目 录

1 IPsec

说明

设备运行于低加密版本时，本特性部分配置相对于高加密版本有所变化，具体差异请见本文相关描述。可以通过安装相应的 license 将设备从低加密版本升级为高加密版本，也可以通过卸载相应的 license 将升级为高加密版本的设备恢复为低加密版本。

1.1 IPsec配置命令

1.1.1 ah authentication-algorithm

ah authentication-algorithm 命令用来配置 AH 协议采用的认证算法。

undo ah authentication-algorithm 命令用来恢复缺省情况。

【命令】

ah authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **sm3** } *

undo ah authentication-algorithm

【缺省情况】

AH 协议未采用任何认证算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：采用 HMAC-AES-XCBC-96 认证算法，密钥长度 128 比特。本参数仅适用于 IKEv2 协商。

md5：采用 HMAC-MD5-96 认证算法，密钥长度 128 比特。

sha1：采用 HMAC-SHA1-96 认证算法，密钥长度 160 比特。

sha256：采用 HMAC-SHA-256 认证算法，密钥长度 256 比特。

sha384：采用 HMAC-SHA-384 认证算法，密钥长度 384 比特。

sha512：采用 HMAC-SHA-512 认证算法，密钥长度 512 比特。

sm3：采用 HMAC-SM3-96 认证算法，密钥长度 256 比特。本参数仅适用于 IKEv1 协商。

【使用指导】

每个 IPsec 安全提议中均可以配置多个 AH 认证算法，其优先级为配置顺序。

对于手工方式以及 IKEv1（第 1 版本的 IKE 协议）协商方式的 IPsec 安全策略，IPsec 安全提议中配置顺序首位的 AH 认证算法生效。为保证成功建立 IPsec 隧道，隧道两端指定的 IPsec 安全提议中配置的首个 AH 认证算法需要一致。

【举例】

配置 IPsec 安全提议采用的 AH 认证算法为 HMAC-SHA1 算法，密钥长度为 160 比特。

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

1.1.2 description

description 命令用来配置 IPsec 安全策略/IPsec 安全策略模板的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

无描述信息。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

text：IPsec 安全策略/IPsec 安全策略模板的描述信息，为 1～80 个字符的字符串，区分大小写。

【使用指导】

当系统中存在多个 IPsec 安全策略/IPsec 安全策略模板时，可通过配置相应的描述信息来有效区分不同的安全策略。

【举例】

配置序号为 1 的 IPsec 安全策略 policy1 的描述信息为 CenterToA。

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

1.1.3 display ipsec { ipv6-policy | policy }

display ipsec { **ipv6-policy** | **policy** }命令用来显示 IPsec 安全策略的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ipv6-policy：显示 IPv6 IPsec 安全策略的信息。

policy：显示 IPv4 IPsec 安全策略的信息。

policy-name：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：IPsec 安全策略表项的顺序号，取值范围为 1～65535。

【使用指导】

如果不指定任何参数，则显示所有 IPsec 安全策略的信息。

如果指定了 *policy-name* 和 *seq-number*，则显示指定的 IPsec 安全策略表项的信息；如果指定了 *policy-name* 而没有指定 *seq-number*，则显示所有名称相同的 IPsec 安全策略表项的信息。

【举例】

显示所有 IPv4 IPsec 安全策略的信息。

```
<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:
  smart-link policy:
  SA trigger mode: Auto
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): 1000 seconds
  SA soft-duration buffer(traffic based): 43200 kilobytes
  SA idle time: 100 seconds
------------------------------------------
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:
  smart-link policy:
  SA trigger mode: Auto
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): 1000 seconds
  SA soft-duration buffer(traffic based): 43200 kilobytes
  SA idle time: 100 seconds
```

显示所有 IPv6 IPsec 安全策略的详细信息。

```
<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:

  ----------------------------
  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: 1000::2
  Transform set:  completetransform
  IKE profile:
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Auto
```

```
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA soft-duration buffer(time based): 1000 seconds
SA soft-duration buffer(traffic based): 43200 kilobytes
SA idle time: 100 seconds
```

表1-1 display ipsec { ipv6-policy | policy }命令显示信息描述表

字段	描述
IPsec Policy	IPsec安全策略的名称
Interface	应用了IPsec安全策略的接口名称
Sequence number	IPsec安全策略表项的顺序号
Mode	IPsec安全策略采用的协商方式 • Mannul：手工方式 • ISAKMP：IKE 协商方式 • Template：策略模板方式
The policy configuration is incomplete	IPsec安全策略配置不完整，可能的原因包括： • ACL 未配置 • IPsec 安全提议未配置 • ACL 中没有 **permit** 规则 • IPsec 安全提议配置不完整 • IPsec 隧道对端 IP 地址未指定 • IPsec SA 的 SPI 和密钥与 IPsec 安全策略的 SPI 和密钥不匹配
Description	IPsec安全策略的描述信息
Traffic Flow Confidentiality	TFC（Traffic Flow Confidentiality）填充功能的开启状态
Security data flow	IPsec安全策略引用的ACL
Selector mode	IPsec安全策略的数据流保护方式 • standard：标准方式 • aggregation：聚合方式 • per-host：主机方式
Local address	IPsec隧道的本端IP地址（仅IKE协商方式的IPsec安全策略下存在）
Remote address	IPsec隧道的对端IP地址或主机名
Transform set	IPsec安全策略引用的IPsec安全提议的名称
IKE profile	IPsec安全策略引用的IKE Profile的名称
IKEv2 profile	IPsec安全策略引用的IKEv2 Profile的名称
smart-link policy	（暂不支持）智能选路策略
SA trigger mode	触发建立IPsec SA的模式，包括： • Auto：自动触发模式 • Traffic-based：流量触发模式

字段	描述
SA duration(time based)	基于时间的IPsec SA生存时间，单位为秒
SA duration(traffic based)	基于流量的IPsec SA生存时间，单位为千字节
SA soft-duration buffer(time based)	IPsec SA软超时缓冲时间，单位为秒，未配置时显示为“--”
SA soft-duration buffer(traffic based)	IPsec SA软超时缓冲流量，单位为千字节，未配置时显示为“--”
SA idle time	IPsec SA的空闲超时时间，单位为秒，未配置时显示为“--”
Inbound AH setting	入方向采用的AH协议的相关设置
Outbound AH setting	出方向采用的AH协议的相关设置
AH SPI	AH协议的SPI
AH string-key	AH协议的字符类型的密钥，若配置，则显示为******，否则显示为空
AH authentication hex key	AH协议的十六进制密钥，若配置，则显示为******，否则显示为空
Inbound ESP setting	入方向采用的ESP协议的相关设置
Outbound ESP setting	出方向采用的ESP协议的相关设置
ESP SPI	ESP协议的SPI
ESP string-key	ESP协议的字符类型的密钥，若配置，则显示为******，否则显示为空
ESP encryption hex key	ESP协议的十六进制加密密钥，若配置，则显示为******，否则显示为空
ESP authentication hex key	ESP协议的十六进制认证密钥，若配置，则显示为******，否则显示为空

【相关命令】

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

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

display ipsec { **ipv6-policy-template** | **policy-template** }命令用来显示 IPsec 安全策略模板的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ipv6-policy-template：显示 IPv6 IPsec 安全策略模板的信息。

policy-template：显示 IPv4 IPsec 安全策略模板的信息。

template-name：指定 IPsec 安全策略模板的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：指定 IPsec 安全策略模板表项的顺序号，取值范围为 1～65535。

【使用指导】

如果不指定任何参数，则显示所有 IPsec 安全策略模板的信息。

如果指定了 *template-name* 和 *seq-number*，则显示指定的 IPsec 安全策略模板表项的信息；如果指定了 *template-name* 而没有指定 *seq-number*，则显示所有名称相同的 IPsec 安全策略模板表项的信息。

【举例】

显示所有 IPv4 IPsec 安全策略模板的信息。

```
<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: 100 seconds
```

显示所有 IPv6 IPsec 安全策略模板的信息。

```
<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
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time: 100 seconds
```

表1-2 display ipsec { ipv6-policy-template | policy-template }命令显示信息描述表

字段	描述
IPsec Policy Template	IPsec安全策略模板名称
Sequence number	IPsec安全策略模板表项的序号
Description	IPsec安全策略模板的描述信息
Traffic Flow Confidentiality	TFC（Traffic Flow Confidentiality）填充功能的开启状态
Security data flow	IPsec安全策略模板引用的ACL
Selector mode	IPsec安全策略模板的数据流保护方式 • standard：标准方式 • aggregation：聚合方式 • per-host：主机方式
Local address	IPsec隧道的本端IP地址
IKE profile	IPsec安全策略模板引用的IKE Profile名称
IKEv2 profile	IPsec安全策略引用的IKEv2 Profile的名称
Remote address	IPsec隧道的对端IP地址
Transform set	IPsec安全策略模板引用的安全提议的名称
IPsec SA local duration(time based)	基于时间的IPsec SA生存时间，单位为秒
IPsec SA local duration(traffic based)	基于流量的IPsec SA生存时间，单位为千字节
SA idle time	IPsec SA的空闲超时时间，单位为秒，未配置时显示为“--”

【相关命令】

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

1.1.5 display ipsec sa

display ipsec sa 命令用来显示 IPsec SA 的相关信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

brief：显示所有的 IPsec SA 的简要信息。

count：显示 IPsec SA 的个数。

interface *interface-type interface-number*：显示指定接口下的 IPsec SA 的详细信息。*interface-type interface-number* 表示接口类型和接口编号。

ipv6-policy：显示由指定 IPv6 IPsec 安全策略创建的 IPsec SA 的详细信息。

policy：显示由指定 IPv4 IPsec 安全策略创建的 IPsec SA 的详细信息。

policy-name：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：IPsec 安全策略的顺序号，取值范围为 1～65535。

remote *ip-address*：显示指定对端 IP 地址的 IPsec SA 的详细信息。

ipv6：显示指定 IPv6 对端地址的 IPsec SA 的详细信息。若不指定本参数，则表示显示指定 IPv4 对端地址的 IPsec SA 的详细信息。

【使用指导】

如果不指定任何参数，则显示所有 IPsec SA 的详细信息。

【举例】

显示 IPsec SA 的简要信息。

```
<Sysname> display ipsec sa brief
-------------------------------------------------------------------------
Interface/Global   Dst Address      SPI         Protocol  Status
-------------------------------------------------------------------------
Vlan100            10.1.1.1         400         ESP       Active
Vlan100            255.255.255.255  4294967295  ESP       Active
Vlan100            100::1/64        500         AH        Active
Global             --               600         ESP       Active
```

表1-3 display ipsec sa brief 命令显示信息描述表

字段	描述
Interface/Global	IPsec SA属于的接口或是全局（全局IPsec SA由IPsec安全框架生成）（暂不支持）
Dst Address	IPsec隧道对端的IP地址
SPI	IPsec SA的SPI
Protocol	IPsec采用的安全协议
Status	IPsec SA的状态：主用（Active）、备用（Standby） • 多机备份环境下，取值为 Active 表示主用、取值为 Standby 表示备用 • 单机运行环境下，仅为 Active，表示 SA 处于可用状态

显示 IPsec SA 的个数。

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

显示所有 IPsec SA 的详细信息。

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

  ----------------------------
  IPsec policy: r2
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 3
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VRF: vp1
    Extended Sequence Numbers 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：  90194313219
      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：  64424509441
      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
```

表1-4 display ipsec sa 命令显示信息描述表

字段	描述
Interface	IPsec SA所在的接口
IPsec policy	采用的IPsec安全策略名
Sequence number	IPsec安全策略表项顺序号
Mode	IPsec安全策略采用的协商方式 • Mannul：手工方式 • ISAKMP：IKE 协商方式 • Template：IKE 模板方式
Tunnel id	IPsec隧道的ID号
Encapsulation mode	采用的报文封装模式，有两种：传输（transport）和隧道（tunnel）模式
Perfect Forward Secrecy	此IPsec安全策略发起协商时使用完善的前向安全（PFS）特性，取值包括： • 768-bit Diffie-Hellman 组（**dh-group1**） • 1024-bit Diffie-Hellman 组（**dh-group2**） • 1536-bit Diffie-Hellman 组（**dh-group5**） • 2048-bit Diffie-Hellman 组（**dh-group14**） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（**dh-group24**） • 256-bit ECP 模式 Diffie-Hellman 组（**dh-group19**） • 384-bit ECP 模式 Diffie-Hellman 组（**dh-group20**）
Extended Sequence Numbers enable	ESN（Extended Sequence Number，扩展序列号）功能是否开启
Traffic Flow Confidentiality enable	TFC（Traffic Flow Confidentiality）填充功能是否开启
Path MTU	IPsec SA的路径MTU值
Tunnel	IPsec隧道的端点地址信息
local address	IPsec隧道的本端IP地址
remote address	IPsec隧道的对端IP地址
Flow	受保护的数据流信息
sour addr	数据流的源IP地址
dest addr	数据流的目的IP地址
port	端口号
protocol	协议类型，取值包括： • ip：IPv4 协议 • ipv6：IPv6 协议
Inbound ESP SAs	入方向的ESP协议的IPsec SA信息

字段	描述
Outbound ESP SAs	出方向的ESP协议的IPsec SA信息
Inbound AH SAs	入方向的AH协议的IPsec SA信息
Outbound AH SAs	出方向的AH协议的IPsec SA信息
SPI	IPsec SA的SPI
Connection ID	IPsec SA标识
Transform set	IPsec安全提议所采用的安全协议及算法
SA duration (kilobytes/sec)	IPsec SA生存时间，单位为千字节或者秒
SA remaining duration (kilobytes/sec)	剩余的IPsec SA生存时间，单位为千字节或者秒
Max received sequence-number	入方向接收到的报文最大序列号
Max sent sequence-number	出方向发送的报文最大序列号
Anti-replay check enable	抗重放检测功能是否开启
Anti-replay window size	抗重放窗口宽度
UDP encapsulation used for NAT traversal	此IPsec SA是否使用NAT穿越功能
Status	IPsec SA的状态： • 多机备份环境下，取值为 Active 表示主用、取值为 Standby 表示备用 • 单机运行环境下，取值仅为 Active，表示 SA 处于可用状态
No duration limit for this SA	手工方式创建的IPsec SA无生存时间

【相关命令】

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

1.1.6 display ipsec statistics

display ipsec statistics 命令用来显示 IPsec 处理的报文的统计信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

tunnel-id *tunnel-id*：显示指定 IPsec 隧道处理的报文统计信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0～4294967295。通过 **display ipsec tunnel brief** 可以查看到已建立的 IPsec 隧道的 ID 号。

【使用指导】

如果不指定任何参数，则显示 IPsec 处理的所有报文的统计信息。

【举例】

显示所有 IPsec 处理的报文统计信息。

```
<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
```

显示 ID 为 1 的 IPsec 隧道处理的报文统计信息。

```
<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
```

表1-5 display ipsec statistics 命令显示信息描述表

字段	描述
IPsec packet statistics	IPsec处理的报文统计信息
Received/sent packets	接收/发送的受安全保护的数据包的数目
Received/sent bytes	接收/发送的受安全保护的字节数目
Dropped packets (received/sent)	被设备丢弃了的受安全保护的数据包的数目（接收/发送）
Dropped packets statistics	被丢弃的数据包的详细信息
No available SA	因为找不到IPsec SA而被丢弃的数据包的数目
Wrong SA	因为IPsec SA错误而被丢弃的数据包的数目
Invalid length	因为数据包长度不正确而被丢弃的数据包的数目
Authentication failure	因为认证失败而被丢弃的数据包的数目
Encapsulation failure	因为加封装失败而被丢弃的数据包的数目
Decapsulation failure	因为解封装失败而被丢弃的数据包的数目
Replayed packets	被丢弃的重放的数据包的数目
ACL check failure	因为ACL检测失败而被丢弃的数据包的数目
MTU check failure	因为MTU检测失败而被丢弃的数据包的数目
Loopback limit exceeded	因为本机处理的次数超过限制而被丢弃的数据包的数目
Crypto speed limit exceeded	因为加密速度的限制而被丢弃的数据包的数目

【相关命令】

- **reset ipsec statistics**

1.1.7 display ipsec transform-set

display ipsec transform-set 命令用来显示 IPsec 安全提议的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

transform-set-name：指定 IPsec 安全提议的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

如果没有指定 IPsec 安全提议的名称，则显示所有 IPsec 安全提议的信息。

【举例】

显示所有 IPsec 安全提议的信息。

```
<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
```

表1-6 display ipsec transform-set 命令显示信息描述表

字段	描述
IPsec transform set	IPsec安全提议的名称
State	IPsec安全提议是否完整
Encapsulation mode	IPsec安全提议采用的封装模式，包括两种：传输（transport）和隧道（tunnel）模式
ESN	ESN（Extended Sequence Number，扩展序列号）功能的开启状态
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性的配置，取值包括： • 768-bit Diffie-Hellman 组（**dh-group1**） • 1024-bit Diffie-Hellman 组（**dh-group2**） • 1536-bit Diffie-Hellman 组（**dh-group5**） • 2048-bit Diffie-Hellman 组（**dh-group14**） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（**dh-group24**） • 256-bit ECP 模式 Diffie-Hellman 组（**dh-group19**） • 384-bit ECP 模式 Diffie-Hellman 组（**dh-group20**）
Transform	IPsec安全提议采用的安全协议，包括三种：AH协议、ESP协议、AH-ESP（先采用ESP协议，再采用AH协议）
AH protocol	AH协议相关配置
ESP protocol	ESP协议相关配置

字段	描述
Integrity	安全协议采用的认证算法
Encryption	安全协议采用的加密算法

【相关命令】

- **ipsec transform-set**

1.1.8 display ipsec tunnel

display ipsec tunnel 命令用来显示 IPsec 隧道的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

brief：显示 IPsec 隧道的简要信息。

count：显示 IPsec 隧道的个数。

tunnel-id *tunnel-id*：显示指定的 IPsec 隧道的详细信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0～4294967295。

【使用指导】

IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

【举例】

显示所有 IPsec 隧道的简要信息。

```
<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
```

表1-7 display ipsec tunnel brief 命令显示信息描述表

字段	描述
Tunn-id	IPsec隧道的ID号

字段	描述
Src Address	IPsec隧道的源地址 在IPsec Profile生成的SA中，该值无意义，显示为“--”
Dst Address	IPsec隧道的目的地址 在IPsec Profile生成的SA中，该值无意义，显示为“--”
Inbound SPI	IPsec隧道中生效的入方向SPI 如果该隧道使用了两种安全协议，则会分为两行分别显示两个入方向的SPI
Outbound SPI	IPsec隧道中生效的出方向SPI 如果该隧道使用了两种安全协议，则会分为两行分别显示两个出方向的SPI
Status	IPsec SA的状态： • 多机备份环境下，取值为 Active 表示主用、取值为 Standby 表示备用 • 单机运行环境下，取值仅为 Active，表示 SA 处于可用状态

显示 IPsec 隧道的数目。

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

显示所有 IPsec 隧道的详细信息。

```
<Sysname> display ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
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:
Inside vpn-instance:
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
```

显示 ID 号为 1 的 IPsec 隧道的详细信息。

```
<Sysname> display ipsec tunnel tunnel-id 1
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
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
```

表1-8 display ipsec tunnel 命令显示信息描述表

字段	描述
Tunnel ID	IPsec隧道的ID，用来唯一地标识一个IPsec隧道
Status	IPsec隧道的状态： • 多机备份环境下，取值为 Active 表示主用、取值为 Standby 表示备用 • 单机运行环境下，取值仅为 Active，表示隧道处于可用状态
Perfect forward secrecy	此IPsec安全策略发起协商时使用完善的前向安全（PFS）特性，取值包括： • 768-bit Diffie-Hellman 组（**dh-group1**） • 1024-bit Diffie-Hellman 组（**dh-group2**） • 1536-bit Diffie-Hellman 组（**dh-group5**） • 2048-bit Diffie-Hellman 组（**dh-group14**） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（**dh-group24**） • 256-bit ECP 模式 Diffie-Hellman 组（**dh-group19**） • 384-bit ECP 模式 Diffie-Hellman 组（**dh-group20**）
Inside vpn-instance	（暂不支持）被保护数据所属的VPN实例名
SA's SPI	出方向和入方向的IPsec SA的SPI
Tunnel	IPsec隧道的端点地址信息
local address	IPsec隧道的本端IP地址
remote address	IPsec隧道的对端IP地址
Flow	IPsec隧道保护的数据流，包括源地址、目的地址、源端口、目的端口、协议
as defined in ACL 3001	手工方式建立的IPsec隧道所保护的数据流的范围，例如IPsec隧道保护ACL 3001中定义的所有数据流

1.1.9 encapsulation-mode

encapsulation-mode 命令用来配置安全协议对报文的封装模式。

undo encapsulation-mode 命令用来恢复缺省情况。

【命令】

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

undo encapsulation-mode

【缺省情况】

使用隧道模式对 IP 报文进行封装。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

transport：采用传输模式。

tunnel：采用隧道模式。

【使用指导】

传输模式下的安全协议主要用于保护上层协议报文，仅传输层数据被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对 ESP 封装）被放置在原 IP 头后面。若要求端到端的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时，才能使用传输模式。

隧道模式下的安全协议用于保护整个 IP 数据包，用户的整个 IP 数据包都被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对 ESP 封装）被封装在一个新的 IP 数据包中。这种模式下，封装后的 IP 数据包有内外两个 IP 头，其中的内部 IP 头为原有的 IP 头，外部 IP 头由提供安全服务的设备添加。在安全保护由设备提供的情况下，数据包进行安全传输的起点或终点不为数据包的实际起点和终点时（例如安全网关后的主机），则必须使用隧道模式。隧道模式用于保护两个安全网关之间的数据传输。

在 IPsec 隧道的两端，IPsec 安全提议所采用的封装模式要一致。

【举例】

指定 IPsec 安全提议 tran1 采用传输模式对 IP 报文进行封装。

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

【相关命令】

- **ipsec transform-set**

1.1.10 esn enable

esn enable 命令用来开启 ESN（Extended Sequence Number，扩展序列号）功能。

undo esn enable 命令用来关闭 ESN 功能。

【命令】

esn enable [both]

undo esn enable

【缺省情况】

ESN 功能处于关闭状态。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

both：既支持扩展序列号，又支持非扩展序列号。若不指定该参数，则表示仅支持扩展序列号。

【使用指导】

ESN 功能用于扩展防重放序列号的范围，可将抗重放序列号长度由传统的 32 比特扩大到 64 比特。在有大量数据流需要使用 IPsec SA 保护进行高速传输的情况下，该功能可避免防重放序列号被过快消耗而引发频繁地重协商。

只有发起方和响应方都开启了 ESN 功能，ESN 功能才能生效。

【举例】

在 IPsec 安全提议中开启 ESN 功能。

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

【相关命令】

- **display ipsec transform-set**

1.1.11 esp authentication-algorithm

esp authentication-algorithm 命令用来配置 ESP 协议采用的认证算法。

undo esp authentication-algorithm 命令用来恢复缺省情况。

【命令】

esp authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **sm3** } *

undo esp authentication-algorithm

【缺省情况】

ESP 协议未采用任何认证算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：采用 HMAC-AES-XCBC-96 认证算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

md5：采用 HMAC-MD5-96 认证算法，密钥长度 128 比特。

sha1：采用 HMAC-SHA1-96 认证算法，密钥长度 160 比特。

sha256：采用 HMAC-SHA-256 认证算法，密钥长度 256 比特。

sha384：采用 HMAC-SHA-384 认证算法，密钥长度 384 比特。

sha512：采用 HMAC-SHA-512 认证算法，密钥长度 512 比特。

【使用指导】

每个 IPsec 安全提议中均可以配置多个 ESP 认证算法，其优先级为配置顺序。

对于手工方式以及 IKEv1（第 1 版本的 IKE 协议）协商方式的 IPsec 安全策略，IPsec 安全提议中配置顺序首位的 ESP 认证算法生效。为保证成功建立 IPsec 隧道，隧道两端指定的 IPsec 安全提议中配置的首个 ESP 认证算法需要一致。

【举例】

在 IPsec 安全提议中配置 ESP 认证算法为 HMAC-SHA1 算法。

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

【相关命令】

- **ipsec transform-set**

1.1.12 esp encryption-algorithm

esp encryption-algorithm 命令用来配置 ESP 协议采用的加密算法。

undo esp encryption-algorithm 命令用来恢复缺省情况。

【命令】

（高加密版本-非 FIPS 模式下）

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.

【缺省情况】

ESP 协议未采用任何加密算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc：采用 CBC 模式的 3DES 算法，密钥长度为 168 比特。

aes-cbc-128：采用 CBC 模式的 AES 算法，密钥长度为 128 比特。

aes-cbc-192：采用 CBC 模式的 AES 算法，密钥长度为 192 比特。

aes-cbc-256：采用 CBC 模式的 AES 算法，密钥长度为 256 比特。

aes-ctr-128：采用 CTR 模式的 AES 算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

aes-ctr-192：采用 CTR 模式的 AES 算法，密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

aes-ctr-256：采用 CTR 模式的 AES 算法，密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-128：采用 CBC 模式的 Camellia 算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-192：采用 CBC 模式的 Camellia 算法，密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-256：采用 CBC 模式的 Camellia 算法，密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

des-cbc：采用 CBC 模式的 DES 算法，密钥长度为 64 比特。

gmac-128：采用 GMAC 算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

gmac-192：采用 GMAC 算法，密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

gmac-256：采用 GMAC 算法，密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

gcm-128：采用 GCM 算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

gcm-192：采用 GCM 算法，密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

gcm-256：采用 GCM 算法，密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

null：采用 NULL 加密算法，表示不进行加密。

【使用指导】

每个 IPsec 安全提议中均可以配置多个 ESP 加密算法，其优先级为配置顺序。

对于手工方式以及 IKEv1（第 1 版本的 IKE 协议）协商方式的 IPsec 安全策略，IPsec 安全提议中配置顺序首位的 ESP 加密算法生效。为保证成功建立 IPsec 隧道，隧道两端指定的 IPsec 安全提议中配置的首个 ESP 加密算法需要一致。

GCM、GMAC 属于组合模式算法（Combined mode algorithm）。其中，GCM 算法能同时为 ESP 协议提供加密与认证服务，GMAC 只能提供认证服务。组合模式算法只能用于仅采用 ESP 协议的配置环境，不能用于同时采用 AH 协议和 ESP 协议的配置环境，且不能与普通的 ESP 认证算法同时使用。

【举例】

在 IPsec 安全提议中配置 ESP 加密算法为 CBC 模式的 AES 算法，密钥长度为 128 比特。

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

【相关命令】

- **ipsec transform-set**

1.1.13 ike-profile

ike-profile 命令用来指定 IPsec 安全策略/IPsec 安全策略模板引用的 IKE profile。

undo ike-profile 命令用来恢复缺省情况。

【命令】

ike-profile *profile-name*

undo ike-profile

【缺省情况】

未引用 IKE profile。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

profile-name：IKE profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全策略、IPsec 安全策略模板中若不引用 IKE profile，则使用系统视图下配置的 IKE profile 进行协商，若系统视图下没有任何 IKE profile，则使用全局的 IKE 参数进行协商。

IPsec 安全策略、IPsec 安全策略模板引用的 IKE profile 中定义了用于 IKE 协商的相关参数。

IPsec 安全策略/IPsec 安全策略模板下只能引用一个 IKE profile。

【举例】

指定 IPsec 安全策略 policy1 中引用的 IKE profile 为 profile1。

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

【相关命令】

- **ike profile**（安全命令参考/IKE）

1.1.14 ikev2-profile

ikev2-profile 命令用来指定 IPsec 安全策略视图/IPsec 安全策略模板视图引用的 IKEv2 profile。

undo ikev2-profile 命令用来恢复缺省情况。

【命令】

ikev2-profile *profile-name*

undo ikev2-profile

【缺省情况】

未引用 IKEv2 profile。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

profile-name：IKEv2 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全策略/IPsec 安全策略模板视图引用的 IKEv2 profile 中定义了用于 IKEv2 协商的相关参数。

一个 IPsec 安全策略视图/一个 IPsec 安全策略模板视图下只能引用一个 IKEv2 profile。发起方必须引用 IKEv2 profile，响应方引用 IKEv2 profile 表示此 IPsec 策略只允许用此 IKEv2 profile 协商，否则表示此 IPsec 策略允许用任何 IKEv2 profile 协商。

【举例】

指定 IPsec 安全策略 policy1 中引用的 IKEv2 profile 为 profile1。

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

【相关命令】

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

1.1.15 ipsec { ipv6-policy | policy }

ipsec { ipv6-policy | policy }命令用来创建一条 IPsec 安全策略，并进入 IPsec 安全策略视图。如果指定的 IPsec 安全策略已经存在，则直接进入 IPsec 安全策略视图。

undo ipsec { ipv6-policy | policy }命令用来删除指定的 IPsec 安全策略。

【命令】

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

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

【缺省情况】

不存在 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy：指定 IPv6 IPsec 安全策略。

policy：指定 IPv4 IPsec 安全策略。

policy-name：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：IPsec 安全策略的顺序号，取值范围为 1～65535。

isakmp：指定通过 IKE 协商建立 IPsec SA。

manual：指定用手工方式建立 IPsec SA。

【使用指导】

创建 IPsec 安全策略时，必须指定协商方式（**isakmp** 或 **manual** ）。进入已创建的 IPsec 安全策略时，可以不指定协商方式。

不能修改已创建的 IPsec 安全策略的协商方式。

一个 IPsec 安全策略是若干具有相同名称、不同顺序号的 IPsec 安全策略表项的集合。在同一个 IPsec 安全策略中，顺序号越小的 IPsec 安全策略表项优先级越高。

对于 **undo** 命令，携带 *seq-number* 参数时表示删除一个 IPsec 安全策略表项，不携带该参数时表示删除一个指定的 IPsec 安全策略。

IPv4 IPsec 安全策略和 IPv6 IPsec 安全策略名称可以相同。

【举例】

创建一个名称为 policy1、顺序号为 100、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

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

创建一个名称为 policy1、顺序号为 101、采用手工方式建立 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

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

【相关命令】

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

1.1.16 ipsec { ipv6-policy | policy } isakmp template

ipsec { **ipv6-policy** | **policy** } **isakmp template** 命令用来引用 IPsec 安全策略模板创建一条 IKE 协商方式的 IPsec 安全策略。

undo ipsec { **ipv6-policy** | **policy** }命令用来删除指定的 IPsec 安全策略。

【命令】

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

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

【缺省情况】

不存在 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy：指定 IPv6 IPsec 安全策略。

policy：指定 IPv4 IPsec 安全策略。

policy-name：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：IPsec 安全策略的顺序号，取值范围为 1～65535，值越小优先级越高。

isakmp template *template-name*：指定被引用的 IPsec 安全策略模板。*template-name* 表示 IPsec 安全策略模板的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

对于 **undo** 命令，携带 *seq-number* 参数时表示删除一个 IPsec 安全策略表项，不携带该参数时表示删除一个指定的 IPsec 安全策略。

应用了该类 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。由于 IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，因此这种方式创建的 IPsec 安全策略适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

【举例】

引用 IPsec 策略模板 temp1，创建名称为 policy2、顺序号为 200 的 IPsec 安全策略。

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

【相关命令】

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

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

ipsec { **ipv6-policy** | **policy** } **local-address** 命令用来配置 IPsec 安全策略为共享源接口 IPsec 安全策略，即将指定的 IPsec 安全策略与一个源接口进行绑定。

undo ipsec { **ipv6-policy** | **policy** } **local-address** 命令用来取消 IPsec 安全策略为共享源接口 IPsec 安全策略。

【命令】

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

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

【缺省情况】

IPsec 安全策略不是共享源接口 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy：指定 IPv6 IPsec 安全策略。

policy：指定 IPv4 IPsec 安全策略。

policy-name：共享该接口 IP 地址的 IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

local-address *interface-type interface-number*：指定的共享源接口的名称。*interface-type interface-nunmber* 为接口类型和接口编号。

【使用指导】

在不同的接口上应用安全策略时，各个接口将分别协商生成 IPsec SA。如果两个互为备份的接口上都引用了 IPsec 安全策略，并采用相同的安全策略，则在主备链路切换时，接口状态的变化会触发重新进行 IKE 协商，从而导致 IPsec 业务流的暂时中断。通过将一个 IPsec 安全策略与一个源接口绑定，使之成为共享源接口 IPsec 安全策略，可以实现多个应用该共享源接口 IPsec 安全策略的出接口共享同一个指定的源接口（称为共享源接口）协商出的 IPsec SA。只要该源接口的状态不变化，各接口上 IPsec 业务就不会中断。

当非共享源接口 IPsec 安全策略应用于业务接口，并已经生成 IPsec SA 时，如果将该安全策略配置为共享源接口安全策略，则已经生成的 IPsec SA 将被删除。

只有 IKE 协商方式的 IPsec 安全策略才能配置为 IPsec 共享源接口安全策略，手工方式的 IPsec 安全策略不能配置为共享源接口 IPsec 安全策略。

一个 IPsec 安全策略只能与一个源接口绑定，多次执行本命令，最后一次执行的命令生效。

一个源接口可以同时与多个 IPsec 安全策略绑定。

推荐使用状态较为稳定的接口作为共享源接口，例如 Loopback 接口。

【举例】

配置 IPsec 安全策略 map 为共享源接口安全策略，共享源接口为 Loopback11。

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

【相关命令】

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

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

ipsec { ipv6-policy-template | policy-template }命令用来创建一个 IPsec 安全策略模板，并进入 IPsec 安全策略模板视图。如果指定的 IPsec 安全策略模板已经存在，则直接进入 IPsec 安全策略模板视图。

undo ipsec { **ipv6-policy-template** | **policy-template** }命令用来删除指定的 IPsec 安全策略模板。

【命令】

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

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

【缺省情况】

不存在 IPsec 安全策略模板。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy-template：指定 IPv6 IPsec 安全策略模板。

policy-template：指定 IPv4 IPsec 安全策略模板。

template-name：IPsec 安全策略模板的名称，为 1～63 个字符的字符串，不区分大小写。

seq-number：IPsec 安全策略模板表项的顺序号，取值范围为 1～65535，值越小优先级越高。

【使用指导】

IPsec 安全策略模板与直接配置的 IKE 协商方式的 IPsec 安全策略中可配置的参数类似，但是配置较为简单，除了 IPsec 安全提议和 IKE 对等体之外的其它参数均为可选。

- 携带 *seq-number* 参数的 **undo** 命令用来删除一个 IPsec 安全策略模板表项。
- 一个 IPsec 安全策略模板是若干具有相同名称、不同顺序号的 IPsec 安全策略模板表项的集合。
- IPv4 IPsec 安全策略模板和 IPv6 IPsec 安全策略模板名称可以相同。

【举例】

创建一个名称为 template1、顺序号为 100 的 IPsec 安全策略模板，并进入 IPsec 安全策略模板视图。

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

【相关命令】

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

1.1.19 ipsec anti-replay check

ipsec anti-replay check 命令用来开启 IPsec 抗重放检测功能。

undo ipsec anti-replay check 用来关闭 IPsec 抗重放检测功能。

【命令】

ipsec anti-replay check

undo ipsec anti-replay check

【缺省情况】

IPsec 抗重放检测功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

对重放报文的解封装无意义，并且解封装过程涉及密码学运算，会消耗设备大量的资源，导致业务可用性下降，造成了拒绝服务攻击。通过开启 IPsec 抗重放检测功能，将检测到的重放报文在解封装处理之前丢弃，可以降低设备资源的消耗。

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

只有 IKE 协商的 IPsec SA 才能够支持抗重放检测，手工方式生成的 IPsec SA 不支持抗重放检测。因此该功能开启与否对手工方式生成的 IPsec SA 没有影响。

【举例】

开启 IPsec 抗重放检测功能。

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

【相关命令】

- **ipsec anti-replay window**

1.1.20 ipsec anti-replay window

ipsec anti-replay window 命令用来配置 IPsec 抗重放窗口的宽度。

undo ipsec anti-replay window 命令用来恢复缺省情况。

【命令】

ipsec anti-replay window *width*

undo ipsec anti-replay window

【缺省情况】

IPsec 抗重放窗口的宽度为 64。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

width：IPsec 抗重放窗口的宽度，取值可以为 64、128、256、512、1024，单位为报文个数。

【使用指导】

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

修改后的抗重放窗口宽度仅对新协商成功的 IPsec SA 生效。

【举例】

配置 IPsec 抗重放窗口的宽度为 128。

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

【相关命令】

- **ipsec anti-replay check**

1.1.21 ipsec apply

ipsec apply 命令用来在接口上应用 IPsec 安全策略。

undo ipsec apply 命令用来从接口上取消应用的 IPsec 安全策略。

【命令】

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

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

【缺省情况】

接口上未应用 IPsec 安全策略。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy：指定 IPv6 IPsec 安全策略。

policy：指定 IPv4 IPsec 安全策略。

policy-name：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

一个接口下最多只能应用一个 IPv4/IPv6 类型的 IPsec 安全策略，但可以同时应用一个 IPv4 类型的 IPsec 安全策略和一个 IPv6 类型的 IPsec 安全策略。

在将 IKE 方式的 IPsec 安全策略可以应用到多个接口上时，请使用共享源接口的 IPsec 安全策略；手工方式的 IPsec 安全策略只能应用到一个接口上。

【举例】

在接口 Vlan-interface100 上应用名为 policy1 的 IPsec 安全策略。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] ipsec apply policy policy1
```

【相关命令】

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

1.1.22 ipsec decrypt-check enable

ipsec decrypt-check enable 命令用来开启解封装后 IPsec 报文的 ACL 检查功能。

undo ipsec decrypt-check 命令用来关闭解封装后 IPsec 报文的 ACL 检查功能。

【命令】

ipsec decrypt-check enable

undo ipsec decrypt-check enable

【缺省情况】

解封装后 IPsec 报文的 ACL 检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在隧道模式下，接口入方向上解封装的 IPsec 报文的内部 IP 头有可能不在当前 IPsec 安全策略引用的 ACL 的保护范围内，如网络中一些恶意伪造的攻击报文就可能有此问题，所以设备需要重新检查解封装后的报文的 IP 头是否在 ACL 保护范围内。开启该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性。

【举例】

开启解封装后 IPsec 报文的 ACL 检查功能。

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

1.1.23 ipsec df-bit

ipsec df-bit 命令用来为当前接口设置 IPsec 封装后外层 IP 头的 DF 位。

undo ipsec df-bit 命令用来恢复缺省情况。

【命令】

ipsec df-bit { clear | copy | set }

undo ipsec df-bit

【缺省情况】

接口下未设置 IPsec 封装后外层 IP 头的 DF 位，采用全局设置的 DF 位。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

clear：表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。

copy：表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

set：表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能分片。

【使用指导】

该功能仅在 IPsec 的封装模式为隧道模式时有效（因为传输模式不会增加新的 IP 头，因此对于传输模式无影响）。

该功能用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。

如果有多个接口应用了共享源接口安全策略，则这些接口上必须使用相同的 DF 位设置。

转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

【举例】

在接口 Vlan-interface100 上设置 IPsec 封装后外层 IP 头的 DF 位。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipsec df-bit set
```

【相关命令】

- **ipsec global-df-bit**

1.1.24 ipsec fragmentation

ipsec fragmentation 命令用来配置 IPsec 分片功能。

undo ipsec fragmentation 命令用来恢复缺省情况。

【命令】

ipsec fragmentation { after-encryption | before-encryption }

undo ipsec fragmentation

【缺省情况】

IPsec 分片功能为封装前分片。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

after-encryption：表示开启 IPsec 封装后分片功能。

before-encryption：表示开启 IPsec 封装前分片功能。

【使用指导】

IPsec 封装前分片功能处于开启状态时，设备会先判断报文在经过 IPsec 封装之后大小是否会超过发送接口的 MTU 值，如果封装后的大小超过发送接口的 MTU 值，且报文的 DF 位未置位那么会先对其分片再封装；如果待报文的 DF 位被置位，那么设备会丢弃该报文，并发送 ICMP 差错控制报文。

IPsec 封装后分片功能处于开启状态时，无论报文封装后大小是否超过发送接口的 MTU 值，设备会直接对其先进行 IPsec 封装处理，再由后续业务对其进行分片。

【举例】

开启 IPsec 封装后分片功能。

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

1.1.25 ipsec global-df-bit

ipsec global-df-bit 命令用来为所有接口设置 IPsec 封装后外层 IP 头的 DF 位。

undo ipsec global-df-bit 命令用来恢复缺省情况。

【命令】

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

undo ipsec global-df-bit

【缺省情况】

IPsec 封装后外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

clear：表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。

copy：表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

set：表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能分片。

【使用指导】

该功能仅在 IPsec 的封装模式为隧道模式时有效（因为传输模式不会增加新的 IP 头，因此对于传输模式无影响）。

该功能用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

【举例】

为所有接口设置 IPsec 封装后外层 IP 头的 DF 位。

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

【相关命令】

- **ipsec df-bit**

1.1.26 ipsec limit max-tunnel

ipsec limit max-tunnel 命令用来配置本端允许建立 IPsec 隧道的最大数。

undo ipsec limit max-tunnel 命令用来恢复缺省情况。

【命令】

ipsec limit max-tunnel *tunnel-limit*

undo ipsec limit max-tunnel

【缺省情况】

不限制本端允许建立 IPsec 隧道的最大数。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

tunnel-limit：指定允许本端建立 IPsec 隧道的最大数，取值范围为 1～4294967295。

【使用指导】

本端允许建立 IPsec 隧道的最大数与内存资源有关。内存充足时可以设置较大的数值，提高 IPsec 的并发性能；内存不足时可以设置较小的数值，降低 IPsec 占用内存的资源。

【举例】

配置本端允许建立 IPsec 隧道的最大数为 5000。

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

【相关命令】

- **ike limit**

1.1.27 ipsec logging negotiation enable

ipsec logging negotiation enable 命令用来开启 IPsec 协商事件日志功能。

undo ipsec logging negotiation enable 命令用来关闭 IPsec 协商事件日志功能。

【命令】

ipsec logging negotiation enable

undo ipsec logging negotiation enable

【缺省情况】

IPsec 协商事件日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 IPsec 协商事件日志记录功能后，设备会输出 IPsec 协商过程中的相关日志。

【举例】

开启 IPsec 协商事件日志记录功能。

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

1.1.28 ipsec logging packet enable

ipsec logging packet enable 命令用来开启 IPsec 报文日志记录功能。

undo ipsec logging packet enable 命令用来关闭 IPsec 报文日志记录功能。

【命令】

ipsec logging packet enable

undo ipsec logging packet enable

【缺省情况】

IPsec 报文日志记录功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 IPsec 报文日志记录功能后，设备会在丢弃 IPsec 报文的情况下，例如入方向找不到对应的 IPsec SA，AH/ESP 认证失败或 ESP 加密失败等时，输出相应的日志信息，该日志信息内容主要包括报文的源和目的 IP 地址、报文的 SPI 值、报文的序列号信息，以及设备丢包的原因。

【举例】

开启 IPsec 报文日志记录功能。

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

1.1.29 ipsec profile

ipsec profile 命令用来创建一个 IPsec 安全框架，并进入 IPsec 安全框架视图。如果指定的 IPsec 安全框架已经存在，则直接进入 IPsec 安全框架视图。

undo ipsec profile 命令用来删除指定的 IPsec 安全框架。

【命令】

ipsec profile *profile-name*

undo ipsec profile *profile-name*

【缺省情况】

不存在 IPsec 安全框架。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：IPsec 安全框架的名称，为 1～63 个字符的字符串，不区分大小写。

manual：手工方式的 IPsec 安全框架。

isakmp：指定通过 IKE 协商建立安全联盟。

【使用指导】

创建 IPsec 安全框架时，必须指定协商方式（**manual** 或 **isakmp**）；进入已创建的 IPsec 安全框架时，可以不指定协商方式。

手工方式 IPsec profile 专门用于为应用协议配置 IPsec 安全策略，它相当于一个手工方式创建的 IPsec 安全策略，其中的应用协议可包括但不限于 OSPFv3、IPv6 BGP、RIPng。

IKE 协商方式 IPsec profile 用于为应用协议模块自动协商生成安全联盟，不限制对端的地址，不需要进行 ACL 匹配，且适用于 IPv4 和 IPv6 应用协议，其中的应用协议模块包括但是不限于 ADVPN 等。

【举例】

配置名称为 profile1 的 IPsec 安全框架，通过手工配置建立安全联盟。

```
<Sysname> system-view
[Sysname] ipsec profile profile1 manual
```

```
[Sysname-ipsec-profile—manual-profile1]
```

配置名称为 profile1 的 IPsec 安全框架，通过 IKE 协商建立安全联盟。

```
<Sysname> system-view
[Sysname] ipsec profile profile1 isakmp
[Sysname-ipsec-profile-isakmp-profile1]
```

【相关命令】

- **display ipsec profile**

1.1.30 ipsec sa global-duration

ipsec sa global-duration 命令用来配置全局的 IPsec SA 生存时间。

undo ipsec sa global-duration 命令用来恢复缺省情况。

【命令】

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

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

【缺省情况】

IPsec SA 基于时间的生存时间为 3600 秒，基于流量的生存时间为 1843200 千字节。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-based *seconds*：指定基于时间的全局生存时间，取值范围为 180～604800，单位为秒。

traffic-based *kilobytes*：指定基于流量的全局生存时间，取值范围为 2560～4294967295，单位为千字节。如果流量达到此值，则生存时间到期。

【使用指导】

IPsec 安全策略/IPsec 安全策略模板视图下也可配置 IPsec SA 的生存时间，若 IPsec 安全策略/IPsec 安全策略模板视图和全局都配置了 IPsec SA 的生存时间，则优先采用 IPsec 安全策略/IPsec 安全策略模板视图下的配置值与对端协商。

IKE 为 IPsec 协商建立 IPsec SA 时，采用本地配置的生存时间和对端提议的 IPsec SA 生存时间中较小的一个。

可同时存在基于时间和基于流量两种方式的 IPsec SA 生存时间，只要 IPsec SA 的生存时间到达指定的时间或流量时，该 IPsec SA 就会失效。IPsec SA 失效前，IKE 将为 IPsec 对等体协商建立新的 IPsec SA，这样，在旧的 IPsec SA 失效前新的 IPsec SA 就已经准备好。在新的 IPsec SA 开始协商而没有协商好之前，继续使用旧的 IPsec SA 保护通信。在新的 IPsec SA 协商好之后，则立即采用新的 IPsec SA 保护通信。

【举例】

配置全局的 IPsec SA 生存时间为两个小时，即 7200 秒。

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

```
[Sysname] ipsec sa global-duration time-based 7200
```

配置全局的 IPsec SA 生存时间为 10M 字节，即传输 10240 千字节的流量后，当前的 IPsec SA 过期。

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

【相关命令】

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

1.1.31 ipsec sa global-soft-duration buffer

ipsec sa global-soft-duration buffer 命令用来设置 IPsec SA 的全局软超时缓冲参数。

undo ipsec sa global-soft-duration buffer 命令用来恢复缺省情况。

【命令】

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

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

【缺省情况】

未配置全局软超时缓冲时间和全局软超时缓冲流量。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-based *seconds*：IPsec SA 的全局软超时缓冲时间，取值范围为 20～201600，单位为秒。

traffic-based *kilobytes*：IPsec SA 的全局软超时缓冲流量，取值范围为 1000～4294901760，单位为 KB。

【使用指导】

本命令只对 IKEv1 有效。

在配置了软超时缓冲时间的情况下，软超时时间（基于时间的生存时间－软超时缓冲时间）需要大于 20 秒。否则，仍然采用未配置软超时缓冲时间的默认算法计算软超时时间。

在配置了软超时缓冲流量的情况下，软超时流量（基于流量的生存时间－软超时缓冲流量）需要大于 1000KB。否则，仍然采用未配置软超时缓冲流量的默认算法计算软超时流量。

同时配置了全局软超时缓冲参数和局部软超时缓冲参数时，以局部软超时缓冲为准。

【举例】

设置所有 IPsec 安全策略的 IPsec SA 的软超时缓冲时间为 600 秒。

```
<Sysname> sytem-view
[Sysname] ipsec sa global-soft-duration buffer time-based 600
```

设置所有 IPsec 安全策略的 IPsec SA 的软超时缓冲流量为 10000KB。

```
<Sysname> sytem-view
```

```
[Sysname] ipsec sa global-soft-duration buffer traffic-based 10000
```

【相关命令】

- **sa soft-duration buffer**

1.1.32 ipsec sa idle-time

ipsec sa idle-time 命令用来开启全局的 IPsec SA 空闲超时功能，并配置全局 IPsec SA 空闲超时时间。在指定超时时间内没有流量匹配的 IPsec SA 即被删除。

undo ipsec sa idle-time 命令用来关闭全局的 IPsec SA 空闲超时功能。

【命令】

ipsec sa idle-time *seconds*

undo ipsec sa idle-time

【缺省情况】

全局的 IPsec SA 空闲超时功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds：IPsec SA 的空闲超时时间，取值范围为 60～86400，单位为秒。

【使用指导】

此功能只适用于 IKE 协商出的 IPsec SA。

IPsec 安全策略/IPsec 安全策略模板视图下也可配置 IPsec SA 的空闲超时时间，若 IPsec 安全策略/IPsec 安全策略模板视图和全局都配置了 IPsec SA 的空闲超时时间，则优先采用 IPsec 安全策略/IPsec 安全策略模板视图下的配置值。

【举例】

开启全局的 IPsec SA 空闲超时功能，并配置全局 IPsec SA 的空闲超时时间为 600 秒。

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

【相关命令】

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

1.1.33 ipsec transform-set

ipsec transform-set 命令用来创建 IPsec 安全提议，并进入 IPsec 安全提议视图。如果指定的 IPsec 安全提议已经存在，则直接进入 IPsec 安全提议视图。

undo ipsec transform-set 命令用来删除指定的 IPsec 安全提议。

【命令】

ipsec transform-set *transform-set-name*

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

【缺省情况】

不存在 IPsec 安全提议。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

transform-set-name：IPsec 安全提议的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全提议是 IPsec 安全策略的一个组成部分，它用于保存 IPsec 需要使用的安全协议、加密/认证算法以及封装模式，为 IPsec 协商 SA 提供各种安全参数。

【举例】

创建名为 tran1 的 IPsec 安全提议，并进入 IPsec 安全提议视图。

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

【相关命令】

- **display ipsec transform-set**

1.1.34 local-address

local-address 命令用来配置 IPsec 隧道的本端 IP 地址。

undo local-address 命令用来恢复缺省情况。

【命令】

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

undo local-address

【缺省情况】

IPsec 隧道的本端 IPv4 地址为应用 IPsec 安全策略的接口的主 IPv4 地址，本端 IPv6 地址为应用 IPsec 安全策略的接口的第一个 IPv6 地址。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：IPsec 隧道的本端 IPv4 地址。

ipv6 *ipv6-address*：IPsec 隧道的本端 IPv6 地址。

【使用指导】

采用 IKE 协商方式的 IPsec 安全策略上，发起方的 IPsec 隧道的对端 IP 地址必须与响应方的 IPsec 隧道本端 IP 地址一致。

【举例】

配置 IPsec 隧道的本端 IP 地址为 1.1.1.1。

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

【相关命令】

- **remote-address**

1.1.35 pfs

pfs 命令用来配置在使用此安全提议发起 IKE 协商时使用 PFS（Perfect Forward Secrecy，完善的前向安全）特性。

undo pfs 命令用来恢复缺省情况。

【命令】

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

undo pfs

【缺省情况】

使用 IPsec 安全策略发起 IKE 协商时不使用 PFS 特性。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

dh-group1：采用 768-bit Diffie-Hellman 组。

dh-group2：采用 1024-bit Diffie-Hellman 组。

dh-group5：采用 1536-bit Diffie-Hellman 组。

dh-group14：采用 2048-bit Diffie-Hellman 组。

dh-group19：采用 256-bit ECP 模式 Diffie-Hellman 组。本参数仅适用于 IKEv2 协商。

dh-group20：采用 384-bit ECP 模式 Diffie-Hellman 组。本参数仅适用于 IKEv2 协商。

dh-group24：采用 2048-bit 和 256_bit 子群 Diffie-Hellman 组。

【使用指导】

384-bit ECP 模式 Diffie-Hellman 组（**dh-group20**）、256-bit ECP 模式 Diffie-Hellman 组（**dh-group19**）、2048-bit 和 256-bit 子群 Diffie-Hellman 组（**dh-group24**）、2048-bit Diffie-Hellman 组（**dh-group14**）、1536-bit Diffie-Hellman 组（**dh-group5**）、1024-bit Diffie-Hellman 组（**dh-group2**）、768-bit Diffie-Hellman 组（**dh-group1**）算法的强度，即安全性和需要计算的时间依次递减。

IKEv1 协商时发起方的 PFS 强度必须大于或等于响应方的 PFS 强度，否则 IKE 协商会失败。IKEv2 不受该限制。

不配置 PFS 特性的一端，按照对端的 PFS 特性要求进行 IKE 协商。

【举例】

配置 IPsec 安全提议使用 PFS 特性，并采用 2048-bit Diffie-Hellman 组。

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

1.1.36 protocol

protocol 命令用来配置 IPsec 安全提议采用的安全协议。

undo protocol 命令用来恢复缺省情况。

【命令】

protocol { ah | ah-esp | esp }

undo protocol

【缺省情况】

使用 ESP 安全协议。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

ah：采用 AH 协议对报文进行保护。

ah-esp：先用 ESP 协议对报文进行保护，再用 AH 协议对报文进行保护。

esp：采用 ESP 协议对报文进行保护。

【使用指导】

在 IPsec 隧道的两端，IPsec 安全提议所采用的安全协议必须一致。

【举例】

配置 IPsec 安全提议采用 AH 协议。

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

1.1.37 qos pre-classify

qos pre-classify 命令用来开启 QoS 预分类功能。

undo qos pre-classify 命令用来关闭 QoS 预分类功能。

【命令】

qos pre-classify

undo qos pre-classify

【缺省情况】

QoS 预分类功能处于关闭状态，即 QoS 使用 IPsec 封装后报文的外层 IP 头信息来对报文进行分类。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【使用指导】

QoS 预分类功能是指，QoS 基于被封装报文的原始 IP 头信息对报文进行分类。

【举例】

在 IPsec 安全策略中开启 QoS 预分类功能。

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

1.1.38 remote-address

remote-address 命令用来指定 IPsec 隧道的对端 IP 地址。

undo remote-address 命令用来恢复缺省情况。

【命令】

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

undo remote-address

【缺省情况】

未指定 IPsec 隧道的对端 IP 地址。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 IPv6 IPsec 隧道的对端地址或主机名称。如果不指定该参数，则表示指定 IPv4 IPsec 隧道的对端地址或主机名称。

hostname：IPsec 隧道的对端主机名，为 1～253 个字符的字符串，不区分大小写。该主机名可被 DNS 服务器解析为 IP 地址。

ipv4-address：IPsec 隧道的对端 IPv4 地址。

ipv6-address：IPsec 隧道的对端 IPv6 地址。

【使用指导】

IKE 协商发起方必须配置 IPsec 隧道的对端 IP 地址，对于使用 IPsec 安全策略模板的响应方可选配。

手工方式的 IPsec 安全策略不支持域名解析，因此只能指定 IP 地址类型的对端 IP 地址。

对于主机名方式的对端地址，地址更新的查询过程有所不同。

- 若此处指定对端主机名由 DNS 服务器来解析，则本端按照 DNS 服务器通知的域名解析有效期，在该有效期超时之后向 DNS 服务器查询主机名对应的最新的 IP 地址。
- 若此处指定对端主机名由本地配置的静态域名解析（通过 **ip host** 命令配置）来解析，则更改此主机名对应的 IP 地址之后，需要在 IPsec 安全策略或 IPsec 安全策略模板中重新配置 **remote-address**，才能使得本端解析到更新后的对端 IP 地址。

例如，本端已经存在一条静态域名解析配置，它指定了主机名 test 对应的 IP 地址为 1.1.1.1。若先后执行以下配置：

在 IPsec 安全策略 policy1 中指定 IPsec 隧道的对端主机名为 test。

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

更改主机名 test 对应的 IP 地址为 2.2.2.2。

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

则，需要在 IPsec 安全策略 policy1 中重新指定对端主机名，使得本端可以根据更新后的本地域名解析配置得到最新的对端 IP 地址 2.2.2.2，否则仍会解析为原来的 IP 地址 1.1.1.1。

重新指定 IPsec 隧道的对端主机名为 test。

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

【举例】

指定 IPsec 隧道的对端 IPv4 地址为 10.1.1.2。

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

【相关命令】

- **ip host**（三层技术-IP 业务/域名解析）
- **local-address**

1.1.39 reset ipsec sa

reset ipsec sa 命令用来清除已经建立的 IPsec SA。

【命令】

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*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*]：表示根据 IPsec 安全策略名称清除 IPsec SA。

- **ipv6-policy**：IPv6 IPsec 安全策略。
- **policy**：IPv4 IPsec 安全策略。
- *policy-name*：IPsec 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。
- *seq-number*：IPsec 安全策略表项的顺序号，取值范围为 1～65535。如果不指定该参数，则表示指定名称为 *policy-name* 的安全策略中所有安全策略表项。

remote：表示根据对端 IP 地址清除 IPsec SA。

- *ipv4-address*：对端的 IPv4 地址。
- **ipv6** *ipv6-address*：对端的 IPv6 地址。

spi { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*：表示根据 SA 的三元组信息（对端 IP 地址、安全协议、安全参数索引）清除 IPsec SA。

- *ipv4-address*：对端的 IPv4 地址。
- **ipv6** *ipv6-address*：对端的 IPv6 地址。
- **ah**：AH 协议。
- **esp**：ESP 协议。
- *spi-num*：安全参数索引，取值范围为 256～4294967295。

【使用指导】

如果不指定任何参数，则清除所有的 IPsec SA。

如果指定了一个 IPsec SA 的三元组信息，则将清除符合该三元组的某一个方向的 IPsec SA 以及对应的另外一个方向的 IPsec SA。若是同时采用了两种安全协议，则还会清除另外一个协议的出方向和入方向的 IPsec SA。

对于出方向 IPsec SA，三元组是它的唯一标识；对于入方向 IPsec SA，SPI 是它的唯一标识。因此，若是希望通过指定出方向的三元组信息来清除 IPsec SA，则需要准确指定三元组信息；若是希望通过指定入方向的三元组信息来清除 IPsec SA，则只需要准确指定 SPI 值即可，另外两个信息可以任意。

通过手工建立的 IPsec SA 被清除后，系统会立即根据对应的手工 IPsec 安全策略建立新的 IPsec SA。

通过 IKE 协商建立的 IPsec SA 被清除后，系统会在有报文需要进行 IPsec 保护时触发协商新的 IPsec SA。

【举例】

清除所有 IPsec SA。

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

清除 SPI 为 256、对端地址为 10.1.1.2、安全协议为 AH 的出方向和入方向的 IPsec SA。

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

清除 IPsec 对端地址为 10.1.1.2 的所有 IPsec SA。

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

清除 IPsec 安全策略名称为 policy1、顺序号为 10 的所有 IPsec SA。

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

清除 IPsec 安全策略 policy1 中的所有 IPsec SA。

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

【相关命令】

- **display ipsec sa**

1.1.40 reset ipsec statistics

reset ipsec statistics 命令用来清除 IPsec 的报文统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

tunnel-id *tunnel-id*：清除指定 IPsec 隧道的报文统计信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0～4294967295。如果未指定本参数，则清除 IPsec 的所有报文统计信息。

【举例】

清除 IPsec 的所有报文统计信息。

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

【相关命令】

- **display ipsec statistics**

1.1.41 reverse-route dynamic

reverse-route dynamic 命令用来开启 IPsec 反向路由注入功能。

undo reverse-route dynamic 命令用来关闭 IPsec 反向路由注入功能。

【命令】

reverse-route [**next-hop** [**ipv6**] *ip-address*] **dynamic**

undo reverse-route dynamic

【缺省情况】

IPsec 反向路由注入功能处于关闭状态。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

next-hop：指定自动生成的静态路由下一跳地址。若未指定下一跳地址，则自动生成的静态路由下一跳为 IPsec 隧道的对端地址。

ipv6：指定自动生成的静态路由下一跳 IPv6 地址。若不指定此参数，则表示 IPv4 地址。

ip-address：下一跳的 IPv4 或 IPv6 地址。

【使用指导】

在企业中心侧网关设备上的某安全策略视图/安全策略模板视图下开启 IPsec 反向路由注入功能后，设备会根据协商的 IPsec SA 自动生成一条静态路由，该路由的目的地址为受保护的对端私网，下一跳地址缺省为 IPsec 隧道的对端地址；在有多条路径到达隧道对端目的地址的情况下，可以通过 **next-hop** 参数指定下一跳来控制隧道到达对端所经过的路径。

开启反向路由注入功能时，会删除本策略协商出的所有 IPsec SA。当有新的流量触发生成 IPsec SA 时，根据新协商的 IPsec 生成路由信息。

关闭反向路由注入功能时，会删除本策略协商出的所有 IPsec SA。

生成的静态路由随 IPsec SA 的创建而创建，随 IPsec SA 的删除而删除。

需要查看生成的路由信息时，可以通过 **display ip routing-table** 命令查看。

【举例】

开启 IPsec 反向路由注入功能，根据协商成功的 IPsec SA 动态生成静态路由，目的地址为受保护的对端私网网段 3.0.0.0/24，下一跳地址为对端隧道地址 1.1.1.2。

```
<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
```

隧道两端的 IPsec SA 协商成功后，可查看到生成如下静态路由（其它显示信息略）。

```
[Sysname] display ip routing-table

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan100
```

开启 IPsec 反向路由注入功能，根据协商成功的 IPsec SA 动态生成静态路由，目的地址为受保护的对端私网网段 4.0.0.0/24，指定下一跳地址为 2.2.2.3。

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route next-hop 2.2.2.3 dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

隧道两端的 IPsec SA 协商成功后，查看路由表，可以看到已生成如下静态路由（其它显示信息略）。

```
[Sysname] display ip routing-table

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
4.0.0.0/24          Static 60   0            2.2.2.3         GE1/0/1
```

【相关命令】

- **display ip routing-table**（网络互通命令参考/IP 路由基础）
- **ipsec policy**
- **ipsec policy-template**

1.1.42 reverse-route preference

reverse-route preference 命令用来设置 IPsec 反向路由注入功能生成的静态路由的优先级。

undo reverse-route preference 命令用来恢复缺省情况。

【命令】

reverse-route preference *number*

undo reverse-route preference

【缺省情况】

IPsec 反向路由注入功能生成的静态路由的优先级为 60。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

number：静态路由的优先级，取值范围为 1～255。该值越小，优先级越高。

【使用指导】

若对静态路由优先级进行修改，会删除本策略协商生成的所有 IPsec SA 和根据这些 IPsec SA 生成的静态路由。

【举例】

配置 IPsec 反向路由注入功能生成的静态路由的优先级为 100。

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

【相关命令】

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

1.1.43 reverse-route tag

reverse-route tag 命令用来设置 IPsec 反向路由注入功能生成的静态路由的 Tag 值。

undo reverse-route tag 命令用来恢复缺省情况。

【命令】

reverse-route tag *tag-value*

undo reverse-route tag

【缺省情况】

IPsec 反向路由注入功能生成的静态路由的 Tag 值为 0。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

tag-value：静态路由的 Tag 值，取值范围为 1～4294967295。

【使用指导】

本 Tag 值用于标识静态路由，以便在路由策略中根据 Tag 值对路由进行灵活的控制，若对静态路由 Tag 值进行修改，则会删除本策略协商生成的所有 IPsec SA 和根据这些 IPsec SA 生成的静态路由。

【举例】

配置 IPsec 反向路由注入功能生成的静态路由的 Tag 值为 50。

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

【相关命令】

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

1.1.44 sa duration

sa duration 命令用来配置 IPsec SA 的生存时间。

undo sa duration 命令用来删除指定的 IPsec SA 生存时间。

【命令】

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

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

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板的 IPsec SA 生存时间为当前全局的 IPsec SA 生存时间。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

time-based *seconds*：指定基于时间的生存时间，取值范围为 180～604800，单位为秒。

traffic-based *kilobytes*：指定基于流量的生存时间，取值范围为 2560～4294967295，单位为千字节。

【使用指导】

当 IKE 协商 IPsec SA 时，如果采用的 IPsec 安全策略/IPsec 安全策略模板下未配置 IPsec SA 的生存时间，将采用全局的 IPsec SA 生存时间（通过命令 **ipsec sa global-duration** 设置）与对端协商。如果 IPsec 安全策略/IPsec 安全策略模板下配置了 IPsec SA 的生存时间，则优先使用 IPsec 安全策略/IPsec 安全策略模板下的配置值与对端协商。

IKE 为 IPsec 协商建立 IPsec SA 时，采用本地配置的生存时间和对端提议的 IPsec SA 生存时间中较小的一个。

【举例】

配置 IPsec 安全策略 policy1 的 IPsec SA 生存时间为两个小时，即 7200 秒。

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

配置 IPsec 安全策略 policy1 的 IPsec SA 生存时间为 20M 字节，即传输 20480 千字节的流量后，当前的 IPsec SA 就过期。

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

【相关命令】

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

1.1.45 sa hex-key authentication

sa hex-key authentication 命令用来为手工创建的 IPsec SA 配置十六进制形式的认证密钥。

undo sa hex-key authentication 命令用来删除指定的 IPsec SA 的认证密钥。

【命令】

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

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

【缺省情况】

未配置 IPsec SA 使用的认证密钥。

【视图】

IPsec 安全策略视图

【缺省用户角色】

network-admin

【参数】

inbound：指定入方向 IPsec SA 使用的认证密钥。

outbound：指定出方向 IPsec SA 使用的认证密钥。

ah：指定 AH 协议。

esp：指定 ESP 协议。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：明文密钥为十六进制格式的字符串，不区分大小写。对于不同的算法，密钥长度不同：HMAC-MD5 算法，密钥长度为 16 个字节；HMAC-SHA1 算法，密钥长度为 20 个字节。密文密钥为 1～85 个字符的字符串，区分大小写。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略。

必须分别配置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的认证密钥必须和对端的出方向 IPsec SA 的认证密钥一致；本端的出方向 IPsec SA 的认证密钥必须和对端的入方向 IPsec SA 的认证密钥一致。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能建立 IPsec 隧道。

在相同方向和协议的情况下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 AH 协议的入方向 IPsec SA 的认证密钥为明文 0x112233445566778899aabbccddeeff00；出方向 IPsec SA 的认证密钥为明文 0xaabbccddeeff001100aabbccddeeff00。

```
<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
```

【相关命令】

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

1.1.46 sa hex-key encryption

sa hex-key encryption 命令用来为手工创建的 IPsec SA 配置十六进制形式的加密密钥。

undo sa hex-key encryption 命令用来删除指定的 IPsec SA 的加密密钥。

【命令】

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

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

【缺省情况】

未配置 IPsec SA 使用的加密密钥。

【视图】

IPsec 安全策略视图

【缺省用户角色】

network-admin

【参数】

inbound：指定入方向 IPsec SA 使用的加密密钥。

outbound：指定出方向 IPsec SA 使用的加密密钥。

esp：指定 ESP 协议。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：明文密钥为 16 进制格式的字符串，不区分大小写。对于不同的算法，密钥长度不同，详见 表 1-9。密文密钥为 1～117 个字符的字符串，区分大小写。

表1-9 算法与密钥长度对照表

算法	密钥长度（字节）
DES-CBC	8
3DES-CBC	24
AES128-CBC	16
AES192-CBC	24
AES256-CBC	32

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略。

必须分别配置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的加密密钥必须和对端的出方向 IPsec SA 的加密密钥一致；本端的出方向 IPsec SA 的加密密钥必须和对端的入方向 IPsec SA 的加密密钥一致。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能建立 IPsec 隧道。

相同方向的情况下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 ESP 协议的入方向 IPsec SA 的加密算法的密钥为明文 0x1234567890abcdef；出方向 IPsec SA 的加密算法的密钥为明文 0xabcdefabcdef1234。

```
<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
```

【相关命令】

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

1.1.47 sa idle-time

sa idle-time 命令用来配置 IPsec SA 的空闲超时时间。在指定的超时时间内，没有流量使用的 IPsec SA 将被删除。

undo sa idle-time 命令用来恢复缺省情况。

【命令】

sa idle-time *seconds*

undo sa idle-time

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板下的 IPsec SA 空闲超时时间为当前全局的 IPsec SA 空闲超时时间。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

seconds：IPsec SA 的空闲超时时间，取值范围为 60～86400，单位为秒。

【使用指导】

此功能只适用于 IKE 协商出的 IPsec SA，且只有通过 **ipsec sa idle-time** 命令开启空闲超时功能后，本功能才会生效。

如果 IPsec 安全策略/IPsec 安全策略模板视图下没有配置 IPsec SA 空闲超时时间，将采用全局的 IPsec SA 空闲超时时间（通过命令 **ipsec sa idle-time** 设置）决定 IPsec SA 是否空闲并进行删除。如果 IPsec 安全策略/IPsec 安全策略模板视图下配置了 IPsec SA 空闲超时时间，则优先使用 IPsec 安全策略/IPsec 安全策略模板视图下的配置值。

【举例】

配置 IPsec 安全策略的 IPsec SA 的空闲超时时间为 600 秒。

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

【相关命令】

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

1.1.48 sa soft-duration buffer

sa soft-duration buffer 命令用来设置 IPsec SA 的软超时缓冲参数。

undo sa soft-duration buffer 命令用来恢复缺省配置。

【命令】

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

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

【缺省情况】

未配置软超时缓冲时间或软超时缓冲流量。

【视图】

IPsec 策略视图

【缺省用户角色】

network-admin

【参数】

time-based *seconds*：IPsec SA 的软超时缓冲时间，取值范围为 20～201600，单位为秒。

traffic-based *kilobytes*：IPsec SA 的软超时缓冲流量，取值范围为 1000～4294901760，单位为 KB。

【使用指导】

本命令只对 IKEv1 有效。

在配置了软超时缓冲时间的情况下，软超时时间（基于时间的生存时间－软超时缓冲时间）需要大于 20 秒。否则，仍然采用未配置软超时缓冲时间的默认算法计算软超时时间。

在配置了软超时缓冲流量的情况下，软超时流量（基于流量的生存时间－软超时缓冲流量）需要大于 1000KB。否则，仍然采用未配置软超时缓冲流量的默认算法计算软超时流量。

【举例】

设置 IPsec SA 的软超时缓冲时间为 600 秒。

```
<Sysname> system-view
[Sysname] ipsec policy example 1 isakmp
[Sysname-ipsec-policy-isakmp-example-1] sa soft-duration buffer time-based 600
```

设置 IPsec SA 的软超时缓冲流量为 10000KB。

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

```
[Sysname] ipsec policy example 1 isakmp
[Sysname-ipsec-policy-isakmp-example-1] sa soft-duration buffer traffic-based 10000
```

【相关命令】

- **ipsec sa global-soft-duration buffer**

1.1.49 sa spi

sa spi 命令用来配置 IPsec SA 的 SPI。

undo sa spi 命令用来删除指定的 IPsec SA 的 SPI。

【命令】

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

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

【缺省情况】

不存在 IPsec SA 的 SPI。

【视图】

IPsec 安全策略视图

【缺省用户角色】

network-admin

【参数】

inbound：指定入方向 IPsec SA 的 SPI。

outbound：指定出方向 IPsec SA 的 SPI。

ah：指定 AH 协议。

esp：指定 ESP 协议。

spi-number：IPsec SA 的安全参数索引，取值范围为 256～4294967295。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略。对于 IKE 协商方式的 IPsec 安全策略，IKE 将自动协商 IPsec SA 的参数并创建 IPsec SA，不需要手工设置 IPsec SA 的参数。

必须分别配置 **inbound** 和 **outbound** 两个方向 IPsec SA 的参数，且保证每一个方向上的 IPsec SA 的唯一性：对于出方向 IPsec SA，必须保证三元组（对端 IP 地址、安全协议、SPI）唯一；对于入方向 IPsec SA，必须保证 SPI 唯一。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的 SPI 必须和对端的出方向 IPsec SA 的 SPI 一样；本端的出方向 IPsec SA 的 SPI 必须和对端的入方向 IPsec SA 的 SPI 一样。

【举例】

配置入方向 IPsec SA 的 SPI 为 10000，出方向 IPsec SA 的 SPI 为 20000。

```
<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
```

【相关命令】

- **display ipsec sa**

1.1.50 sa string-key

sa string-key 命令用来为手工创建的 IPsec SA 配置字符串形式的密钥。

undo sa string-key 命令用来删除指定的 IPsec SA 的字符串形式的密钥。

【命令】

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

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

【缺省情况】

未配置 IPsec SA 使用的密钥。

【视图】

IPsec 安全策略视图

【缺省用户角色】

network-admin

【参数】

inbound：指定入方向 IPsec SA 的密钥。

outbound：指定出方向 IPsec SA 的密钥。

ah：指定 AH 协议。

esp：指定 ESP 协议。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1～255 个字符的字符串，密文密钥为 1～373 个字符的字符串。对于不同的算法，系统会根据输入的字符串自动生成符合算法要求的密钥。对于 ESP 协议，系统会自动地同时生成认证算法的密钥和加密算法的密钥。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略。

必须分别配置 **inbound** 和 **outbound** 两个方向 IPsec SA 的参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端入方向 IPsec SA 的密钥必须和对端出方向 IPsec SA 的密钥一样；本端出方向 IPsec SA 的密钥必须和对端入方向 IPsec SA 的密钥一样。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能正确地建立 IPsec 隧道。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 AH 协议的入方向 IPsec SA 的密钥为明文字符串 abcdef；出方向 IPsec SA 的密钥为明文字符串 efcdab。

```
<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
```

在 IPv6 IPsec 策略中，配置采用 AH 协议的入方向 IPsec SA 的密钥为明文字符串 abcdef；出方向 IPsec SA 的密钥为明文字符串 abcdef。

```
<Sysname> system-view
[Sysname] ipsec ipv6-policy policy1 100 manual
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key outbound ah simple abcdef
```

【相关命令】

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

1.1.51 sa trigger-mode

sa trigger-mode 命令用来配置触发建立 IPsec SA 的模式。

undo sa trigger-mode 命令用来恢复缺省情况。

【命令】

sa trigger-mode { **auto** | **traffic-based** }

undo sa trigger-mode

【缺省情况】

触发建立 IPSec SA 的模式为流量触发。

【视图】

IPsec 安全策略视图

【缺省用户角色】

network-admin

【参数】

auto：自动触发模式，完成 IPsec 的基本配置后设备自动触发协商建立 IPsec SA。

traffic-based：流量触发模式，当存在符合 IPsec 安全策略条件的数据流时才会触发 IPSec SA 协商。

【使用指导】

- 此功能只适用于 IKE 协商方式的 IPsec 安全策略。
- 自动触发模式下，无论是否有流量需要保护，都会在配置条件满足的情况下触发建立 IPsec SA，这在一定程度上占用了系统资源；而流量触发模式只在有流量需要保护时才会触发建立 IPsec SA，相对于自动模式，系统资源占用率较低，但 IPsec SA 成功建立之前的流量不会受到保护。
- 如果 IPsec 安全策略下引用了智能选路策略，将自动触发建立 IPsec SA，则此配置不会生效。
- IPsec 隧道两端的设备上并不要求配置一致的触发建立 IPsec SA 的模式。
- 修改模式，对当前已经存在的 IPsec SA 无影响。如果已经配置了 **auto** 模式，IPsec SA 建立完成后，建议修改为 **traffic-based** 模式。

【举例】

配置序号为 10 的 IPsec 安全策略 policy1 触发建立 IPsec SA 的模式为自动触发。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] sa trigger-mode auto
```

1.1.52 security acl

security acl 命令用来指定 IPsec 安全策略/IPsec 安全策略模板引用的 ACL。

undo security acl 命令用来恢复缺省情况。

【命令】

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

undo security acl

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板未引用 ACL。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 IPv6 ACL。

acl-number：ACL 编号，取值范围为 3000～3999。

name *acl-name*：ACL 名称，为 1～63 个字符的字符串，不区分大小写。

aggregation：指定 IPsec 安全策略的数据流保护方式为聚合方式。不支持对 IPv6 数据流采用该保护方式。

per-host：指定 IPsec 安全策略的数据流保护方式为主机方式。

【使用指导】

对于 IKE 协商方式的 IPsec 安全策略，数据流的保护方式包括以下几种：

- 标准方式：一条隧道保护一条数据流。ACL 中的每一个规则对应的数据流都会由一条单独创建的隧道来保护。不指定 **aggregation** 和 **per-host** 参数的情况下，缺省采用此方式。
- 聚合方式：一条隧道保护 ACL 中定义的所有数据流。ACL 中的所有规则对应的数据流只会由一条创建的隧道来保护。对于聚合方式和标准方式都支持的设备，聚合方式仅用于和老版本的设备互通。
- 主机方式：一条隧道保护一条主机到主机的数据流。ACL 中的每一个规则对应的不同主机之间的数据流，都会由一条单独创建的隧道来保护。这种方式下，受保护的网段之间存在多条数据流的情况下，将会消耗更多的系统资源。

手工方式的 IPsec 安全策略缺省使用聚合方式，且仅支持聚合方式；IKE 协商方式的 IPsec 安全策略中可以通过配置来选择不同的保护方式。

【举例】

配置 IPsec 安全策略引用 IPv4 高级 ACL 3001。

```
<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
```

配置 IPsec 安全策略引用 IPv4 高级 ACL 3002，并设置数据流保护方式为聚合方式。

```
<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-acl-ipv4-adv-3002] quit
[Sysname] ipsec policy policy2 1 isakmp
[Sysname-ipsec-policy-isakmp-policy2-1] security acl 3002 aggregation
```

【相关命令】

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

1.1.53 snmp-agent trap enable ipsec

snmp-agent trap enable ipsec 命令用来开启 IPsec 告警功能。

undo snmp-agent trap enable ipsec 命令用来关闭指定的 IPsec 告警功能。

【命令】

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

【缺省情况】

IPsec 的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

auth-failure：表示认证失败时的告警功能。

connection-start：表示相同 description 的安全策略表项下创建第一个 IPsec 隧道时的告警功能。

connection-stop：表示相同 description 的安全策略表项下删除最后一个 IPsec 隧道时的告警功能。

decrypt-failure：表示解密失败时的告警功能。

encrypt-failure：表示加密失败时的告警功能。

global：表示全局告警功能。

invalid-sa-failure：表示无效 SA 的告警功能。

no-sa-failure：表示无法查找到 SA 时的告警功能。

policy-add：表示添加 IPsec 安全策略时的告警功能。

policy-attach：表示将 IPsec 安全策略应用到接口时的告警功能。

policy-delete：表示删除 IPsec 安全策略时的告警功能。

policy-detach：表示将 IPsec 安全策略从接口下删除时的告警功能。

tunnel-start：表示创建 IPsec 隧道时的告警功能。

tunnel-stop：表示删除 IPsec 隧道时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的 IPsec 告警功能。

如果希望生成并输出某种类型的 IPsec 告警信息，则需要保证 IPsec 的全局告警功能以及相应类型的告警功能均处于开启状态。

【举例】

开启全局 IPsec Trap 告警。

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

开启创建 IPsec 隧道时的告警功能。

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

1.1.54 tfc enable

tfc enable 命令用来开启 TFC（Traffic Flow Confidentiality）填充功能。

undo tfc enable 命令用来关闭 TFC 填充功能。

【命令】

tfc enable

undo tfc enable

【缺省情况】

TFC 填充功能处于关闭状态。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【使用指导】

TFC 填充功能可隐藏原始报文的长度，但可能对报文的加封装及解封装处理性能稍有影响，且仅对于使用 ESP 协议以传输模式封装的 UDP 报文以及使用 ESP 协议以隧道模式封装的原始 IP 报文生效。

【举例】

指定 IPsec 安全策略 policy1 中开启 TFC 填充功能。

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

【相关命令】

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

1.1.55 transform-set

transform-set 命令用来指定 IPsec 安全策略/IPsec 安全策略模板所引用的 IPsec 安全提议。

undo transform-set 命令用来取消 IPsec 安全策略/IPsec 安全策略模板引用的 IPsec 安全提议。

【命令】

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

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

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板未引用 IPsec 安全提议。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

transform-set-name&<1-6>：IPsec 安全提议的名称，为 1～63 个字符的字符串，不区分大小写。&<1-6>表示前面的参数最多可以输入 6 次。需要注意的是，同时指定的多个安全提议名称不可重复，否则提示参数出错。

【使用指导】

对于手工方式的 IPsec 安全策略，只能引用一个 IPsec 安全提议。多次执行本命令，最后一次执行的命令生效。

对于 IKE 协商方式的 IPsec 安全策略，一条 IPsec 安全策略最多可以引用六个 IPsec 安全提议。IKE 协商过程中，IKE 将会在隧道两端配置的 IPsec 安全策略中查找能够完全匹配的 IPsec 安全提议。如果 IKE 在两端找不到完全匹配的 IPsec 安全提议，则 SA 不能协商成功，需要被保护的报文将被丢弃。

若不指定任何参数，则 **undo transform-set** 命令表示删除所有引用的 IPsec 安全提议。

【举例】

配置 IPsec 安全策略引用名称为 prop1 的 IPsec 安全提议。

```
<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
```

【相关命令】

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

1.1.56 tunnel protection ipsec

tunnel protection ipsec 命令用来在隧道接口上应用 IPsec 安全框架。

undo tunnel protection ipsec 命令用来恢复缺省情况。

【命令】

tunnel protection ipsec profile *profile-name*

undo tunnel protection ipsec profile

【缺省情况】

Tunnel 接口下未引用 IPsec 安全框架。

【视图】

Tunnel 接口视图

【缺省用户角色】

network-admin

【参数】

profile *profile-name*：指定使用的 IPsec 安全框架，且必须为 IKE 协商方式的 IPsec 安全框架。其中，*profile-name* 为 IPsec 安全框架的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

在隧道接口上应用 IPsec 安全框架后，隧道两端会通过 IKE 协商建立 IPsec 隧道对隧道接口上传输的数据流进行 IPsec 保护。

【举例】

配置使用 IPsec 安全框架 prf1 来保护接口 Tunnel1 的报文。

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn gre
```

```
[Sysname-Tunnel1] tunnel protection ipsec profile prf1
```

【相关命令】

- **ipsec profile**

2 IKE

2.1 IKE配置命令

2.1.1 aaa authorization

aaa authorization 命令用来开启 IKE 的 AAA 授权功能。

undo aaa authorization 命令用来关闭 IKE 的 AAA 授权功能。

【命令】

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

undo aaa authorization

【缺省情况】

IKE 的 AAA 授权功能处于关闭状态。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*：申请授权属性时使用的 ISP 域名，为 1～255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“””、“:”、“*”、“?”、“<”、“>”以及“@”字符，且不能为字符串“d”、“de”、“def”、“defa”、“defau”、“defaul”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow”和“if-unknown”。

username *user-name*：申请授权属性时使用的用户名，为 1～55 个字符的字符串，区分大小写。用户名不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。

【使用指导】

开启 AAA 授权功能后，IKE 可以向 AAA 模块申请授权属性，例如 IKE 本地地址池属性。IKE 模块使用指定的ISP域名和用户名向AAA模块发起授权请求，AAA模块采用域中的授权配置向远程AAA服务器或者本地用户数据库请求该用户的授权信息。用户名验证成功之后，IKE 本端将会得到相应的授权属性。该功能适合于由 AAA 模块集中管理和部署相关授权属性的组网环境。

【举例】

创建 IKE profile，名称为 profile1。

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

在 IKE profile prof1 中开启 AAA 授权功能，指定 ISP 域为 abc，用户名为 test。

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

2.1.2 authentication-algorithm

authentication-algorithm 命令用来指定 IKE 提议使用的认证算法。

undo authentication-algorithm 命令用来恢复缺省情况。

【命令】

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

undo authentication-algorithm

【缺省情况】

IKE 提议使用的认证算法为 HMAC-SHA1

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

md5：指定认证算法为 HMAC-MD5。

sha：指定认证算法为 HMAC-SHA1。

sha256：指定认证算法为 HMAC-SHA256。

sha384：指定认证算法为 HMAC-SHA384。

sha512：指定认证算法为 HMAC-SHA512。

【举例】

指定 IKE 提议 1 的认证算法为 HMAC-SHA1。

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

【相关命令】

- **display ike proposal**

2.1.3 authentication-method

authentication-method 命令用来指定 IKE 提议使用的认证方法。

undo authentication-method 命令用来恢复缺省情况。

【命令】

authentication-method { **dsa-signature** | **pre-share** | **rsa-de** | **rsa-signature** | **sm2-de** }

undo authentication-method

【缺省情况】

IKE 提议使用预共享密钥的认证方法。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

dsa-signature：指定认证方法为 DSA 数字签名方法。

pre-share：指定认证方法为预共享密钥方法。

rsa-de：指定认证方法为 RSA 数字信封方法。

rsa-signature：指定认证方法为 RSA 数字签名方法。

sm2-de：指定认证方法为 SM2 数字信封方法。

【使用指导】

认证方法分为预共享密钥认证、数字签名认证（包括 RSA 数字签名认证和 DSA 数字签名认证）和数字信封认证（包括 RSA 数字信封认证和 SM2 数字信封认证）。

- 预共享密钥认证机制简单、不需要证书，常在小型组网环境中使用；
- 数字签名认证安全性更高，常在“中心—分支”模式的组网环境中使用。例如，在“中心—分支”组网中使用预共享密钥认证进行 IKE 协商时，中心侧可能需要为每个分支配置一个预共享密钥，当分支很多时，配置会很复杂，而使用数字签名认证时中心只需配置一个 PKI 域；
- 数字信封认证用于设备需要符合国家密码管理局要求时使用，此认证方法只能在 IKEv1 的协商过程中支持。

协商双方必须有匹配的认证方法。

如果指定认证方法为 RSA 数字签名方法或者 DSA 数字签名方法，则还必须保证对端从 CA（证书认证机构）获得数字证书。

如果指定认证方法为预共享密钥方法，必须使用 **pre-shared-key** 命令在两端配置相同的预共享密钥。

【举例】

指定 IKE 提议 1 的认证方法为预共享密钥。

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

【相关命令】

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

2.1.4 certificate domain

certificate domain 命令用来指定 IKE 协商采用数字签名认证时使用的 PKI 域。

undo certificate domain 命令用来取消指定 IKE 协商时使用的 PKI 域。

【命令】

certificate domain *domain-name*

undo certificate domain *domain-name*

【缺省情况】

未指定用于 IKE 协商的 PKI 域。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

domain-name：PKI 域的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

可通过多次执行本命令指定多个 PKI 域，一个 IKE profile 中最多可以引用六个 PKI 域。如果在 IKE profile 中指定了 PKI 域，则使用指定的 PKI 域发送本端证书请求、验证对端证书请求、发送本端证书、验证对端证书、进行数字签名。如果 IKE profile 中没有指定 PKI 域，则使用设备上配置的 PKI 域进行以上证书相关的操作。

IKE 可以通过 PKI 自动获取 CA 证书、自动申请证书，对这种情况，有几点需要说明：

- 对于发起方：若在 IKE profile 中指定了 PKI 域，且 PKI 域中的证书申请为自动申请方式，则发起方会自动获取 CA 证书；若在 IKE profile 中没有指定 PKI 域，则发起方不会自动获取 CA 证书，需要手动获取 CA 证书。
- 对于响应方：第一阶段采用主模式的 IKE 协商时，响应方不会自动获取 CA 证书，需要手动获取 CA 证书；第一阶段采用野蛮模式的 IKE 协商时，若响应方找到了匹配的 IKE profile 并且 IKE profile 下指定了 PKI 域，且 PKI 域中的证书申请为自动申请方式，则会自动获取 CA 证书；否则，响应方不会自动获取 CA 证书，需要手动获取 CA 证书。
- 在 IKE 协商过程中先自动获取 CA 证书，再自动申请证书。若 CA 证书存在，则不获取 CA 证书，直接自动申请证书。

【举例】

在 IKE profile 1 中指定 IKE 协商时使用的 PKI 域。

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

【相关命令】

- **authentication-method**
- **pki domain**（安全命令参考/PKI）

2.1.5 client-authentication

client-authentication 命令用来开启对客户端的认证。

undo client-authentication 命令用来关闭对客户端的认证。

【命令】

client-authentication xauth

undo client-authentication

【缺省情况】

对客户端的认证处于关闭状态。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

xauth：表示采用 XAUTH （Extended Authentication within ISAKMP/Oakley）方式认证。

【使用指导】

在部署多分支远程访问企业中心的 IPsec VPN 应用时，为区别不同的客户端，通常需要中心侧的网管人员为每一个远程客户端设置不同 IPsec 安全策略和认证密码，此工作量巨大，也不方便管理。在中心侧开启了对客户端认证之后，远程客户端与中心侧设备进行 IKE 协商的过程中，中心侧设备可以利用 RADIUS 服务器来对客户端进行用户名和密码的验证，要求每个远程客户端在接入时，都需要提供不同的用户名和密码，这样可以简化中心侧的配置负担，保证了远程接入客户端的安全性。

【举例】

开启基于 XAUTH 方式的认证。

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

【相关命令】

- **local-user**

2.1.6 description

description 命令用来配置 IKE 提议的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

不存在 IKE 提议的描述信息。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

text：IKE 提议的描述信息，为 1～80 个字符的字符串，区分大小写。

【使用指导】

当系统中存在多个 IKE 提议时，可通过配置相应的描述信息来有效区分不同的 IKE 提议。

【举例】

配置序号为 1 的 IKE 提议的描述信息为 test。

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

2.1.7 dh

dh 命令用来配置 IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数。

undo dh 命令用来恢复缺省情况。

【命令】

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

undo dh

【缺省情况】

IKE 提议使用的 DH 密钥交换参数为 **group1**，即 768-bit 的 Diffie-Hellman group。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

group1：指定阶段 1 密钥协商时采用 768-bit 的 Diffie-Hellman group。

group14：指定阶段 1 密钥协商时采用 2048-bit 的 Diffie-Hellman group。

group2：指定阶段 1 密钥协商时采用 1024-bit 的 Diffie-Hellman group。

group24：指定阶段 1 密钥协商时采用含 256-bit 的 sub-group 的 2048-bit Diffie-Hellman group。

group5：指定阶段 1 密钥协商时采用 1536-bit 的 Diffie-Hellman group。

【使用指导】

group1 提供了最低的安全性，但是处理速度最快。**group24** 提供了最高的安全性，但是处理速度最慢。其它的 Diffie-Hellman group 随着其位数的增加提供更高的安全性，但是处理速度会相应减慢。请根据实际组网环境中对安全性和性能的要求选择合适的 Diffie-Hellman group。

【举例】

指定 IKE 提议 1 使用 2048-bit 的 Diffie-Hellman group。

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

【相关命令】

- **display ike proposal**

2.1.8 display ike proposal

display ike proposal 命令用来显示所有 IKE 提议的配置信息。

【命令】

display ike proposal

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

IKE 提议按照优先级的先后顺序显示。如果没有配置任何 IKE 提议，则只显示缺省的 IKE 提议。

【举例】

显示 IKE 提议的配置信息。

```
<Sysname> display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
------------------------------------------------------------------------------
 1        RSA-SIG            MD5        DES-CBC     Group 1        5000
 11       PRE-SHARED-KEY     MD5        DES-CBC     Group 1        50000
 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```

表2-1 display ike proposal 命令显示信息描述表

字段	描述
Priority	IKE提议的优先级
Authentication method	IKE提议使用的认证方法，包括： • DSA-SIG：DSA 签名 • PRE-SHARED-KEY：预共享密钥 • RSA-DE：RSA 数字信封 • RSA-SIG：RSA 签名 • SM2-DE：SM2 数字信封
Authentication algorithm	IKE提议使用的认证算法，包括： • MD5：HMAC-MD5 算法 • SHA1：HMAC-SHA1 算法 • SHA256：HMAC-SHA256 算法 • SHA384：HMAC-SHA384 算法 • SHA512：HMAC-SHA512 算法

字段	描述
Encryption algorithm	IKE提议使用的加密算法，包括： • 3DES-CBC：168 位 CBC 模式的 3DES 算法 • AES-CBC-128：128 位 CBC 模式的 AES 算法 • AES-CBC-192：192 位 CBC 模式的 AES 算法 • AES-CBC-256：256 位 CBC 模式的 AES 算法 • DES-CBC：56 位 CBC 模式的 DES 算法
Diffie-Hellman group	IKE阶段1密钥协商时所使用的DH密钥交换参数，包括： • Group 1：DH group1 • Group 2：DH group2 • Group 5：DH group5 • Group 14：DH group14 • Group 24：DH group24
Duration (seconds)	IKE提议中指定的IKE SA存活时间，单位为秒

【相关命令】

- **ike proposal**

2.1.9 display ike sa

display ike sa 命令用来显示当前 IKE SA 的信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

verbose：显示当前 IKE SA 的详细信息。

connection-id *connection-id*：按照连接标识符显示 IKE SA 的详细信息，取值范围为 1～2000000000。

remote-address：显示指定对端 IP 地址的 IKE SA 的详细信息。

ipv6：指定 IPv6 地址。

remote-address：对端的 IP 地址。

【使用指导】

若不指定任何参数，则显示当前所有 IKE SA 的摘要信息。

【举例】

显示当前所有 IKE SA 的摘要信息。

```
<Sysname> display ike sa
    Connection-ID  Remote          Flag        DOI
  -----------------------------------------------------------
      1            202.38.0.2      RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

表2-2 display ike sa 命令显示信息描述表

字段	描述
Connection-ID	IKE SA的标识符
Remote	此IKE SA的对端的IP地址
Flags	IKE SA的状态，包括： • RD--READY：表示此 IKE SA 已建立成功 • RL--REPLACED：表示此 IKE SA 已经被新的 IKE SA 代替，一段时间后将被删除 • FD-FADING：表示此 IKE SA 正在接近超时时间，目前还在使用，但即将被删除 • RK-REKEY：表示此 IKE SA 是 Rekey SA • Unknown：表示 IKE 协商的状态未知
DOI	IKE SA所属解释域，包括： • IPsec：表示此 IKE SA 使用的 DOI 为 IPsec DOI • Group 表示此 IKE SA 使用的 DOI 为 GDOI（暂不支持）

显示当前 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose
    -----------------------------------------------
    Connection ID: 2
    Outside VPN: 1
    Inside VPN: 1
    Profile: prof1
    Transmitting entity: Initiator
    Initiator cookie: 1bcf453f0a217259
    Responder cookie: 5e32a74dfa66a0a4
    -----------------------------------------------
    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
    Vendor ID index: 0xa1d
    Vendor ID sequence number: 0x0
```

显示目的地址为 4.4.4.5 的 IKE SA 的详细信息。

```
<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
    Initiator cookie: 1bcf453f0a217259
    Responder cookie: 5e32a74dfa66a0a4
    -----------------------------------------------
    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
    Vendor ID index: 0xa1d
    Vendor ID sequence number: 0x0
```

表2-3 display ike sa verbose 命令显示信息描述表

字段	描述
Connection ID	IKE SA的标识符
Outside VPN	（暂不支持）接收报文的接口所属的MPLS L3VPN的VPN实例名称
Inside VPN	（暂不支持）被保护数据所属的MPLS L3VPN的VPN实例名称
Profile	IKE SA协商过程中匹配到的IKE profile的名称，如果协商过程中没有匹配到任何profile，则该字段不会显示任何KE profile名称
Transmitting entity	IKE协商中的实体角色，包括： • Initiator：发起方 • Responder：响应方
Initiator cookie	IKE SA发起者Cookie
Responder cookie	IKE SA响应者Cookie
Local IP	本端安全网关的IP地址
Local ID type	本端安全网关的身份信息类型
Local ID	本端安全网关的身份信息
Remote IP	对端安全网关的IP地址
Remote ID type	对端安全网关的身份信息类型
Remote ID	对端安全网关的身份信息
Authentication-method	IKE提议使用的认证方法，包括： • DSA-SIG：DSA 签名 • PRE-SHARED-KEY：预共享密钥 • RSA-DE：RSA 数字信封 • RSA-SIG：RSA 签名
Authentication-algorithm	IKE提议使用的认证算法，包括： • MD5：HMAC-MD5 算法 • SHA1：HMAC-SHA1 算法 • SHA256：HMAC-SHA256 算法 • SHA384：HMAC-SHA384 算法 • SHA512：HMAC-SHA512 算法
Encryption-algorithm	IKE提议使用的加密算法，包括： • 3DES-CBC：168 位 CBC 模式的 3DES 算法 • AES-CBC-128：128 位 CBC 模式的 AES 算法 • AES-CBC-192：192 位 CBC 模式的 AES 算法 • AES-CBC-256：256 位 CBC 模式的 AES 算法 • DES-CBC：56 位 CBC 模式的 DES 算法 •
Life duration(sec)	IKE SA的存活时间，单位为秒

字段	描述
Remaining key duration(sec)	IKE SA的剩余存活时间，单位为秒
Exchange-mode	IKE第一阶段的协商模式，包括： • Aggressive：野蛮模式 • Main：主模式
Diffie-Hellman group	IKE第一阶段密钥协商时所使用的DH密钥交换参数，包括： • Group 1：DH group1 • Group 2：DH group2 • Group 5：DH group5 • Group 14：DH group14 • Group 24：DH group24
NAT traversal	是否检测到协商双方之间存在NAT网关设备
Extend authentication	是否开启扩展认证： • Enabled：开启 • Disabled：关闭
Assigned IP address	本端分配给对端的IP地址，如果没有分配则不显示
Vendor ID index	触发IKE协商时，使用的厂商自定义常量索引
Vendor ID sequence number	触发IKE协商时，使用的厂商自定义常量序列号

2.1.10 display ike statistics

display ike statistics 命令用来显示 IKE 的统计信息。

【命令】

display ike statistics

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示 IKE 的统计信息。

```
<Sysname> display ike statistics
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 exchange type: 0
  No available SA: 1
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
  Failures to send R_U_THERE DPD packets: 0
  Failures to receive R_U_THERE DPD packets: 0
  Failures to send ACK DPD packets: 0
  Failures to receive ACK DPD packets: 0
  Sent P1 SA lifetime change packets: 0
  Received P1 SA lifetime change packets: total=0, process failures=0 (no SA=0, failures to
reset SA soft lifetime=0, failures to reset SA hard lifetime=0)
  Sent P2 SA lifetime change packets: 0
  Received P2 SA lifetime change packets: total=0, process failures=0
```

表2-4 display ike statistics 命令显示信息描述表

字段	描述
No matching proposal	提议不匹配
Invalid ID information	无效的ID信息
Unavailable certificate	本地未发现此证书
Unsupported DOI	不支持的DOI
Unsupported situation	不支持的形式
Invalid proposal syntax	无效的提议语法
Invalid SPI	无效的SPI
Invalid protocol ID	无效的协议ID
Invalid certificate	无效的证书
Authentication failure	认证失败
Invalid flags	无效的标记

字段	描述
Invalid message id	无效的消息ID
Invalid cookie	无效的cookie
Invalid transform ID	无效的transform ID
Malformed payload	畸形载荷
Invalid key information	无效的密钥信息
Invalid hash information	无效的hash信息
Unsupported attribute	不支持的属性
Unsupported certificate type	不支持的证书类型
Invalid certificate authority	无效的证书授权
Invalid signature	无效的签名
Unsupported exchange type	不支持的交换类型
No available SA	没有可用的SA
Retransmit timeout	重传超时
Not enough memory	内存不足
Enqueue fails	入队列失败
Failures to send R_U_THERE DPD packets	发送R_U_THERE类型DPD报文失败的次数
Failures to receive R_U_THERE DPD packets	接收R_U_THERE类型DPD报文失败的次数
Failures to send ACK DPD packets	发送DPD ACK报文失败的次数
Failures to receive ACK DPD packets	接收DPD ACK报文失败的次数
Sent P1 SA lifetime change packets	发送P1阶段改变生存周期的info类型报文的个数

Received P1 SA lifetime change packets: total=*N*， process failures=*N* (no SA=*N*, failures to reset SA soft lifetime=*N*, failures to reset SA hard lifetime=*N*)	接收P1阶段改变生存周期的info类型报文的个数
	• 总个数
	• 处理失败的个数
	  ○ 因为没有 sa 记录的个数
	  ○ 软超时定时器流程处理失败的个数
	生存时间定时器流程处理失败的个数

Sent P2 SA lifetime change packets	发送P2阶段改变生存周期的info类型报文的个数
Received P2 SA lifetime change packets: total=*N*， process failures=*N*	接收P2阶段改变生存周期的info类型报文的个数 • 总个数 • 处理失败的个数

【相关命令】

- **reset ike statistics**

2.1.11 dpd

dpd 命令用来配置 IKE DPD 功能。

undo dpd 命令用来关闭 IKE DPD 功能。

【命令】

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

undo dpd interval

【缺省情况】

IKE DPD 功能处于关闭状态。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

interval *interval*：指定触发 IKE DPD 探测的时间间隔，取值范围为 1～300，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry *seconds*：指定 DPD 报文的重传时间间隔，取值范围为 1～60，单位为秒。缺省情况下，DPD 报文的重传时间间隔为 5 秒。

on-demand：指定按需探测模式，根据流量来探测对端是否存活，在本端发送用户报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKE DPD 探测的时间间隔，则触发 DPD 探测。

periodic：指定定时探测模式，按照触发 IKE DPD 探测的时间间隔定时探测对端是否存活。

【使用指导】

IKE DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。

如果 IKE profile 视图下和系统视图下都配置了 IKE DPD 功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 IKE DPD 功能，则采用系统视图下的 DPD 配置。

建议配置的 **interval** 时间大于 **retry** 时间，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，在重传 DPD 报文过程中不会触发新的 DPD 探测。

【举例】

为 IKE profile 1 配置 IKE DPD 功能，指定若 10 秒内没有从对端收到 IPsec 报文，则触发 IKE DPD 探测，DPD 请求报文的重传时间间隔为 5 秒，探测模式为按需探测。

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

【相关命令】

- **ike dpd**

2.1.12 encryption-algorithm

encryption-algorithm 命令用来指定 IKE 提议使用的加密算法。

undo encryption-algorithm 命令用来恢复缺省情况。

【命令】

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

undo encryption-algorithm

【缺省情况】

IKE 提议使用的加密算法为 **des-cbc**，即 CBC 模式的 56-bit DES 加密算法。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 3DES 算法，3DES 算法采用 168 比特的密钥进行加密。

aes-cbc-128：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

aes-cbc-192：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 192 比特的密钥进行加密。

aes-cbc-256：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 256 比特的密钥进行加密。

des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

【举例】

指定 IKE 提议 1 的加密算法为 128 比特的 CBC 模式的 AES。

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

【相关命令】

- **display ike proposal**

2.1.13 exchange-mode

exchange-mode 命令用来选择 IKE 第一阶段的协商模式。

undo exchange-mode 命令用来恢复缺省情况。

【命令】

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

undo exchange-mode

【缺省情况】

IKE 第一阶段的协商模式为主模式。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

aggressive：野蛮模式。

main：主模式。

【使用指导】

当本端的 IP 地址为自动获取（如本端用户为拨号方式，IP 地址为动态分配），且采用预共享密钥认证方式时，建议将本端的协商模式配置为野蛮模式。

当本端使用 RSA-DE 或者 SM2-DE 数字信封方式认证时，必须将本端的协商模式配置为国密主模式。

【举例】

配置 IKE 第一阶段协商使用主模式。

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] exchange-mode main
```

【相关命令】

- **display ike proposal**

2.1.14 ike address-group

ike address-group 命令用来配置为对端分配 IPv4 地址的 IKE 本地地址池。

undo ike address-group 命令用来删除指定的 IKE 本地地址池。

【命令】

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

undo ike address-group *group-name*

【缺省情况】

未配置 IKE 本地 IPv4 地址池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name：IPv4 地址池名称，为 1～63 个字符的字符串，不区分大小写。

start-ipv4-address end-ipv4-address：IPv4 地址池的地址范围。其中，*start-ipv4-address* 为 IPv4 地址池的起始地址，*end-ipv4-address* 为 IPv4 地址池的结束地址。

mask：IPv4 地址掩码。

mask-length：IPv4 地址掩码长度。

【使用指导】

每个地址池中包括的 IPv4 地址的最大数目为 8192。

如果修改或者删除地址池，则需要删除所有的 IKE SA 和 IPsec SA，否则，可能会导致已经分配的地址无法回收。

【举例】

配置 IKE 本地 IPv4 地址池，名称为 ipv4group，地址池范围为 1.1.1.1～1.1.1.2，掩码为 255.255.255.0。

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

配置 IKE 本地 IPv4 地址池，名称为 ipv4group，地址池范围为 1.1.1.1～1.1.1.2，掩码长度为 32。

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

【相关命令】

- **aaa authorization**

2.1.15 ike dpd

ike dpd 命令用来配置全局 IKE DPD 功能。

undo ike dpd 命令用来关闭全局 IKE DPD 功能。

【命令】

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

undo ike dpd interval

【缺省情况】

全局 IKE DPD 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval *interval*：指定触发 IKE DPD 探测的时间间隔，取值范围为 1～300，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry *seconds*：指定 DPD 报文的重传时间间隔，取值范围为 1～60，单位为秒，缺省值为 5 秒。

on-demand：指定按需探测模式，根据流量来探测对端是否存活，在本端发送 IPsec 报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKE DPD 探测的时间间隔（即通过 *interval* 指定的时间），则触发 DPD 探测。

periodic：指定定时探测模式，按照触发 IKE DPD 探测的时间间隔（即通过 *interval* 指定的时间）定时探测对端是否存活。

【使用指导】

IKE DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。

如果 IKE profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。

建议配置的 **interval** 大于 **retry**，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

配置流量触发 IKE DPD 探测间隔时间为 10 秒，重传时间间隔为 5 秒，探测模式为按需探测。

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

【相关命令】

- **dpd**

2.1.16 ike identity

ike identity 命令用来配置本端身份信息，用于在 IKE 认证协商阶段向对端标识自己的身份。

undo ike identity 命令用来恢复缺省情况。

【命令】

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

undo ike identity

【缺省情况】

使用 IP 地址标识本端的身份，该 IP 地址为 IPsec 安全策略应用的接口 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从数字证书中获得的 DN 名作为本端身份。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称，*fqdn-name* 表示 FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 www.test.com。不指定 *fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 FQDN 类型的身份。

user-fqdn *user-fqdn-name*：指定标识本端身份的 User FQDN 名称，*user-fqdn-name* 表示 User FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 adc@test.com。不指定 *user-fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 user FQDN 类型的身份。

【使用指导】

本命令用于全局配置 IKE 对等体的本端身份，适用于所有 IKE SA 的协商，而 IKE profile 下的 **local-identity** 为局部配置身份，仅适用于使用本 IKE profile 的 IKE SA 的协商。

如果本端的认证方式为数字签名方式，则本端可以配置任何类型的身份信息；如果本端的认证方式为预共享密钥方式，则只能配置除 DN 之外的其它类型的身份信息。

如果希望在采用数字签名认证时，总是从证书中的主题字段取得本端身份，则可以通过 **ike signature-identity from-certificate** 命令实现。如果没有配置 **ike signature-identity from-certificate**，并且 IPsec 安全策略或 IPsec 安全策略模板下指定的 IKE profile 中配置了本端身份（由 **local-identity** 命令指定），则使用 IKE profile 中配置的本端身份；若 IPsec 安全策略或 IPsec 安全策略模板下未指定 IKE profile 或 IKE profile 下没有配置本端身份，则使用全局配置的本端身份（由 **ike identity** 命令指定）。

【举例】

指定使用 IP 地址 2.2.2.2 标识本端身份。

```
<sysname> system-view
[sysname] ike identity address 2.2.2.2
```

【相关命令】

- **local-identity**
- **ike signature-identity from-certificate**

2.1.17 ike invalid-spi-recovery enable

ike invalid-spi-recovery enable 命令用来开启针对无效 IPsec SPI 的 IKE SA 恢复功能。

undo ike invalid-spi-recovery enable 命令用来关闭针对无效 IPsec SPI 的 IKE SA 恢复功能。

【命令】

ike invalid-spi-recovery enable

undo ike invalid-spi-recovery enable

【缺省情况】

针对无效 IPsec SPI 的 IKE SA 恢复功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当 IPsec 隧道一端的安全网关出现问题（例如安全网关重启）导致本端 IPsec SA 丢失时，会造成 IPsec 流量黑洞现象：一端（接收端）的 IPsec SA 已经完全丢失，而另一端（发送端）还持有对应的 IPsec SA 且不断地向对端发送报文，当接收端收到发送端使用此 IPsec SA 封装的 IPsec 报文时，就会因为找不到对应的 SA 而持续丢弃报文，形成流量黑洞。该现象造成 IPsec 通信链路长时间得不到恢复（只有等到发送端旧的 IPsec SA 生存时间超时，并重建 IPsec SA 后，两端的 IPsec 流量才能得以恢复），因此需要采取有效的 IPsec SA 恢复手段来快速恢复中断的 IPsec 通信链路。

SA 由 SPI 唯一标识，接收方根据 IPsec 报文中的 SPI 在 SA 数据库中查找对应的 IPsec SA，若接收方找不到处理该报文的 IPsec SA，则认为此报文的 SPI 无效。如果接收端当前存在 IKE SA，则会向对端发送删除对应 IPsec SA 的通知消息，发送端 IKE 接收到此通知消息后，就会立即删除此无效 SPI 对应的 IPsec SA。之后，当发送端需要继续向接收端发送报文时，就会触发两端重建 IPsec SA，使得中断的 IPsec 通信链路得以恢复；如果接收端当前不存在 IKE SA，就不会触发本端向对端发送删除 IPsec SA 的通知消息，接收端将默认丢弃无效 SPI 的 IPsec 报文，使得链路无法恢复。后一种情况下，如果开启了 IPsec 无效 SPI 恢复 IKE SA 功能，就会触发本端与对端协商新的 IKE SA 并发送删除消息给对端，从而使链路恢复正常。

由于开启此功能后，若攻击者伪造大量源 IP 地址不同但目的 IP 地址相同的无效 SPI 报文发给设备，会导致设备因忙于与无效对端协商建立 IKE SA 而面临受到 DoS（Denial of Sevice）攻击的风险，通常情况下，建议关闭针对无效 IPsec SPI 的 IKE SA 恢复功能。

【举例】

开启 IPsec 无效 SPI 恢复 IKE SA 功能。

```
<Sysname> system-view
[Sysname] ike invalid-spi-recovery enable
```

2.1.18 ike keepalive interval

ike keepalive interval 命令用来配置通过 IKE SA 向对端发送 IKE Keepalive 报文的时间间隔。

undo ike keepalive interval 命令用来恢复缺省情况。

【命令】

ike keepalive interval *interval*

undo ike keepalive interval

【缺省情况】

不向对端发送 IKE Keepalive 报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：指定向对端发送 IKE SA 的 Keepalive 报文的时间间隔，取值范围为 20～28800，单位为秒。

【使用指导】

当有检测对方 IKE SA 和 IPsec SA 是否存活的需求时，通常建议配置 IKE DPD，不建议配置 IKE Keepalive 功能。仅当对方不支持 IKE DPD 特性，但支持 IKE Keepalive 功能时，才考虑配置 IKE Keepalive 功能。

本端配置的 IKE Keepalive 报文的等待超时时间要大于对端发送的时间间隔。由于网络中一般不会出现超过三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

【举例】

配置本端向对端发送 Keepalive 报文的时间间隔为 200 秒。

```
<Sysname> system-view
[Sysname] ike keepalive interval 200
```

【相关命令】

- **ike keepalive timeout**

2.1.19 ike keepalive timeout

ike keepalive timeout 命令用来配置本端等待对端发送 IKE Keepalive 报文的超时时间。

undo ike keepalive timeout 命令用来恢复缺省情况。

【命令】

ike keepalive timeout *seconds*

undo ike keepalive timeout

【缺省情况】

未配置本端等待对端发送 IKE Keepalive 报文的超时时间。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds：指定本端等待对端发送 IKE Keepalive 报文的超时时间，取值范围为 20～28800，单位为秒。

【使用指导】

当本端 IKE SA 在配置的超时时间内未收到 IKE Keepalive 报文时，则删除该 IKE SA 以及由其协商的 IPsec SA。

本端配置的等待对端发送 IKE Keepalive 报文的超时时间要大于对端发送 IKE Keepalive 报文的时间间隔。由于网络中一般不会出现超过三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

【举例】

配置本端等待对端发送 IKE Keepalive 报文的超时时间为 20 秒。

```
<Sysname> system-view
[Sysname] ike keepalive timeout 20
```

【相关命令】

- **ike keepalive interval**

2.1.20 ike keychain

ike keychain 命令用来创建 IKE keychain，并进入 IKE keychain 视图。如果指定的 IKE keychain 已经存在，则直接进入 IKE keychain 视图。

undo ike keychain 命令用来删除指定的 IKE keychain。

【命令】

ike keychain *keychain-name*

undo ike keychain *keychain-name*

【缺省情况】

不存在 IKE keychain。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keychain-name：IKE keychain 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

在 IKE 需要通过预共享密钥方式进行认证时，需要创建并指定 IKE keychain。

【举例】

创建 IKE keychain key1 并进入 IKE keychain 视图。

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1]
```

【相关命令】

- **authentication-method**

- **pre-shared-key**

2.1.21 ike limit

ike limit 命令用来配置对本端 IKE SA 数目的限制。

undo ike limit 命令用来恢复缺省情况。

【命令】

ike limit { **max-negotiating-sa** *negotiation-limit* | **max-sa** *sa-limit* }

undo ike limit { **max-negotiating-sa** | **max-sa** }

【缺省情况】

不限制 IKE SA 数目。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-negotiating-sa *negotiation-limit*：指定允许同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数，取值范围为 1~99999。

max-sa *sa-limit*：指定允许建立的 IKE SA 的最大数，取值范围为 1~99999。

【使用指导】

可以通过 **max-negotiating-sa** 参数设置允许同时协商更多的 IKE SA，以充分利用设备处理能力，以便在设备有较强处理能力的情况下得到更高的新建性能；可以通过该参数设置允许同时协商更少的 IKE SA，以避免产生大量不能完成协商的 IKE SA，以便在设备处理能力较弱时保证一定的新建性能。

可以通过 **max-sa** 参数设置允许建立更多的 IKE SA，以便在设备有充足内存的情况下得到更高的并发性能；可以通过该参数设置允许建立更少的 IKE SA，以便在设备没有充足的内存的情况下，使 IKE 不过多占用系统内存。

【举例】

配置本端允许同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数为 200。

```
<Sysname> system-view
[Sysname] ike limit max-negotiating-sa 200
```

配置本端允许成功建立的 IKE SA 的最大数为 5000。

```
<Sysname> system-view
[Sysname] ike limit max-sa 5000
```

2.1.22 ike logging negotiation enable

ike logging negotiation enable 命令用来开启 IKE 协商事件日志功能。

undo ike logging negotiation enable 命令用来关闭 IKE 协商事件日志功能。

【命令】

ike logging negotiation enable

undo ike logging negotiation enable

【缺省情况】

IKE 协商事件日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 IKE 协商事件日志记录功能后，设备会输出 IKE 协商过程中的相关日志。

【举例】

开启 IKE 事件协商日志功能。

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

2.1.23 ike nat-keepalive

ike nat-keepalive 命令用来配置向对端发送 NAT Keepalive 报文的时间间隔。

undo ike nat-keepalive 命令用来恢复缺省情况。

【命令】

ike nat-keepalive *seconds*

undo ike nat-keepalive

【缺省情况】

向对端发送 NAT Keepalive 报文的时间间隔为 20 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds：指定向对端发送 NAT Keepalive 报文的时间间隔，取值范围为 5～300，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备（即该设备位于 NAT 设备连接的私网侧）有意义。NAT 之后的 IKE 网关设备需要定时向 NAT 之外的 IKE 网关设备发送 NAT Keepalive 报文，以便维持 NAT 设备上对应的 IPsec 流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。

因此，需要确保该命令配置的时间小于 NAT 设备上会话表项的存活时间。关于如何查看 NAT 表项的存活时间，请参见“网络互通命令参考”中的“NAT”。

【举例】

配置向对端发送 NAT Keepalive 报文的时间间隔为 5 秒。

```
<Sysname> system-view
[Sysname] ike nat-keepalive 5
```

2.1.24 ike profile

ike profile 命令用来创建一个 IKE profile，并进入 IKE profile 视图。如果指定的 IKE profile 已经存在，则直接进入 IKE profile 视图。

undo ike profile 命令用来删除指定的 IKE profile。

【命令】

ike profile *profile-name*

undo ike profile *profile-name*

【缺省情况】

不存在 IKE profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：IKE profile 名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

创建 IKE profile 1，并进入其视图。

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

2.1.25 ike proposal

ike proposal 命令用来创建 IKE 提议，并进入 IKE 提议视图。如果指定的 IKE 提议已经存在，则直接进入 IKE 提议视图。

undo ike proposal 命令用来删除指定 IKE 提议。

【命令】

ike proposal *proposal-number*

undo ike proposal *proposal-number*

【缺省情况】

系统提供一条缺省的 IKE 提议，此缺省的 IKE 提议具有最低的优先级。缺省的提议的参数不可修改，其参数包括：

- 加密算法：DES-CBC

- 认证算法：HMAC-SHA1
- 认证方法：预共享密钥
- DH 密钥交换参数：group1
- IKE SA 存活时间：86400 秒

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

proposal-number：IKE 提议序号，取值范围为 1～65535。该序号同时表示优先级，数值越小，优先级越高。

【使用指导】

在进行 IKE 协商的时候，协商发起方会将自己的 IKE 提议发送给对端，由对端进行匹配。若发起方使用的 IPsec 安全策略中没有引用 IKE profile，则会将当前系统中所有的 IKE 提议发送给对端；否则，发起方会将引用的 IKE profle 中的所有 IKE 提议发送给对端。

响应方则以对端发送的 IKE 提议优先级从高到低的顺序与本端所有的 IKE 提议进行匹配，一旦找到匹配项则停止匹配并使用匹配的提议，否则继续查找其它的 IKE 提议。如果本端配置中没有和对端匹配的 IKE 提议，则使用系统缺省的 IKE 提议进行匹配。

【举例】

创建 IKE 提议 1，并进入 IKE 提议视图。

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

【相关命令】

- **display ike proposal**

2.1.26 ike signature-identity from-certificate

ike signature-identity from-certificate 命令用来配置设备使用由本端证书中获得的身份信息参与数字签名认证。

undo ike signature-identity from-certificate 命令用来恢复缺省情况。

【命令】

ike signature-identity from-certificate

undo ike signature-identity from-certificate

【缺省情况】

当使用数字签名认证方式时，本端身份信息由 **local-identity** 或 **ike identity** 命令指定。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当使用数字签名认证方式时，本端的身份总是从本端证书的主题字段中获得，不论 **local-identity** 或 **ike identity** 如何配置。

在采用 IPsec 野蛮协商模式以及数字签名认证方式的情况下，与仅支持使用 DN 类型身份进行数字签名认证的 ComwareV5 设备互通时需要配置本命令。

如果没有配置 **ike signature-identity from-certificate**，并且 IPsec 安全策略或 IPsec 安全策略模板下指定的 IKE profile 中配置了本端身份（由 **local-identity** 命令指定），则使用 IKE profile 中配置的本端身份；若 IPsec 安全策略或 IPsec 安全策略模板下未指定 IKE profile 或 IKE profile 下没有配置本端身份，则使用全局配置的本端身份（由 **ike identity** 命令指定）。

【举例】

在采用数字签名认证时，指定总从本端证书中的主题字段取得本端身份。

```
<Sysname> system-view
[sysname] ike signature-identity from-certificate
```

【相关命令】

- **local-identity**
- **ike identity**

2.1.27 keychain

keychain 命令用来指定采用预共享密钥认证时使用的 IKE keychain。

undo keychain 命令用取消指定的 IKE keychain。

【命令】

keychain *keychain-name*

undo keychain *keychain-name*

【缺省情况】

未指定采用预共享密钥认证时使用的 IKE keychain。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

keychain-name：IKE keychain 名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

一个 IKE profile 中最多可以指定六个 IKE keychain，先配置的 IKE keychain 优先级高。

【举例】

在 IKE profile 1 中指定名称为 abc 的配置的 IKE keychain。

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

【相关命令】

- **ike keychain**

2.1.28 local-identity

local-identity 命令用来配置本端身份信息，用于在 IKE 认证协商阶段向对端标识自己的身份。

undo local-identity 命令用来恢复缺省情况。

【命令】

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

undo local-identity

【缺省情况】

未配置本端身份信息。此时使用系统视图下通过 **ike identity** 命令配置的身份信息作为本端身份信息。若两者都没有配置，则使用 IP 地址标识本端的身份，该 IP 地址为 IPsec 安全策略应用的接口的 IP 地址。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从本端数字证书中获得的 DN 名作为本端身份。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称，*fqdn-name* 为 1～255 个字符的字符串，区分大小写，例如 www.test.com。不指定 *fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 FQDN 类型的身份。

user-fqdn *user-fqdn-name*：指定标识本端身份的 user FQDN 名称，*user-fqdn-name* 为 1～255 个字符的字符串，区分大小写，例如 adc@test.com。不指定 *user-fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 user FQDN 类型的身份。

【使用指导】

如果本端的认证方式为数字签名方式，则本端可以配置任何类型的身份信息；如果本端的认证方式为预共享密钥方式，则只能配置除 DN 之外的其它类型的身份信息。

如果本端的认证方式为数字签名方式，且配置的本端身份为 IP 地址，但这个 IP 地址与本端证书中的 IP 地址不同，则设备将使用 FQDN 类型的本端身份标识，该标识为使用 **sysname** 命令配置的设备名称。

响应方使用发起方的身份信息查找本地的 IKE profile，通过与 **match remote** 命令中指定的发起方身份信息进行匹配，可查找到本端要采用的 IKE profile。

一个 IKE profile 中只能配置一条本端身份信息。

IKE profile 下的本端身份信息优先级高于系统视图下通过 **ike identity** 命令配置的本端身份信息。如果 IKE profile 下未配置本端身份信息，则使用系统视图下配置的本端身份信息。

【举例】

指定使用 IP 地址 2.2.2.2 标识本端身份。

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] local-identity address 2.2.2.2
```

【相关命令】

- **match remote**
- **ike identity**

2.1.29 match local address (IKE keychain view)

match local address 命令用来限制 IKE keychain 的使用范围，即 IKE keychain 只能用于指定地址或指定接口的地址上的 IKE 协商。

undo match local address 命令用来恢复缺省情况。

【命令】

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address

【缺省情况】

未限制 IKE keychain 的使用范围。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：本端接口名称。可以是任意的三层接口。

ipv4-address：本端接口的 IPv4 地址。

ipv6 *ipv6-address*：本端接口的 IPv6 地址。

【使用指导】

此命令用于限制 IKE keychain 只能用于指定地址或指定接口的地址上的协商，这里的地址指的是 IPsec 安全策略/IPsec 安全策略模板下配置的本端地址（通过命令 **local-address** 配置），若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址。

一个 IKE profile 中最多可以指定六个 IKE keychain，先配置的 IKE keychain 优先级高。若希望本端在匹配某些 IKE keychain 的时候，不按照配置的优先级来查找，则可以通过本命令来指定这类 IKE

keychain 的使用范围。例如，IKE keychain A 中的预共享密钥的匹配地址范围大（2.2.0.0/16），IKE keychain B 中的预共享密钥的匹配地址范围小（2.2.2.0/24），IKE keychain A 先于 IKE keychain B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 keychain A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 keychain B 与对端协商，可以配置 keychain B 在指定地址 3.3.3.3 的接口上使用。

【举例】

创建 IKE keychain，名称为 key1。

```
<Sysname> system-view
[Sysname] ike keychain key1
```

限制 IKE keychain key1 只能在 2.2.2.1 的 IP 地址上使用。

```
[sysname-ike-keychain-key1] match local address 2.2.2.1
```

2.1.30 match local address (IKE profile view)

match local address 命令用来限制 IKE profile 的使用范围，即 IKE profile 只能用于指定地址或指定接口的地址上的 IKE 协商。

undo match local address 命令用来恢复缺省情况。

【命令】

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address

【缺省情况】

未限制 IKE profile 的使用范围。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：本端接口名称。可以是任意三层接口。

ipv4-address：本端接口 IPv4 地址。

ipv6 *ipv6-address*：本端接口 IPv6 地址。

【使用指导】

此命令用于限制IKE profile只能用于指定地址或指定接口的地址上的协商，这里的地址指的是IPsec安全策略/IPsec 安全策略模板下配置的本端地址（通过命令 **local-address** 配置），若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址。

先配置的 IKE profile 优先级高，若希望本端在匹配某些 IKE profile 的时候，不按照配置的优先级来查找，则可以通过本命令来指定这类 IKE profile 的使用范围。例如，IKE profile A 中的 match remote 地址范围大（match remote identity address range 2.2.2.1 2.2.2.100），IKE profile B 中的 match remote 地址范围小（match remote identity address range 2.2.2.1 2.2.2.10），IKE profile A 先于 IKE

profile B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 profile A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 profile B 与对端协商，可以配置 profile B 在指定地址 3.3.3.3 的接口上使用。

【举例】

创建 IKE profile，名称为 prof1。

```
<Sysname> system-view
[Sysname] ike profile prof1
```

限制 IKE profile prof1 只能在 2.2.2.1 的 IP 地址上使用。

```
[sysname-ike-profile-prof1] match local address 2.2.2.1
```

2.1.31 match remote

match remote 命令用来配置一条用于匹配对端身份的规则。

undo match remote 命令用来删除一条用于匹配对端身份的规则。

【命令】

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* } }

【缺省情况】

未配置用于匹配对端身份的规则。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

certificate *policy-name*：基于对端数字证书中的信息匹配 IKE profile。其中，*policy-name* 是证书访问控制策略的名称，为 1～31 个字符的字符串。本参数用于响应方根据收到的发起方证书中的 DN 字段来过滤使用的 IKE profile。

identity：基于指定的对端身份信息匹配 IKE profile。本参数用于响应方根据发起方通过 **local-identity** 命令配置的身份信息来选择使用的 IKE profile。

address *ipv4-address* [*mask* | *mask-length*]：对端 IPv4 地址或 IPv4 网段。其中，*ipv4-address* 为 IPv4 地址，*mask* 为子网掩码，*mask-length* 为子网掩码长度，取值范围为 0～32，不指定子网掩码相关参数时默认为 32 位掩码。

address range *low-ipv4-address high-ipv4-address*：对端 IPv4 地址范围。其中 *low-ipv4-address* 为起始 IPv4 地址，*high-ipv4-address* 为结束 IPv4 地址。结束地址必须大于起始地址。

address ipv6 *ipv6-address* [*prefix-length*]：对端 IPv6 地址或 IPv6 网段。其中，*ipv6-address* 为 IPv6 地址，*prefix-length* 为 IPv6 前缀，取值范围为 0～128，不指定 IPv6 前缀时默认为 128 位前缀。

address ipv6 range *low-ipv6-address high-ipv6-address*：对端 IPv6 地址范围。其中 *low-ipv6-address* 为起始 IPv6 地址，*high-ipv6-address* 为结束 IPv6 地址。结束地址必须大于起始地址。

fqdn *fqdn-name*：对端 FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 www.test.com。

user-fqdn *user-fqdn-name*：对端 User FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 abc@test.com。

【使用指导】

响应方根据发起发的身份信息通过本配置查找 IKE profile 并验证对端身份，发起方根据响应方的身份信息通过本配置验证对端身份。

协商双方都必须配置至少一个 **match remote** 规则，当对端的身份与 IKE profile 中配置的 **match remote** 规则匹配时，则使用此 IKE profile 中的信息与对端完成认证。为了使得每个对端能够匹配到唯一的 IKE profile，不建议在两个或两个以上 IKE profile 中配置相同的 **match remote** 规则，否则能够匹配到哪个 IKE profile 是不可预知的。

match remote 规则可以配置多个，并同时都有效，其匹配优先级为配置顺序。

【举例】

创建 IKE profile，名称为 prof1。

```
<Sysname> system-view
[Sysname] ike profile prof1
```

指定需要匹配对端身份类型为 FQDN，取值为 www.test.com。

```
[Sysname-ike-profile-prof1] match remote identity fqdn www.test.com
```

指定需要匹配对端身份类型为 IP 地址，取值为 10.1.1.1。

```
[Sysname-ike-profile-prof1] match remote identity address 10.1.1.1
```

【相关命令】

- **local-identity**

2.1.32 pre-shared-key

pre-shared-key 命令用来配置预共享密钥。

undo pre-shared-key 命令用来取消指定的预共享密钥。

【命令】

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* }

【缺省情况】

未配置预共享密钥。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

address：对端的地址。

ipv4-address：对端的 IPv4 地址。

mask：对端的 IPv4 地址掩码，缺省值为 255.255.255.255。

mask-length：对端的 IPv4 地址掩码长度，取值范围为 0～32，缺省值为 32。

ipv6：指定对端的 IPv6 地址。

ipv6-address：对端的 IPv6 地址。

prefix-length：对端的 IPv6 地址前缀长度，取值范围为 0～128，缺省值为 128。

hostname *host-name*：对端主机名。取值范围为 1～255，区分大小写。

key：设置的预共享密钥。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1～128 个字符的字符串；密文密钥为 1～201 个字符的字符串。

【使用指导】

配置预共享密钥的同时，还通过参数 **address** 和 **hostname** 指定了使用该预共享密钥的匹配条件，即与哪些 IP 地址或哪些主机名的对端协商时，才可以使用该预共享密钥。

以 **hostname** 方式设置预共享密钥时，IKE 协商只能采用野蛮模式，设备本身只能作为响应方，且对端 IKE 身份 ID 需采用 FQDN 方式来匹配主机名。

IKE 协商双方必须配置了相同的预共享密钥，预共享密钥类型的身份认证才会成功。

支持以交互式方式设置预共享密钥，且为 15～128 个字符的字符串，区分大小写，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符），但不能包含问号字符“？”。

【举例】

创建 IKE keychain key1 并进入 IKE keychain 视图。

```
<Sysname> system-view
[Sysname] ike keychain key1
```

配置与地址为 1.1.1.2 的对端使用的预共享密钥为明文的 123456TESTplat&!。

```
[Sysname-ike-keychain-key1] pre-shared-key address 1.1.1.2 255.255.255.255 key simple
123456TESTplat&!
```

【相关命令】

- **authentication-method**
- **keychain**

2.1.33 priority (IKE keychain view)

priority 命令用来指定 IKE keychain 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

priority *priority*

undo priority

【缺省情况】

IKE keychain 的优先级为 100。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

priority *priority*：IKE keychain 优先级，取值范围为 1～65535。该数值越小，优先级越高。

【使用指导】

配置了 **match local address** 的 IKE keychain，优先级高于所有未配置 **match local address** 的 IKE keychain。即 IKE keychain 的使用优先级首先决定于其中是否配置了 **match local address**，其次取决于它的优先级。

【举例】

指定 IKE keychain key1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1] priority 10
```

2.1.34 priority (IKE profile view)

priority 命令用来指定 IKE profile 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

priority *priority*

undo priority

【缺省情况】

IKE profile 的优先级为 100。

【视图】

IKE-Profile 视图

【缺省用户角色】

network-admin

【参数】

priority *priority*：IKE profile 优先级号，取值范围为 1～65535。该数值越小，优先级越高。

【使用指导】

配置了 **match local address** 的 IKE profile，优先级高于所有未配置 **match local address** 的 IKE profile。即 IKE profile 的匹配优先级首先决定于其中是否配置了 **match local address**，其次决定于它的优先级。

【举例】

指定在 IKE profile prof1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] priority 10
```

2.1.35 proposal

proposal 命令用来配置 IKE profile 引用的 IKE 提议。

undo proposal 命令用来恢复缺省情况。

【命令】

proposal *proposal-number*&<1-6>

undo proposal

【缺省情况】

IKE profile 未引用 IKE 提议，使用系统视图下配置的 IKE 提议进行 IKE 协商。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

proposal-number&<1-6>：IKE 提议序号，取值范围为 1～65535。该序号在 IKE profile 中与优先级无关，先配置的 IKE 提议优先级高。&<1-6>表示前面的参数最多可以输入 6 次。

【使用指导】

IKE 协商过程中，对于发起方，如果使用的 IPsec 安全策略下指定了 IKE profile，则使用 IKE profile 中引用的 IKE 提议进行协商；对于响应方，则使用系统视图下配置的 IKE 提议与对端发送的 IKE 提议进行匹配。

【举例】

设置 IKE profile prof1 引用序号为 10 的 IKE 安全提议。

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] proposal 10
```

【相关命令】

- **ike proposal**

2.1.36 reset ike sa

reset ike sa 命令用来清除 IKE SA。

【命令】

reset ike sa [**connection-id** *connection-id*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

connection-id *connection-id*：清除指定连接 ID 的 IKE SA，取值范围为 1～2000000000。

【使用指导】

删除 IKE SA 时，会向对端发送删除通知消息。

【举例】

查看当前的 IKE SA。

```
<Sysname> display ike sa
    Connection-ID  Remote           Flag        DOI
  -----------------------------------------------------------
      1            202.38.0.2       RD          IPsec
      2            202.38.0.3       RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

清除连接 ID 号为 2 的 IKE SA。

```
<Sysname> reset ike sa connection-id 2
```

查看当前的 IKE SA。

```
<Sysname> display ike sa
    Connection-ID  Remote           Flag        DOI
  -----------------------------------------------------------
      1            202.38.0.2       RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

2.1.37 reset ike statistics

reset ike statistics 命令用于清除 IKE 的 MIB 统计信息。

【命令】

reset ike statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 IKE 的 MIB 统计信息。

```
<Sysname> reset ike statistics
```

【相关命令】

- **snmp-agent trap enable ike**

2.1.38 sa duration

sa duration 命令用来指定一个 IKE 提议的 IKE SA 存活时间。

undo sa duration 命令用来恢复缺省情况。

【命令】

sa duration *seconds*

undo sa duration

【缺省情况】

IKE 提议的 IKE SA 存活时间为 86400 秒。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

seconds：指定 IKE SA 存活时间，取值范围为 60～604800，单位为秒。

【使用指导】

在指定的 IKE SA 存活时间超时前，设备会提前协商另一个 IKE SA 来替换旧的 IKE SA。在新的 IKE SA 还没有协商完之前，依然使用旧的 IKE SA；在新的 IKE SA 建立后，将立即使用新的 IKE SA，而旧的 IKE SA 在存活时间超时后，将被自动清除。

如果协商双方配置了不同的 IKE SA 存活时间，则时间较短的存活时间生效。

若配置中同时存在 IPsec SA 存活时间，则建议 IKE SA 存活时间大于 IPsec SA 存活时间。

【举例】

指定 IKE 提议 1 的 IKE SA 存活时间 600 秒（10 分钟）。

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] sa duration 600
```

【相关命令】

- **display ike proposal**

2.1.39 sa soft-duration buffer

sa soft-duration buffer 命令用来设置 IKE SA 的软超时缓冲时间。

undo sa soft-duration buffer 命令用来恢复缺省情况。

【命令】

sa soft-duration buffer *seconds*

undo sa soft-duration buffer

【缺省情况】

未配置 IKE SA 的软超时缓冲时间。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

seconds：IKE SA 的软超时缓冲时间，取值范围为 10～36000，单位为秒。

【使用指导】

本命令只对 IKEv1 有效。

若未配置软超时缓冲时间，则系统会基于 IKE SA 存活时间使用默认算法计算软超时时间，软超时时间到达后会立即进行新的 IKE SA 协商。

需要注意的是，在配置了软超时缓冲时间的情况下，软超时时间（基于时间的生存时间－软超时缓冲时间）需要大于 10 秒。否则，仍然采用未配置软超时缓冲时间的默认算法计算软超时时间。

【举例】

设置 IKE SA 的软超时缓冲时间为 600 秒。

```
<Sysname> system-view
[Sysname] ike profile abc
[Sysname-ike-profile-abc] sa soft-duration buffer 600
```

【相关命令】

- **display ike sa**

2.1.40 snmp-agent trap enable ike

snmp-agent trap enable ike 命令用来开启 IKE 的告警功能。

undo snmp-agent trap enable ike 命令用来关闭指定的 IKE 告警功能。

【命令】

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]*

【缺省情况】

IKE 的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

attr-not-support：表示属性参数不支持时的告警功能。

auth-failure：表示认证失败时的告警功能。

cert-type-unsupport：表示证书类型不支持时的告警功能。

cert-unavailable：表示无法获取证书时的告警功能。

decrypt-failure：表示解密失败时的告警功能。

encrypt-failure：表示加密失败时的告警功能。

global：表示全局告警功能。

invalid-cert-auth：表示证书认证无效时的告警功能。

invalid-cookie：表示 cookie 无效时的告警功能。

invalid-id：表示身份信息无效时的告警功能。

invalid-proposal：表示 IKE 提议无效时的告警功能。

invalid-protocol：表示安全协议无效时的告警功能。

invalid-sign：表示证书签名无效时的告警功能。

no-sa-failure：表示无法查到 SA 时的告警功能。

proposal-add：表示添加 IKE 提议时的告警功能。

proposal-delete：表示删除 IKE 提议时的告警功能。

tunnel-start：表示创建 IKE 隧道时的告警功能。

tunnel-stop：表示删除 IKE 隧道时的告警功能。

unsupport-exch-type：表示协商类型不支持时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的 IKE 告警功能。

如果希望生成并输出某种类型的 IKE 告警信息，则需要保证 IKE 的全局告警功能以及相应类型的告警功能均处于开启状态。

【举例】

开启全局 IKE 告警功能。

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

开启创建 IKE 隧道时的告警功能。

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

3 IKEv2

3.1 IKEv2配置命令

3.1.1 aaa authorization

aaa authorization 命令用来开启 IKEv2 的 AAA 授权功能。

undo aaa authorization 命令用来关闭 IKEv2 的 AAA 授权功能。

【命令】

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

undo aaa authorization

【缺省情况】

IKEv2 的 AAA 授权功能处于关闭状态。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*：申请授权属性时使用的 ISP 域名，为 1～255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“””、“:”、“*”、“?”、“<”、“>”以及“@”字符，且不能为字符串“d”、“de”、“def”、“defa”、“defau”、“defaul”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow”和“if-unknown”。

username *user-name*：申请授权属性时使用的用户名，为 1～55 个字符的字符串，区分大小写。用户名不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。

【使用指导】

开启 AAA 授权功能后，IKEv2 可以向 AAA 模块申请授权属性，例如 IKEv2 本地地址池属性。IKEv2 模块使用指定的 ISP 域名和用户名向 AAA 模块发起授权请求，AAA 模块采用域中的授权配置向远程 AAA 服务器或者本地用户数据库请求该用户的授权信息。用户名验证成功之后，IKEv2 本端将会得到相应的授权属性。该功能适合于由 AAA 模块集中管理和部署相关授权属性的组网环境。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

在 IKEv2 profile prof1 中开启 AAA 授权功能，指定 ISP 域为 abc，用户名为 test。

```
[Sysname-ikev2-profile-profile1] aaa authorization domain abc username test
```

【相关命令】

- **display ikev2 profile**

3.1.2 address

address 命令用来指定 IKEv2 peer 的主机地址。

undo address 命令用来恢复缺省情况。

【命令】

address { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] }

undo address

【缺省情况】

未指定 IKEv2 peer 的主机地址。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：IKEv2 peer 的 IPv4 主机地址。

Mask：IPv4 地址子网掩码。

mask-length：IPv4 地址的掩码长度，取值范围为 0～32。

ipv6 *ipv6-address*：IKEv2 peer 的 IPv6 主机地址。

prefix-length：IPv6 地址的前缀长度，取值范围为 0～128。

【使用指导】

使用主机地址查询 IKEv2 peer 对于 IKEv2 协商中的发起方和响应方均适用。

同一 keychain 视图下的不同 IKEv2 peer 不能配置相同的地址。

【举例】

创建一个 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

指定 IKEv2 peer 的 IP 地址为 3.3.3.3，掩码为 255.255.255.0。

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.3 authentication-method

authentication-method 命令用来指定 IKEv2 本端和对端的身份认证方式。

undo authentication-method 命令用来删除指定的 IKEv2 本端或对端身份认证方式。

【命令】

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** }

【缺省情况】

未配置本端和对端的认证方式。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

local：指定本端的身份认证方式。

remote：指定对端的身份认证方式。

dsa-signature：表示身份认证方式为 DSA 数字签名方式。

ecdsa-signature：表示身份认证方式为 ECDSA 数字签名方式。

pre-share：表示身份认证方式为预共享密钥方式。

rsa-signature：表示身份认证方式为 RSA 数字签名方式。

【使用指导】

一个 IKEv2 profile 中，必须配置 IKEv2 本端和对端的身份认证方式。本端和对端可以采用不同的身份认证方式。

只能指定一个本端身份认证方式，可以指定多个对端身份认证方式。在有多个对端且对端身份认证方式未知的情况下，可以通过多次执行本命令指定多个对端的身份认证方式。

如果本端或对端的身份认证方式为 RSA、DSA 或 ECDSA 数字签名方式（**rsa-signature**、**dsa-signature** 或 **ecdsa-signature**），则还必须通过命令 **certificate domain** 指定 PKI 域来获取用于签名和验证的数字证书。若没有指定 PKI 域，则使用系统视图下通过命令 **pki domain** 配置的 PKI 域。

如果本端或对端的认证方式为预共享密钥方式（**pre-share**），则还必须在本 IKEv2 profile 引用的 keychain 中指定对等体的预共享密钥。

【举例】

创建 IKEv2 profile profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

指定本端的认证方式为预共享密钥方式，对端的认证方式为 RSA 数字签名方式。

```
[Sysname-ikev2-profile-profile1] authentication local pre-share
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
```

指定对端用于签名和验证的 certificate 域为 genl。

```
[Sysname-ikev2-profile-profile1] certificate domain genl
```

指定 IKEv2 profile 引用的 keychain 为 keychain1。

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

【相关命令】

- **display ikev2 profile**
- **certificate domain** (ikev2 profile view)
- **keychain** (ikev2 profile view)

3.1.4 certificate domain

certificate domain 命令用来指定 IKEv2 协商采用数字签名认证时使用的 PKI 域。

undo certificate domain 命令用来取消配置 IKEv2 协商时使用的 PKI 域。

【命令】

certificate domain *domain-name* [**sign** | **verify**]

undo certificate domain *domain-name*

【缺省情况】

使用系统视图下配置的 PKI 域来验证证书。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

domain-name：PKI 域的名称，为 1～31 个字符的字符串，不区分大小写。

sign：指定本端使用该 PKI 域中的本地证书生成数字签名。

verify：指定本端使用该 PKI 域中的 CA 证书来验证对端证书。

【使用指导】

如果没有指定 **sign** 和 **verify**，则表示指定的 PKI 域既用于签名也用于验证。一个 PKI 域用于签名还是验证取决于最后一次的配置，例如，先配了 **certificate domain abc sign**，然后再配 **certificate domain abc verify**，那么最终 PKI 域 abc 只用于验证功能。

可通过多次执行本命令分别指定用于数字签名的 PKI 域和用于验证的 PKI 域。

如果本端的认证方式配置为 RSA、DSA 或 ECDSA 数字签名方式，则必须通过本命令指定 PKI 域来获取用于签名的本地证书；如果对端的认证方式配置为 RSA、DSA 或 ECDSA 数字签名方式，则使用本命令指定 PKI 域来获取用于验证的 CA 证书，若未指定 PKI 域，则使用系统视图下的所有 PKI 域来验证。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

配置 IKEv2 profile 引用的 PKI 域 abc 用于签名，PKI 域 def 用于验证。

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

【相关命令】

- **authentication-method**
- **pki domain**（安全命令参考/PKI）

3.1.5 config-exchange

config-exchange 命令用来开启指定的配置交换功能。

undo config-exchange 命令用来关闭指定的配置交换功能。

【命令】

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** { **accept** | **send** } }

【缺省情况】

所有的配置交换功能均处于关闭状态。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

request：表示本端在 Auth 交换请求报文中携带配置交换请求载荷。

set：表示本端在 Info 报文中携带配置交换设置载荷。

accept：表示本端可接受配置交换设置载荷。

send：表示本端可发送配置交换设置载荷。

【使用指导】

配置交换包括请求数据、回应数据、主动推数据和回应推数据，请求和推送的数据可以为网关地址，内部地址，路由信息等，目前仅支持中心侧内部地址分配。分支侧可以申请地址，但申请到的地址暂无用。

本端可以同时配置 **request** 和 **set** 参数。

如果本端配置了 **request** 参数，则只要对端能通过 AAA 授权获取到对应的请求数据，就会对本端的请求进行响应。

如果本端配置了 **set send** 参数，则对端必须配置 **set accept** 参数来配合使用。

如果本端配置了 **set send** 参数，且没有收到配置请求时，IKEv2 SA 协商成功后才会推送地址给对端。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

配置本端在 Auth 交换请求报文中携带配置交换请求载荷。

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

【相关命令】

- **aaa authorization**
- **display ikev2 profile**

3.1.6 dh

dh 命令用来配置 IKEv2 密钥协商时所使用的 DH 密钥交换参数。

undo dh 命令用来恢复缺省情况。

【命令】

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

undo dh

【缺省情况】

IKEv2 安全提议未定义 DH 组。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

group1：指定密钥协商时采用 768-bit 的 Diffie-Hellman group。

group2：指定密钥协商时采用 1024-bit 的 Diffie-Hellman group。

group5：指定密钥协商时采用 1536-bit 的 Diffie-Hellman group。

group14：指定密钥协商时采用 2048-bit 的 Diffie-Hellman group。

group24：指定密钥协商时采用含 256-bit 的 sub-group 的 2048-bit Diffie-Hellman group。

group19：指定密钥协商时采用 ECP 模式含 256-bit 的 Diffie-Hellman group。

group20：指定密钥协商时采用 ECP 模式含 384-bit 的 Diffie-Hellman group。

【使用指导】

group1 提供了最低的安全性，但是处理速度最快。group24 提供了最高的安全性，但是处理速度最慢。其他的 group 随着位数的增加，提供了更高的安全性，但是处理速度会相应减慢。请根据实际组网环境中对安全性和性能的要求选择合适的 Diffie-Hellman group。

一个 IKEv2 安全提议中至少需要配置一个 DH 组，否则该安全提议不完整。

一个 IKEv2 安全提议中可以配置多个 DH 组，其使用优先级按照配置顺序依次降低。

【举例】

指定 IKEv2 提议 1 使用 768-bit 的 Diffie-Hellman group。

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

【相关命令】

- **ikev2 proposal**

3.1.7 display ikev2 policy

display ikev2 policy 命令用来显示 IKEv2 安全策略的配置信息。

【命令】

display ikev2 policy [*policy-name* | **default**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

policy-name：IKEv2 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

default：缺省的 IKEv2 安全策略。

【使用指导】

如果未指定任何参数，则表示显示所有 IKEv2 安全策略的配置信息。

【举例】

显示所有 IKEv2 安全策略的配置信息。

```
<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:
  Proposal: 1
  Proposal: 2
IKEv2 policy: default
  Match VRF:
  Proposal: default
```

display ikev2 policy 命令显示信息描述表

字段	描述
IKEv2 policy	IKEv2安全策略的名称
Priority	IKEv2安全策略优先级

字段	描述
Match local address	匹配IKEv2安全策略的本端IPv4地址
Match local address ipv6	匹配IKEv2安全策略的本端IPv6地址
Match VRF	（暂不支持）匹配IKEv2安全策略的VPN实例名
Proposal	IKEv2安全策略引用的IKEv2安全提议名称

【相关命令】

- **ikev2 policy**

3.1.8 display ikev2 profile

display ikev2 profile 命令用来显示 IKEv2 profile 的配置信息。

【命令】

display ikev2 profile [*profile-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

profile-name：IKEv2 profile 的名称，为 1～63 个字符的字符串，不区分大小写。如果不指定本参数，则表示显示所有 IKEv2 profile 的配置信息。

【举例】

显示所有 IKEv2 profile 的配置信息。

```
<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 ipv4 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
DPD: Interval 32, retry 23, periodic
Config-exchange: Request, Set send, Set accept
NAT keepalive: 10
AAA authorization: Domain domain1, username ikev2
```

表3-1 display ikev2 profile 命令显示信息描述表

字段	描述
IKEv2 profile	IKEv2 profile的名称
Priority	IKEv2 profile的优先级
Match criteria	查找IKEv2 profile的匹配条件
Inside-vrf	（暂不支持）内网VPN实例名称
Local identity	本端身份信息
Local authentication method	本端认证方法
Remote authentication methods	对端认证方法
Keychain	IKEv2 profile引用的keychain
Sign certificate domain	用于签名的PKI域
Verify certificate domain	用于验证的PKI域
SA duration	IKEv2 SA生存时间
DPD	DPD功能参数：探测的间隔时间（单位为秒）、重传时间间隔（单位为秒）、探测模式（按需探测或周期探测） 若未开启DPD功能，则显示为Disabled
Config-exchange	配置交换功能： • Request：表示本端将在 Auth 交换请求报文中携带配置交换请求载荷 • Set accept：表示本端可接受配置交换设置载荷 • Set send：表示本端可发送配置交换设置载荷
NAT keepalive	发送NAT保活报文的时间间隔（单位为秒）
AAA authorization	请求AAA授权信息时使用的参数：ISP域名、用户名

【相关命令】

- **ikev2 profile**

3.1.9 display ikev2 proposal

display ikev2 proposal 命令用来显示 IKEv2 安全提议的配置信息。

【命令】

display ikev2 proposal [*name* | **default**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

name：IKEv2 安全提议的名称，为 1～63 个字符的字符串，不区分大小写。

default：缺省的 IKEv2 安全提议。

【使用指导】

IKEv2 安全提议按照优先级从高到低的顺序显示。若不指定任何参数，则显示所有 IKEv2 提议的配置信息。

【举例】

显示所有 IKEv2 安全提议的配置信息。

```
<Sysname> display ikev2 proposal
IKEv2 proposal : 1
  Encryption: 3DES-CBC AES-CBC-128 AES-CTR-192 CAMELLIA-CBC-128
  Integrity: MD5 SHA256 AES-XCBC-MAC
  PRF: MD5 SHA256 AES-XCBC-MAC
  DH Group: MODP1024/Group2 MODP1536/Group5

IKEv2 proposal : default
  Encryption: AES-CBC-128 3DES-CBC
  Integrity: SHA1 MD5
  PRF: SHA1 MD5
  DH Group: MODP1536/Group5 MODP1024/Group2
```

表3-2 display ikev2 proposal 命令显示信息描述表

字段	描述
IKEv2 proposal	IKEv2安全提议的名称
Encryption	IKEv2安全提议采用的加密算法
Integrity	IKEv2安全提议采用的完整性校验算法
PRF	IKEv2安全提议采用的PRF算法
DH Group	IKEv2安全提议采用的DH组

【相关命令】

- **ikev2 proposal**

3.1.10 display ikev2 sa

display ikev2 sa 命令用来显示 IKEv2 SA 的信息。

【命令】

display ikev2 sa [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] [**verbose** [**tunnel** *tunnel-id*]]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

count：显示 IKEv2 SA 的数量。

local：显示指定本端地址的 IKEv2 SA 信息。

remote：显示指定对端地址的 IKEv2 SA 信息。

ipv4-address：本端或对端的 IPv4 地址。

ipv6 *ipv6-address*：本端或对端的 IPv6 地址。

verbose：显示 IKEv2 SA 的详细信息。如果不指定该参数，则表示显示 IKEv2 SA 的摘要信息。

tunnel *tunnel-id*：显示指定 IPsec 隧道的 IKEv2 SA 详细信息。*tunnel-id* 为 IPsec 隧道标识符，取值范围为 1～2000000000。

【使用指导】

若不指定任何参数，则显示所有 IKEv2 SA 的摘要信息。

【举例】

显示所有 IKEv2 SA 的摘要信息。

```
<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
```

显示对端地址为 1.1.1.2 的 IKEv2 SA 的摘要信息。

```
<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
```

表3-3 display ikev2 sa 命令显示信息描述表

字段	描述
Tunnel ID	IKEv2 SA的隧道标识符
Local	IKEv2 SA的本端IP地址
Remote	IKEv2 SA的对端IP地址
Status	IKEv2 SA的状态： • IN-NEGO（Negotiating）：表示此 IKE SA 正在协商 • EST（Established）：表示此 IKE SA 已建立成功 • DEL（Deleting）：表示此 IKE SA 将被删除

显示当前所有 IKEv2 SA 的详细信息。

```
<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
```

显示对端地址为 1.1.1.2 的 IKEv2 SA 的详细信息。

```
<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 interval 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
```

表3-4 display ikev2 sa verbose 命令显示信息描述表

字段	描述
Tunnel ID	IKEv2 SA的隧道标识符
Local IP/Port	本端安全网关的IP地址/端口号
Remote IP/Port	对端安全网关的IP地址/端口号

字段	描述
Outside VRF	（暂不支持）出方向被保护数据所属的VRF名称，-表示属于公网
Inside VRF	（暂不支持）入方向被保护数据所属的VRF名称，-表示属于公网
Local SPI	本端安全参数索引
Remote SPI	对端安全参数索引
Local ID type	本端安全网关的身份信息类型
Local ID	本端安全网关的身份信息
Remote ID type	对端安全网关的身份信息类型
Remote ID	对端安全网关的身份信息
Auth sign method	IKEv2安全提议中认证使用的签名方法
Auth verify method	IKEv2安全提议中认证使用的验证方法
Integrity algorithm	IKEv2安全提议中使用的完整性算法
PRF algorithm	IKEv2安全提议中使用的PRF算法
Encryption algorithm	IKEv2安全提议中使用的加密算法
Life duration	IKEv2 SA的生存时间（单位为秒）
Remaining key duration	IKEv2 SA的剩余生存时间（单位为秒）
Diffie-Hellman group	IKEv2密钥协商时所使用的DH密钥交换参数
NAT traversal	是否检测到协商双方之间存在NAT网关设备
DPD	DPD探测的时间间隔和重传时间（单位为秒），若未开启DPD探测功能，则显示为Disabled
Transmitting entity	IKEv2协商中的实体角色：发起方、响应方
Local window	本端IKEv2协商的窗口大小
Remote window	对端IKEv2协商的窗口大小
Local request message ID	本端下一次要发送的请求消息的序号
Remote request message ID	对端下一次要发送的请求消息的序号
Local next message ID	本端期望下一个接收消息的序号
Remote next message ID	对端期望下一个接收消息的序号
Pushed IP address	对端推送给本端的IP地址
Assigned IP address	本端分配给对端的IP地址

显示所有 IKEv2 SA 的个数。

```
[Sysname] display ikev2 sa count
IKEv2 SAs count: 0
```

表3-5 display ikev2 sa count 命令显示信息描述表

字段	描述
IKEv2 SAs count	IKEv2 SA的总数

3.1.11 display ikev2 statistics

display ikev2 statistics 命令用来显示 IKEv2 统计信息。

【命令】

display ikev2 statistics

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示 IKEv2 的统计信息。

```
<Sysname> display ikev2 statistics
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
  Temporary 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
```

表3-6 display ikev2 statistics 命令显示信息描述表

字段	描述
IKEv2 statistics	IKEv2统计信息
Unsupported critical payload	不支持的重要载荷
Invalid IKE SPI	无效的IKE SPI信息
Invalid major version	无效的主版本号
Invalid syntax	无效的语法
Invalid message ID	无效的Message ID
Invalid SPI	无效的SPI
No proposal chosen	提议不匹配
Invalid IKE payload	无效的IKE载荷
Authentication failed	认证失败
Single pair required	需要特定的地址对
TS unacceptable	不可接受的Traffic Selectors
Invalid selectors	无效的Selector
Temporary failure	临时错误
No child SA	找不到Child SA
Unknown other notify	未定义的其它通知类型
No enough resource	资源不够
Enqueue error	入队列错误
No IKEv2 SA	没有IKEv2 SA
Packet error	报文错误
Other error	其它错误
Retransmit timeout	重传超时
Dpd detect error	DPD探测失败
Del child for IPsec message	由于收到IPsec消息删除Child SA
Del child for deleting IKEv2 SA	由于删除IKEv2 SA删除Chlid SA
Del child for receiving delete message	由于收到删除消息删除Child SA

【相关命令】

- **reset ikev2 statistics**

3.1.12 dpd

dpd 用来配置 IKEv2 DPD 探测功能。

undo dpd 命令用来关闭 IKEv2 DPD 探测功能。

【命令】

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

undo dpd interval

【缺省情况】

IKEv2 profile 视图下的 DPD 探测功能处于关闭状态，使用全局的 DPD 配置。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

interval *interval*：指定 IKEv2 DPD 探测的间隔时间，取值范围为 10～3600，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则本端发送 IPsec 报文时触发 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry *seconds*：指定 DPD 报文的重传时间间隔，取值范围为 2～60，单位为秒。缺省值为 5 秒。

on-demand：指定按需探测模式，即根据流量来探测对端是否存活，在本端发送用户报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKEv2 DPD 探测的时间间隔，则触发 DPD 探测。

periodic：指定定时探测模式，即按照触发 IKEv2 DPD 探测的时间间隔定时探测对端是否存活。

【使用指导】

IKEv2 DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKEv2 对端通信时，应优先考虑使用按需探测模式。

配置的 **interval** 一定要大于 **retry**，保证在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

为 IKEv2 profile1 配置 IKEv2 DPD 功能，指定若 10 秒内没有从对端收到 IPsec 报文，则触发 IKEv2 DPD 探测，DPD 请求报文的重传时间间隔为 5 秒，探测模式为按需探测。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

【相关命令】

- **ikev2 dpd**

3.1.13 encryption

encryption 命令用来指定 IKEv2 安全提议使用的加密算法。

undo encryption 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

IKEv2 安全提议未定义加密算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 3DES 算法，3DES 算法采用 168 比特的密钥进行加密。

aes-cbc-128：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

aes-cbc-192：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 192 比特的密钥进行加密。

aes-cbc-256：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 256 比特的密钥进行加密。

aes-ctr-128：指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法，密钥长度为 128 比特。

aes-ctr-192：指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法，密钥长度为 192 比特。

aes-ctr-256：指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法，密钥长度为 256 比特。

camellia-cbc-128：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 128 比特。

camellia-cbc-192：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 192 比特。

camellia-cbc-256：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 256 比特。

des-cbc：指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

【使用指导】

IKEv2 安全提议中至少需要配置一个加密算法，否则该安全提议不完整，也不可用。一个 IKEv2 安全提议中可以配置多个加密算法，其使用优先级按照配置顺序依次降低。

【举例】

指定 IKEv2 安全提议 1 的加密算法为 CBC 模式的 168-bit 3DES。

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

【相关命令】

- **ikev2 proposal**

3.1.14 hostname

hostname 命令用来指定 IKEv2 peer 的主机名称。

undo hostname 命令用来恢复缺省情况。

【命令】

hostname *name*

undo hostname

【缺省情况】

未配置 IKEv2 peer 的主机名称。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

name：IKEv2 peer 主机名称，为 1～253 个字符的字符串，不区分大小写。

【使用指导】

主机名仅适用于在基于 IPsec 安全策略的 IKEv2 协商中发起方查询 IKEv2 peer，不适用于基于 IPsec 虚拟隧道接口的 IKEv2 协商。

【举例】

创建 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

指定 IKEv2 peer 的主机名为 test。

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.15 identity

identity 命令用来指定 IKEv2 peer 的身份信息。

undo identity 命令用来恢复缺省情况。

【命令】

identity { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }

undo identity

【缺省情况】

未指定 IKEv2 peer 的身份信息。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：对端 IPv4 地址。

ipv6 *ipv6-address*：对端 IPv6 地址。

fqdn *fqdn-name*：对端 FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 www.test.com。

email *email-string*：指定标识对端身份的 E-mail 地址。*email-string* 为按照 RFC 822 定义的 1～255 个字符的字符串，区分大小写，例如 esec@test.com。

key-id *key-id-string*：指定标识对端身份的 Key-ID 名称。*key-id-string* 为 1～255 个字符的字符串，区分大小写，通常为具体厂商的某种私有标识字符串。

【使用指导】

对等体身份信息仅用于 IKEv2 协商的响应方查询 IKEv2 peer，因为发起方在发起 IKEv2 协商时并不知道对端的身份信息。

【举例】

创建一个 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

指定 IKEv2 peer 的身份信息为地址 1.1.1.2。

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.16 identity local

identity local 命令用来配置本端身份信息，用于在 IKEv2 认证协商阶段向对端标识自己的身份。

undo identity local 命令用来恢复缺省情况。

【命令】

identity local { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }

undo identity local

【缺省情况】

未指定 IKEv2 本端身份信息，使用应用 IPsec 安全策略的接口的 IP 地址作为本端身份。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从本端数字证书中获得的 DN 名作为本端身份。

email *email-string*：指定标识本端身份的 E-mail 地址。*email-string* 为按照 RFC 822 定义的 1～255 个字符的字符串，区分大小写，例如 sec@abc.com。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称。*fqdn-name* 为 1～255 个字符的字符串，区分大小写，例如 www.test.com。

key-id *key-id-string*：指定标识本端身份的 Key-ID 名称。*key-id-string* 为 1～255 个字符的字符串，区分大小写，通常为具体厂商的某种私有标识字符串。

【使用指导】

交换的身份信息用于协商双方在协商时识别对端身份。

【举例】

#创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

指定使用 IP 地址 2.2.2.2 标识本端身份。

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

【相关命令】

- **peer**

3.1.17 ikev2 address-group

ikev2 address-group 命令用来配置为对端分配 IPv4 地址的 IKEv2 本地 IPv4 地址池。

undo ikev2 address-group 命令用来删除指定的 IKEv2 本地地址池。

【命令】

ikev2 address-group *group-name start-ipv4-address end-ipv4-address* [*mask* | *mask-length*]

undo ikev2 address-group *group-name* [*start-ipv4-address* [*end-ipv4-address*]]

【缺省情况】

未定义 IKEv2 本地 IPv4 地址池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name：IPv4 地址池名称，为 1～63 个字符的字符串，不区分大小写。

start-ipv4-address：IPv4 地址池的起始地址。

end-ipv4-address：IPv4 地址池的结束地址。

mask：IPv4 地址掩码。

mask-length：IPv4 地址掩码长度。

【使用指导】

每个地址池中包括的 IPv4 地址的最大数目为 8192。

执行 **undo ikev2 address-group** 时：

- 如果不指定起始和结束地址，则会删除所有指定名称的地址池。
- 如果指定起始地址而不指定结束地址，则结束地址的取值与起始地址相同，即删除单地址的地址池。
- 如果同时指定起始和结束地址，则删除指定地址池。
- 若要删除的地址池不存在，则不执行任何操作。

【举例】

配置 IKEv2 本地 IPv4 地址池，名称为 ipv4group，地址池范围为 1.1.1.1～1.1.1.2，掩码为 255.255.255.0。

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

配置 IKEv2 本地 IPv4 地址池，名称为 ipv4group，地址池范围为 1.1.1.1～1.1.1.2，掩码长度为 32。

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 32
```

删除 IKEv2 本地 IPv4 地址池，名称为 ipv4group，地址池范围为 1.1.1.1～1.1.1.2。

```
<Sysname> system-view
[Sysname] undo ikev2 address-group ipv4group 1.1.1.1 1.1.1.2
```

【相关命令】

- **address-group**

3.1.18 ikev2 cookie-challenge

ikev2 cookie-challenge 命令用来开启 cookie-challenge 功能。

undo ikev2 cookie-challenge 命令用来关闭 cookie-challenge 功能。

【命令】

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

【缺省情况】

IKEv2 cookie-challenge 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

number：指定触发响应方启用 cookie-challenge 功能的阈值，取值范围为 0～1000。

【使用指导】

若响应方配置了 cookie-challenge 功能，当响应方发现存在的半开 IKE SA 超过指定的数目时，就启用 cookie-challenge 机制。响应方收到 IKE_SA_INIT 请求后，构造一个 Cookie 通知载荷并响应发起方，若发起方能够正确携带收到的 Cookie 通知载荷向响应方重新发起 IKE_SA_INIT 请求，则可以继续后续的协商过程，防止由于源 IP 仿冒而耗费大量响应方的系统资源，造成对响应方的 DoS 攻击。

【举例】

开启 cookie-challenge 功能，并配置启用 cookie-challenge 功能的阈值为 450。

```
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

3.1.19 ikev2 dpd

ikev2 dpd 命令用来配置全局 IKEv2 DPD 功能。

undo ikev2 dpd 命令用来关闭全局 IKEv2 DPD 功能。

【命令】

ikev2 dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ikev2 dpd interval

【缺省情况】

IKEv2 DPD 探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval *interval*：指定触发 IKEv2 DPD 探测的时间间隔，取值范围为 10～3600，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则发送报文前触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry *seconds*：指定 DPD 报文的重传时间间隔，取值范围为 2～60，单位为秒，缺省值为 5 秒。

on-demand：指定按需探测模式，即根据流量来探测对端是否存活，在本端发送 IPsec 报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKEv2 DPD 探测的时间间隔（即通过 *interval* 指定的时间），则触发 DPD 探测。

periodic：指定定时探测模式，即按照触发 IKEv2 DPD 探测的时间间隔（即通过 *interval* 指定的时间）定时探测对端是否存活。

【使用指导】

IKEv2 DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKEv2 对端通信时，应优先考虑使用按需探测模式。

如果 IKEv2 profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKEv2 profile 视图下的 DPD 配置生效，如果 IKEv2 profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。

配置的 **interval** 一定要大于 **retry**，保证在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

配置根据流量来触发 IKEv2 DPD 探测的时间间隔为 15 秒。

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

配置定时触发 IKEv2 DPD 探测的时间间隔为 15 秒。

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

【相关命令】

- **dpd**（IKEv2 profile view）

3.1.20 ikev2 ipv6-address-group

ikev2 ipv6-address-group 命令用来配置为对端分配 IPv6 地址的 IKEv2 本地地址池。

undo ikev2 ipv6-address-group 命令用来删除指定的 IKEv2 本地地址池。

【命令】

ikev2 ipv6-address-group *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

undo ikev2 ipv6-address-group *group-name*

【缺省情况】

未定义 IKEv2 本地 IPv6 地址池。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name：IPv6 地址池名称，为 1～63 个字符的字符串，不区分大小写。

prefix *prefix/prefix-len*：指定 IPv6 地址池的地址前缀。*prefix/prefix-len* 为 IPv6 前缀/前缀长度，其中，*prefix-len* 取值范围为 1～128。

assign-len *assign-len*：指定地址池分配给对端的前缀长度。*assign-len* 的取值范围为 0～128，必须大于或等于 *prefix-len*，且与 *prefix-len* 之差小于或等于 16。

【使用指导】

与 IPv4 地址池不同，IPv6 地址池每次可分配的是一个 IPv6 地址段。对端收到该地址段后可继续为其它设备分配地址。

所有 IKEv2 本地 IPv6 地址池包含的前缀范围之间不能重叠，即前缀范围不能相交也不能相互包含。

【举例】

配置 IKEv2 本地 IPv6 地址池，名称为 ipv6group，前缀为 1:1::，前缀长度为 64，分配给使用者的前缀长度为 80。

```
<Sysname> system-view
[Sysname] ikev2 ipv6-address-group ipv6group prefix 1:1::/64 assign-len 80
```

【相关命令】

- **ipv6-address-group**

3.1.21 ikev2 keychain

ikev2 keychain 命令用来创建 IKEv2 keychain，并进入 IKEv2 keychain 视图。如果指定的 IKEv2 keychain 已经存在，则直接进入 IKEv2 keychain 视图。

undo ikev2 keychain 命令用来删除指定的 IKEv2 keychain。

【命令】

ikev2 keychain *keychain-name*

undo ikev2 keychain *keychain-name*

【缺省情况】

不存在 IKEv2 keychain。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keychain-name：IKEv2 keychain 的名称，为 1～63 个字符的字符串，不区分大小写，且不能包括字符“-”。

【使用指导】

任何一端采用了预共享密钥认证方式时，IKEv2 profile 下必须引用 keychain，且只能引用一个。配置的预共享密钥的值需要与对端 IKEv2 网关上配置的预共享密钥的值相同。

一个 IKEv2 keychain 下可以配置多个 IKEv2 peer。

【举例】

创建 IKEv2 keychain key1 并进入 IKEv2 keychain 视图。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

3.1.22 ikev2 nat-keepalive

ikev2 nat-keepalive 命令用来配置向对端发送 NAT Keepalive 报文的时间间隔。

undo ikev2 nat-keepalive 命令用来恢复缺省情况。

【命令】

ikev2 nat-keepalive *seconds*

undo ikev2 nat-keepalive

【缺省情况】

探测到 NAT 后发送 NAT Keepalive 报文的时间间隔为 10 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds：向对端发送 NAT Keepalive 报文的时间间隔，取值范围为 5～3600，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备（即该设备位于 NAT 设备连接的私网侧）有意义。NAT 之后的 IKEv2 网关设备需要定时向 NAT 之外的 IKEv2 网关设备发送 NAT Keepalive 报文，以确保 NAT 设备上相应于该流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。因此，配置的发送 NAT Keepalive 报文的时间间隔需要小于 NAT 设备上会话表项的存活时间。

【举例】

配置向 NAT 发送 NAT Keepalive 报文的时间间隔为 5 秒。

```
<Sysname> system-view
[Sysname] ikev2 nat-keepalive 5
```

3.1.23 ikev2 policy

ikev2 policy 命令用来创建 IKEv2 安全策略，并进入 IKEv2 安全策略视图。如果指定的 IKEv2 安全策略已经存在，则直接进入 IKEv2 安全策略视图。

undo ikev2 policy 命令用来删除指定的 IKEv2 安全策略。

【命令】

ikev2 policy *policy-name*

undo ikev2 policy *policy-name*

【缺省情况】

系统中存在一个名称为 default 的缺省 IKEv2 安全策略，该缺省的策略中包含一个缺省的 IKEv2 安全提议 default，且可与所有的本端地址相匹配。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name：IKEv2 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

IKE_SA_INIT 协商时，发起方根据应用 IPsec 安全策略的接口地址来选择要使用的 IKEv2 安全策略；响应方根据收到 IKEv2 报文的接口地址来选择要使用的 IKEv2 安全策略。选定 IKEv2 安全策略后，设备将根据安全策略中的安全提议进行加密算法、完整性校验算法、PRF 算法和 DH 组的协商。

可以配置多个 IKEv2 安全策略。一个 IKEv2 安全策略中必须至少包含一个 IKEv2 安全提议，否则该策略不完整。

若发起方使用共享源接口方式 IPsec 策略，则 IKE_SA_INIT 协商时，使用共享源接口地址来选择要是使用的 IKEv2 安全策略。

相同匹配条件下，配置的优先级可用于调整匹配 IKEv2 安全策略的顺序。

如果没有配置 IKEv2 安全策略，则使用默认的 IKEv2 安全策略 default。用户不能进入并配置默认的 IKEv2 安全策略 default。

【举例】

创建 IKEv2 安全策略 policy1，并进入 IKEv2 安全策略视图。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

【相关命令】

- **display ikev2 policy**

3.1.24 ikev2 profile

ikev2 profile 命令用来创建 IKEv2 profile，并进入 IKEv2 profile 视图。如果指定的 IKEv2 profile 已经存在，则直接进入 IKEv2 profile 视图。

undo ikev2 profile 命令用来删除指定的 IKEv2 profile。

【命令】

ikev2 profile *profile-name*

undo ikev2 profile *profile-name*

【缺省情况】

不存在 IKEv2 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：IKEv2 profile 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

IKEv2 profile 用于保存非协商的 IKEv2 SA 的参数，如本端和对端的身份、本端和对端的认证方式、用于查找 IKEv2 profile 的匹配条件等。

【举例】

创建 IKEv2 profile，名称为 profile1，并进入 IKEv2 profile 视图。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

【相关命令】

- **display ikev2 profile**

3.1.25 ikev2 proposal

ikev2 proposal 命令用来创建 IKEv2 安全提议，并进入 IKEv2 安全提议视图。如果指定的 IKEv2 安全提议已经存在，则直接进入 IKEv2 安全提议视图。

undo ikev2 proposal 命令用来删除指定的 IKEv2 安全提议。

【命令】

ikev2 proposal *proposal-name*

undo ikev2 proposal *proposal-name*

【缺省情况】

系统中存在一个名称为 default 的缺省 IKEv2 安全提议。

缺省提议使用的算法：

- 加密算法：AES-CBC-128 和 3DES
- 完整性校验算法：HMAC-SHA1 和 HMAC-MD5
- PRF 算法：HMAC-SHA1 和 HMAC-MD5
- DH：group5 和 group2

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

proposal-name：指定 IKEv2 安全提议的名称，为 1～63 个字符的字符串，不区分大小写，且不能为 default。

【使用指导】

IKEv2 安全提议用于保存 IKE_SA_INIT 交换中所使用的安全参数，包括加密算法、完整性验证算法、PRF（pseudo-random function）算法和 DH 组。

在一个 IKEv2 安全提议中，至少需要配置一组安全参数，即一个加密算法、一个完整性验证算法、一个 PRF 算法和一个 DH 组。

在一个 IKEv2 安全提议中，可以配置多组安全参数，即多个加密算法、多个完整性验证算法、多个 PRF 算法和多个 DH 组，这些安全参数在实际协商过程中，将会形成多种安全参数的组合与对端进行匹配。若实际协商过程中仅希望使用一组安全参数，请保证在 IKEv2 安全提议中仅配置了一套安全参数。

【举例】

创建 IKEv2 安全提议 prop1，并配置加密算法为 aes-cbc-128，完整性校验算法为 sha1，PRF 算法为 sha1，DH 组为 group2。

```
<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
```

【相关命令】

- **encryption-algorithm**

- **integrity**
- **prf**
- **dh**

3.1.26 integrity

integrity 命令用来指定 IKEv2 安全提议使用的完整性校验算法。

undo integrity 命令用来恢复缺省情况。

【命令】

integrity { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

【缺省情况】

未指定 IKEv2 安全提议使用的完整性校验算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-AES-XCBC-MAC。

md5：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-MD5。

sha1：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-1。

sha256：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-256。

sha384：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-384。

sha512：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-512。

【使用指导】

一个 IKEv2 安全提议中至少需要配置一个完整性校验算法，否则该安全提议不完整。一个 IKEv2 安全提议中可以配置多个完整性校验算法，其使用优先级按照配置顺序依次降低。

【举例】

创建 IKEv2 安全提议 prop1。

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

指定该安全提议使用的完整性校验算法为 MD5 和 SHA1，且优先选择 SHA1。

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

【相关命令】

- **ikev2 proposal**

3.1.27 keychain

keychain 命令用来配置采用预共享密钥认证时使用的 Keychain。

undo keychain 命令用来恢复缺省情况。

【命令】

keychain *keychain-name*

undo keychain

【缺省情况】

IKEv2 profile 中未引用 Keychain。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

keychain-name：IKEv2 keychain 名称，为 1～63 个字符的字符串，不区分大小写，且不能包括字符-。

【使用指导】

任何一端采用了预共享密钥认证方式时，IKEv2 profile 下必须引用 keychain，且只能引用一个。

不同的 IKEv2 profile 可以共享同一个 IKEv2 keychain 。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

指定 IKEv2 profile 引用的 keychain，keychain 的名称为 keychain1。

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

【相关命令】

- **display ikev2 profile**
- **ikev2 keychain**

3.1.28 match local (IKEv2 profile view)

match local 命令用来限制 IKEv2 profile 的使用范围。

undo match local 命令用来取消对 IKEv2 profile 使用范围的限制。

【命令】

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* }

【缺省情况】

未限制 IKEv2 profile 的使用范围。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

address：指定 IKEv2 profile 只能用于指定地址或指定接口的地址上的 IKEv2 协商。

interface-type interface-number：本端接口编号和接口名称，可以是任意三层接口。

ipv4-address：本端接口 IPv4 地址。

ipv6 *ipv6-address*：本端接口 IPv6 地址。

【使用指导】

此命令用于限制 IKEv2 profile 只能用于指定地址或指定接口上的地址协商，这里的地址指的是本端收到 IKEv2 报文的接口 IP 地址，即只有 IKEv2 协商报文从该地址接收时，才会采用该 IKEv2 profile。IKEv2 profile 优先级可以手工配置，先配置的优先级高。若希望本端在匹配某些 IKEv2 profile 的时候，不按照手工配置的顺序来查找，则可以通过本命令来指定这类 IKEv2 profile 的使用范围。例如，IKEv2 profile A 中的 **match remote** 地址范围大（**match remote identity address range 2.2.2.1 2.2.2.100**），IKEv2 profile B 中的 **match remote** 地址范围小（**match remote identity address range 2.2.2.1 2.2.2.10**），IKEv2 profile A 先于 IKEv2 profile B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 profile A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 profile B 与对端协商，可以配置 profile B 在指定地址 3.3.3.3 的接口上使用。

通过该命令可以指定多个本端匹配条件。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

限制 IKEv2 profile profile1 只能在 IP 地址为 2.2.2.2 的接口上使用。

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

【相关命令】

- **match remote**

3.1.29 match local address (IKEv2 policy view)

match local address 命令用来指定匹配 IKEv2 安全策略的本端地址。

undo match local address 命令用来删除指定的用于匹配 IKEv2 安全策略的本端地址。

【命令】

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* }

【缺省情况】

未指定用于匹配 IKEv2 安全策略的本端地址，表示本策略可匹配所有本端地址。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：本端接口编号和接口名称，可以是任意三层接口。

ipv4-address：本端接口 IPv4 地址。

ipv6 *ipv6-address*：本端接口 IPv6 地址。

【使用指导】

根据本端地址匹配 IKEv2 安全策略时，优先匹配指定了本端地址匹配条件的策略，其次匹配未指定本端地址匹配条件的策略。

【举例】

指定用于匹配 IKEv2 安全策略 policy1 的本端地址为 3.3.3.3。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

【相关命令】

- **display ikev2 policy**

3.1.30 match remote

match remote 命令用来配置匹配对端身份的规则。

undo match remote 命令用来删除一条用于匹配对端身份的规则。

【命令】

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* } }

【缺省情况】

未配置用于匹配对端身份的规则。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

certificate *policy-name*：基于对端数字证书中的信息匹配 IKEv2 profile。其中，*policy-name* 是证书访问控制策略的名称，为 1～31 个字符的字符串，不区分大小写。本参数用于基于对端数字证书中的信息匹配 IKEv2 profile。

identity：基于指定的对端身份信息匹配 IKEv2 profile。本参数用于响应方根据发起方通过 **identity local** 命令配置的身份信息来选择使用的 IKEv2 profile。

address *ipv4-address* [*mask* | *mask-length*]：对端 IPv4 地址或 IPv4 网段。其中，*ipv4-address* 为 IPv4 地址，*mask* 为子网掩码，*mask-length* 为子网掩码长度，取值范围为 0～32，不指定子网掩码相关参数时默认为 32 位掩码。

address range *low-ipv4-address high-ipv4-address*：对端 IPv4 地址范围。其中 *low-ipv4-address* 为起始 IPv4 地址，*high-ipv4-address* 为结束 IPv4 地址。结束地址必须大于起始地址。

address ipv6 *ipv6-address* [*prefix-length*]：对端 IPv6 地址或 IPv6 网段。其中，*ipv6-address* 为 IPv6 地址，*prefix-length* 为 IPv6 前缀长度，取值范围为 0～128，不指定 IPv6 前缀时默认为 128 位前缀。

address ipv6 range *low-ipv6-address high-ipv6-address*：对端 IPv6 地址范围。其中 *low-ipv6-address* 为起始 IPv6 地址，*high-ipv6-address* 为结束 IPv6 地址。结束地址必须大于起始地址。

fqdn *fqdn-name*：对端 FQDN 名称，为 1～255 个字符的字符串，区分大小写，例如 www.test.com。

email *email-string*：指定标识对等体身份的 E-mail 地址。*email-string* 为按照 RFC 822 定义的 1~255 个字符的字符串，区分大小写，例如 sec@abc.com。

key-id *key-id-string*：指定标识对等体身份的 Key-ID 名称。*key-id-string* 为 1～255 个字符的字符串，区分大小写，通常为具体厂商的某种私有标识字符串。

【使用指导】

查找对端匹配的 IKEv2 profile 时，对端需要同时满足以下条件：

- 将对端的身份信息与本命令配置的匹配规则进行比较，二者必须相同。
- 查找 IKEv2 profile 和验证对端身份时，需要使用 **match remote**、**match local address** 一起匹配，若有其中一项不符合，则表示该 IKEv2 profile 不匹配。

查找到匹配的 IKEv2 profile 后，本端设备将用该 IKEv2 profile 中的信息与对端完成认证。

为了使得每个对端能够匹配到唯一的 IKEv2 profile，不建议在两个或两个以上 IKEv2 profile 中配置相同的 **match remote** 规则，否则能够匹配到哪个 IKEv2 profile 是不可预知的。**match remote** 规则可以配置多个，并同时都有效，其匹配优先级为配置顺序。

【举例】

创建 IKEv2 profile，名称为 profile1。

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

```
[Sysname] ikev2 profile profile1
```

指定匹配采用 FQDN 作为身份标识、且取值为 www.test.com 的对端。

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

指定匹配采用 IP 地址作为身份标识、且取值为 10.1.1.1。

```
[Sysname-ikev2-profile-profile1]match remote identity address 10.1.1.1
```

【相关命令】

- **identity local**
- **match local address**

3.1.31 nat-keepalive

nat-keepalive 命令用来配置发送 NAT keepalive 的时间间隔。

undo nat-keepalive 命令用来恢复缺省情况。

【命令】

nat-keepalive *seconds*

undo nat-keepalive

【缺省情况】

使用全局的 IKEv2 NAT keepalive 配置。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

seconds：发送 NAT keepalive 报文的时间间隔，取值范围为 5～3600，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备（即该设备位于 NAT 设备连接的私网侧）有意义。NAT 之后的 IKEv2 网关设备需要定时向 NAT 之外的 IKEv2 网关设备发送 NAT Keepalive 报文，以确保 NAT 设备上相应于该流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。因此，配置的发送 NAT Keepalive 报文的时间间隔需要小于 NAT 设备上会话表项的存活时间。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

配置发送 NAT keepalive 报文的时间间隔为 1200 秒。

```
[Sysname-ikev2-profile-profile1]nat-keepalive 1200
```

【相关命令】

- **display ikev2 profile**
- **ikev2 nat-keepalive**

3.1.32 peer

peer 命令用来创建 IKEv2 peer，并进入 IKEv2 peer 视图。如果指定的 IKEv2 peer 已经存在，则直接进入 IKEv2 peer 视图。

undo peer 命令用来删除指定的 IKEv2 peer。

【命令】

peer *name*

undo peer *name*

【缺省情况】

不存在 IKEv2 peer。

【视图】

IKEv2 keychain 视图

【缺省用户角色】

network-admin

【参数】

name：IKEv2 peer 名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

一个 IKEv2 peer 中包含了一个预共享密钥以及用于查找该 peer 的匹配条件，包括对端的主机名称（由命令 **hostname** 配置）、对端的 IP 地址（由命令 **address** 配置）和对端的身份（由命令 **identity** 配置）。其中，IKEv2 协商的发起方使用对端的主机名称或 IP 地址查找 peer，响应方使用对端的身份或 IP 地址查找 peer。

【举例】

创建 IKEv2 keychain key1 并进入 IKEv2 keychain 视图。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

【相关命令】

- **ikev2 keychain**

3.1.33 pre-shared-key

pre-shared-key 命令用来配置 IKEv2 peer 的预共享密钥。

undo pre-shared-key 命令用来删除 IKEv2 peer 的预共享密钥。

【命令】

pre-shared-key [**local** | **remote**] { **ciphertext** | **plaintext** } *string*

undo pre-shared-key [**local** | **remote**]

【缺省情况】

未配置 IKEv2 peer 的预共享密钥。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

local：表示签名密钥。

remote：表示验证密钥。

ciphertext：以密文方式设置密钥。

plaintext：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1～128 个字符的字符串；密文密钥为 1～201 个字符的字符串。

【使用指导】

如果指定了参数 **local** 或 **remote**，则表示指定的是非对称密钥；若参数 **local** 和 **remote** 均不指定，则表示指定的是对称密钥。

执行 **undo** 命令时，指定要删除的密钥类型必须和已配置的密钥类型完全一致，该 **undo** 命令才会执行成功。例如，IKEv2 peer 视图下仅有 **pre-shared-key local** 的配置，则执行 **undo pre-shared-key** 和 **undo pre-shared-key remote** 命令均无效。

多次执行本命令，最后一次执行的命令生效。

【举例】

- 发起方示例

创建一个 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

配置 peer1 的对称预共享密钥为明文 111-key。

```
[Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-key1-peer-peer1] quit
```

创建一个 IKEv2 peer，名称为 peer2。

```
[Sysname-ikev2-keychain-key1] peer peer2
```

配置 peer2 的非对称预共享密钥，签名密钥为明文 111-key-a，验证密钥为明文 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
```

- 响应方示例

创建一个 IKEv2 keychain，名称为 telecom。

```
<Sysname> system-view
[Sysname] ikev2 keychain telecom
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-telecom] peer peer1
```

配置 peer1 的对称预共享密钥为明文 111-key。

```
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
```

创建一个 IKEv2 peer，名称为 peer2。

```
[Sysname-ikev2-keychain-telecom] peer peer2
```

配置 IKEv2 peer 的非对称预共享密钥，签名密钥为明文 111-key-b，验证密钥为明文 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
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.34 prf

prf 命令用来指定 IKEv2 安全提议使用的 PRF 算法。

undo prf 命令用来恢复缺省情况。

【命令】

prf { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

【缺省情况】

IKEv2 安全提议使用配置的完整性校验算法作为 PRF 算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-AES-XCBC-MAC。

md5：指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-MD5。

sha1：指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-1。

sha256：指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-256。

sha384:指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-384。

sha512:指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-512。

【使用指导】

一个 IKEv2 安全提议中可以配置多个 PRF 算法，其使用优先级按照配置顺序依次降低。

【举例】

创建 IKEv2 安全提议 prop1。

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

```
[Sysname] ikev2 proposal prop1
```

指定该安全提议使用的 PRF 算法为 MD5 和 SHA1，且优先选择 SHA1。

```
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

【相关命令】

- **ikev2 proposal**
- **integrity**

3.1.35 priority (IKEv2 policy view)

priority 命令用来指定 IKEv2 安全策略的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

priority *priority*

undo priority

【缺省情况】

IKEv2 安全策略的优先级为 100。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

priority：IKEv2 安全策略优先级，取值范围为 1～65535。该数值越小，优先级越高。

【使用指导】

本命令配置的优先级仅用于响应方在查找 IKEv2 安全策略时调整 IKEv2 安全策略的匹配顺序。

【举例】

指定 IKEv2 安全策略 policy1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

【相关命令】

- **display ikev2 policy**

3.1.36 priority (IKEv2 profile view)

priority 命令用来配置 IKEv2 profile 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

priority *priority*

undo priority

【缺省情况】

IKEv2 profile 的优先级为 100。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

priority：IKEv2 profile 优先级，取值范围为 1～65535。该数值越小，优先级越高。

【使用指导】

本命令配置的优先级仅用于响应方在查找 IKEv2 Profile 时调整 IKEv2 Profile 的匹配顺序。

【举例】

指定 IKEv2 profile profile1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

3.1.37 proposal

proposal 命令用来指定 IKEv2 安全策略引用的 IKEv2 安全提议。

undo proposal 命令用来取消 IKEv2 安全策略引用的 IKEv2 安全提议。

【命令】

proposal *proposal-name*

undo proposal *proposal-name*

【缺省情况】

IKEv2 安全策略未引用 IKEv2 安全提议。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

proposal-name：被引用的 IKEv2 安全提议的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

若同时指定了多个 IKEv2 安全提议，则它们的优先级按照配置顺序依次降低。

【举例】

配置 IKEv2 安全策略 policy1 引用 IKEv2 安全提议 proposal1。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
```

```
[Sysname-ikev2-policy-policy1] proposal proposal1
```

【相关命令】

- **display ikev2 policy**
- **ikev2 proposal**

3.1.38 reset ikev2 sa

reset ikev2 sa 命令用来清除 IKEv2 SA。

【命令】

reset ikev2 sa [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] | **tunnel** *tunnel-id*] [**fast**]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

local：清除指定本端地址的 IKEv2 SA 信息。

remote：清除指定对端地址的 IKEv2 SA 信息。

ipv4-address：本端或对端的 IPv4 地址。

ipv6 *ipv6-address*：本端或对端的 IPv6 地址。

tunnel *tunnel-id*：清除指定 IPsec 隧道的 IKEv2 SA 信息，*tunnel-id* 为 IPsec 隧道标识符，取值范围为 1～2000000000。

fast：不等待对端的回应，直接删除本端的 IKEv2 SA。若不指定本参数，则表示需要在收到对端的删除通知响应之后，再删除本端的 IKEv2 SA。

【使用指导】

清除 IKEv2 SA 时，会向对端发送删除通知消息，同时删除子 SA。

如果不指定任何参数，则删除所有 IKEv2 SA 及其协商生成的子 SA。

【举例】

删除对端地址为 1.1.1.2 的 IKEv2 SA。

```
<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
<Sysname> reset ikev2 sa remote 1.1.1.2
<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
```

【相关命令】

- **display ikev2 sa**

3.1.39 reset ikev2 statistics

reset ikev2 statistics 命令用来清除 IKEv2 统计信息。

【命令】

reset ikev2 statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 IKEv2 的统计信息。

```
<Sysname> reset ikev2 statistics
```

【相关命令】

- **display ikev2 statistics**

3.1.40 sa duration

sa duration 命令用来配置 IKEv2 SA 的生存时间。

undo sa duration 命令用来恢复缺省情况。

【命令】

sa duration *seconds*

undo sa duration

【缺省情况】

IKEv2 SA 的生存时间为 86400 秒。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

seconds：IKEv2 SA 的的生存时间，取值范围为 120～86400，单位为秒。

【使用指导】

在一个 IKEv2 SA 的生存时间到达之前，可以用该 IKEv2 SA 进行其它 IKEv2 协商。因此一个生存时间较长的 IKEv2 SA 可以节省很多用于重新协商的时间。但是，IKEv2 SA 的生存时间越长，攻击者越容易收集到更多的报文信息来对它实施攻击。

本端和对端的 IKEv2 SA 生存时间可以不一致，也不需要进行协商，由生存时间较短的一方在本端 IKEv2 SA 生存时间到达之后发起重协商。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

配置 IKEv2 SA 的生存时间为 1200 秒。

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

【相关命令】

- **display ikev2 profile**