目 录

1 IPsec

说明

目前只有 WAC360 系列、WX2540E 和 WX3000E 系列支持在 AC 与 AC 间建立 IPsec 隧道，其他型号的 AC 都不支持 AC 与 AC 间建立 IPsec 隧道，所有 AC 都支持 AC 与 AP 间建立 IPsec 隧道。

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】

IPsec 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：

- 在 FIPS 模式下，设备不支持 MD5 算法，缺省认证算法为 SHA-1。
- 在非 FIPS 模式下，未指定 AH 协议采用的认证算法。

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 transform-set** 和 **transform**。

【举例】

配置 IPsec 安全提议 prop1，设定 AH 协议采用 SHA-1 算法。

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

1.1.2 connection-name

【命令】

connection-name *name*

undo connection-name

【视图】

IPsec 安全策略视图/IPsec 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 IPsec 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 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 IPsec 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 IPsec 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 IPsec 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
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
------------------------------------------------------------------------
```

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 目前，无线控制器不支持手工方式
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: Vlan-interface2
=========================================

  -----------------------------------
  IPsec policy name: "policy_isakmp"
  sequence number: 10
  acl version: IPv4
  mode: isakmp
  -----------------------------------
    security data flow : 3000
    selector mode: standard
    ike-peer name:  per
    perfect forward secrecy:
    transform-set name: prop1
    synchronization inbound anti-replay-interval: 1000 packets
    synchronization outbound anti-replay-interval: 10000 packets
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes
    policy enable: True
    tfc enable: False
```

表1-2 display ipsec policy 命令显示信息描述表

字段	描述
IPsec Policy Group	IPsec安全策略组的名称
security data flow	IPsec安全策略引用的访问控制列表
Interface	应用了IPsec安全策略的接口名称
IPsec policy name	IPsec安全策略的名称
sequence number	IPsec安全策略的顺序号
acl version	访问控制列表的版本，目前仅支持ACL4 若未引用访问控制列表，则显示为None
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 目前，WX系列无线控制器不支持手工方式
policy template name	IPsec安全策略模板名称
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
ike-peer name	IPsec安全策略引用的IKE对等体名称

字段	描述
perfect forward secrecy	是否使用完善的前向安全（Perfect Forward Secrecy）特性
transform-set name	IPsec安全策略引用的提议的名字
policy enable	IPsec安全策略是否被使能
tfc enable	TFC填充功能是否被使能
synchronization inbound anti-replay-interval	入方向同步防重放窗口的间隔，单位为报文数
synchronization outbound anti-replay-interval	出方向同步防重放序号的间隔，单位为报文数
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

1.1.4 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 IPsec 安全策略模板的简要信息。

name：显示指定 IPsec 安全策略模板的详细信息。

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

seq-number：指定 IPsec 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 IPsec 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 IPsec 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 IPsec 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 IPsec 安全策略模板的简要信息。

```
<Sysname> display ipsec policy-template brief
Policy-Template-Name     acl            Remote-Address
-----------------------------------------------------
test-300                 2200
```

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

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

显示所有 IPsec 安全策略模板详细信息。

```
<Sysname> display ipsec policy-template

==============================================
IPsec Policy Template Group: "test"
==============================================

  ---------------------------------
  Policy template name: "test"
  sequence number: 1
  ---------------------------------
    security data flow :
    ACL’s Version:  acl4
    ike-peer name:  per
    perfect forward secrecy:  DH group 5
    transform-set name:  testprop
    synchronization inbound anti-replay-interval: 1000 packets
    synchronization outbound anti-replay-interval: 10000 packets
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes
```

表1-4 display ipsec policy-template 命令显示信息描述表

字段	描述
IPsec Policy Template Group	IPsec安全策略模板组名称
Policy template name	IPsec安全策略模板名称
sequence number	IPsec安全策略模板的序号
security data flow	IPsec安全策略模板引用的访问控制列表
ACL’s Version	访问控制列表的版本，目前仅支持IPv4 ACL

字段	描述
ike-peer name	IPsec安全策略模板引用的IKE对等体名称
perfect forward secrecy	是否使用完善的前向安全（Perfect Forward Secrecy）特性
DH group	使用的DH组，取值可包括1、2、5、14
transform-set name	IPsec安全策略模板引用的提议的名字
synchronization inbound anti-replay-interval	入方向IPsec SA防重放窗口的间隔，以报文数量为单位
synchronization outbound anti-replay-interval	出方向IPsec SA防重放序号的间隔，以报文数量为单位
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

1.1.5 display ipsec sa

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

active：显示双机热备环境下主用安全联盟的详细信息。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

brief：显示所有的安全联盟的简要信息。

policy：显示由指定 IPsec 安全策略创建的安全联盟的详细信息。

policy-name：指定 IPsec 安全策略的名字，为 1～15 个字符的字符串。

seq-number：指定 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 地址的安全联盟的详细信息。

standby：显示双机热备环境下备用安全联盟的详细信息。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

|：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
total phase-2 IPv4 SAs: 2
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
total phase-2 IPv6 SAs: 0
Src Address            Dst Address            SPI        Protocol Algorithm
-------------------------------------------------------------------------------
```

表1-5 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

显示所有安全联盟的详细信息。

```
<Sysname> display ipsec sa
==============================
Interface: Vlan-interface2
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "r2"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    connection id: 3
    encapsulation mode: tunnel
    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)
  transform-set: 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
  status: active

[outbound ESP SAs]
  spi: 801701189 (0x2fc8fd45)
  transform-set: 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
```

表1-6 display ipsec sa 命令显示信息描述表

字段	描述
Interface	应用了IPsec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
IPsec policy name	采用的安全策略名
sequence number	IPsec安全策略顺序号
acl version	访问控制列表的版本，目前仅支持IPv4 ACL 若未引用访问控制列表，则显示为None
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
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

字段	描述
protocol	协议类型
inbound	输入端安全联盟的信息
spi	安全参数索引号
transform-set	IPsec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

1.1.6 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1-7 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

字段	描述
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
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

1.1.7 display ipsec transform-set

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

transform-set-name：显示指定的 IPsec 安全提议。*transform-set-name* 表示 IPsec 安全提议的名字，为 1～32 个字符的字符串。如果不指定本参数，则显示所有 IPsec 安全提议的信息。

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

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

相关配置可参考命令 **ipsec transform-set**。

【举例】

显示所有 IPsec 安全提议的信息。

```
<Sysname> display ipsec transform-set

  IPsec transform-set name: tran1
    encapsulation mode: tunnel
    ESN : disable
```

```
    ESN scheme: NO
    transform: esp-new
    ESP protocol:
      Integrity: md5-hmac-96
      Encryption: des

  IPsec transform-set name: tran2
    encapsulation mode: transport
    ESN : disable
    ESN scheme: NO
    transform: esp-new
    ESP protocol:
      Integrity: md5-hmac-96
      Encryption: des
```

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

字段	描述
IPsec transform-set name	IPsec安全提议的名字
encapsulation mode	提议采用的封装模式，包括两种：传输（transport）和隧道（tunnel）模式
ESN	ESN功能是否使能
ESN scheme	ESN取值（NO表示不支持，YES表示支持）
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 tunnel

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

active：显示双机热备环境下主用 IPsec 隧道的相关信息。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

standby：显示双机热备环境下备用 IPsec 隧道的相关信息。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

|：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。

不指定任何参数的情况下，则显示所有 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
    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
```

显示聚合方式下的 IPsec 隧道信息。

```
<Sysname> display ipsec tunnel
    total tunnel: 2
    -----------------------------------------------
    connection id: 4
    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
```

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
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

字段	描述
as defined in acl 3001	IPsec隧道保护ACL 3001中定义的所有数据流

1.1.9 encapsulation-mode

【命令】

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

undo encapsulation-mode

【视图】

IPsec 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。

相关配置可参考命令 **ipsec transform-set**。

【举例】

配置名为 tran1 的安全提议采用传输模式对 IP 报文进行封装。

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

1.1.10 esp authentication-algorithm

【命令】

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

undo esp authentication-algorithm

【视图】

IPsec 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** 命令用来恢复缺省情况。

缺省情况下：

- 在 FIPS 模式下，设备不支持 MD5 算法，缺省认证算法为 SHA-1。
- 在非 FIPS 模式下，未指定 ESP 协议采用的认证算法。

需要注意的是：

- MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。对于保密及安全性要求较高的地方，建议采用 SHA-1 算法；对于普通安全需求，采用 MD5 算法即可。
- 未配置 FIPS 模式时，ESP 协议采用的加密算法和认证算法不能同时设置为空；配置了 FIPS 模式时，ESP 协议必须同时设置加密算法和认证算法。

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

【举例】

配置 IPsec 安全提议 prop1 采用 ESP 协议并使用 SHA-1 认证算法。

```
<Sysname> system-view
[Sysname] ipsec transform-set prop1
[Sysname-ipsec-transform-set-prop1] transform esp
[Sysname-ipsec-transform-set-prop1] esp authentication-algorithm sha1
```

1.1.11 esp encryption-algorithm

【命令】

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

undo esp encryption-algorithm

【视图】

IPsec 安全提议视图

【缺省级别】

2：系统级

【参数】

3des：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：CBC 模式的 AES 算法，密钥长度为 128 比特。

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

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

des：CBC 模式的 DES 算法，密钥长度为 56 比特。

【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** 命令用来恢复缺省情况。

缺省情况下：

- 在 FIPS 模式下，设备不支持 DES 和 3DES 算法，缺省认证算法为 AES-128。
- 在非 FIPS 模式下，未指定 ESP 协议采用的加密算法。

需要注意的是：未配置 FIPS 模式时，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。在实际配置过程中，ESP 协议采用的加密算法和认证算法不能同时为空，要求至少指定其中之一；配置了 FIPS 模式时，ESP 协议必须对报文同时进行加密和认证。

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

【举例】

配置 IPsec 安全提议 prop1 采用 ESP 协议并使用 3DES 加密算法。

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

1.1.12 ike-peer (IPsec policy view/IPsec policy template view)

【命令】

ike-peer *peer-name*

undo ike-peer *peer-name*

【视图】

IPsec 安全策略视图/IPsec 安全策略模板视图

【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 IPsec 安全策略或者 IPsec 安全策略模板中引用 IKE 对等体。**undo ike peer** 命令用来取消在 IPsec 安全策略或者 IPsec 安全策略模板中引用 IKE 对等体。

相关配置可参考命令 **ipsec policy**。

【举例】

配置在 IPsec 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
```

1.1.13 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
```

1.1.14 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
```

1.1.15 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
```

1.1.16 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 IPsec 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 IPsec 安全策略组。

【描述】

ipsec policy 命令用来在接口上应用指定的 IPsec 安全策略组。**undo ipsec policy** 命令用来从接口上取消应用的 IPsec 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 IPsec 安全策略组。在一个接口上应用一个 IPsec 安全策略组，实际上是同时应用了 IPsec 安全策略组中所有的 IPsec 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 IPsec 安全策略组，必须先从接口上取消应用的 IPsec 安全策略组。一个 IPsec 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 IPsec 安全策略组中每一条 IPsec 安全策略。如果报文匹配了一条 IPsec 安全策略引用的访问控制列表，则使用这条 IPsec 安全策略对报文进行处理；如果报文没有匹配 IPsec 安全策略引用的访问控制列表，则继续查找下一条 IPsec 安全策略；如果报文对所有 IPsec 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 Vlan-interface3 接口上应用名为 pg1 的 IPsec 安全策略组。

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] ipsec policy pg1
```

1.1.17 ipsec policy (system view)

【命令】

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

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：IPsec 安全策略的名字，为 1～15 个字符的字符串，不区分大小写，不能包括减号“-”。

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

isakmp：指定通过 IKE 协商建立安全联盟。

【描述】

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

缺省情况下，没有任何 IPsec 安全策略存在。

需要注意的是：

- 使用此命令创建 IPsec 安全策略时，必须指定协商方式，但进入已创建的 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，只能先删除该 IPsec 安全策略，再重新创建。

- 具有相同名字的 IPsec 安全策略一起组成一个 IPsec 安全策略组。由名字和顺序号一起确定一条唯一的 IPsec 安全策略。在一个 IPsec 安全策略组中，顺序号 *seq-number* 越小的 IPsec 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 IPsec 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 IPsec 安全策略。

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

1.1.18 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：IPsec 安全策略的名字，为 1～15 个字符的字符串，不区分大小写，不能包括减号“-”。

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 安全策略模板的名字。

【描述】

ipsec policy isakmp template 命令用来引用 IPsec 安全策略模板创建一条 IPsec 安全策略，该 IPsec 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 IPsec 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 IPsec 安全策略组；
- 在配置此命令前，必须已经创建 IPsec 安全策略模板。
- 引用 IPsec 安全策略模板创建一条 IPsec 安全策略之后，就不能进入该 IPsec 安全策略视图下进行 IPsec 安全策略的配置与修改了，只能进入 IPsec 安全策略模板视图下配置或修改。
- 不能修改已创建的 IPsec 安全策略的协商方式，只能先删除该 IPsec 安全策略，再重新创建。

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 IPsec 安全策略。

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

1.1.19 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 IPsec 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，不能包括减号“-”。

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

【描述】

ipsec 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。

undo ipsec policy-template 命令用来删除指定的一个 IPsec 安全策略模板。

缺省情况下，没有任何 IPsec 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 IPsec 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 IPsec 安全策略模板。

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

1.1.20 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 IPsec 安全策略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 IPsec 安全策略配置了自己的生存周期，则系统使用 IPsec 安全策略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。
- 可同时配置基于时间和基于流量的生存周期，只要到达指定的时间或指定的流量，SA 就会老化。

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周期为 10M 字节，即传输 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
```

1.1.21 ipsec transform-set

【命令】

ipsec transform-set *transform-set-name*

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

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

transform-set-name：指定 IPsec 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 transform-set 命令用来创建一个 IPsec 安全提议，并进入 IPsec 提议视图。**undo ipsec transform-set** 命令用来删除指定的 IPsec 安全提议。

缺省情况下，没有任何 IPsec 安全提议存在。

相关配置可参考命令 **display ipsec transform-set**。

【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-ipsec-transform-set-tran1]
```

1.1.22 ipsec synchronization enable

【命令】

ipsec synchronization enable

undo ipsec synchronization enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ipsec synchronization enable 命令用来开启 IPsec 双机热备功能。**undo ipsec synchronization enable** 命令用来关闭 IPsec 双机热备功能。

缺省情况下，IPsec 双机热备功能处于开启状态。

关闭 IPsec 双机热备功能将会删除当前设备上所有主用/备用 IKE SA 和主用/备用 IPsec SA。

说明

本命令的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

【举例】

开启 IPsec 双机热备功能。

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

1.1.23 policy enable

【命令】

policy enable

undo policy enable

【视图】

IPsec 安全策略视图/IPsec 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 IPsec 安全策略。**undo policy enable** 命令用来去使能 IPsec 安全策略。

缺省情况下，IPsec 安全策略处于使能状态。

需要注意的是：如果 IKE 对等体未使能 IPsec 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 IPsec 安全策略。

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

1.1.24 reset ipsec sa

【命令】

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

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

active：指定双机热备环境下的所有主用安全联盟。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

parameters：指定一个安全联盟所对应的目的 IP 地址、安全协议和 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。

policy-name：指定 IPsec 安全策略的名字，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*：指定安全联盟对应的对端 IP 地址。

ip-address：指定对端 IP 地址。

standby：指定双机热备环境下的所有备份安全联盟。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

【描述】

reset ipsec sa 命令用来清除已经建立的 IPsec SA。

如果不指定任何参数，则清除所有的 IPsec SA。

需要注意的是：

- 通过 IKE 协商建立的 IPsec SA 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 IPsec SA。
- 如果指定了 **parameters** 关键字，由于 IPsec SA 是成对出现的，清除了一个方向的 IPsec SA，另一个方向的 IPsec SA 也会被清除。

在双机热备环境中，执行本命令后的具体情况如下：

- 清除设备上的主用 IPsec SA 的同时，本设备会通知处于备用状态的设备将相应的备用 IPsec SA 也清除掉。
- 清除设备上的备用 IPsec SA 之后，本设备会请求处于主用状态的设备将相应的主用 IPsec SA 重新同步给本设备。

如果既未指定 active 关键字也未指定 standby 关键字，则本命令将会清除设备上的所有的或符合指定条件的主用和备用 IPsec SA，但备用 IPsec SA 被删除之后，设备会请求处于主用状态的设备重新同步所有备用的 IPsec SA。

相关配置可参考命令 **display ipsec sa**。

【举例】

清除所有 IPsec SA。

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

清除对端地址为 10.1.1.2 的 IPsec SA。

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

清除安全策略模板 policy1 中的所有 IPsec SA。

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

清除安全策略名字为 policy1、顺序号为 10 的 IPsec SA。

```
<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 IPsec SA。

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

1.1.25 reset ipsec statistics

【命令】

reset ipsec statistics

【视图】

用户视图

【缺省级别】

1：监控级

【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
```

1.1.26 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

【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 IPsec 安全策略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，IPsec 安全策略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 IPsec 安全策略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 IPsec 安全策略配置了自己的生存周期，则系统使用 IPsec 安全策略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。

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

【举例】

配置 IPsec 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 IPsec 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
```

1.1.27 security acl

【命令】

security acl *acl-number* [**aggregation** | **per-host**]

undo security acl

【视图】

IPsec 安全策略视图/IPsec 安全策略模板视图

【缺省级别】

2：系统级

【参数】

acl-number：指定 IPsec 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 IPsec 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 IPsec 安全策略的数据流保护方式为标准方式。

per-host：指定 IPsec 安全策略的数据流保护方式为主机方式。

【描述】

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

缺省情况下，IPsec 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，IPsec 安全策略的数据流保护方式包括以下三种：

- 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。
- 主机方式：一条隧道保护一条主机到主机之间的数据流。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。

需要注意的是：

- 若不指定 **aggregation** 和 **per-host** 参数，则表示 IPsec 安全策略的数据流保护方式为标准方式。
- 聚合方式仅用于和老版本的设备互通。这种情况下，要求两端的配置必须一致，即两端同时配置聚合方式。
- 一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。
- 主机方式仅支持在 IKE 协商方式下的 IPsec 策略视图下配置。
- 若需要采用主机方式来保护主机之间的数据流，则只需要在 IPsec 协商发起方的 IPsec 策略中引用主机方式的 ACL，响应方的 IPsec 策略中无需指定该参数。

- 由于在对等体保护的主机数目较多时，采用主机方式会导致触发 IPsec 建立大量的 SA 并迅速大量消耗系统资源，因此建议慎重使用主机方式。

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

【举例】

配置 IPsec 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
```

配置 IPsec 安全策略引用 ACL 3003，并设置数据流保护方式为主机方式。

```
<Sysname> system-view
[Sysname] acl number 3003
[Sysname-acl-adv-3003] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[Sysname-acl-adv-3003] quit
[Sysname] ipsec policy policy3 10 isakmp
[Sysname-ipsec-policy-isakmp-policy3-10] security acl 3003 per-host
```

1.1.28 synchronization anti-replay-interval

【命令】

synchronization anti-replay-interval inbound *inbound-number* **outbound** *outbound-number*

undo synchronization anti-replay-interval

【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】

inbound-number：同步入方向防重放窗口的间隔，单位为报文数，即主设备在入方向上每接收多少个报文后才会向备用设备同步一次防重放窗口，取值范围为 0～1000，取值为 0 表示不同步防重放窗口。

outbound-number：同步出方向防重放序号的间隔，单位为报文数，即主设备在出方向上每发送多少个报文后才会向备用设备同步一次防重放序号，取值范围为 1000～100000。

【描述】

synchronization anti-replay-interval 命令用来配置 IPsec 双机热备环境下由主设备向备用设备发送防重放同步信息的间隔，包括同步入方向防重放窗口的间隔和同步出方向防重放序号的间隔。

undo synchronization anti-replay-interval 命令用来恢复缺省情况。

缺省情况下，同步入方向防重放窗口的间隔为每接收 1000 个报文同步一次；同步出方向防重放序号的间隔为每发送 100000 个报文同步一次。

在 IPsec 双机热备环境下，通过给备用设备同步防重放信息，使得备用设备可以在主设备发生故障后，代替主设备正确处理对端发送的 IPsec 报文，防止主备切换后原本合法的 IPsec 报文被切换后的设备认为是重放报文而丢弃。

若将同步防重放信息的间隔调小一些，可以增强互为备份的两台设备上的防重放窗口和防重放序号的一致性，这同时会增加防重放同步信息的发送频率，因此会对报文的转发性能产生一定的影响，建议根据设备的实际情况做适当调整。

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

说明

本命令的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

【举例】

设置同步入方向防重放窗口的间隔为 800 个报文，同步出方向防重放序号的间隔为 50000 个报文。

```
<Sysname> system-view
[Sysname] ipsec policy test 10 isakmp
[Sysname-ipsec-policy-isakmp-test-10] synchronization anti-replay-interval inbound 800
outbound 50000
```

1.1.29 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，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 transform-set**。

【举例】

配置一个采用 AH 协议的 IPsec 安全提议。

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

1.1.30 transform-set

【命令】

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

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

【视图】

IPsec 安全策略视图/IPsec 安全策略模板视图

【缺省级别】

2：系统级

【参数】

transform-set-name&<1-6>：所采用的提议名字，为 1～32 个字符的字符串。&<1-6>表示前面的参数最多可以输入 6 次。

【描述】

transform-set 命令用来配置 IPsec 安全策略所引用的 IPsec 安全提议。**undo transform-set** 命令用来取消 IPsec 安全策略引用的 IPsec 安全提议。

缺省情况下，IPsec 安全策略没有引用任何 IPsec 安全提议。

需要注意的是：

- 引用的 IPsec 安全提议必须已经存在。
- 如果 IPsec 安全策略是 IKE（**isakmp**）协商方式的，则一条 IPsec 安全策略最多可以引用六个 IPsec 安全提议，IKE 协商时将在 IPsec 安全策略中搜索能够完全匹配的 IPsec 安全提议。

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

【举例】

配置 IPsec 安全策略引用名字为 tran1 的 IPsec 安全提议。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] quit
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] transform-set tran1
```

2 IKE

2.1 IKE配置命令

2.1.1 authentication-algorithm

【命令】

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

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。

sha256：指定认证算法为 HMAC-SHA256。

【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。

需要注意的是，在 FIPS 模式下不支持 MD5 算法，缺省使用 SHA2-256 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】

非 FIPS 模式：

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

undo dh

FIPS 模式：

dh 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；FIPS 模式下 DH 密钥交换参数缺省为 **group14**。

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 1～32 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 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 1～32 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 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 ******
   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，配置值显示为******
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 [**active** | **standby** | **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】

active：显示双机热备环境下主用 IKE SA 和 IPsec SA 的摘要信息。请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

standby：显示双机热备环境下备用 IKE SA 和 IPsec SA 的摘要信息。请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

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：按照对端 IP 地址显示 IKE SA 的详细信息。

remote-address：指定对端 IP 地址。

|：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 和 IPsec 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 和 IPsec 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	IKE SA和IPsec 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 IKE 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
    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
```

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
    transmitting entity: initiator
    status: active
    ---------------------------------------------
    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
```

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
    transmitting entity: initiator
    status: active
    ---------------------------------------------
    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
    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	IKE SA和IPsec SA的标识符
transmitting entity	IKE协商中的实体

字段	描述
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)	IKE SA的生命周期（秒）
remaining key duration(sec)	IKE SA的剩余生命周期（秒）
exchange-mode	IKE第一阶段的协商模式
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：

- 在 FIPS 模式下，设备不支持 DES-CBC 和 3DES-CBC，IKE 提议使用 CBC 模式的 128-bit AES-CBC 加密算法。
- 在非 FIPS 模式下， 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：

- 当对端的 IP 地址为自动获取（如一端用户为拨号方式），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 aggressive。
- 在 FIPS 模式下，设备不支持 aggressive 协商模式。

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，如下表所示：

缺省参数	非 FIPS 模式缺省值	FIPS 模式缺省值
加密算法	DES-CBC	AES_CBC_128
认证算法	HMAC-SHA1	SHA
认证方法	预共享密钥	预共享密钥
DH组标识	MODP_768	MODP_1024
安全联盟的存活时间	86400秒	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 IPsec 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】

local-name 命令用来配置本端安全网关的名字。**undo 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】

cipher：表示以密文方式设置预共享密钥。

simple：表示以明文方式设置预共享密钥。

key：设置的明文密钥或密文密钥，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。不指定 **cipher** 或 **simple** 时，表示以明文方式设置密钥。

【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。

如果不指定任何参数，则表示以交互式方式设置预共享密钥，用户以明文方式输入两次预共享密钥，二次输入完全相同时，完成配置。

以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

在 FIPS 模式下，仅支持 cipher 和交互式方式设置预共享密钥，共享密钥至少需要设置为 8 位，包含数字、大写字母、小写字母和特殊符号。

在非 FIPS 模式下，不支持交互式方式设置预共享密钥，仅支持 simple、cipher 以及直接输入密钥方式设置密钥。

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明文 abcde。

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

以交互式方式设置 IKE 对等体 peer1 的预共享密钥为 123Abc!@#。

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key
Enter pre-share-key: *********
Re-enter pre-share-key: *********
```

2.1.28 proposal

【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 IPsec 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* | **active** | **standby**]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

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

active：清除所有主用 IKE SA。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

standby：清除所有备用 IKE SA。本参数的支持情况与设备的型号有关，请参见“命令参考导读”中的“命令行及参数差异情况”部分的介绍。

【描述】

reset ike sa 命令用来清除 IKE SA。

需要注意的是：

- 如果未指定任何参数，则表示清除所有 IKE SA。
- 清除本地的 IPsec SA 时，如果相应的 IKE SA 还存在，将在此 IKE 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 IKE 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】

清除连接 ID 号为 2 的 IKE SA。

```
<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
```