目 录

1 IPsec配置命令

1.1 IPsec配置命令

1.1.1 ah authentication-algorithm

【命令】

ah authentication-algorithm { **md5** | **sha1** }

undo ah authentication-algorithm

【视图】

安全提议视图

【缺省级别】

2：系统级

【参数】

md5：采用 MD5 认证算法。

sha1：采用 SHA-1 认证算法。

【描述】

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。

缺省情况下，AH 协议采用 MD5 认证算法。

需要注意的是，只有先使用 **transform** 命令选择了 **ah** 或 **ah-esp** 安全协议后，才能够配置 **ah** 认证算法。

相关配置可参考命令 **ipsec proposal** 和 **transform**。

【举例】

配置安全提议 prop1，设定 AH 协议采用 SHA-1 算法。

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform ah
[Sysname-ipsec-proposal-prop1] ah authentication-algorithm sha1
```

1.1.2 connection-name

【命令】

connection-name *name*

undo connection-name

【视图】

安全策略视图/安全策略模板视图

【缺省级别】

2：系统级

【参数】

name：IPsec 连接的名称，为 1～32 个字符的字符串，不区分大小写。

【描述】

connection-name 命令用来配置 IPsec 连接名，该连接名用于描述一个 IPsec 安全策略。**undo connection-name** 命令用来恢复缺省情况。

缺省情况下，无 IPsec 连接名。

【举例】

配置一个 IPsec 连接名来描述序号为 1 的安全策略 policy1。

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

1.1.3 cryptoengine enable

【命令】

集中式设备：

cryptoengine enable

undo cryptoengine enable

分布式设备：

cryptoengine enable [**slot** *slot-number*]

undo cryptoengine enable [**slot** *slot-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

slot *slot-number*：指定分布式设备上的单板，*slot-number* 为单板所在的槽位号。

【描述】

cryptoengine enable 命令用来使能加密引擎功能。**undo cryptoengine enable** 命令用来禁止加密引擎功能。

缺省情况下，加密引擎功能处于使能状态。

【举例】

使能加密引擎功能。

```
<Sysname> system-view
[Sysname] cryptoengine enable
```

1.1.4 display ipsec policy

【命令】

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

brief：显示所有安全策略的简要信息。

name：显示指定安全策略的详细信息。

policy-name：指定安全策略的名字，为 1～15 个字符的字符串。

seq-number：指定安全策略的顺序号，取值范围为 1～65535。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ipsec policy 命令用来显示安全策略的信息。

需要注意的是：

- 如果不指定任何参数，则显示所有安全策略的详细信息。
- 如果指定了 **name** *policy-name*，而没有指定 *seq-number*，则显示指定的安全策略组的详细信息。

相关配置可参考命令 **ipsec policy** (system-view)。

【举例】

显示所有安全策略的简要信息。

```
<Sysname> display ipsec policy brief
IPsec-Policy-Name     Mode    acl    ike-peer name    Mapped Template
-----------------------------------------------------------------------
bbbbbbbbbbbbbbb-1     template                        aaaaaaaaaaaaaaa
man-1                 manual  3400
map-1                 isakmp  3000   peer
nat-1                 isakmp  3500   nat
test-1                isakmp  3200   test
toccccc-1             isakmp  3003   tocccc

IPsec-Policy-Name     Mode    acl          Local-Address  Remote-Address
-----------------------------------------------------------------------
```

```
man-1                   manual  3400        3.3.3.1         3.3.3.2
```

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

字段	描述
IPsec-Policy-Name	安全策略的名字和顺序号（例如 map-1 表示安全策略组名为 map、顺序号为 1）
Mode	安全策略采用的协商方式 ● manual：手工方式 ● isakmp：IKE 协商方式 ● template：策略模板方式
acl	安全策略引用的访问控制列表
ike-peer name	对等体的名称
Mapped Template	引用的安全策略模板名
Local-Address	本端的 IP 地址
Remote-Address	对端的 IP 地址

显示所有安全策略的详细信息。

```
<Sysname> display ipsec policy
==========================================
IPsec Policy Group: "policy_isakmp"
Interface: GigabitEthernet1/0/1
==========================================

  ----------------------------------
  IPsec policy name: "policy_isakmp"
  sequence number: 10
  mode: isakmp
  ----------------------------------
    security data flow : 3000
    selector mode: standard
    ike-peer name:  per
    perfect forward secrecy: None
    proposal name: prop1
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes
    policy enable: True
==========================================
IPsec Policy Group: "policy_man"
Interface: GigabitEthernet1/0/2
==========================================

  ----------------------------------------
  IPsec policy name: "policy_man"
  sequence number: 10
  mode: manual
```

```
  ----------------------------------------
    security data flow : 3002
    tunnel local  address: 162.105.10.1
    tunnel remote address: 162.105.10.2
    proposal name: prop1
    inbound AH setting:
      AH spi: 12345 (0x3039)
      AH string-key:
      AH authentication hex key : 12345678901234567890123456789012345678901234567890
    inbound ESP setting:
      ESP spi: 23456 (0x5ba0)
      ESP string-key:
      ESP encryption hex key: 1234567890abcdef1234567890abcdef1234567812345678
      ESP authentication hex key: 1234567890abcdef1234567890abcdef
    outbound AH setting:
      AH spi: 54321 (0xd431)
      AH string-key:
      AH authentication hex key: 11223344556677889900112233445566778899001122334455667788990011223344556677889900
    outbound ESP setting:
      ESP spi: 65432 (0xff98)
      ESP string-key:
      ESP encryption hex key: 1122334455667788990011223344556677889900aabbccddeeff1234567812345678
      ESP authentication hex key: 1122334455667788990011223344556677889900aabbccddeeff

==========================================
IPsec Policy Group: "manual"
Interface:
Protocol: OSPFv3, RIPng, BGP
==========================================

  ----------------------------
  IPsec policy name: "policy001"
  sequence number: 10
  mode: manual
  ----------------------------
    security data flow :
    tunnel local  address:
    tunnel remote address:
    proposal name: prop1
    inbound AH setting:
      AH spi:
      AH string-key:
      AH authentication hex key:
    inbound ESP setting:
      ESP spi: 23456 (0x5ba0)
      ESP string-key:
      ESP encryption hex key: 1234567890abcdef1234567890abcdef1234567812345678
      ESP authentication hex key: 1234567890abcdef1234567890abcdef
```

```
  outbound AH setting:
    AH spi:
    AH string-key:
    AH authentication hex key:
  outbound ESP setting:
    ESP spi: 23456 (0x5ba0)
    ESP string-key:
    ESP encryption hex key: 1234567890abcdef1234567890abcdef1234567812345678
    ESP authentication hex key: 1234567890abcdef1234567890abcdef
```

表1-2 display ipsec policy 命令显示信息描述表

字段	描述
IPsec Policy Group	安全策略组的名称
security data flow	安全策略引用的访问控制列表
Interface	应用了安全策略的接口名称
Protocol	应用了安全策略的协议名称（策略未应用在任何路由协议上时，不显示该字段）
IPsec policy name	安全策略的名称
sequence number	安全策略的顺序号
mode	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
policy template name	安全策略模板名称
selector mode	安全策略的数据流保护方式 • standard：标准方式 • aggregation：聚合方式
ike-peer name	安全策略引用的 IKE 对等体名称
tunnel local address	隧道本端的 IP 地址
tunnel remote address	隧道对端的 IP 地址
perfect forward secrecy	是否采用了完善的前向安全性（PFS）
proposal name	安全策略引用的提议的名字
policy enable	安全策略是否被使能
inbound/outbound AH/ESP setting	输入/输出端采用 AH/ESP 协议的有关设置，包括 SPI 和密钥

1.1.5 display ipsec policy-template

【命令】

display ipsec policy-template [**brief** | **name** *template-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

brief：显示所有安全策略模板的简要信息。

name：显示指定安全策略模板的详细信息。

template-name：指定安全策略模板的名字，为 1～15 个字符的字符串。

seq-number：指定安全策略模板的顺序号，取值范围为 1～65535。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ipsec policy-template 命令用来显示安全策略模板的信息。

需要注意的是：

- 如果不指定任何参数，则显示所有安全策略模板的详细信息。
- 如果指定了 **name** *template-name*，而没有指定 *seq-number*，则显示指定的安全策略模板组的详细信息。

相关配置可参考命令 **ipsec policy-template**。

【举例】

显示所有安全策略模板的简要信息。

```
<Sysname> display ipsec policy-template brief
Policy-template-Name     acl            Remote-Address
-------------------------------------------------------
test-tplt300             2200
```

表1-3 display ipsec policy-template 命令显示信息描述表

字段	描述
Policy-template-Name	安全策略模板的名字和顺序号（例如 test-tplt300 表示安全策略组名为 test-tplt、顺序号为 300）
acl	安全策略模板引用的访问控制列表
Remote Address	对端的 IP 地址

1.1.6 display ipsec profile

【命令】

display ipsec profile [**name** *profile-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

name *profile-name*：显示指定安全框架的配置信息。其中，*profile-name* 表示安全框架的名称，为 1～15 个字符的字符串，不区分大小写。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ipsec profile 命令用来显示安全框架的配置信息。

需要注意的是，如果没有指定安全框架的名称，则显示所有安全框架的配置信息。

相关配置可参考命令 **ipsec profile**。

【举例】

显示所有安全框架的配置信息。

```
<Sysname> display ipsec profile

==========================================
IPsec profile: "2"
Using interface: {Tunnel2}
==========================================

  ----------------------------
  IPsec profile name: "2"
  mode: dvpn
  ----------------------------
    security data flow : 0
    ike-peer name:  peer1
    perfect forward secrecy: None
    proposal name:  prop1
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes

==========================================
```

```
IPsec profile: "btoa"
Using interface: {Tunnel1}
============================================

  ----------------------------
  IPsec profile name: "btoa"
  mode: tunnel
  ----------------------------
    security data flow : 0
    ike-peer name:  btoa
    perfect forward secrecy: None
    proposal name:  method1
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes
```

表1-4 display ipsec profile 命令显示信息描述表

字段	描述
IPsec profile	指定的安全框架
Using interface	应用了安全框架的接口名称
IPsec profile name	安全框架的名称
mode	安全框架所采用的封装模式 • dvpn：DVPN 隧道模式 • tunnel：IPsec 虚拟隧道模式
security data flow	安全策略引用的访问控制列表 由于安全框架无需引用任何访问控制列表，因此此处显示为“0”，但无任何实际意义
ike-peer name	安全框架引用的 IKE 对等体名称
perfect forward secrecy	是否采用了完善的前向安全性（PFS）
proposal name	安全框架引用的提议的名称
IPsec sa local duration(time based)	安全联盟的基于时间的本地生存时间
IPsec sa local duration(traffic based)	安全联盟的基于流量的本地生存时间

1.1.7 display ipsec proposal

【命令】

display ipsec proposal [*proposal-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

proposal-name：指定提议的名字，为 1～32 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ipsec proposal 命令用来显示安全提议的信息。

如果没有指定提议的名字，则显示所有安全提议的信息。

相关配置可参考命令 **ipsec proposal**。

【举例】

显示所有安全提议的信息。

```
<Sysname> display ipsec proposal

  IPsec proposal name: prop2
    encapsulation mode: tunnel
    transform: ah-new
    AH protocol: authentication sha1-hmac-96

  IPsec proposal name: prop1
    encapsulation mode: transport
    transform: esp-new
    ESP protocol: authentication md5-hmac-96, encryption des
```

表1-5 display ipsec proposal 命令显示信息描述表

字段	描述
IPsec proposal name	提议的名字
encapsulation mode	提议采用的封装模式，包括两种：传输（transport）和隧道（tunnel）模式
transform	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 协议采用的认证算法
ESP protocol	ESP 协议采用的认证算法和加密算法

1.1.8 display ipsec sa

【命令】

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

brief：显示所有的安全联盟的简要信息。

policy：显示由指定安全策略创建的安全联盟的详细信息。

policy-name：指定安全策略的名字，为 1～15 个字符的字符串。

seq-number：指定安全策略的顺序号，取值范围为 1～65535。

remote *ip-address*：显示对端地址为 *ip-address* 的安全联盟的详细信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ipsec sa 命令用来显示安全联盟的相关信息。

需要注意的是，当未指定任何参数时，显示所有的安全联盟的信息。

相关配置可参考命令 **reset ipsec sa** 和 **ipsec sa global-duration**。

【举例】

显示安全联盟的简要信息。

```
<Sysname> display ipsec sa brief
Src Address  Dst Address  SPI    Protocol     Algorithm
-------------------------------------------------------
10.1.1.1     10.1.1.2     300    ESP          E:DES;
                                               A:HMAC-MD5-96
10.1.1.2     10.1.1.1     400    ESP          E:DES;
                                               A:HMAC-MD5-96
```

表1-6 display ipsec sa brief 命令显示信息描述表

字段	描述
Src Address	本端的 IP 地址
Dst Address	对端的 IP 地址
SPI	安全参数索引
Protocol	IPsec 采用的安全协议
Algorithm	安全协议采用的认证算法和加密算法，其中，以“E:”开头表示加密算法；以“A:”开头表示认证算法；NULL 表示未指定相关算法

显示安全联盟的全局生存时间。

```
<Sysname> display ipsec sa duration
     IPsec sa global duration（traffic based）: 1843200 kilobytes
     IPsec sa global duration（time based）: 3600 seconds
```

显示所有安全联盟的详细信息。

```
<Sysname> display ipsec sa
==============================
Interface: GigabitEthernet1/0/1
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "r2"
  sequence number: 1
  mode: isakmp
  ----------------------------
    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy:
    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)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      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

    [outbound ESP SAs]
      spi: 801701189 (0x2fc8fd45)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      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

==============================
Protocol: OSPFv3
==============================
```

```
-----------------------------
IPsec policy name: "manual"
sequence number: 1
mode: manual
-----------------------------
  connection id: 2
  encapsulation mode: transport
  perfect forward secrecy:
  tunnel:
  flow :

  [inbound AH SAs]
    spi: 1234563 (0x12d683)
    proposal: AH-MD5HMAC96
    No duration limit for this sa

  [outbound AH SAs]
    spi: 1234563 (0x12d683)
    proposal: AH-MD5HMAC96
    No duration limit for this sa
```

表1-7 display ipsec sa 命令显示信息描述表

字段	描述
Interface	应用了安全策略的接口
path MTU	从该接口发送出去的最大 IP 数据报文长度
Protocol	应用了安全策略的协议
IPsec policy name	采用的安全策略名
sequence number	安全策略顺序号
mode	IPsec 协商方式
connection id	安全隧道标识符
encapsulation mode	采用的封装模式，有两种：传输（transport）和隧道（tunnel）模式
perfect forward secrecy	此安全策略发起协商时使用完善的前向安全特性
tunnel	安全隧道
local address	安全隧道本端的 IP 地址
remote address	安全隧道对端的 IP 地址
flow	数据流
sour addr	数据流的源地址
dest addr	数据流的目的地址
port	端口号
protocol	协议类型

字段	描述
inbound	输入端安全联盟的信息
spi	安全参数索引号
proposal	安全提议所采用的安全协议及算法
sa duration	安全联盟生命周期
sa remaining duration	安全联盟剩余的生命周期
max received sequence-number	接收的报文最大序列号（安全协议提供的防重放功能）
udp encapsulation used for nat traversal	此安全联盟是否使用 NAT 穿越功能
outbound	输出端安全联盟的信息
max sent sequence-number	发送的报文最大序列号（安全协议提供的防重放功能）
anti-replay check enable	抗重放检测开关是否使能
anti-replay window size	抗重放窗口宽度

1.1.9 display ipsec statistics

【命令】

display ipsec statistics [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

tunnel-id *integer*：显示指定 IPsec 隧道的报文统计信息。其中，*integer* 为隧道的 ID 号，取值范围为 1～2000000000。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

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

需要注意的是，如果不指定任何参数，则显示所有 IPsec 处理的报文统计信息。

相关配置可参考命令 **reset ipsec statistics**。

【举例】

显示所有 IPsec 处理的报文统计信息。

```
<Sysname> display ipsec statistics
  the security packet statistics:
    input/output security packets: 47/62
    input/output security bytes: 3948/5208
    input/output dropped security packets: 0/45
    dropped security packet detail:
      not enough memory: 0
      can't find SA: 45
      queue is full: 0
      authentication has failed: 0
      wrong length: 0
      replay packet: 0
      packet too long: 0
      wrong SA: 0
```

显示隧道 ID 为 3 的 IPsec 报文统计信息。

```
<Sysname> display ipsec statistics tunnel-id 3
-----------------------------------------------
  Connection ID : 3
 -----------------------------------------------
  the security packet statistics:
    input/output security packets: 5124/8231
    input/output security bytes: 52348/64356
    input/output dropped security packets: 0/0
    dropped security packet detail:
      not enough memory: 0
      queue is full: 0
      authentication has failed: 0
      wrong length: 0
      replay packet: 0
      packet too long: 0
      wrong SA: 0
```

表1-8 display ipsec statistics 命令显示信息描述表

字段	描述
Connection ID	隧道 ID 号
input/output security packets	受安全保护的输入/输出数据包
input/output security bytes	受安全保护的输入/输出字节数
input/output dropped security packets	被设备丢弃了的受安全保护的输入/输出数据包
dropped security packet detail	被丢弃的输入/输出数据包的详细信息（包括以下各项）
not enough memory	因为内存不足而被丢弃的数据包的数目
can't find SA	因为找不到安全联盟而被丢弃的数据包的数目
queue is full	因为队列满而被丢弃的数据包的数目
authentication has failed	因为认证失败而被丢弃的数据包的数目
wrong length	因为数据包长度不正确而被丢弃的数据包的数目

字段	描述
replay packet	重放的数据包的数目
packet too long	因为数据包过长而被丢弃的数据包的数目
wrong SA	因为安全联盟不正确而被丢弃的数据包的数目

1.1.10 display ipsec tunnel

【命令】

display ipsec tunnel [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

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

【举例】

显示 IPsec 隧道的信息。

```
<Sysname> display ipsec tunnel
    total tunnel : 2
    -----------------------------------------------
    connection id: 3
    perfect forward secrecy:
    SA's SPI:
        inbound:  187199087 (0xb286e6f) [ESP]
        outbound: 3562274487 (0xd453feb7) [ESP]
    tunnel:
        local  address:  44.44.44.44
        remote address : 44.44.44.55
    flow:
        sour addr : 44.44.44.0/255.255.255.0  port: 0  protocol : IP
        dest addr : 44.44.44.0/255.255.255.0  port: 0  protocol : IP
    current Encrypt-card: None
```

```
-----------------------------------------------
    connection id: 5
    perfect forward secrecy:
    SA's SPI:
        inbound:  12345 (0x3039) [ESP]
        outbound: 12345 (0x3039) [ESP]
    tunnel:
    flow:
    current Encrypt-card:
```

显示聚合方式下的 IPsec 隧道信息。

```
<Sysname> display ipsec tunnel
    total tunnel: 2
    -----------------------------------------------
    connection id: 4
    perfect forward secrecy:
    SA's SPI:
        inbound :  2454606993 (0x924e5491) [ESP]
        outbound : 675720232 (0x2846ac28) [ESP]
    tunnel :
        local address:  44.44.44.44
        remote address : 44.44.44.45
    flow :
        as defined in acl 3001
    current Encrypt-card : None
```

表1-9 display ipsec tunnel 命令显示信息描述表

字段	描述
connection id	连接标识符，用来唯一地标识一个 IPsec Tunnel
perfect forward secrecy	完善的前向安全，标志 IKE 第二阶段快速模式使用哪个 DH 组
SA's SPI	出方向和入方向的安全策略索引
tunnel	IPsec 隧道端点的地址
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	IPsec 隧道保护 ACL 3001 中定义的所有数据流
current Encrypt-card	当前 Tunnel 使用的加密卡接口

1.1.11 encapsulation-mode

【命令】

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

undo encapsulation-mode

【视图】

安全提议视图

【缺省级别】

2：系统级

【参数】

transport：采用传输模式。

tunnel：采用隧道模式。

【描述】

encapsulation-mode 命令用来配置安全协议对 IP 报文的封装形式。**undo encapsulation-mode** 命令用来恢复缺省情况。

缺省情况下，安全协议采用隧道模式对 IP 报文进行封装。

若要配置应用于 IPv6 路由协议的手工安全策略，则该安全策略引用的安全提议仅支持传输模式的封装模式。

相关配置可参考命令 **ipsec proposal**。

【举例】

配置名为 prop2 的提议采用传输模式对 IP 报文进行封装。

```
<Sysname> system-view
[Sysname] ipsec proposal prop2
[Sysname-ipsec-proposal-prop2] encapsulation-mode transport
```

1.1.12 esp authentication-algorithm

【命令】

esp authentication-algorithm { **md5** | **sha1** }

undo esp authentication-algorithm

【视图】

安全提议视图

【缺省级别】

2：系统级

【参数】

md5：采用 MD5 认证算法，密钥长度 128 位。

sha1：采用 SHA-1 认证算法，密钥长度 160 位。

【描述】

esp authentication-algorithm 命令用来配置 ESP 协议采用的认证算法。**undo esp authentication-algorithm** 命令用来配置 ESP 协议不对报文进行认证。

缺省情况下，ESP 协议采用 MD5 认证算法。

相关配置可参考命令 **ipsec proposal**、**esp encryption-algorithm**、**proposal** 和 **transform**。

【举例】

配置提议 prop1 采用 ESP 协议并使用 SHA-1 认证算法。

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
```

```
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp authentication-algorithm sha1
```

1.1.13 esp encryption-algorithm

【命令】

esp encryption-algorithm { **3des** | **aes** [*key-length*] | **des** }

undo esp encryption-algorithm

【视图】

安全提议视图

【缺省级别】

2：系统级

【参数】

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

aes：指定安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128bits、192bits、256bits 的密钥进行加密。

key-length：AES 算法采用的密钥长度，取值可以为 128、192、256，缺省值为 128。采用 AES 算法时，此参数有效。

des：指定安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56bits 的密钥进行加密。

【描述】

esp encryption-algorithm 命令用来配置 ESP 协议采用的加密算法。**undo esp encryption-algorithm** 命令用来配置 ESP 协议不对报文进行加密。

缺省情况下，ESP 协议采用 DES 加密算法。

需要注意的是：

- 对于保密及安全性要求非常高的地方，采用 3DES 算法可以满足需要，但 3DES 加密速度比较慢；对于普通的安全要求，DES 算法就可以满足需要。
- ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。
- ESP 协议采用的加密算法和认证算法不能同时设置为空。当认证算法不为空时，**undo esp encryption-algorithm** 命令才起作用。

相关配置可参考命令 **ipsec proposal**、**esp authentication-algorithm**、**proposal** 和 **transform**。

【举例】

配置提议 prop1 采用 ESP 协议并使用 3DES 加密算法。

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp encryption-algorithm 3des
```

1.1.14 ike-peer (IPsec policy view/IPsec policy template view/IPsec profile view)

【命令】

ike-peer *peer-name*

undo ike-peer *peer-name*

【视图】

安全策略视图/安全策略模板视图/安全框架视图

【缺省级别】

2：系统级

【参数】

peer-name：IKE 对等体名，为 1～32 个字符的字符串。

【描述】

ike-peer 命令用来在 IKE 协商方式配置的安全策略、安全策略模板或者安全框架中引用 IKE 对等体。

undo ike peer 命令用来取消在安全策略、安全策略模板或者安全框架中引用 IKE 对等体。

相关配置可参考命令 **ipsec policy** 或 **ipsec profile**。

【举例】

配置在安全策略中引用 IKE 对等体。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-peer peer1
```

配置在安全框架中引用 IKE 对等体。

```
<Sysname> system-view
[Sysname] ipsec profile profile1
[Sysname-ipsec-profile- profile1] ike-peer peer1
```

1.1.15 ipsec anti-replay check

【命令】

ipsec anti-replay check

undo ipsec anti-replay check

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

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。

缺省情况下，IPsec 抗重放检测功能处于开启状态。

【举例】

开启 IPsec 抗重放检测。

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

1.1.16 ipsec anti-replay window

【命令】

ipsec anti-replay window *width*

undo ipsec anti-replay window

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

width：IPsec 抗重放窗口的宽度，可取的值为 32、64、128、256、512、1024。

【描述】

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。

缺省情况下，IPsec 抗重放窗口的宽度为 32。

需要注意的是，修改后的配置仅对于新协商成功的 IPsec SA 生效。

【举例】

配置 IPsec 抗重放窗口的宽度为 64。

```
<Sysname> system-view
[Sysname] ipsec anti-replay window 64
```

1.1.17 ipsec decrypt check

【命令】

ipsec decrypt check

undo ipsec decrypt check

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ipsec decrypt check 命令用来使能解封装后 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。

缺省情况下，解封装后 IPsec 报文的 ACL 检查功能处于使能状态。

【举例】

使能对解封装后 IPsec 报文的 ACL 检查功能。

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

1.1.18 ipsec invalid-spi-recovery enable

【命令】

ipsec invalid-spi-recovery enable

undo ipsec invalid-spi-recovery enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ipsec invalid-spi-recovery enable 命令用来使能 IPsec 无效 SPI（Security Parameter Index，安全参数索引）恢复功能。**undo ipsec invalid-spi-recovery enable** 命令用来恢复缺省情况。

缺省情况下，IPsec 无效 SPI 恢复功能处于关闭状态，将丢弃收到的无效 SPI 的 IPsec 报文。

使能了 IPsec 无效 SPI 恢复功能的接收端收到无效 SPI 的 IPsec 报文后，即根据报文中的 SPI 查找不到指定的 IPsec SA 时，则触发本端 IKE 向报文的源端发送 INVALID SPI NOTIFY 消息，通知源端删除此 SPI 对应的 SA，若源端后续还存在到本端的流量时，则可触发 IPsec 通信两端重建 SA。

【举例】

使能 IPsec 无效 SPI 恢复功能。

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

1.1.19 ipsec policy (interface view)

【命令】

ipsec policy *policy-name*

undo ipsec policy [*policy-name*]

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

policy-name：指定应用在接口上的安全策略组的名字，为 1～15 个字符的字符串。在系统视图下，必须已经配置了名字为 *policy-name* 的安全策略组。

【描述】

ipsec policy 命令用来在接口上应用指定的安全策略组。**undo ipsec policy** 命令用来从接口上取消应用的安全策略组，使此接口不再具有 IPsec 的安全保护功能。

需要注意的是：

- 在一个接口上，只能应用一个安全策略组。在一个接口上应用一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，从而能够对不同的数据流采用不同的安全联盟进行保护。如果要在接口上应用另一个安全策略组，必须先从接口上取消应用的安全策略组。一个安全策略组可应用到多个接口上。
- 当从一个接口发送报文时，将按照顺序号从小到大的顺序查找安全策略组中每一条安全策略。如果报文匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对报文进行处理；如果报文没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果报文对所有安全策略引用的访问控制列表都不匹配，则报文直接被发送（IPsec 不对报文加以保护）。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

在 Serial2/0/2 接口上应用名为 pg1 的安全策略组。

```
<Sysname> system-view
[Sysname] interface serial 2/0/2
[Sysname-Serial2/0/2] ipsec policy pg1
```

1.1.20 ipsec policy (system view)

【命令】

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

undo ipsec policy *policy-name* [*seq-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：安全策略的名字，为 1～15 个字符的字符串，不区分大小写，字符可以是英文字母或者数字或者其他特殊字符，如“!”、“@”、“#”、“$”、“%”、“^”、“&”等，不能包括减号“-”。

seq-number：安全策略的顺序号，取值范围为 1～65535。

isakmp：指定通过 IKE 协商建立安全联盟。

manual：指定用手工方式建立安全联盟。

【描述】

ipsec policy 命令用来创建一条安全策略，并进入安全策略视图。**undo ipsec policy** 命令用来删除指定的安全策略。

缺省情况下，没有任何安全策略存在。

需要注意的是：

- 使用此命令创建安全策略时，必须指定协商方式，但进入已创建的安全策略时，可以不指定协商方式。
- 不能修改已创建的安全策略的协商方式，只能先删除该安全策略，再重新创建。
- 具有相同名字的安全策略一起组成一个安全策略组。由名字和顺序号一起确定一条唯一的安全策略。在一个安全策略组中，顺序号 *seq-number* 越小的安全策略，优先级越高。
- 不带 *seq-number* 参数的 **undo** 命令用来删除一个安全策略组。

相关配置可参考命令 **ipsec policy** (Interface view)和 **display ipsec policy**。

【举例】

配置名字为 policy1，顺序号为 100，采用 IKE 方式协商安全联盟的安全策略。

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

配置名字为 policy1，顺序号为 101，采用手工方式建立安全联盟的安全策略。

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

1.1.21 ipsec policy isakmp template

【命令】

ipsec policy *policy-name seq-number* **isakmp template** *template-name*

undo ipsec policy *policy-name* [*seq-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：安全策略的名字，为 1～15 个字符的字符串，不区分大小写，字符可以是英文字母或者数字或者其他特殊字符，如“!”、“@”、“#”、“$”、“%”、“^”、“&”等，不能包括减号“-”。

seq-number：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*：指定被引用的安全策略模板的名字。

【描述】

ipsec policy isakmp template 命令用来引用安全策略模板创建一条安全策略，该安全策略由 IKE 协商建立安全联盟。**undo ipsec policy** 命令用来删除指定的安全策略。

需要注意的是：

- 不带 *seq-number* 参数的 **undo** 命令用来删除一个安全策略组；
- 在配置此命令前，必须已经创建策略模板。

相关配置可参考命令 **ipsec policy** (System view)和 **ipsec policy-template**。

【举例】

引用策略模板 temp1 创建名字为 policy2，顺序号为 200 的一条安全策略。

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

1.1.22 ipsec policy-template

【命令】

ipsec policy-template *template-name seq-number*

undo ipsec policy-template *template-name* [*seq-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

template-name：为安全策略模板的名字，为 1～41 个字符的字符串，不区分大小写，字符可以是英文字母或者数字或者其他特殊字符，如“!”、“@”、“#”、“$”、“%”、“^”、“&”等，不能包括减号“-”。

seq-number：为此安全策略模板的顺序号，取值范围为 1～65535。在一个安全策略模板中，顺序号越小的安全策略模板，优先级越高。

【描述】

ipsec policy-template 命令用来创建一个安全策略模板，并进入安全策略模板视图。**undo ipsec policy-template** 命令用来删除指定的一个安全策略模板。

缺省情况下，没有任何安全策略模板存在。

需要注意的是，不带 *seq-number* 参数的 **undo** 命令用来删除一个安全策略模板组。

相关配置可参考命令 **display ipsec policy-template**。

【举例】

创建一个模板名字为 template1，顺序号为 100 的安全策略模板。

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

1.1.23 ipsec profile (system view)

【命令】

ipsec profile *profile-name*

undo ipsec profile *profile-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

profile-name：安全框架的名称，为 1～15 个字符的字符串，不区分大小写。

【描述】

ipsec profile 命令用来创建一个安全框架，并进入安全框架视图。安全框架定义了对数据流进行 IPsec 保护所使用的安全提议，以及用于自动协商安全联盟所需要的 IKE 协商参数。**undo ipsec profile** 命令用于删除指定的安全框架。

缺省情况下，没有安全框架存在。

目前，安全框架只能应用于 DVPN 虚拟隧道接口和 IPsec 虚拟隧道接口下。

相关配置可参考命令 **ipsec profile** (Tunnel interface view)和 **display ipsec profile**。

【举例】

创建 IPsec 安全框架 profile1，并进入该 IPsec 安全框架视图。

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

1.1.24 ipsec profile (tunnel interface view)

【命令】

ipsec profile *profile-name*

undo ipsec profile

【视图】

Tunnel 接口视图

【缺省级别】

2：系统级

【参数】

profile-name：安全框架名称，为 1～15 个字符的字符串，不区分大小写。

【描述】

ipsec profile 命令用于在 IPsec 虚拟隧道接口上应用安全框架。**undo ipsec profile** 命令用于取消在 IPsec 虚拟隧道接口上应用安全框架。

缺省情况下， IPsec 虚拟隧道接口上没有引用任何安全框架，即不对隧道进行保护。

需要注意的是：

- 一个隧道接口上只能应用一个安全框架。
- 如果隧道接口上需要应用新的安全框架，则需要先取消当前应用的安全框架。

相关配置可参考命令 **ipsec profile** （System view）和“三层技术-IP 业务命令参考/隧道”中命令的 **interface tunnel**。

【举例】

在 IPsec 虚拟隧道接口上应用保护 IPsec 隧道的安全框架 vtiprofile。

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] tunnel-protocol ipsec ipv4
[Sysname-Tunnel0] ipsec profile vtiprofile
```

1.1.25 ipsec proposal

【命令】

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

proposal-name：指定安全提议的名字，为 1～32 个字符的字符串，不区分大小写。

【描述】

ipsec proposal 命令用来创建一个安全提议，并进入 IPsec 提议视图。**undo ipsec proposal** 命令用来删除指定的安全提议。

缺省情况下，没有任何安全提议存在。

需要注意的是，在使用该命令创建一个新的 IPsec 安全提议后，其缺省参数为采用 ESP 协议、DES 加密算法、MD5 认证算法。

相关配置可参考命令 **display ipsec proposal**。

【举例】

创建名为 newprop1 的安全提议。

```
<Sysname> system-view
[Sysname] ipsec proposal newprop1
```

1.1.26 ipsec sa global-duration

【命令】

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

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

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

seconds：指定基于时间的全局生存周期，取值范围为 180～604800，单位为秒。

kilobytes：指定基于流量的全局生存周期，取值范围为 2560～4294967295，单位为千字节。如果流量达到此值，则生存周期到期。

【描述】

ipsec sa global-duration 命令用来配置全局的安全联盟生存周期。**undo ipsec sa global-duration** 命令用来恢复缺省情况。

缺省情况下，安全联盟基于时间的全局生存周期为 3600 秒，基于流量的全局生存周期为 1843200 千字节。

需要注意的是：

- 当 IKE 协商安全联盟时，如果采用的安全策略或者安全框架没有配置自己的生存周期，将采用此命令所定义的全局生存周期与对端协商。如果安全策略或者安全框架配置了自己的生存周期，则系统使用安全策略或者安全框架自己的生存周期与对端协商。
- IKE 为 IPsec 协商建立安全联盟时，采用本地配置的生存周期和对端提议的生存周期中较小的一个。
- 安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **sa duration** 和 **display ipsec sa duration**。

【举例】

配置全局的安全联盟生存周期为 2 小时。

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

配置全局的安全联盟生存周期为：传输 10M 字节的流量后，当前的安全联盟即过期。

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

1.1.27 pfs

【命令】

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }

undo pfs

【视图】

安全策略视图/安全策略模板视图/安全框架视图

【缺省级别】

2：系统级

【参数】

dh-group1：指定使用 768-bit Diffie-Hellman 组。

dh-group2：指定使用 1024-bit Diffie-Hellman 组。

dh-group5：指定使用 1536-bit Diffie-Hellman 组。

dh-group14：指定使用 2048-bit Diffie-Hellman 组。

【描述】

pfs 命令用来配置使用此安全策略或安全框架发起协商时使用完善的前向安全（Perfect Forward Secrecy）特性。**undo pfs** 命令用来配置在协商时不使用 PFS 特性。

缺省情况下，安全策略或安全框架发起协商时没有使用 PFS 特性。

需要注意的是：

- 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**）安全性和需要的计算时间依次递减。
- 此命令使 IPsec 在使用此安全策略或安全框架发起一个协商时，在阶段 2 的协商中进行一次附加的密钥交换以提高通讯的安全性。
- 本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。
- 此命令仅在通过 IKE 方式建立安全联盟时才可以进行配置。

相关配置可参考命令 **ipsec policy-template**、**ipsec policy** (System view)和 **ipsec profile**(System view)。

【举例】

配置使用安全策略 policy1 进行协商时使用 PFS 特性。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 200 isakmp
[Sysname-ipsec-policy-isakmp-policy1-200] pfs dh-group1
```

1.1.28 policy enable

【命令】

policy enable

undo policy enable

【视图】

安全策略视图/安全策略模板视图

【缺省级别】

2：系统级

【参数】

无

【描述】

policy enable 命令用来使能安全策略。**undo policy enable** 命令用来去使能安全策略。

缺省情况下，安全策略处于使能状态。

需要注意的是：

- 本命令不适用于手工方式的安全策略；
- 如果 IKE 对等体未使能安全策略，则不能触发 IKE 协商或是作为响应方参与 IKE 协商。

相关配置可参考命令 **ipsec policy** (System view)和 **ipsec policy-template**。

【举例】

使能名字为 policy1，顺序号为 100 的安全策略。

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

1.1.29 proposal (IPsec policy view/ IPsec policy template view/ IPsec profile view)

【命令】

proposal *proposal-name*

undo proposal [*proposal-name*]

【视图】

安全策略视图/安全策略模板视图/安全框架视图

【缺省级别】

2：系统级

【参数】

proposal-name：所采用的提议名字，为 1～32 个字符的字符串。

【描述】

proposal 命令用来配置安全策略或安全框架所引用的提议。**undo proposal** 命令用来取消安全策略或安全框架引用的提议。

缺省情况下，安全策略或安全框架没有引用任何提议。

需要注意的是：

- 在使用此命令之前，必须已经配置了相应的安全提议。
- 如果安全策略是手工（**manual**）方式的，则安全策略在引用提议时只能指定一个安全提议。如果需要改变已配置好的安全提议，必须先使用命令 **undo proposal** 取消原先的安全提议，再配置新的安全提议。
- 如果安全策略是 IKE（**isakmp**）协商方式的，则一条安全策略最多可以引用六个安全提议，IKE 协商时将在安全策略中搜索能够完全匹配的安全提议。
- 一条安全框架最多可以引用六个安全提议，IKE 协商时将在安全框架中搜索能够完全匹配的安全提议。

相关配置可参考命令 **ipsec proposal**、**ipsec policy** (System view)和 **ipsec profile** (System view)。

【举例】

配置安全策略引用名字为 prop1 的安全提议。

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

配置安全框架引用名字为 prop2 的安全提议。

```
<Sysname> system-view
[Sysname] ipsec proposal prop2
[Sysname-ipsec-proposal-prop2] quit
[Sysname] ipsec profile profile1
[Sysname-ipsec-profile-profile1] proposal prop2
```

1.1.30 qos pre-classify

【命令】

qos pre-classify

undo qos pre-classify

【视图】

安全策略视图/安全策略模板视图

【缺省级别】

2：系统级

【参数】

无

【描述】

qos pre-classify 命令用来配置报文信息的预提取功能。**undo qos pre-classify** 命令用来恢复缺省情况。

缺省情况下，未配置报文信息的预提取功能。

QoS 预分类功能是指，在报文进行 IPsec 封装之前，QoS 根据原始 IP 头信息进行报文分类。

相关配置可参考命令 **ipsec policy** (System view) 和 **ipsec policy-template**。

【举例】

配置报文信息的预提取功能。

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

1.1.31 reset ipsec sa

【命令】

reset ipsec sa [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

parameters *dest-address protocol spi*：指定一个安全联盟所对应的目的 IP 地址、安全协议、SPI。*dest-address*：指定目的地址。

protocol：指定安全协议，可选关键字为 **ah** 或 **esp**，不区分大小写。

spi：指定安全参数索引，取值范围为 256～4294967295。

policy：指定安全策略或者安全框架。

policy-name：指定安全策略或者安全框架的名字，为 1～15 个字符的字符串，区分大小写，字符可以是英文字母或者数字。

seq-number：指定安全策略的顺序号，取值范围为 1～65535。如果不指定 *seq-number*，则是指名字为 *policy-name* 的安全策略组中所有安全策略。

remote *ip-address*：指定对端地址。

【描述】

reset ipsec sa 命令用来清除已经建立的安全联盟（无论是手工建立的还是通过 IKE 协商建立的）。如果不指定任何参数，则清除所有的安全联盟。

需要注意的是：

- 通过手工建立的安全联盟被清除后，系统会自动根据对应的手工安全策略建立新的安全联盟。
- 通过 IKE 协商建立的安全联盟被清除后，如果有报文重新触发 IKE 协商，IKE 将重新协商建立新的安全联盟。
- 如果指定了 **parameters** 关键字，由于安全联盟是成对出现的，清除了一个方向的安全联盟，另一个方向的安全联盟也会被清除。

相关配置可参考命令 **display ipsec sa**。

【举例】

清除所有安全联盟。

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

清除对端地址为 10.1.1.2 的安全联盟。

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

清除安全策略模板 policy1 中的所有安全联盟。

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

清除安全策略名字为 policy1、顺序号为 10 的安全联盟。

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

清除对端地址为 10.1.1.2、安全协议为 AH、安全参数索引为 10000 的安全联盟。

```
<Sysname> reset ipsec sa parameters 10.1.1.2 ah 10000
```

清除安全框架 policy1 中的所有安全联盟。

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

1.1.32 reset ipsec statistics

【命令】

reset ipsec statistics

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

无

【描述】

reset ipsec statistics 命令用来清除 IPsec 的报文统计信息，所有的统计信息都被设置成零。

相关配置可参考命令 **display ipsec statistics**。

【举例】

清除 IPsec 的报文统计信息。

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

1.1.33 reverse-route

【命令】

reverse-route [**remote-peer** *ip-address* [**gateway** | **static**] | **static**]

undo reverse-route

【视图】

安全策略视图/安全策略模板视图

【缺省级别】

2：系统级

【参数】

static：采用静态方式生成静态路由。若未指定本参数，则表示采用动态方式生成静态路由。该参数仅在安全策略视图下支持，安全策略模板下不支持。

remote-peer *ip-address*：指定静态路由的下一跳地址。手工指定下一跳地址的静态路由可用于实现路由备份或者负载分担。

gateway：表示利用静态路由的路由迭代功能，自动生成两条路由，一条路由的目的地址为对端私网，下一跳地址为隧道对端地址；另外一条路由的目的地址为隧道对端地址，下一跳地址为 *ip-address* 指定的地址，出接口为应用安全策略的接口。通常，在 IKE 协商方式的安全策略中指定该参数，可为受该安全策略保护的 IPsec 流量指定一条明确的缺省转发路径。

【描述】

reverse-route 命令用来开启 IPsec 反向路由注入功能。**undo reverse-route** 命令用来关闭反向路由注入功能。

缺省情况下，IPsec 反向路由注入功能处于关闭状态。

当本命令中指定关键字 **static** 时，即表示通过静态方式生成静态路由，生成的静态路由指向的目的 IP 地址和 IP 地址的掩码，均通过本策略应用的 ACL 来获取，下一跳可通过参数 *ip-address* 指定，不指定该参数的情况下为配置的隧道对端地址，具体情况如下：

- **reverse-route static** 命令用来根据本安全策略下引用的 ACL 的目的地址信息和对端安全网关地址静态生成路由：目的地址为 ACL 规则的目的地址，下一跳地址为安全策略视图下配置的 **tunnel remote** 地址（手工安全策略方式）或 IKE-Peer 视图下配置的 **remote-address** 地址（IKE 协商安全策略方式）。
- **reverse-route remote-peer** *ip-address* **static** 命令用来根据本安全策略策略下引用的 ACL 规则的目的地址信息和 *ip-address* 静态生成路由：目的地址为 ACL 规则的目的地址，下一跳地址为配置的 *ip-address*。

当本命令中不指定 **static** 关键字时，即表示通过动态方式来生成静态路由，生成的静态路由指向的目的 IP 地址和 IP 地址掩码从成功建立的 IPsec SA 中获取，下一跳通过参数 *ip-address* 配置或为从协商成功的 IPsec SA 中获取的隧道对端地址，若指定参数 **gateway** 的情况下，可根据 IPsec SA 生成两条路由，具体情况如下：

- **reverse-route** 命令用来自动生成一条路由：目的地址为受保护的对端私网，下一跳地址为对端隧道地址。
- **reverse-route remote-peer** *ip-address* 命令用来自动生成一条路由：目的地址为受保护的对端私网，下一跳地址为配置的 *ip-address*，该地址通常为应用本策略接口的下一跳地址。
- **reverse-route remote-peer** *ip-address* **gateway** 命令用来自动生成两条路由：一条路由的目的地址为受保护的对端私网网段，下一跳地址为隧道对端地址；另外一条路由的目的地址为隧道对端地址，下一跳地址为配置的 *ip-address*，出接口为应用安全策略的接口。

需要注意的是：

- 当配置（开启、关闭或修改）反向路由注入功能时，会删除本策略生成的或协商出的所有 IPsec SA。
- 由于静态方式生成静态路由，需要根据安全策略下引用的 ACL 中的目的地址信息生成，所以若选择通过静态方式生成静态路由，则安全策略下必须引用 ACL。
- 动态方式生成的静态路由随 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，关于路由表项的详细信息，请参见“三层技术-IP 路由配置指导”中的“IP 路由基础”。

相关配置可参考命令 **reverse-route preference** 和 **reverse-route tag**。

【举例】

根据 ACL 3000 的信息和对端安全网关地址静态生成静态路由，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] ike peer 1
[Sysname-ike-peer-1] remote-address 1.1.1.2
[Sysname-ike-peer-1] quit
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 2.0.0.0 0.0.0.255 destination 3.0.0.0
0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] security acl 3000
[Sysname-ipsec-policy-isakmp-1-1] ike-peer 1
[Sysname-ipsec-policy-isakmp-1-1] reverse-route static
[Sysname-ipsec-policy-isakmp-1-1] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipsec policy 1
[Sysname-GigabitEthernet1/0/1]quit
```

可立即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         GE1/0/1
```

根据 ACL 3000 的信息静态生成静态路由，目的地址为受保护的对端私网网段 3.0.0.0/24，下一跳地址为指定的 1.1.1.3。

```
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3 static
[Sysname-ipsec-policy-isakmp-1-1] quit
```

可立即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            1.1.1.3         GE1/0/1
```

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] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route
[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         GE1/0/1
```

根据协商成功的 IPsec SA 动态生成静态路由，且指定下一跳地址为 1.1.1.3。

```
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3
[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            1.1.1.3         GE1/0/1
```

根据协商成功的 IPsec SA 动态生成两条静态路由：一条路由的目的地址为受保护的对端私网网段 3.0.0.0/24，下一跳地址为隧道对端地址 1.1.1.2；另外一条路由的目的地址为隧道对端地址 1.1.1.2/32，下一跳地址为 1.1.1.3。

```
[Sysname]ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route remote-peer 1.1.1.3 gateway
```

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
```

```
1.1.1.2/32          Static 60   0           1.1.1.3         GE1/0/1
3.0.0.0/24          Static 60   0           1.1.1.2         GE1/0/1
```

1.1.34 reverse-route preference

【命令】

reverse-route preference *preference-value*

undo reverse-route preference

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

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

【描述】

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。

缺省情况下，IPsec 反向路由注入功能生成的静态路由的优先级为 60。

需要注意的是，若对静态路由优先级进行修改，则在静态工作机制下的反向路由注入功能会根据新的路由优先级重新生成静态路由，而在动态工作机制下的反向路由注入功能不会修改已生成的静态路由的优先级，修改后的路由优先级仅对新增的静态路由有效。

相关配置可参考命令 **reverse-route**。

【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
```

1.1.35 reverse-route tag

【命令】

reverse-route tag *tag-value*

undo reverse-route tag

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

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

【描述】

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，该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。**undo reverse-route tag** 命令用来恢复缺省情况。

缺省情况下，IPsec 反向路由注入功能生成的静态路由的 Tag 值为 0。

需要注意的是，若对静态路由 Tag 值进行修改，则在静态工作机制下的反向路由注入功能会根据新的路由 Tag 值重新生成静态路由，而在动态工作机制下的反向路由注入功能不会修改已生成的静态路由的 Tag 值，修改后的路由 Tag 值仅对新增的静态路由有效。

关于路由策略的详细介绍请参见“三层技术-IP 路由配置指导”中的“路由策略”。

相关配置可参考命令 **reverse-route**。

【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
```

1.1.36 sa authentication-hex

【命令】

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

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

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

inbound：入方向，IPsec 使用入方向安全联盟处理接收的报文。

outbound：出方向，IPsec 使用出方向安全联盟处理发送的报文。

ah：采用 AH 协议。

esp：采用 ESP 协议。

hex-key：指定安全联盟的认证密钥，以 16 进制格式输入。如果使用 MD5 算法，密钥长度为 16 个字节；如果使用 SHA1 算法，密钥长度为 20 个字节。

【描述】

sa authentication-hex 命令用来对配置安全联盟的认证密钥。**undo sa authentication-hex** 命令用来删除配置的安全联盟的认证密钥。

需要注意的是：

- 此命令仅用于 **manual** 方式的安全策略。
- 在配置 **manual** 方式的安全策略时，必须分别配置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

- 在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的密钥必须和对端的出方向安全联盟的密钥一样；本端的出方向安全联盟密钥必须和对端的入方向安全联盟的密钥一样。
- 对于要应用于 IPv6 路由协议的安全策略，还必须保证本端出方向 SA 的 SPI 和本端入方向 SA 的 SPI 一致。
- 在安全隧道的两端，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 16 进制方式输入密钥，则不能通讯。而且，任何一端出入方向的 SA 使用的密钥也应当以相同的方式输入。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置采用 AH 协议的入方向安全联盟的认证密钥为 0x112233445566778899aabbccddeeff00；出方向安全联盟的认证密钥为 0xaabbccddeeff001100aabbccddeeff00。

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

1.1.37 sa duration

【命令】

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

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

【视图】

安全策略视图/安全策略模板视图/安全框架视图

【缺省级别】

2：系统级

【参数】

seconds：指定基于时间的生存周期，取值范围为 180～604800，单位为秒。

kilobytes：指定基于流量的生存周期，取值范围为 2560～4294967295，单位为千字节。

【描述】

sa duration 命令用来为安全策略或者安全框架配置安全联盟的生存周期。**undo sa duration** 命令用来恢复缺省情况。

缺省情况下，安全策略或者安全框架的安全联盟生存周期为当前全局的安全联盟生存周期值。

需要注意的是：

- 当 IKE 协商安全联盟时，如果采用的安全策略或者安全框架没有配置自己的生存周期，将采用全局生存周期（通过命令 **ipsec sa global-duration** 设置）与对端协商。如果安全策略或者安全框架配置了自己的生存周期，则系统使用安全策略或者安全框架自己的生存周期与对端协商。

- IKE 为 IPsec 协商建立安全联盟时，采用本地配置的生存周期和对端提议的生存周期中较小的一个。
- 安全联盟的生存周期只对通过 IKE 协商的安全联盟起作用，而对通过手工方式建立的安全联盟不起作用。

相关配置可参考命令 **ipsec sa global-duration**、**ipsec policy** (System view)和 **ipsec profile** (System view)。

【举例】

配置安全策略 policy1 的安全联盟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
```

配置安全策略 policy1 的安全联盟生存周期为 20M 字节，即传输 20480 千字节的流量后，当前的安全联盟就过期。

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

配置安全框架 profile1 的安全联盟生存时间为两个小时，即 7200 秒。

```
<Sysname> system-view
[Sysname] ipsec profile profile1
[Sysname-ipsec-profile-profile1] sa duration time-based 7200
```

配置安全框架 profile1 的安全联盟生存周期为 20M 字节，即传输 20480 千字节的流量后，当前的安全联盟就过期。

```
<Sysname> system-view
[Sysname] ipsec profile profile1
[Sysname-ipsec-profile-profile1] sa duration traffic-based 20480
```

1.1.38 sa encryption-hex

【命令】

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

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

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

inbound：入方向，IPsec 使用入方向安全联盟处理接收的报文。

outbound：出方向，IPsec 使用出方向安全联盟处理发送的报文。

esp：采用 ESP 协议。

hex-key：指定安全联盟的加密密钥。以 16 进制格式输入，输入的密钥长度必须符合所采用的加密算法的要求：DES-CBC 算法，密钥长度为 8 个字节；3DES-CBC 算法，密钥长度为 24 个字节；

AES128-CBC 算法，密钥长度为 64 字节；AES128-CBC 算法，密钥长度为 16 字节；AES192-CBC 算法，密钥长度为 24 字节；AES256-CBC 算法，密钥长度为 42 字节。

【描述】

sa encryption-hex 命令用来配置安全联盟的加密密钥参数。**undo sa encryption-hex** 命令用来删除配置的安全联盟的加密密钥参数。

需要注意的是：

- 此命令仅用于 **manual** 方式的安全策略。
- 在配置安全策略时，必须分别配置 **inbound** 和 **outbound** 两个方向安全联盟的参数。
- 在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的加密密钥必须和对端的出方向安全联盟的加密密钥一样；本端的出方向安全联盟的加密密钥必须和对端的入方向安全联盟的加密密钥一样。
- 对于要应用于 IPv6 路由协议的安全策略，还必须保证本端出方向 SA 的 SPI 和本端入方向 SA 的 SPI 一致。
- 在安全隧道的两端，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 16 进制方式输入密钥，则不能通讯。而且，任何一端出入方向的 SA 使用的密钥也应当以相同的方式输入。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置采用 ESP 协议的入方向安全联盟的加密算法的密钥为 0x1234567890abcdef；出方向加密算法的密钥为 0xabcdefabcdef1234。

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

1.1.39 sa spi

【命令】

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

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

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

inbound：入方向，IPsec 使用入方向安全联盟处理接收的报文。

outbound：出方向，IPsec 使用出方向安全联盟处理发送的报文。

ah：采用 AH 协议。

esp：采用 ESP 协议。

spi-number：安全联盟三元组标识中的安全参数索引，取值范围为 256～4294967295。

【描述】

sa spi 命令用来配置安全联盟的安全参数索引参数。**undo sa spi** 命令用来删除配置的安全联盟的安全参数索引参数。

需要注意的是：

- 此命令仅用于 **manual** 方式的安全策略。
- 对于 **isakmp** 方式的安全策略，IKE 将自动协商安全联盟的参数并创建安全联盟，不需要手工设置安全联盟的参数。
- 在配置安全策略时，必须分别配置 **inbound** 和 **outbound** 两个方向安全联盟的参数。配置基于 ACL 的 IPsec 手工安全策略时，必须保证 SA 的唯一性，即不同 SA 对应不同的 SPI。
- 在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

在配置应用于 IPv6 路由协议的安全策略时，还需要注意的是：

- 本端出方向 SA 的 SPI 必须和本端入方向 SA 的 SPI 保持一致；
- 同一个范围内的，所有设备上的 SA 的 SPI 均要保持一致。该范围内容与协议相关：对于 OSPF，是 OSPF 邻居之间或邻居所在的区域；对于 RIPng，是 RIPng 直连邻居之间或邻居所在的进程；对于 BGP，是 BGP 邻居之间或邻居所在的一个组。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置入方向安全联盟的 SPI 为 10000，出方向安全联盟的 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
```

1.1.40 sa string-key

【命令】

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

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

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

inbound：入方向，IPsec 使用入方向安全联盟处理接收的报文。

outbound：出方向，IPsec 使用出方向安全联盟处理发送的报文。

ah：采用 AH 协议。

esp：采用 ESP 协议。

string-key：指定安全联盟的密钥，为 1～255 个字符的字符串。对不同的算法，均可输入不超过长度范围的字符串，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。

【描述】

sa string-key 命令用来配置安全联盟的密钥。**undo sa string-key** 命令用来删除配置的安全联盟的密钥。

需要注意的是：

- 此命令仅用于 **manual** 方式的安全策略。
- 在配置安全策略时，必须分别配置 **inbound** 和 **outbound** 两个方向安全联盟的参数。
- 在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端入方向安全联盟的密钥必须和对端出方向安全联盟的密钥一样；本端出方向安全联盟的密钥必须和对端入方向安全联盟的密钥一样。
- 在安全隧道的两端，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 16 进制方式输入密钥，则不能正确地建立安全隧道。

在配置应用于 IPv6 路由协议的安全策略时，还需要注意的是：

- 本端出方向 SA 的密钥必须和本端入方向 SA 的密钥保持一致；
- 同一个范围内的，所有设备上的 SA 的密钥均要保持一致。该范围内容与协议相关：对于 OSPF，是 OSPF 邻居之间或邻居所在的区域；对于 RIPng，是 RIPng 直连邻居之间或邻居所在的进程；对于 BGP，是 BGP 邻居之间或邻居所在的一个组。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置采用 AH 协议的入方向安全联盟的密钥为字符串 abcdef；出方向安全联盟的密钥为字符串 efcdab。

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

在要应用于 IPv6 路由协议的安全策略中，配置采用 AH 协议的入方向安全联盟的密钥为字符串 abcdef；出方向安全联盟的密钥为字符串 abcdef。

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

1.1.41 security acl

【命令】

security acl *acl-number* [**aggregation**]

undo security acl

【视图】

安全策略视图/安全策略模板视图

【缺省级别】

2：系统级

【参数】

acl-number：指定安全策略所引用的访问控制列表号，取值范围为 3000～3999。

aggregation：指定安全策略的数据流保护方式为聚合方式。如果不指定该参数，则安全策略的数据流保护方式为标准方式。

【描述】

security acl 命令用来配置安全策略引用的访问控制列表。**undo security acl** 命令用来取消安全策略引用的访问控制列表。

缺省情况下，安全策略没有指定访问控制列表。

配置 IKE 协商安全策略的情况下，安全策略的数据流保护方式包括以下两种：

- 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；
- 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。

需要注意的是，对于聚合方式和标准方式都支持的设备，要求两端的配置必须一致，即两端要么同时配置聚合方式，要么同时配置标准方式。聚合方式仅在一端设备使用的是 Comware V5 的软件版本，而另一端为 Comware V3 的软件版本时使用。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置安全策略引用 ACL 3001。

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-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-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

配置安全策略引用 ACL 3002，并设置数据流保护方式为聚合方式。

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

1.1.42 transform

【命令】

transform { **ah** | **ah-esp** | **esp** }

undo transform

【视图】

安全提议视图

【缺省级别】

2：系统级

【参数】

ah：采用 AH 协议。

ah-esp：先用 ESP 协议对报文进行保护，再用 AH 协议进行保护。

esp：采用 ESP 协议。

【描述】

transform 命令用来配置提议采用的安全协议。**undo transform** 命令用来恢复缺省情况。

缺省情况下，采用 ESP 协议。

需要注意的是：

- 如果采用 ESP 协议，则缺省的加密算法为 DES，认证算法为 MD5。
- 如果采用 AH 协议，则缺省的认证算法为 MD5。
- 如果指定参数 **ah-esp**，则 AH 缺省的认证算法为 MD5；ESP 协议缺省的加密算法为 DES，不使用认证算法。
- 在安全隧道的两端，IPsec 提议所使用的安全协议需要匹配。

相关配置可参考命令 **ipsec proposal**。

【举例】

配置一个采用 AH 协议的提议。

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform ah
```

1.1.43 tunnel local

【命令】

tunnel local *ip-address*

undo tunnel local

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

ip-address：本端地址。

【描述】

tunnel local 命令用来配置安全隧道的本端地址。**undo tunnel local** 命令用来删除在安全隧道中设定的本端地址。

缺省情况下，没有配置安全隧道的本端地址。

需要注意的是：

- 仅用于 manual 方式的安全策略。
- 如果没有设置本端地址，本端地址将采用安全策略应用的接口地址。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置安全隧道的本端地址为 Loopback0 的地址 10.0.0.1。

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address  10.0.0.1 32
[Sysname-LoopBack0] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] tunnel local 10.0.0.1
```

1.1.44 tunnel remote

【命令】

tunnel remote *ip-address*

undo tunnel remote [*ip-address*]

【视图】

安全策略视图

【缺省级别】

2：系统级

【参数】

ip-address：安全策略的隧道对端地址。

【描述】

tunnel remote 命令用来配置安全隧道的对端地址。**undo tunnel remote** 命令用来删除安全隧道的对端地址。

缺省情况下，没有配置安全隧道的对端地址。

需要注意的是：

- 仅用于 manual 方式的安全策略；
- 设置新的对端地址将会覆盖已经设置的对端地址；
- 安全隧道是建立在本端和对端之间，在安全隧道的两端，当前端点的对端地址需要与对端的本端地址保持一致。

相关配置可参考命令 **ipsec policy** (System view)。

【举例】

配置安全策略的对端地址为 10.1.1.2。

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

2 IKE配置命令

2.1 IKE配置命令

2.1.1 authentication-algorithm

【命令】

authentication-algorithm { **md5** | **sha** }

undo authentication-algorithm

【视图】

IKE 提议视图

【缺省级别】

2：系统级

【参数】

md5：指定认证算法为 HMAC-MD5。

sha：指定认证算法为 HMAC-SHA1。

【描述】

authentication-algorithm 命令用来指定一个供 IKE 提议使用的认证算法。**undo authentication-algorithm** 命令用来恢复缺省情况。

缺省情况下，IKE 提议使用 SHA1 认证算法。

相关配置可参考命令 **ike proposal** 和 **display ike proposal**。

【举例】

指定 IKE 提议 10 的认证算法为 MD5。

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-algorithm md5
```

2.1.2 authentication-method

【命令】

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

undo authentication-method

【视图】

IKE 提议视图

【缺省级别】

2：系统级

【参数】

pre-share：指定认证方法为预共享密钥方法。

rsa-signature：指定认证方法为 RSA 数字签名方法。

【描述】

authentication-method 命令用来指定一个供 IKE 提议使用的认证方法。**undo authentication-method** 命令用来恢复缺省情况。

缺省情况下，IKE 提议使用预共享密钥的认证方法。

相关配置可参考命令 **ike proposal** 和 **display ike proposal**。

【举例】

指定 IKE 提议 10 的认证方法为预共享密钥。

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-method pre-share
```

2.1.3 certificate domain

【命令】

certificate domain *domain-name*

undo certificate domain

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

domain-name：指定的 PKI 域名称，为 1～15 个字符的字符串。

【描述】

certificate domain 命令用来配置 IKE 协商采用数字签名认证时，证书所属的 PKI 域。**undo certificate domain** 命令用来取消配置证书所属的 PKI 域。

相关配置可参考命令 **authentication-method**，以及“安全命令参考/PKI”中的命令 **pki domain**。

【举例】

配置 IKE 协商所使用的 PKI 域为 abcde。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] certificate domain abcde
```

2.1.4 dh

【命令】

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

undo dh

【视图】

IKE 提议视图

【缺省级别】

2：系统级

【参数】

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

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

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

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

【描述】

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。

缺省情况下，IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数为 **group1**，即 768-bit 的 Diffie-Hellman 组。

相关配置可参考命令 **ike proposal** 和 **display ike proposal**。

【举例】

指定 IKE 提议 10 使用 768-bit 的 Diffie-Hellman 组。

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] dh group1
```

2.1.5 display ike dpd

【命令】

display ike dpd [*dpd-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

dpd-name：指定 DPD 的名字，为 1～15 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ike dpd 命令用来显示 DPD 配置的参数。

如果不指定参数 *dpd-name*，将显示所有 DPD 配置的参数。

相关配置可参考命令 **ike dpd**。

【举例】

显示 DPD 配置的参数。

```
<Sysname> display ike dpd

---------------------------
 IKE dpd: dpd1
   references: 1
   interval-time: 10
   time_out: 5
---------------------------
```

表2-1 display ike dpd 命令显示信息描述表

字段	描述
references	引用该 DPD 配置的 IKE 对等体的个数
Interval-time	经过多长时间没有从对端收到 IPsec 报文则触发 DPD，单位为秒
time_out	DPD 报文的重传时间间隔，单位为秒

2.1.6 display ike peer

【命令】

display ike peer [*peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

peer-name：IKE 对等体名，为 1～15 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ike peer 命令用来显示 IKE 对等体配置的参数。

相关配置可参考命令 **ike peer**。

【举例】

显示 IKE 对等体配置的参数信息。

```
<Sysname> display ike peer

---------------------------
 IKE Peer: rtb4tunn
   exchange mode: main on phase 1
   pre-shared-key simple 123
   peer id type: ip
   peer ip address: 44.44.44.55
   local ip address:
   peer name:
   nat traversal: disable
   dpd: dpd1
---------------------------
```

表2-2 display ike peer 命令显示信息描述表

字段	描述
exchange mode	IKE 第一阶段的协商模式
pre-shared-key	IKE 第一阶段协商所使用的预共享密钥
peer id type	IKE 第一阶段的协商过程中使用 ID 的类型
peer ip address	对端安全网关的 IP 地址
local ip address	本端安全网关的 IP 地址
peer name	对端安全网关的名字
nat traversal	是否启动 IPsec/IKE 的 NAT 穿越功能
dpd	对等体存活检测的名称

2.1.7 display ike proposal

【命令】

display ike proposal [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ike proposal 命令用来显示所有 IKE 提议配置的参数。

IKE 提议按照优先级的先后顺序显示。

相关配置可参考命令 **authentication-method**、**ike proposal**、**encryption-algorithm**、**authentication-algorithm**、**dh** 和 **sa duration**。

【举例】

显示 IKE 提议配置的参数信息。

```
<Sysname> display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
 10       PRE_SHARED     SHA            DES_CBC     MODP_1024      5000
 11       PRE_SHARED     MD5            DES_CBC     MODP_768       50000
 default  PRE_SHARED     SHA            DES_CBC     MODP_768       86400
```

表2-3 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
authentication algorithm	IKE 提议使用的认证算法
encryption algorithm	IKE 提议使用的加密算法
Diffie-Hellman group	IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数
duration (seconds)	IKE 提议的 ISAKMP SA 存活时间（秒）

2.1.8 display ike sa

【命令】

display ike sa [**verbose** [**connection-id** *connection-id* | **remote-address** *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

verbose：显示当前 IKE SA 的详细信息。

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：按照对端地址显示 IKE SA 的详细信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ike sa 命令用来显示当前 IKE SA 的信息。

需要注意的是，若不选择任何参数则显示当前 IKE SA 的摘要信息。

相关配置可参考命令 **ike proposal** 和 **ike peer**。

【举例】

显示当前 IKE SA 的摘要信息。

```
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  -----------------------------------------------------------
      1            202.38.0.2      RD|ST        1      IPSEC
      2            202.38.0.2      RD|ST        2      IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO--TIMEOUT
```

表2-4 display ike sa 命令显示信息描述表

字段	描述
total phase-1 SAs	所有第一阶段安全联盟的总数
connection-id	ISAKMP SA 的标识符
peer	此安全联盟的对端的 IP 地址
flag	显示此安全联盟的状态： ● RD（READY）：表示此安全联盟已建立成功 ● ST（STAYALIVE）：表示此端是隧道协商发起方 ● RL（REPLACED）：表示此隧道已经被新的隧道代替，一段时间后将被删除 ● FD（FADING）：表示此隧道已发生过一次软超时，目前还在使用，在硬超时发生时，会删除此隧道 ● TO（TIMEOUT）：表示此安全联盟在上次 keepalive 超时发生后还没有收到 keepalive 报文，如果在下次 keepalive 超时发生时仍没有收到 keepalive 报文，此安全联盟将被删除
phase	此安全联盟所属阶段： ● Phase 1：建立安全隧道进行通信的阶段，此阶段建立 ISAKMP SA ● Phase 2：协商安全服务的阶段，此阶段建立 IPsec SA
doi	安全联盟所属解释域

显示当前 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose
    ----------------------------------------------
    connection id: 2
    vpn-instance: 1
    transmitting entity: initiator
    ----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 86379
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

按照连接标识符显示 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose connection-id 2
    ----------------------------------------------
    connection id: 2
    vpn-instance: vpn1
    transmitting entity: initiator
    ----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82480
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

按照对端地址显示 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
    ----------------------------------------------
    connection id: 2
    vpn-instance: vpn1
    transmitting entity: initiator
    ----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82236
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

表2-5 display ike sa verbose 命令显示信息描述表

字段	描述
connection id	ISAKMP SA 的标识符
vpn-instance	被保护数据所属的 MPLS L3VPN
transmitting entity	IKE 协商中的实体
local ip	本端安全网关的 IP 地址
local id type	本端安全网关的 ID 类型
local id	本端安全网关的 ID
remote ip	对端安全网关的 IP 地址
remote id type	对端安全网关的 ID 类型
remote id	对端安全网关的 ID
authentication-method	IKE 提议使用的认证方法
authentication-algorithm	IKE 提议使用的认证算法
encryption-algorithm	IKE 提议使用的加密算法
life duration(sec)	ISAKMP SA 的生命周期（秒）
remaining key duration(sec)	ISAKMP SA 的剩余生命周期（秒）

字段	描述
exchange-mode	IKE 第一阶段的协商模式
diffie-hellman group	IKE 第一阶段密钥协商时所使用的 DH 密钥交换参数
nat traversal	是否使能 NAT 穿越功能

2.1.9 dpd

【命令】

dpd *dpd-name*

undo dpd

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

dpd-name：指定 DPD 的名字，为 1～32 个字符的字符串。

【描述】

dpd 命令用来为 IKE 对等体应用一个 DPD。**undo dpd** 命令用来取消 IKE 对等体对 DPD 的应用。缺省情况下，IKE 对等体没有应用 DPD。

【举例】

为对等体 peer1 应用名称为 dpd1 的 DPD。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] dpd dpd1
```

2.1.10 encryption-algorithm

【命令】

encryption-algorithm { **3des-cbc** | **aes-cbc** [*key-length*] | **des-cbc** }

undo encryption-algorithm

【视图】

IKE 提议视图

【缺省级别】

2：系统级

【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 bits 的密钥进行加密。

aes-cbc：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 bits、192bits、256bits 的密钥进行加密。

key-length：AES 算法采用的密钥长度，取值可以为 128、192、256，缺省值为 128。

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 bits 的密钥进行加密。

【描述】

encryption-algorithm 命令用来指定一个供 IKE 提议使用的加密算法。**undo encryption-algorithm** 命令用来恢复缺省情况。

缺省情况下，IKE 提议使用 CBC 模式的 56-bit DES 加密算法。

相关配置可参考命令 **ike proposal** 和 **display ike proposal**。

【举例】

指定 IKE 提议 10 的加密算法为 CBC 模式的 56-bit DES。

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] encryption-algorithm des-cbc
```

2.1.11 exchange-mode

【命令】

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

undo exchange-mode

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

aggressive：野蛮模式。

main：主模式。

【描述】

exchange-mode 命令用来选择 IKE 阶段的协商模式。**undo exchange-mode** 命令用来恢复缺省情况。

缺省情况下，IKE 阶段的协商模式使用主模式。

需要注意的是，当安全隧道一端的 IP 地址为自动获取时（如一端用户为拨号方式），则协商模式必须配置为 **aggressive**。这种情况下，只要建立安全联盟时使用的用户名和密码正确，就可以建立安全联盟。

相关配置可参考命令 **id-type**。

【举例】

配置 IKE 使用主模式。

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

```
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] exchange-mode main
```

2.1.12 id-type

【命令】

id-type { **ip** | **name** | **user-fqdn** }

undo id-type

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

ip：选择 IP 地址作为 IKE 协商过程中使用的 ID。

name：选择 FQDN（Fully Qualified Domain Name，完全合格域名）类型的名字作为 IKE 协商过程中使用的 ID。

user-fqdn：选择 User FQDN 类型的名字作为 IKE 协商过程中使用的 ID。

【描述】

id-type 命令用来选择 IKE 协商过程中使用的 ID 的类型。**undo id-type** 命令用来恢复缺省情况。

缺省情况下，使用 IP 地址作为 IKE 协商过程中使用的 ID。

需要注意的是：

- 在预共享密钥认证的主模式下，只能使用 IP 地址类型的身份进行 IKE 协商，建立安全联盟。
- 在 IKE 野蛮模式下，不但可以使用 IP 地址类型的身份进行协商，也可以使用 FQDN 或者 User FQDN 类型的身份进行 IKE 协商，并建立安全联盟。
- 若选择使用 FQDN 类型的 ID，为保证 IKE 协商成功，建议本端网关的名称配置为不携带@字符的字符串，例如 foo.bar.com。
- 若选择使用 User FQDN 类型的 ID，为保证 IKE 协商成功，建议本端网关的名称配置为携带@字符的字符串，例如 test@foo.bar.com。

相关配置可参考命令 **local-name**、**ike local-name**、**remote-name**、**remote-address**、**local-address** 和 **exchange-mode**。

【举例】

配置使用名字作为 IKE 协商过程中使用的 ID。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] id-type name
```

2.1.13 ike dpd

【命令】

ike dpd *dpd-name*

undo ike dpd *dpd-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dpd-name：指定 DPD 的名字，为 1～32 个字符的字符串。

【描述】

ike dpd 命令用来创建一个 DPD，并进入 DPD 视图。**undo ike dpd** 命令用来删除指定名字的 DPD 配置。

【举例】

创建一个名称为 dpd2 的 DPD。

```
<Sysname> system-view
[Sysname] ike dpd dpd2
```

2.1.14 ike local-name

【命令】

ike local-name *name*

undo ike local-name

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

name：指定 IKE 协商时的本端安全网关的名字，为 1～32 个字符的字符串，区分大小写。

【描述】

ike local-name 命令用来配置本端安全网关的名字。**undo ike local-name** 命令用来恢复缺省情况。

缺省情况下，使用设备名作为本端安全网关的名字。

当 IKE 协商的发起端使用安全网关名字进行协商时（即配置了 **id-type name** 或 **id-type user-fqdn**），发起端需要配置本端安全网关的名字，该名字既可以在系统视图下进行配置（使用命令 **ike local-name**），也可以在 IKE 对等体视图下配置（使用命令 **local-name**），若两个视图下都配置了本端安全网关的名字，则采用 IKE 对等体视图下的配置。

在 IKE 协商过程中，发起端会将本端安全网关的名字发送给对端来标识自己的身份，而响应端使用配置的对端安全网关的名字（使用命令 **remote-name**）来认证发起端，故此时响应端上配置的对端安全网关的名字应与发起端上所配的本端安全网关的名字保持一致。

相关配置可参考命令 **remote-name** 和 **id-type**。

【举例】

为 IKE 配置本端安全网关的名字为 app。

```
<Sysname> system-view
[Sysname] ike local-name app
```

2.1.15 ike next-payload check disabled

【命令】

ike next-payload check disabled

undo ike next-payload check disabled

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ike next-payload check disabled 命令用来配置在 IKE 协商过程中取消对最后一个 payload 的 next payload 域的检查，以便与某些公司的产品互通。**undo ike next-payload check disabled** 命令用来恢复缺省情况。

缺省情况下，在 IKE 协商过程中对 next payload 域进行检查。

【举例】

配置在 IKE 协商过程中取消对最后一个 payload 的 next payload 域的检查。

```
<Sysname> system-view
[Sysname] ike next-payload check disabled
```

2.1.16 ike peer (system view)

【命令】

ike peer *peer-name*

undo ike peer *peer-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

peer-name：IKE 对等体名，为 1～32 个字符的字符串。

【描述】

ike peer 命令用来创建一个 IKE 对等体，并进入 IKE-Peer 视图。**undo ike peer** 命令用来删除一个 IKE 对等体。

【举例】

创建 IKE 对等体为 peer1，并进入 IKE-Peer 视图。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1]
```

2.1.17 ike proposal

【命令】

ike proposal *proposal-number*

undo ike proposal *proposal-number*

【视图】

系统视图

【缺省级别】

2：系统级

【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。在进行 IKE 协商的时候，会从序号最小的 IKE 提议进行匹配，如果匹配则直接使用，否则继续查找。

【描述】

ike proposal 命令用来创建 IKE 提议，并进入 IKE 提议视图。**undo ike proposal** 命令用来删除一个 IKE 提议。

缺省情况下，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。缺省的提议具有缺省的参数，包括：

- 加密算法：DES-CBC
- 认证算法：HMAC-SHA1
- 认证方法：预共享密钥
- DH 组标识：MODP_768
- 安全联盟的存活时间：86400 秒

相关配置可参考命令 **display ike proposal**。

【举例】

创建 IKE 提议 10，并进入 IKE 提议视图。

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

2.1.18 ike sa keepalive-timer interval

【命令】

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

seconds：指定通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔，取值范围为 20～28800，单位为秒。

【描述】

ike sa keepalive-timer interval 命令用来配置 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。**undo ike sa keepalive-timer interval** 命令用来取消该功能。

缺省情况下，ISAKMP SA 不向对端发送 Keepalive 报文。

需要注意的是，本端配置的 Keepalive 报文的发送时间间隔应小于对端等待 Keepalive 报文的超时时间。

相关配置可参考命令 **ike sa keepalive-timer timeout**。

【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 sa keepalive-timer interval 200
```

2.1.19 ike sa keepalive-timer timeout

【命令】

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

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

【描述】

ike sa keepalive-timer timeout 命令用来配置 ISAKMP SA 等待 Keepalive 报文的超时时间。**undo ike sa keepalive-timer timeout** 命令用来使此功能失效。

缺省情况下，ISAKMP SA 不向对端发送 Keepalive 报文。

需要注意的是，本端配置的 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 Keepalive 报文的发送时间间隔的三倍。

相关配置可参考命令 **ike sa keepalive-timer interval**。

【举例】

配置本端等待对端发送 Keepalive 报文的超时时间为 20 秒。

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

2.1.20 ike sa nat-keepalive-timer interval

【命令】

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

seconds：指定 ISAKMP SA 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。

【描述】

ike sa nat-keepalive-timer interval 命令用来配置 ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔。**undo ike sa nat-keepalive-timer interval** 命令用来使此功能失效。

缺省情况下，ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔为 20 秒。

【举例】

配置 ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔为 5 秒。

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

2.1.21 interval-time

【命令】

interval-time *interval-time*

undo interval-time

【视图】

IKE-DPD 视图

【缺省级别】

2：系统级

【参数】

interval-time：指定经过多长时间没有从对端收到 IPsec 报文，则触发 DPD，取值范围为 1～300，单位为秒。

【描述】

interval-time 命令用来为 IKE DPD 配置触发 DPD 的时间间隔。**undo interval-time** 命令用来恢复缺省情况。

缺省情况下，触发 DPD 的时间间隔为 10 秒。

【举例】

为 dpd2 配置触发 DPD 的时间间隔为 1 秒。

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] interval-time 1
```

2.1.22 local

【命令】

local { **multi-subnet** | **single-subnet** }

undo local

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

local 命令用来配置 IKE 协商时本端安全网关的子网类型。**undo local** 命令用来恢复缺省情况。

缺省情况下，为单子网类型。

本命令用于与 NETSCREEN 设备互通时使用。

【举例】

配置 IKE 协商时本端安全网关的子网类型为多子网类型。

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local multi-subnet
```

2.1.23 local-address

【命令】

local-address *ip-address*

undo local-address

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

ip-address：IKE 协商时的本端安全网关的 IP 地址。

【描述】

local-address 命令用来配置 IKE 协商时的本端安全网关的 IP 地址。**undo local-address** 命令用来取消本端安全网关的 IP 地址。

缺省情况下，IKE 协商时的本端安全网关 IP 地址使用应用安全策略的接口的主地址。只有当用户需要指定特殊的本端安全网关地址时才需要配置此命令。

【举例】

配置本端安全网关 IP 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local-address 1.1.1.1
```

2.1.24 local-name

【命令】

local-name *name*

undo local-name

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

name：IKE 协商时的本端安全网关的名字，为 1～32 个字符的字符串，区分大小写。

【描述】

ike local-name 命令用来配置本端安全网关的名字。**undo ike local-name** 命令用来恢复缺省情况。

缺省情况下，未定义本端安全网关的名字，使用系统视图下本端安全网关的名字。

当 IKE 协商的发起端使用安全网关名字进行协商时（即配置了 **id-type name** 或 **id-type user-fqdn**），发起端需要配置本端安全网关的名字，该名字既可以在系统视图下进行配置（使用命令 **ike local-name**），也可以在 IKE 对等体视图下配置（使用命令 **local-name**），若两个视图下都配置了本端安全网关的名字，则采用 IKE 对等体视图下的配置。

在 IKE 协商过程中，发起端会将本端安全网关的名字发送给对端来标识自己的身份，而响应端使用配置的对端安全网关的名字（使用命令 **remote-name**）来认证发起端，故此时响应端上配置的对端安全网关的名字应与发起端上所配的本端安全网关的名字保持一致。

相关配置可参考命令 **remote-name** 和 **id-type**。

【举例】

为 IKE 对等体 peer1 配置本端安全网关的名字为 localgw。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] local-name localgw
```

2.1.25 nat traversal

【命令】

nat traversal

undo nat traversal

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

无

【描述】

nat traversal 命令用来配置 IPsec/IKE 的 NAT 穿越功能。**undo nat traversal** 命令用来取消 IPsec/IKE 的 NAT 穿越功能。

缺省情况下，没有配置 NAT 穿越功能。

【举例】

为 IKE 对等体 peer1 配置 NAT 穿越功能。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] nat traversal
```

2.1.26 peer

【命令】

peer { **multi-subnet** | **single-subnet** }

undo peer

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

multi-subnet：指定多子网类型。

single-subnet：指定单子网类型。

【描述】

peer 命令用来配置 IKE 协商时对端安全网关的子网类型。**undo peer** 命令用来恢复缺省情况。

缺省情况下，为单子网类型。

本命令用于与 NETSCREEN 设备互通时使用。

【举例】

配置 IKE 协商时对端安全网关的子网类型为多子网类型。

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] peer multi-subnet
```

2.1.27 pre-shared-key

【命令】

pre-shared-key [**cipher** | **simple**] *key*

undo pre-shared-key

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

key：指定以密文方式显示的明文预共享密钥，为 1～128 个字符的字符串，区分大小写。

cipher *key*：指定以密文方式显示的预共享密钥。其中，*key* 表示密文的预共享密钥，为 1～184 个字符的字符串，区分大小写。

simple *key*：指定以明文方式显示的预共享密钥。其中，*key* 表示明文的预共享密钥，为 1～128 个字符的字符串，区分大小写。

【描述】

pre-shared-key 命令用来配置 IKE 协商采用预共享密钥认证时，所使用的预共享密钥，**undo pre-shared-key** 命令用来取消 IKE 协商所使用的预共享密钥。

相关配置可参考命令 **authentication-method**。

【举例】

配置 IKE 协商所使用的预共享密钥为 abcde。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key abcde
```

2.1.28 proposal (IKE peer view)

【命令】

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

undo proposal [*proposal-number*]

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

proposal-number&<1-6>：IKE 安全提议序号，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。

【描述】

proposal 命令用来配置 IKE 对等体引用的 IKE 安全提议。**undo proposal** 命令用来取消指定的或所有引用的 IKE 安全提议。

缺省情况下，IKE 对等体未引用任何 IKE 安全提议，使用系统视图下已配置的 IKE 安全提议进行 IKE 协商。

IKE 第一阶段的协商过程中，如果本端引用了指定的 IKE 安全提议，那么就使用指定的安全提议与对端进行协商；如果没有指定，则使用系统视图下已配置的 IKE 安全提议与对端进行协商。

需要注意的是：

- 一个 IKE 对等体中最多可以引用六个 IKE 安全提议。
- IKE 协商中的响应方使用系统视图下已经配置的安全提议与对端发送的安全提议进行协商。

相关配置可参考命令 **ike proposal** 和 **ike peer** (System view)。

【举例】

设置 IKE 对等体 peer1 引用序号为 10 的 IKE 安全提议。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] proposal 10
```

2.1.29 remote-address

【命令】

remote-address { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }

undo remote-address

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

hostname：IPsec 对端安全网关的主机名，为 1～255 个字符的字符串，不区分大小写。该主机名是 IPsec 对端在网络中的唯一标识，可被 DNS 服务器解析为 IP 地址。

dynamic：表示 IPsec 对端安全网关的主机名会进行动态地址解析。如果不配置该参数，则表示仅在配置对端主机名后执行一次 DNS 查询。

low-ip-address：IPsec 对端安全网关的 IP 地址。如果配置对端安全网关 IP 地址为连续的地址范围，则该参数为地址范围中的最小地址。

high-ip-address：如果配置对端安全网关 IP 地址为连续的地址范围，则该参数为地址范围中的最大地址。

【描述】

remote-address 命令用来配置 IPsec 对端安全网关的 IP 地址。**undo remote-address** 命令用来删除 IPsec 对端安全网关的 IP 地址。

需要注意的是：

- 本端通过命令 **remote-address** 配置的对端安全网关的 IP 地址，应该与对端 IKE 协商时使用的本端安全网关的 IP 地址一致（可通过 **local-address** 命令配置，若不配置，则为应用安全策略的接口的主地址）。
- 如果配置对端地址为精确值（主机名方式与之等价），则本端可以作为 IKE 协商的发起端；如果配置对端地址为一个地址范围，则本端只能作为响应方，而这个范围表示的是本端能接受的协商对象的地址范围。
- 如果对端地址经常变动，建议配置对端主机名时采用 **dynamic** 参数，以便本端在 IKE 协商协商时及时更新对端地址。

相关配置可参考命令 **id-type ip** 和 **local-address**。

【举例】

配置对端安全网关 IP 地址为 10.0.0.1。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-address 10.0.0.1
```

配置对端安全网关地址为 test.com，并采用动态更新方式。

```
<Sysname> system-view
[Sysname] ike peer peer2
[Sysname-ike-peer-peer2] remote-address test.com dynamic
```

2.1.30 remote-name

【命令】

remote-name *name*

undo remote-name

【视图】

IKE-Peer 视图

【缺省级别】

2：系统级

【参数】

name：指定 IKE 协商时对端的名字，为 1～32 字符的字符串。

【描述】

remote-name 命令用来配置对端安全网关的名字。**undo remote-name** 命令用来取消对端安全网关名称的配置。

当 IKE 协商的发起端使用安全网关名字进行协商时（即配置了 **id-type name** 或 **id-type user-fqdn**），发起端会发送自己名字给对端来标识自己的身份，而对端使用 **remote-name** *name* 来认证发起端，故此时 *name* 应与发起端上令所配的本端安全网关的名字保持一致。

相关配置可参考命令 **id-type**、**local-name** 和 **ike local-name**。

【举例】

为 IKE 对等体 peer1 配置对端安全网关名字为 apple。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-name apple
```

2.1.31 reset ike sa

【命令】

reset ike sa [*connection-id*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

connection-id：指定要清除的安全隧道的连接 ID 号，取值范围为 1～2000000000。

【描述】

reset ike sa 命令用来清除 IKE 建立的安全隧道。

需要注意的是：

- 如果未指定 *connection-id*，所有阶段 1 的安全联盟（ISAKMP SA）都会被清除。
- 清除本地的 IPsec SA 时，如果相应的 ISAKMP SA 还存在，将在此 ISAKMP SA 的保护下，向对端发送删除消息，通知对方清除相应的 IPsec SA。
- 如果先清除 ISAKMP SA，那么再清除本地 IPsec SA 时，就无法通知对端清除相应的 IPsec SA。

相关配置可参考命令 **display ike sa**。

【举例】

清除一个到 202.38.0.2 的安全隧道。

```
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------
      1            202.38.0.2      RD|ST       1       IPSEC
      2            202.38.0.2      RD|ST       2       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO--TIMEOUT
<Sysname> reset ike sa 2
<Sysname> display ike sa
    total phase-1 SAs:  1
```

```
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------
      1            202.38.0.2      RD|ST       1       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD—FADING TO—TIMEOUT
```

2.1.32 sa duration

【命令】

sa duration *seconds*

undo sa duration

【视图】

IKE 提议视图

【缺省级别】

2：系统级

【参数】

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

【描述】

sa duration 命令用来指定一个 IKE 提议的 ISAKMP SA 存活时间，超时后 ISAKMP SA 将自动更新。**undo sa duration** 命令用来恢复缺省情况。

缺省情况下，IKE 提议的 ISAKMP SA 存活时间为 86400 秒。

在设定的存活时间超时前，会提前协商另一个安全联盟来替换旧的安全联盟。在新的安全联盟还没有协商完之前，依然使用旧的安全联盟；在新的安全联盟建立后，将立即使用新的安全联盟，而旧的安全联盟在存活时间超时后，被自动清除。

相关配置可参考命令 **ike proposal** 和 **display ike proposal**。

【举例】

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

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] sa duration 600
```

2.1.33 time-out

【命令】

time-out *time-out*

undo time-out

【视图】

IKE-DPD 视图

【缺省级别】

2：系统级

【参数】

time-out：指定 DPD 报文的重传时间间隔，取值范围为 1～60，单位为秒。

【描述】

time-out 命令用来为 IKE DPD 配置 DPD 报文的重传时间间隔。**undo time-out** 命令用来恢复缺省情况。

缺省情况下，DPD 报文的重传时间间隔为 5 秒。

【举例】

配置 dpd2 的 DPD 报文重传时间间隔为 1 秒。

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] time-out 1
```