN in the local certificate as the local ID.

**email** *email-string*: Uses an email address as the local ID. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

**fqdn** *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

**key-id** *key-id*: Uses the device's key ID as the local ID. The *key-id* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

## Usage guidelines

Peers exchange local IDs for identifying each other in negotiation.

## Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Use the IP address 2.2.2.2 as the local ID.

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

## Related commands

**peer**

# ikev2 address-group

Use **ikev2 address-group** to configure an IKEv2 IPv4 address pool for assigning IPv4 addresses to remote peers.

Use **undo ikev2 address-group** to delete an IKEv2 IPv4 address pool.

### Syntax

**ikev2 address-group** *group-name start-ipv4-address end-ipv4-address* [ *mask* | *mask-length* ]

**undo ikev2 address-group** *group-name*

### Default

No IKEv2 IPv4 address pool exists.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*group-name*: Specifies an name for the IKEv2 IPv4 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

*start-ipv4-address end-ipv4-address*: Specifies an IPv4 address range. The *start-ipv4-address* argument specifies the start IPv4 address. The *end-ipv4-address* argument specifies the end IPv4 address.

*mask*: Specifies the IPv4 address mask.

*mask-length*: Specifies the length of the IPv4 address mask.

### Usage guidelines

An IKE IPv4 address pool can contain a maximum of 8192 IPv4 addresses.

### Examples

# Configure an IKEv2 IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask 255.255.255.0.

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

# Configure an IKEv2 IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask length 32.

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 32
```

### Related commands

**address-group**

## ikev2 cookie-challenge

Use **ikev2 cookie-challenge** to enable the cookie challenging feature.

Use **undo ikev2 cookie-challenge** to disable the cookie challenging feature.

### Syntax

**ikev2 cookie-challenge** *number*

**undo ikev2 cookie-challenge**

### Default

The cookie challenging feature is disabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*number*: Sets the threshold for triggering the cookie challenging feature. The value range for this argument is 1 to 1000 half-open IKE SAs.

### Usage guidelines

When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

This feature can protect the responder against DoS attacks which aim to exhaust the responder's system resources by using a large number of IKE_SA_INIT requests with forged source IP addresses.

### Examples

# Enable the cookie challenging feature and set the threshold to 450.

```
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

## ikev2 dpd

Use **ikev2 dpd** to configure the global IKEv2 DPD feature.

Use **undo ikev2 dpd** to disable the global IKEv2 DPD feature.

### Syntax

**ikev2 dpd interval** *interval* [ **retry** *seconds* ] { **on-demand | periodic** }

**undo ikev2 dpd interval**

### Default

The global IKEv2 DPD feature is disabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**interval** *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

- If the **on-demand** keyword is specified, the device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.
- If the **periodic** keyword is specified, the device triggers DPD at the specified intervals.

**retry** *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

**on-demand**: Triggers DPD on demand.

**periodic**: Triggers DPD at regular intervals.

### Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, but it consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply. If you configure IKEv2 DPD in both IKEv2 profile view and system view, the IKEv2 DPD settings in IKEv2 profile view apply.

### Examples

# Configure the device to trigger IKEv2 DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

# Configure the device to trigger IKEv2 DPD every 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

### Related commands

**dpd** (IKEv2 profile view)

## ikev2 ipv6-address-group

Use **ikev2 ipv6-address-group** to configure an IKEv2 IPv6 address pool for assigning IPv6 addresses to remote peers.

Use **undo ikev2 ipv6-address-group** to delete an IKEv2 IPv6 address pool.

### Syntax

**ikev2 ipv6-address-group** *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

**undo ikev2 ipv6-address-group** *group-name*

### Default

No IKEv2 IPv6 address pool exists.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*group-name*: Specifies a name for the IKEv2 IPv6 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

**prefix** *prefix/prefix-len*: Specifies an IPv6 prefix in the format of *prefix/prefix length*. The value range for the *prefix-len* argument is 1 to 128.

**assign-len** *assign-len*: Specifies the assigned prefix length. The value range for the *assign-len* argument is 0 to 128, and the value must be greater than or equal to *prefix-len.* The difference between *assign-len* and *prefix-len* must be no more than 16.

### Usage guidelines

Different from the IKEv2 IPv4 address pool, the device assigns an IPv6 subnet to a peer from the IKEv2 IPv6 address pool. The peer can use the assigned IPv6 subnet to assign IPv6 addresses to other devices.

IKEv2 IPv6 address pools cannot overlap with each other.

### Examples

# Configure an IKEv2 IPv6 address pool with the name **ipv6group**, prefix 1:1::/64, and the assigned prefix length 80.

```
<Sysname> system-view
[Sysname] ikev2 ipv6-address-group ipv6group prefix 1:1::/64 assign-len 80
```

### Related commands

**ipv6-address-group**

## ikev2 keychain

Use **ikev2 keychain** to create an IKEv2 keychain and enter its view, or enter the view of an existing IKEv2 keychain.

Use **undo ikev2 keychain** to delete an IKEv2 keychain.

### Syntax

**ikev2 keychain** *keychain-name*

**undo ikev2 keychain** *keychain-name*

### Default

No IKEv2 keychain exists.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*keychain-name*: Specifies a name for the IKEv2 keychain. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

### Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication. The pre-shared key configured on both ends must be the same.

You can configure multiple IKEv2 peers in an IKEv2 keychain.

### Examples

# Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

## ikev2 nat-keepalive

Use **ikev2 nat-keepalive** to set the NAT keepalive interval.

Use **undo ikev2 nat-keepalive** to restore the default.

### Syntax

**ikev2 nat-keepalive** *seconds*

**undo ikev2 nat-keepalive**

### Default

The NAT keepalive interval is 10 seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the NAT keepalive interval in seconds, in the range of 5 to 3600.

### Usage guidelines

This command takes effect when the device resides behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

### Examples

# Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 nat-keepalive 5
```

## ikev2 policy

Use **ikev2 policy** to create an IKEv2 policy and enter its view, or enter the view of an existing IKEv2 policy.

Use **undo ikev2 policy** to delete an IKEv2 policy.

### Syntax

**ikev2 policy** *policy-name*

**undo ikev2 policy** *policy-name*

### Default

The device has a system default IKEv2 policy named **default**. The default IKEv2 policy uses the default IKEv2 proposal and matches any local addresses.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*policy-name*: Specifies a name for the IKEv2 policy. The policy name is a case-insensitive string of 1 to 63 characters.

### Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet.

An IKEv2 policy uses IKEv2 proposals to define the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups to be used for negotiation.

You can configure multiple IKEv2 policies.

An IKEv2 policy must have a minimum of one IKEv2 proposal. Otherwise, the policy is incomplete.

If the initiator uses an IPsec policy that is bound to a source interface, the initiator looks up an IKEv2 policy by the IP address of the source interface.

You can set priorities to adjust the match order of IKEv2 policies that have the same match criteria.

You cannot enter the view of the default IKEv2 policy, nor modify it.

### Examples

# Create an IKEv2 policy named **policy1** and enter IKEv2 policy view.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

### Related commands

**display ikev2 policy**

## ikev2 profile

Use **ikev2 profile** to create an IKEv2 profile and enter its view, or enter the view of an existing IKEv2 profile.

Use **undo ikev2 profile** to delete an IKEv2 profile.

### Syntax

**ikev2 profile** *profile-name*

**undo ikev2 profile** *profile-name*

### Default

No IKEv2 profile exists.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*profile-name*: Specifies a name for the IKEv2 profile. The profile name is a case-insensitive string of 1 to 63 characters.

### Usage guidelines

An IKEv2 profile contains the IKEv2 SA parameters that are not negotiated, such as the identity information and authentication methods of the peers, and the matching criteria for profile lookup.

### Examples

# Create an IKEv2 profile named **profile1** and enter IKEv2 profile view.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

### Related commands

**display ikev2 profile**

# ikev2 proposal

Use **ikev2 proposal** to create an IKEv2 proposal and enter its view, or enter the view of an existing IKEv2 proposal.

Use **undo ikev2 proposal** to delete an IKEv2 proposal.

### Syntax

**ikev2 proposal** *proposal-name*

**undo ikev2 proposal** *proposal-name*

### Default

The device has a system default IKEv2 proposal named **default**. This proposal has the lowest priority and uses the following settings:

- **Encryption algorithm**—AES-CBC-128 and 3DES.
- **Integrity protection algorithm**—HMAC-SHA1 and HMAC-MD5.
- **PRF algorithm**—HMAC-SHA1 and HMAC-MD5.
- **DH group**—Group 5 and group 2.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*proposal-name*: Specifies a name for the IKEv2 proposal. The proposal name is a case-insensitive string of 1 to 63 characters and cannot be **default**.

### Usage guidelines

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups.

An IKEv2 proposal must have a minimum of one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

In an IKEv2 proposal, you can specify multiple parameters of the same type. The parameters of different types combine and form multiple sets of security parameters. If you want to use only one set of security parameters, configure only one set of security parameters for the IKEv2 proposal.

### Examples

# Create an IKEv2 proposal named **prop1**. Specify the encryption algorithm AES-CBC-128, integrity protection algorithm SHA1, PRF algorithm SHA1, and DH group 2.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption aes-cbc-128
[Sysname-ikev2-proposal-prop1] integrity sha1
[Sysname-ikev2-proposal-prop1] prf sha1
[Sysname-ikev2-proposal-prop1] dh group2
```

### Related commands

- **encryption-algorithm**
- **integrity**
- **prf**
- **dh**

# integrity

Use **integrity** to specify integrity protection algorithms for an IKEv2 proposal.

Use **undo integrity** to restore the default.

### Syntax

**integrity** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

**undo integrity**

### Default

No integrity protection algorithm is specified for an IKEv2 proposal.

### Views

IKEv2 proposal view

### Predefined user roles

network-admin

### Parameters

**aes-xcbc-mac**: Uses the HMAC-AES-XCBC-MAC algorithm.

**md5**: Uses the HMAC-MD5 algorithm.

**sha1**: Uses the HMAC-SHA1 algorithm.

**sha256**: Uses the HMAC-SHA256 algorithm.

**sha384**: Uses the HMAC-SHA384 algorithm.

**sha512**: Uses the HMAC-SHA512 algorithm.

### Usage guidelines

You can specify multiple integrity protection algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

You must specify a minimum of one integrity protection algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

### Examples

# Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

# Specify HMAC-SHA1 and HMAC-MD5 as the integrity protection algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

### Related commands

**ikev2 proposal**

# keychain

Use **keychain** to specify an IKEv2 keychain for pre-shared key authentication.

Use **undo keychain** to restore the default.

### Syntax

**keychain** *keychain-name*

**undo keychain**

### Default

No IKEv2 keychain is specified for an IKEv2 profile.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

*keychain-name*: Specifies an IKEv2 keychain by its name. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

### Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication.

You can specify only one IKEv2 keychain for an IKEv2 profile.

You can specify the same IKEv2 keychain for different IKEv2 profiles.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Specify the IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

### Related commands

- **display ikev2 profile**
- **ikev2 keychain**

# match local (IKEv2 profile view)

Use **match local** to specify a local interface or a local IP address to which an IKEv2 profile can be applied.

Use **undo match local** to remove a local interface or a local IP address to which an IKEv2 profile can be applied.

### Syntax

**match local address** { *interface-type interface-number* **|** *ipv4-address* **| ipv6** *ipv6-address* }

**undo match local address** { *interface-type interface-number* **|** *ipv4-address* **| ipv6** *ipv6-address* }

### Default

An IKEv2 profile can be applied to any local interface or IP address.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**address**: Specifies a local interface or IP address to which an IKEv2 profile can be applied.

*interface-type interface-number*: Specifies a local interface by its type and number. It can be any Layer 3 interface.

*ipv4-address*: Specifies the IPv4 address of a local interface.

**ipv6** *ipv6-address*: Specifies the IPv6 address of a local interface.

### Usage guidelines

Use this command to specify which address or interface can use the IKEv2 profile for IKEv2 negotiation. The interface is the interface that receives IKEv2 packets. The IP address is the IP address of the interface that receives IKEv2 packets.

An IKEv2 profile configured earlier has a higher priority. To give an IKEv2 profile that is configured later a higher priority, you can configure the **priority** command or this command for the profile. For example, suppose you configured IKEv2 profile A before configuring IKEv2 profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKEv2 profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKEv2 profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKEv2 profile A is preferred because IKEv2 profile A was configured earlier. To use IKEv2 profile B, you can use this command to restrict the application scope of IKEv2 profile B to IPv4 address 3.3.3.3.

You can specify multiple applicable local interfaces or IP addresses for an IKEv2 profile.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Apply the IKEv2 profile **profile1** to the interface whose IP address is 2.2.2.2.

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

### Related commands

**match remote**

# match local address (IKEv2 policy view)

Use **match local address** to specify a local interface or a local address that an IKEv2 policy matches.

Use **undo match local address** to remove a local interface or a local address that an IKEv2 policy matches.

### Syntax

**match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

**undo match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

### Default

No local interface or address is specified, and the IKEv2 policy matches any local interface or address.

### Views

IKEv2 policy view

### Predefined user roles

network-admin

### Parameters

*interface-type interface-number*: Specifies a local interface by its type and number. It can be any Layer 3 interface.

*ipv4-address*: Specifies the IPv4 address of a local interface.

**ipv6** *ipv6-address*: Specifies the IPv6 address of a local interface.

### Usage guidelines

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

### Examples

# Configure the IKEv2 policy **policy1** to match the local address 3.3.3.3.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

### Related commands

- **display ikev2 policy**
- **match vrf**

# match remote

Use **match remote** to specify a peer ID that an IKEv2 profile matches.

Use **undo match remote** to delete a peer ID that an IKEv2 profile matches.

### Syntax

**match remote** { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [ *mask* **|** *mask-length* ] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [ *prefix-length* ] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **email** *email-string* **|** **key-id** *key-id-string* } }

**undo match remote** { **certificate** *policy-name* **|** **identity** { **address** { { *ipv4-address* [ *mask* **|***mask-length* ] **|** **range** *low-ipv4-address high-ipv4-address* } **|** **ipv6** { *ipv6-address* [ *prefix-length* ] **|** **range** *low-ipv6-address high-ipv6-address* } } **|** **fqdn** *fqdn-name* **|** **email** *email-string* **|** **key-id** *key-id-string* } }

### Default

No matching peer ID is specified for the IKEv2 profile.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

**certificate** *policy-name*: Uses the information in the peer's digital certificate as the peer ID for IKEv2 profile matching. The *policy-name* argument specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

**identity**: Uses the specified information as the peer ID for IKEv2 profile matching. The specified information is configured on the peer by using the **local-identity** command.

**address** *ipv4-address* [ *mask* **|** *mask-length* ]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKEv2 profile matching. The value range for the *mask-length* argument is 0 to 32.

**address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.

**address ipv6** *ipv6-address* [ *prefix-length* ]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKEv2 profile matching. The value range for the *prefix-length* argument is 0 to 128.

**address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.

**fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKEv2 profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

**email** *email-string*: Uses peer's email address as the peer ID for IKEv2 profile matching. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

**key-id** *key-id*: Uses the peer's key ID as the peer ID for IKEv2 profile matching. The *key-id* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

### Usage guidelines

The device compares the received peer ID with the peer IDs specified in local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. If you have configured the **match local address** and **match vrf** commands, the IKEv2 profile must also match the specified local interface or address and the specified VPN instance.

To make sure only one IKEv2 profile is matched for a peer, do not specify the same peer ID for two or more IKEv2 profiles. If you configure the same peer ID for two or more IKEv2 profiles, which IKEv2 profile is selected for IKEv2 negotiation is unpredictable.

You can configure an IKEv2 profile to match multiple peer IDs. A peer ID specified earlier has a higher priority.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Configure the IKEv2 profile to match the peer ID that is the FQDN name www.test.com.

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

# Configure the IKEv2 profile to match the peer ID that is the IP address 10.1.1.1.

```
[Sysname-ikev2-profile-profile1]match remote identity address 10.1.1.1
```

### Related commands

- **identity local**
- **match local address**
- **match vrf**

## nat-keepalive

Use **nat-keepalive** to set the NAT keepalive interval.

Use **ikev2 nat-keepalive** to restore the default.

### Syntax

**nat-keepalive** *seconds*

**undo nat-keepalive**

### Default

The NAT keepalive interval set in system view is used.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the NAT keepalive interval in seconds, in the range of 5 to 3600.

### Usage guidelines

This command takes effect when the device resides behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Set the NAT keepalive interval to 1200 seconds.

```
[Sysname-ikev2-profile-profile1]nat-keepalive 1200
```

### Related commands

- **display ikev2 profile**
- **ikev2 nat-keepalive**

## peer

Use **peer** to create an IKEv2 peer and enter its view, or enter the view of an existing IKEv2 peer.

Use **undo peer** to delete an IKEv2 peer.

### Syntax

**peer** *name*

**undo peer** *name*

### Default

No IKEv2 peer exists.

### Views

IKEv2 keychain view

### Predefined user roles

network-admin

### Parameters

*name*: Specifies a name for the IKEv2 peer. The peer name is a case-insensitive string of 1 to 63 characters.

### Usage guidelines

An IKEv2 peer contains a pre-shared key and the criteria for looking up the peer. The criteria for peer lookup includes the peer's host name, IP address, IP address range, and ID. The IKEv2 negotiation initiator uses the peer's host name, IP address, or IP address range to look up its peer. The responder uses the peer's IP address, IP address range, or ID to look up its peer.

### Examples

# Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

# Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

### Related commands

- **address**
- **hostname**
- **identity**
- **ikev2 keychain**

## pre-shared-key

Use **pre-shared-key** to configure a pre-shared key.

Use **undo pre-shared-key** to delete a pre-shared key.

### Syntax

**pre-shared-key** [ **local** | **remote** ] { **ciphertext** | **plaintext** } *srting*

**undo pre-shared-key** [ **local** | **remote** ]

### Default

No pre-shared key exists.

### Views

IKEv2 peer view

### Predefined user roles

network-admin

### Parameters

**local**: Specifies a pre-shared key for certificate signing.

**remote**: Specifies a pre-shared key for certificate authentication.

**ciphertext**: Specifies a pre-shared key in encrypted form.

**plaintext**: Specifies a pre-shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

*string*: Specifies the pre-shared key. The key is case sensitive. Its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters.

## Usage guidelines

If you specify the **local** or **remote** keyword, you configure an asymmetric key. If you specify neither the **local** nor the **remote** keyword, you configure a symmetric key.

To delete a key by using the **undo** command, you must specify the correct key type. For example, if you configure a key by using the **pre-shared-key local** command, you cannot delete the key by using the **undo pre-shared-key** or **undo pre-shared-key remote** command.

If you use this command multiple times, the most recent configuration takes effect.

## Examples

- On the initiator:

  # Create an IKEv2 keychain named **key1**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain key1
  ```

  # Create an IKEv2 peer named **peer1**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer1
  ```

  # Configure the symmetric plaintext pre-shared key 111-key.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
  [Sysname-ikev2-keychain-key1-peer-peer1] quit
  ```

  # Create an IKEv2 peer named **peer2**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer2
  ```

  # Configure asymmetric plaintext pre-shared keys. The key for certificate signing is 11-key-a and the key for certificate authentication is 111-key-b.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
  ```

- On the responder:

  # Create an IKEv2 keychain named **telecom**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain telecom
  ```

  # Create an IKEv2 peer named **peer1**.

  ```
  [Sysname-ikev2-keychain-telecom] peer peer1
  ```

  # Configure the symmetric plaintext pre-shared key 111-key.

  ```
  [Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
  [Sysname-ikev2-keychain-telecom-peer-peer1] quit
  ```

  # Create an IKEv2 peer named **peer2**.

  ```
  [Sysname-ikev2-keychain-telecom] peer peer2
  ```

  # Configure asymmetric plaintext pre-shared keys. The key for certificate signing is 11-key-b and the key for certificate authentication is 111-key-a.

  ```
  [Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext
  111-key-b
  [Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext
  111-key-a
  ```

## Related commands

- **ikev2 keychain**
- **peer**

# prf

Use **prf** to specify pseudo-random function (PRF) algorithms for an IKEv2 proposal.

Use **undo prf** to restore the default.

### Syntax

**prf** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

**undo prf**

### Default

An IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.

### Views

IKEv2 proposal view

### Predefined user roles

network-admin

### Parameters

**aes-xcbc-mac**: Uses the HMAC-AES-XCBC-MAC algorithm.

**md5**: Uses the HMAC-MD5 algorithm.

**sha1**: Uses the HMAC-SHA1 algorithm.

**sha256**: Uses the HMAC-SHA256 algorithm.

**sha384**: Uses the HMAC-SHA384 algorithm.

**sha512**: Uses the HMAC-SHA512 algorithm.

### Usage guidelines

You can specify multiple PRF algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

### Examples

# Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

# Specify HMAC-SHA1 and HMAC-MD5 as the PRF algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

### Related commands

- **ikev2 proposal**
- **integrity**

# priority (IKEv2 policy view)

Use **priority** to set a priority for an IKEv2 policy.

Use **undo priority** to restore the default.

### Syntax

**priority** *priority*

**undo priority**

### Default

The priority of an IKEv2 policy is 100.

### Views

IKEv2 policy view

### Predefined user roles

network-admin

### Parameters

*priority*: Sets the priority of the IKEv2 policy, in the range of 1 to 65535. A smaller number represents a higher priority.

### Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 policies.

### Examples

# Set the priority to 10 for the IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

### Related commands

**display ikev2 policy**

## priority (IKEv2 profile view)

Use **priority** to set a priority for an IKEv2 profile.

Use **undo priority** to restore the default.

### Syntax

**priority** *priority*

**undo priority**

### Default

The priority of an IKEv2 profile is 100.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

*priority*: Sets the priority of the IKEv2 profile, in the range of 1 to 65535. A smaller number represents a higher priority.

### Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 profiles.

### Examples

# Set the priority to 10 for the IKEv2 profile **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

```
[Sysname-ikev2-profile-profile1] priority 10
```

# proposal

Use **proposal** to specify an IKEv2 proposal for an IKEv2 policy.

Use **undo proposal** to remove an IKEv2 proposal from an IKEv2 policy.

### Syntax

**proposal** *proposal-name*

**undo proposal** *proposal-name*

### Default

No IKEv2 proposal is specified for an IKEv2 policy.

### Views

IKEv2 policy view

### Predefined user roles

network-admin

### Parameters

*proposal-name*: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

### Usage guidelines

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

### Examples

# Specify the IKEv2 proposal **proposal1** for the IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] proposal proposal1
```

### Related commands

- **display ikev2 policy**
- **ikev2 proposal**

# reset ikev2 sa

Use **reset ikev2 sa** to delete IKEv2 SAs.

### Syntax

**reset ikev2 sa** [ [ { **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } ] | **tunnel** *tunnel-id* ] [ **fast** ]

### Views

User view

### Predefined user roles

network-admin

### Parameters

**local**: Deletes IKEv2 SAs for a local IP address.

**remote**: Deletes IKEv2 SAs for a remote IP address.

*ipv4-address*: Specifies a local or remote IPv4 address.

**ipv6** *ipv6-address*: Specifies a local or remote IPv6 address.

**tunnel** *tunnel-id*: Deletes IKEv2 SAs for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

**fast**: Notifies the peers of the deletion and deletes IKEv2 SAs directly before receiving the peers' responses. If you do not specify this keyword, the device notifies the peers of the deletion and deletes IKEv2 SAs after it receives the peers' responses.

### Usage guidelines

Deleting an IKEv2 SA will also delete the child SAs negotiated through the IKEv2 SA.

If you do not specify any parameters, this command deletes all IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.

### Examples

# Display information about IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local              Remote             Status
  -------------------------------------------------------------------
     1                  1.1.1.1/500        1.1.1.2/500        EST
     2                  2.2.2.1/500        2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating EST: Established, DEL: Deleting
```

# Delete the IKEv2 SA whose remote IP address is 1.1.1.2.

```
<Sysname> reset ikev2 sa remote 1.1.1.2
```

# Display information about IKEv2 SAs again. Verify that the IKEv2 SA is deleted.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local              Remote             Status
  -------------------------------------------------------------------
     2                  2.2.2.1/500        2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating EST: Established, DEL: Deleting
```

### Related commands

**display ikev2 sa**

## reset ikev2 statistics

Use **reset ikev2 statistics** to clear IKEv2 statistics.

### Syntax

**reset ikev2 statistics**

### Views

User view

### Predefined user roles

network-admin

### Examples

# Clear IKEv2 statistics.

```
<Sysname> reset ikev2 statistics
```

### Related commands

**display ikev2 statistics**

## sa duration

Use **sa duration** to set the IKEv2 SA lifetime.

Use **undo sa duration** to restore the default.

### Syntax

**sa duration** *seconds*

**undo sa duration**

### Default

The IKEv2 SA lifetime is 86400 seconds.

### Views

IKEv2 profile view

### Predefined user roles

network-admin

### Parameters

*seconds*: Sets the IKEv2 SA lifetime in seconds, in the range of 120 to 86400.

### Usage guidelines

An IKEv2 SA can be used for subsequent IKEv2 negotiations before its lifetime expires, saving a lot of negotiation time. However, the longer the lifetime, the higher the possibility that attackers collect enough information and initiate attacks.

Two peers can have different IKEv2 SA lifetime settings, and they do not perform lifetime negotiation. The peer with a shorter lifetime always initiates the rekeying.

### Examples

# Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

# Set the IKEv2 SA lifetime to 1200 seconds.

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

### Related commands

**display ikev2 profile**