

# 在Cisco IOS和strongSwan配置示例之间的IKEv1/IKEv2

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[开放源L2L IPSec VPN](#)

[在Cisco IOS之间的IKEv1和strongSwan](#)

[Cisco IOS配置](#)

[strongSwan配置](#)

[在Cisco IOS之间的IKEv2和strongSwan](#)

[Cisco IOS配置](#)

[strongSwan配置](#)

[验证](#)

[故障排除](#)

[在Cisco IOS之间的IKEv1和strongSwan](#)

**[Cisco IOS](#)**

[Cisco IOS触发的隧道建立](#)

[Cisco IOS : 检查IPSec计数器](#)

[Cisco IOS : 验证IKEv1和IPSec参数](#)

[strongSwan : 隧道建立](#)

[strongSwan : 验证IPSec连接状态](#)

[strongSwan : 验证IPSec策略](#)

[在Cisco IOS之间的IKEv2和strongSwan](#)

**[Cisco IOS](#)**

[Cisco IOS触发的隧道建立](#)

[Cisco IOS : 检查IPSec计数器](#)

[Cisco IOS : 验证IKEv2和IPSec参数](#)

[strongSwan : 隧道建立](#)

[strongSwan : 验证IPSec连接状态](#)

[strongSwan : 验证IPSec策略](#)

[相关信息](#)

## 简介

本文为在Cisco IOS之间的LAN对LAN (L2L) VPN提供配置示例和strongSwan。配置提交互联网密钥交换版本1 (IKEv1)和互联网密钥交换版本2 (IKEv2)。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 关于Linux配置的基础知识
- 关于VPN配置的知识在Cisco IOS
- 关于这些协议的知识：IKEv1IKEv2Internet协议安全性(IPSec)

### 使用的组件

本文档中的信息基于以下软件版本：

- Cisco IOS版本15.3T
- strongSwan 5.0.4
- Linux内核3.2.12

## 配置

### 网络图

拓扑是相同的为两示例，在Cisco IOS之间的L2L通道和strongSwan。

流量保护在192.168.1.0/24<->192.168.2.0/24之间。

### 开放源L2L IPSec VPN

有使用Internet Key Exchange (IKE)和IPSec协议构建安全L2L通道的几个开放源项目：

- 释放安全广域网(freeS/WAN)：历史记录，不积极地维护
- ipsec工具：浣熊-不支持IKEv2，更旧的Linux内核2.6
- Openswan：非常基本IKEv2支持、更旧的Linux内核2.6和更早的API，不积极地维护
- strongSwan：支持IKEv2和EAP/mobility扩展，使用NETKEY API (是名称对于本地IPSec实施在内核2.6及以后)的新建的Linux内核3.x和以后，积极地维护，有大量文件证明

目前，最好的选择通常strongSwan。它类似于在配置方面Openswan，有几较小差异。此指南着重strongSwan和Cisco IOS配置。

### 在Cisco IOS之间的IKEv1和strongSwan

## Cisco IOS配置

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 5
crypto isakmp key cisco address 172.16.10.2

crypto ipsec transform-set TS esp-aes esp-sha-hmac
mode tunnel

crypto map cmap 10 ipsec-isakmp
  set peer 172.16.10.2
  set transform-set TS
  match address cryptoacl

interface Ethernet0/1
  ip address 192.168.1.1 255.255.255.0

interface Ethernet0/0
  ip address 172.16.10.1 255.255.255.0
  crypto map cmap

ip access-list extended cryptoacl
  permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

## strongSwan配置

左侧与strongSwan涉及，并且右侧是远程(在本例中的Cisco IOS)。

### /etc/ipsec.conf

```
config setup
  # strictcrlpolicy=yes
  # uniqueids = no

conn %default
  ikelifetime=1440m
  keylife=60m
  rekeymargin=3m
  keyingtries=1
  keyexchange=ikev1
  authby=secret

conn ciscoios
  left=172.16.10.2 #strongswan outside address
  leftsubnet=192.168.2.0/24 #network behind strongswan
  leftid=172.16.10.2 #IKEID sent by strongswan
  leftfirewall=yes
  right=172.16.10.1 #IOS outside address
  rightsubnet=192.168.1.0/24 #network behind IOS
  rightid=172.16.10.1 #IKEID sent by IOS
  auto=add
  ike=aes128-md5-modp1536 #P1: modp1536 = DH group 5
  esp=aes128-sha1 #P2
```

默认情况下，Cisco IOS使用地址作为IKE ID -所以地址使用了作为‘rightid”并且“leftid”。strongSwan，类似Cisco IOS，支持下一代加密算法(套件B) -如此与AES256和SHA512一起使用4096 Diffie-Hellman (DH)密钥是可能的。

对于自动参数，“请添加”参数使用了。在获得关注数据流后，那启动通道。为了立即开始它，能使用“启动”参数。

/etc/ipsec.secrets

```
172.16.10.2 172.16.10.1 : PSK cisco
```

对于IKEv1两密钥需要是同样，在本例中“cisco”。

## 在Cisco IOS之间的IKEv2和strongSwan

### Cisco IOS配置

```
crypto ikev2 proposal ikev2proposal
  encryption aes-cbc-128
  integrity sha1
  group 5

crypto ikev2 policy ikev2policy
  match fvrfl any
  proposal ikev2proposal

crypto ikev2 keyring keys
  peer strongswan
  address 172.16.10.2
  pre-shared-key local cisco
  pre-shared-key remote cisco

crypto ikev2 profile ikev2profile
  match identity remote address 172.16.10.2 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local keys

crypto ipsec transform-set TS esp-aes esp-sha-hmac
  mode tunnel

crypto map cmap 10 ipsec-isakmp
  set peer 172.16.10.2
  set transform-set TS
  set ikev2-profile ikev2profile
  match address cryptoacl

interface Ethernet0/1
  ip address 192.168.1.1 255.255.255.0

interface Ethernet0/0
  ip address 172.16.10.1 255.255.255.0
  crypto map cmap

ip access-list extended cryptoacl
  permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

### strongSwan配置

与IKEv1比较，只有两更改：keyexchange和可能密钥。

## /etc/ipsec.conf

```
config setup
    # strictcrlpolicy=yes
    # uniqueids = no

conn %default
    ikelifetime=1440m
    keylife=60m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev1
    authby=secret

conn ciscoios
    left=172.16.10.2
    leftsubnet=192.168.2.0/24
    leftid=172.16.10.2
    leftfirewall=yes
    right=172.16.10.1
    rightsubnet=192.168.1.0/24
    rightid=172.16.10.1
    auto=add
    ike=aes128-sha1-modp1536
    esp=aes128-sha1
    keyexchange=ikev2
```

## /etc/ipsec.secrets

```
config setup
    # strictcrlpolicy=yes
    # uniqueids = no

conn %default
    ikelifetime=1440m
    keylife=60m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev1
    authby=secret

conn ciscoios
    left=172.16.10.2
    leftsubnet=192.168.2.0/24
    leftid=172.16.10.2
    leftfirewall=yes
    right=172.16.10.1
    rightsubnet=192.168.1.0/24
    rightid=172.16.10.1
    auto=add
    ike=aes128-sha1-modp1536
    esp=aes128-sha1
    keyexchange=ikev2
```

在IKEv2中，每个站点的密钥可以不同的。

## 验证

请参阅Troubleshoot部分关于验证程序。

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

### 在Cisco IOS之间的IKEv1和strongSwan

#### Cisco IOS

```
R1#ping 192.168.2.1 source e0/1 repeat 1
```

#### Cisco IOS触发的隧道建立

```
*May 24 18:02:48.464: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 172.16.10.1:500, remote= 172.16.10.2:500,
  local_proxy= 192.168.1.0/255.255.255.0/256/0,
  remote_proxy= 192.168.2.0/255.255.255.0/256/0,
  protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 24 18:02:48.465: ISAKMP:(0): SA request profile is (NULL)
*May 24 18:02:48.465: ISAKMP: Created a peer struct for 172.16.10.2, peer port 500
*May 24 18:02:48.465: ISAKMP: New peer created peer = 0xF334E7E0 peer_handle =
0x80000006
*May 24 18:02:48.465: ISAKMP: Locking peer struct 0xF334E7E0, refcount 1 for
isakmp_initiator
*May 24 18:02:48.465: ISAKMP: local port 500, remote port 500
*May 24 18:02:48.465: ISAKMP: set new node 0 to QM_IDLE
*May 24 18:02:48.465: ISAKMP: Find a dup sa in the avl tree during calling
isadb_insert sa = F49C9890
*May 24 18:02:48.465: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*May 24 18:02:48.465: ISAKMP:(0):found peer pre-shared key matching 172.16.10.2
*May 24 18:02:48.465: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
*May 24 18:02:48.465: ISAKMP:(0): constructed NAT-T vendor-07 ID
*May 24 18:02:48.465: ISAKMP:(0): constructed NAT-T vendor-03 ID
*May 24 18:02:48.465: ISAKMP:(0): constructed NAT-T vendor-02 ID
*May 24 18:02:48.465: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
*May 24 18:02:48.465: ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1

*May 24 18:02:48.465: ISAKMP:(0): beginning Main Mode exchange
*May 24 18:02:48.465: ISAKMP:(0): sending packet to 172.16.10.2 my_port 500
peer_port 500 (I) MM_NO_STATE
*May 24 18:02:48.465: ISAKMP:(0):Sending an IKE IPv4 Packet.
*May 24 18:02:48.466: ISAKMP (0): received packet from 172.16.10.2 dport 500
sport 500 Global (I) MM_NO_STATE
*May 24 18:02:48.466: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*May 24 18:02:48.466: ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

*May 24 18:02:48.466: ISAKMP:(0): processing SA payload. message ID = 0
*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload
*May 24 18:02:48.466: ISAKMP:(0): vendor ID seems Unity/DPD but major 215 mismatch
*May 24 18:02:48.466: ISAKMP:(0): vendor ID is XAUTH
*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload
*May 24 18:02:48.466: ISAKMP:(0): vendor ID is DPD
*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload
*May 24 18:02:48.466: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
*May 24 18:02:48.466: ISAKMP (0): vendor ID is NAT-T RFC 3947
```

\*May 24 18:02:48.466: ISAKMP:(0):found peer pre-shared key matching 172.16.10.2  
\*May 24 18:02:48.466: ISAKMP:(0): local preshared key found  
\*May 24 18:02:48.466: ISAKMP : Scanning profiles for xauth ...  
\*May 24 18:02:48.466: ISAKMP:(0):Checking ISAKMP transform 1 against priority  
10 policy  
\*May 24 18:02:48.466: ISAKMP: encryption AES-CBC  
\*May 24 18:02:48.466: ISAKMP: keylength of 128  
\*May 24 18:02:48.466: ISAKMP: hash SHA  
\*May 24 18:02:48.466: ISAKMP: default group 5  
\*May 24 18:02:48.466: ISAKMP: auth pre-share  
\*May 24 18:02:48.466: ISAKMP: life type in seconds  
\*May 24 18:02:48.466: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
\*May 24 18:02:48.466: ISAKMP:(0):atts are acceptable. Next payload is 0  
\*May 24 18:02:48.466: ISAKMP:(0):Acceptable atts:actual life: 0  
\*May 24 18:02:48.466: ISAKMP:(0):Acceptable atts:life: 0  
\*May 24 18:02:48.466: ISAKMP:(0):Fill atts in sa vpi\_length:4  
\*May 24 18:02:48.466: ISAKMP:(0):Fill atts in sa life\_in\_seconds:86400  
\*May 24 18:02:48.466: ISAKMP:(0):Returning Actual lifetime: 86400  
\*May 24 18:02:48.466: ISAKMP:(0)::Started lifetime timer: 86400.  
  
\*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload  
\*May 24 18:02:48.466: ISAKMP:(0): vendor ID seems Unity/DPD but major 215 mismatch  
\*May 24 18:02:48.466: ISAKMP:(0): vendor ID is XAUTH  
\*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload  
\*May 24 18:02:48.466: ISAKMP:(0): vendor ID is DPD  
\*May 24 18:02:48.466: ISAKMP:(0): processing vendor id payload  
\*May 24 18:02:48.466: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch  
\*May 24 18:02:48.466: ISAKMP (0): vendor ID is NAT-T RFC 3947  
\*May 24 18:02:48.466: ISAKMP:(0):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
\*May 24 18:02:48.466: ISAKMP:(0):Old State = IKE\_I\_MM2 New State = IKE\_I\_MM2  
  
\*May 24 18:02:48.466: ISAKMP:(0): sending packet to 172.16.10.2 my\_port 500  
peer\_port 500 (I) MM\_SA\_SETUP  
\*May 24 18:02:48.466: ISAKMP:(0):Sending an IKE IPv4 Packet.  
\*May 24 18:02:48.466: ISAKMP:(0):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
\*May 24 18:02:48.466: ISAKMP:(0):Old State = IKE\_I\_MM2 New State = IKE\_I\_MM3  
  
\*May 24 18:02:48.474: ISAKMP (0): received packet from 172.16.10.2 dport 500 sport  
500 Global (I) MM\_SA\_SETUP  
\*May 24 18:02:48.474: ISAKMP:(0):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH  
\*May 24 18:02:48.474: ISAKMP:(0):Old State = IKE\_I\_MM3 New State = IKE\_I\_MM4  
  
\*May 24 18:02:48.474: ISAKMP:(0): processing KE payload. message ID = 0  
\*May 24 18:02:48.482: ISAKMP:(0): processing NONCE payload. message ID = 0  
\*May 24 18:02:48.482: ISAKMP:(0):found peer pre-shared key matching 172.16.10.2  
\*May 24 18:02:48.482: ISAKMP:received payload type 20  
\*May 24 18:02:48.482: ISAKMP (1003): His hash no match - this node outside NAT  
\*May 24 18:02:48.482: ISAKMP:received payload type 20  
\*May 24 18:02:48.482: ISAKMP (1003): No NAT Found for self or peer  
\*May 24 18:02:48.482: ISAKMP:(1003):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
\*May 24 18:02:48.482: ISAKMP:(1003):Old State = IKE\_I\_MM4 New State = IKE\_I\_MM4  
  
\*May 24 18:02:48.482: ISAKMP:(1003):Send initial contact  
\*May 24 18:02:48.482: ISAKMP:(1003):SA is doing pre-shared key authentication using  
id type ID\_IPV4\_ADDR  
\*May 24 18:02:48.482: ISAKMP (1003): ID payload  
next-payload : 8  
type : 1  
address : 172.16.10.1  
protocol : 17  
port : 500  
length : 12  
\*May 24 18:02:48.482: ISAKMP:(1003):Total payload length: 12  
\*May 24 18:02:48.482: ISAKMP:(1003): sending packet to 172.16.10.2 my\_port 500

```

peer_port 500 (I) MM_KEY_EXCH
*May 24 18:02:48.482: ISAKMP:(1003):Sending an IKE IPv4 Packet.
*May 24 18:02:48.482: ISAKMP:(1003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*May 24 18:02:48.482: ISAKMP:(1003):Old State = IKE_I_MM4 New State = IKE_I_MM5

*May 24 18:02:48.483: ISAKMP (1003): received packet from 172.16.10.2 dport 500
sport 500 Global (I) MM_KEY_EXCH
*May 24 18:02:48.483: ISAKMP:(1003): processing ID payload. message ID = 0
*May 24 18:02:48.483: ISAKMP (1003): ID payload
    next-payload : 8
    type          : 1
    address       : 172.16.10.2
    protocol      : 0
    port          : 0
    length        : 12
*May 24 18:02:48.483: ISAKMP:(0):: peer matches *none* of the profiles
*May 24 18:02:48.483: ISAKMP:(1003): processing HASH payload. message ID = 0
*May 24 18:02:48.483: ISAKMP:(1003):SA authentication status:
    authenticated
*May 24 18:02:48.483: ISAKMP:(1003):SA has been authenticated with 172.16.10.2
*May 24 18:02:48.483: ISAKMP: Trying to insert a peer 172.16.10.1/172.16.10.2/500/,
and inserted successfully F334E7E0.
*May 24 18:02:48.483: ISAKMP:(1003):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*May 24 18:02:48.483: ISAKMP:(1003):Old State = IKE_I_MM5 New State = IKE_I_MM6

*May 24 18:02:48.483: ISAKMP:(1003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*May 24 18:02:48.483: ISAKMP:(1003):Old State = IKE_I_MM6 New State = IKE_I_MM6

*May 24 18:02:48.487: ISAKMP:(1003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*May 24 18:02:48.487: ISAKMP:(1003):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

*May 24 18:02:48.487: ISAKMP:(1003):beginning Quick Mode exchange, M-ID of 2605730229
*May 24 18:02:48.487: ISAKMP:(1003):QM Initiator gets spi
*May 24 18:02:48.487: ISAKMP:(1003): sending packet to 172.16.10.2 my_port 500
peer_port 500 (I) QM_IDLE
*May 24 18:02:48.487: ISAKMP:(1003):Sending an IKE IPv4 Packet.
*May 24 18:02:48.488: ISAKMP:(1003):Node 2605730229, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
*May 24 18:02:48.488: ISAKMP:(1003):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
*May 24 18:02:48.488: ISAKMP:(1003):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*May 24 18:02:48.488: ISAKMP:(1003):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*May 24 18:02:48.488: ISAKMP (1003): received packet from 172.16.10.2 dport 500
sport 500 Global (I) QM_IDLE
*May 24 18:02:48.488: ISAKMP:(1003): processing HASH payload. message ID = 2605730229
*May 24 18:02:48.488: ISAKMP:(1003): processing SA payload. message ID = 2605730229
*May 24 18:02:48.488: ISAKMP:(1003):Checking IPsec proposal 1
*May 24 18:02:48.488: ISAKMP: transform 1, ESP_AES
*May 24 18:02:48.488: ISAKMP:   attributes in transform:
*May 24 18:02:48.488: ISAKMP:     key length is 128
*May 24 18:02:48.488: ISAKMP:     authenticator is HMAC-SHA
*May 24 18:02:48.488: ISAKMP:     encaps is 1 (Tunnel)
*May 24 18:02:48.488: ISAKMP:     SA life type in seconds
*May 24 18:02:48.488: ISAKMP:     SA life duration (basic) of 3600
*May 24 18:02:48.488: ISAKMP:     SA life type in kilobytes
*May 24 18:02:48.488: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*May 24 18:02:48.488: ISAKMP:(1003):atts are acceptable.
*May 24 18:02:48.488: IPSEC(validate_proposal_request): proposal part #1
*May 24 18:02:48.488: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.10.1:0, remote= 172.16.10.2:0,
    local_proxy= 192.168.1.0/255.255.255.0/256/0,
    remote_proxy= 192.168.2.0/255.255.255.0/256/0,
    protocol= ESP, transform= NONE (Tunnel),

```



```

    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 24 18:02:48.488: Crypto mapdb : proxy_match
    src addr      : 192.168.1.0
    dst addr      : 192.168.2.0
    protocol      : 0
    src port      : 0
    dst port      : 0
*May 24 18:02:48.488: ISAKMP:(1003): processing NONCE payload. message ID = 2605730229
*May 24 18:02:48.488: ISAKMP:(1003): processing ID payload. message ID = 2605730229
*May 24 18:02:48.488: ISAKMP:(1003): processing ID payload. message ID = 2605730229
*May 24 18:02:48.488: ISAKMP:(1003):Node 2605730229, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*May 24 18:02:48.488: ISAKMP:(1003):Old State = IKE_QM_I_QM1 New State =
IKE_QM_IPSEC_INSTALL_AWAIT
*May 24 18:02:48.488: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*May 24 18:02:48.488: Crypto mapdb : proxy_match
    src addr      : 192.168.1.0
    dst addr      : 192.168.2.0
    protocol      : 256
    src port      : 0
    dst port      : 0
*May 24 18:02:48.488: IPSEC(crypto_ipsec_create_ipsec_sas): Map found cmap
*May 24 18:02:48.489: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the
same proxies and peer 172.16.10.2
*May 24 18:02:48.489: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
    sa_spi= 0x4C0D0EF0(1275924208),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 7
    sa_lifetime(k/sec)= (4608000/3600)
*May 24 18:02:48.489: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.10.2, sa_proto= 50,
    sa_spi= 0xC72072C6(3340792518),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 8
    sa_lifetime(k/sec)= (4608000/3600)

```

在相位互联网安全协会和密钥管理协议(ISAKMP)和IPSec请是UP。

## Cisco IOS : 检查IPSec计数器

```

R1#show crypto session detail
Crypto session current status

```

```

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

```

```

Interface: Ethernet0/0
Uptime: 00:00:05
Session status: UP-ACTIVE
Peer: 172.16.10.2 port 500 fvrf: (none) ivrf: (none)
    Phase1_id: 172.16.10.2
    Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.10.2/500 Active
    Capabilities:(none) connid:1003 lifetime:23:59:54
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
    Active SAs: 2, origin: crypto map
    Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4164218/3594
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4164218/3594A

```

在100数据包以后发送：

```
R1#ping 192.168.2.1 source e0/1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/4/5 ms
R1#
```

```
R1#show crypto session detail
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Ethernet0/0
Uptime: 00:00:09
Session status: UP-ACTIVE
Peer: 172.16.10.2 port 500 fvrf: (none) ivrf: (none)
  Phase1_id: 172.16.10.2
  Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.10.2/500 Active
  Capabilities:(none) connid:1003 lifetime:23:59:50
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
  Active SAs: 2, origin: crypto map
  Inbound:  #pkts dec'ed 100 drop 0 life (KB/Sec) 4164202/3590
  Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4164202/3590
```

## Cisco IOS : 验证IKEv1和IPSec参数

```
R1#show crypto isakmp sa detail
```

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local          Remote          I-VRF  Status Encr Hash  Auth DH Lifetime Cap.
-----
1003  172.16.10.1      172.16.10.2          ACTIVE aes  sha  psk  5  23:59:35
      Engine-id:Conn-id = SW:3
```

```
R1#show crypto ipsec sa
```

```
interface: Ethernet0/0
  Crypto map tag: cmap, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 172.16.10.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.10.2
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xC72072C6(3340792518)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0x4C0D0EF0(1275924208)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 7, flow_id: SW:7, sibling_flags 80000040, crypto map: cmap
sa timing: remaining key lifetime (k/sec): (4164202/3562)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0xC72072C6(3340792518)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 8, flow_id: SW:8, sibling_flags 80000040, crypto map: cmap
sa timing: remaining key lifetime (k/sec): (4164202/3562)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

两个相位是UP。IPSec安全参数索引(SPI)协商。在100数据包被发送后，计数器增加到100。

## strongSwan : 隧道建立

```
pluton# /etc/init.d/ipsec start
```

```
May 24 20:02:48 localhost charon: 10[NET] received packet: from 172.16.10.1[500]
to 172.16.10.2[500] (168 bytes)
May 24 20:02:48 localhost charon: 10[ENC] parsed ID_PROT request 0 [ SA V V V V ]
May 24 20:02:48 localhost charon: 10[IKE] received NAT-T (RFC 3947) vendor ID
May 24 20:02:48 localhost charon: 10[IKE] received draft-ietf-ipsec-nat-t-ike-07
vendor ID
May 24 20:02:48 localhost charon: 10[IKE] received draft-ietf-ipsec-nat-t-ike-03
vendor ID
May 24 20:02:48 localhost charon: 10[IKE] received draft-ietf-ipsec-nat-t-ike-02\n
vendor ID
May 24 20:02:48 localhost charon: 10[IKE] 172.16.10.1 is initiating a Main Mode IKE_SA
May 24 20:02:48 localhost charon: 10[IKE] 172.16.10.1 is initiating a Main Mode IKE_SA
May 24 20:02:48 localhost charon: 10[ENC] generating ID_PROT response 0 [ SA V V V V ]
May 24 20:02:48 localhost charon: 10[NET] sending packet: from 172.16.10.2[500] to
172.16.10.1[500] (140 bytes)
May 24 20:02:48 localhost charon: 11[NET] received packet: from 172.16.10.1[500] to
172.16.10.2[500] (348 bytes)
May 24 20:02:48 localhost charon: 11[ENC] parsed ID_PROT request 0
[ KE No V V V NAT-D NAT-D ]
May 24 20:02:48 localhost charon: 11[ENC] generating ID_PROT response 0
[ KE No NAT-D NAT-D ]
May 24 20:02:48 localhost charon: 11[NET] sending packet: from 172.16.10.2[500]
to 172.16.10.1[500] (308 bytes)
May 24 20:02:48 localhost charon: 12[NET] received packet: from 172.16.10.1[500]
```

```

to 172.16.10.2[500] (108 bytes)
May 24 20:02:48 localhost charon: 12[ENC] parsed ID_PROT request 0
[ ID HASH N(INITIAL_CONTACT) ]
May 24 20:02:48 localhost charon: 12[CFG] looking for pre-shared key peer configs
matching 172.16.10.2...172.16.10.1[172.16.10.1]
May 24 20:02:48 localhost charon: 12[CFG] selected peer config "ciscoios"
May 24 20:02:48 localhost charon: 12[IKE] IKE_SA ciscoios{2} established between
172.16.10.2[172.16.10.2]...172.16.10.1[172.16.10.1]
May 24 20:02:48 localhost charon: 12[IKE] IKE_SA ciscoios{2} established between
172.16.10.2[172.16.10.2]...172.16.10.1[172.16.10.1]
May 24 20:02:48 localhost charon: 12[IKE] scheduling reauthentication in 3289s
May 24 20:02:48 localhost charon: 12[IKE] maximum IKE_SA lifetime 3469s
May 24 20:02:48 localhost charon: 12[ENC] generating ID_PROT response 0 [ ID HASH ]
May 24 20:02:48 localhost charon: 12[NET] sending packet: from 172.16.10.2[500] to
172.16.10.1[500] (76 bytes)
May 24 20:02:48 localhost charon: 14[NET] received packet: from 172.16.10.1[500] to
172.16.10.2[500] (188 bytes)
May 24 20:02:48 localhost charon: 14[ENC] parsed QUICK_MODE request 2605730229
[ HASH SA No ID ID ]
May 24 20:02:48 localhost charon: 14[IKE] received 3600s lifetime, configured 1200s
May 24 20:02:48 localhost charon: 14[IKE] received 4608000000 lifebytes, configured 0
May 24 20:02:48 localhost charon: 14[ENC] generating QUICK_MODE response 2605730229
[ HASH SA No ID ID ]
May 24 20:02:48 localhost charon: 14[NET] sending packet: from 172.16.10.2[500] to
172.16.10.1[500] (188 bytes)
May 24 20:02:48 localhost charon: 15[NET] received packet: from 172.16.10.1[500] to
172.16.10.2[500] (60 bytes)
May 24 20:02:48 localhost charon: 15[ENC] parsed QUICK_MODE request 2605730229 [ HASH ]
May 24 20:02:48 localhost charon: 15[IKE] CHILD_SA ciscoios{2} established with SPIs
c72072c6_i 4c0d0ef0_o and TS 192.168.2.0/24 === 192.168.1.0/24
May 24 20:02:48 localhost charon: 15[IKE] CHILD_SA ciscoios{2} established with SPIs
c72072c6_i 4c0d0ef0_o and TS 192.168.2.0/24 === 192.168.1.0/24
May 24 20:02:48 localhost vpn: + 172.16.10.1 192.168.1.0/24 == 172.16.10.1 --
172.16.10.2 == 192.168.2.0/24

```

两个相位是UP。保护192.168.2.0/24和192.168.1.0/24之间的流量的正确斯皮协商。

## strongSwan : 验证IPSec连接状态

```

pluton ~ # ipsec statusall
Status of IKE charon daemon (strongSwan 5.0.4, Linux 3.2.12-gentoo, x86_64):
  uptime: 4 minutes, since May 24 20:02:15 2013
  malloc: sbrk 393216, mmap 0, used 274064, free 119152
  worker threads: 8 of 16 idle, 7/1/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon mysql sqlite aes des sha1 sha2 md5 random nonce x509
  revocation constraints pubkey pkcs1 pkcs8 pgp dnskey pem openssl gcrypt fips-prf
  gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke updown
  eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth
  eap-md5 eap-gtc eap-mschapv2 eap-radius xauth-generic
Listening IP addresses:
  10.0.0.100
  192.168.10.1
  172.16.10.2
  192.168.2.1
Connections:
  ciscoios: 172.16.10.2...172.16.10.1 IKEv1
  ciscoios: local: [172.16.10.2] uses pre-shared key authentication
  ciscoios: remote: [172.16.10.1] uses pre-shared key authentication
  ciscoios: child: 192.168.2.0/24 === 192.168.1.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
  ciscoios{2}: ESTABLISHED 4 minutes ago, 172.16.10.2[172.16.10.2]...
172.16.10.1[172.16.10.1]

```

```

ciscoios[2]: IKEv1 SPIs: 278f22e3c3e5f606_i dbb5a27f3e0eccd1_r*,
pre-shared key reauthentication in 50 minutes
ciscoios[2]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
ciscoios{2}:  INSTALLED, TUNNEL, ESP SPIs: c72072c6_i 4c0d0ef0_o
ciscoios{2}:  AES_CBC_128/HMAC_SHA1_96, 10000 bytes_i (100 pkts, 255s ago),
10000 bytes_o (100 pkts, 255s ago), rekeying in 11 minutes
ciscoios{2}:  192.168.2.0/24 === 192.168.1.0/24

```

关于经过协商的ISAKMP的详细信息和IPSec参数是可用的。

## strongSwan : 验证IPSec策略

```

pluton ~ # ip -s xfrm policy
src 192.168.1.0/24 dst 192.168.2.0/24 uid 0
  dir fwd action allow index 258 priority 1859 share any flag (0x00000000)
  lifetime config:
    limit: soft (INF)(bytes), hard (INF)(bytes)
    limit: soft (INF)(packets), hard (INF)(packets)
    expire add: soft 0(sec), hard 0(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    0(bytes), 0(packets)
    add 2013-05-24 20:02:48 use -
  tmpl src 172.16.10.1 dst 172.16.10.2
    proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
    level required share any
    enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff
src 192.168.1.0/24 dst 192.168.2.0/24 uid 0
  dir in action allow index 248 priority 1859 share any flag (0x00000000)
  lifetime config:
    limit: soft (INF)(bytes), hard (INF)(bytes)
    limit: soft (INF)(packets), hard (INF)(packets)
    expire add: soft 0(sec), hard 0(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    0(bytes), 0(packets)
    add 2013-05-24 20:02:48 use 2013-05-24 20:02:56
  tmpl src 172.16.10.1 dst 172.16.10.2
    proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
    level required share any
    enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff
src 192.168.2.0/24 dst 192.168.1.0/24 uid 0
  dir out action allow index 241 priority 1859 share any flag (0x00000000)
  lifetime config:
    limit: soft (INF)(bytes), hard (INF)(bytes)
    limit: soft (INF)(packets), hard (INF)(packets)
    expire add: soft 0(sec), hard 0(sec)
    expire use: soft 0(sec), hard 0(sec)
  lifetime current:
    0(bytes), 0(packets)
    add 2013-05-24 20:02:48 use 2013-05-24 20:02:56
  tmpl src 172.16.10.2 dst 172.16.10.1
    proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
    level required share any
    enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff

```

上一个详细信息包括内政表。

## 在Cisco IOS之间的IKEv2和strongSwan

## Cisco IOS

```
R1#ping 192.168.2.1 source e0/1 repeat 1
```

### Cisco IOS触发的隧道建立

```
*May 24 19:14:10.485: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 172.16.10.1:500, remote= 172.16.10.2:500,
  local_proxy= 192.168.1.0/255.255.255.0/256/0,
  remote_proxy= 192.168.2.0/255.255.255.0/256/0,
  protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 24 19:14:10.486: IKEv2:% Getting preshared key from profile keyring keys
*May 24 19:14:10.486: IKEv2:% Matched peer block 'strongswan'
*May 24 19:14:10.486: IKEv2:Searching Policy with fvrf 0, local address 172.16.10.1
*May 24 19:14:10.486: IKEv2:Found Policy 'ikev2policy'
*May 24 19:14:10.486: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public
key, DH Group 5
*May 24 19:14:10.486: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
*May 24 19:14:10.486: IKEv2:(SA ID = 1):Request queued for computation of DH key
*May 24 19:14:10.486: IKEv2:IKEv2 initiator - no config data to send in IKE_SA_INIT exch
*May 24 19:14:10.486: IKEv2:(SA ID = 1):Generating IKE_SA_INIT message
*May 24 19:14:10.486: IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0
(initial negotiation),
Num. transforms: 4
  AES-CBC  SHA1  SHA96  DH_GROUP_1536_MODP/Group 5
*May 24 19:14:10.486: IKEv2:(SA ID = 1):Sending Packet [To 172.16.10.2:500/From
172.16.10.1:500/VRF i0:f0]
Initiator SPI : 9FFC38791FFEF212 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
  SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
*May 24 19:14:10.486: IKEv2:(SA ID = 1):Insert SA
*May 24 19:14:10.495: IKEv2:(SA ID = 1):Received Packet [From 172.16.10.2:500/To
172.16.10.1:500/VRF i0:f0]
Initiator SPI : 9FFC38791FFEF212 - Responder SPI : 6CDC17F5B0B10C1A Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
  SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
NOTIFY(Unknown - 16404)
*May 24 19:14:10.495: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
*May 24 19:14:10.495: IKEv2:(SA ID = 1):Verify SA init message
*May 24 19:14:10.495: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
*May 24 19:14:10.495: IKEv2:(SA ID = 1):Checking NAT discovery
*May 24 19:14:10.495: IKEv2:(SA ID = 1):NAT not found
*May 24 19:14:10.495: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH
secret key, DH Group 5
*May 24 19:14:10.504: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation
PASSED
*May 24 19:14:10.504: IKEv2:(SA ID = 1):Request queued for computation of DH secret
*May 24 19:14:10.504: IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED
and create rekeyed IKEv2 SA
*May 24 19:14:10.504: IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED
calculation and creation of
rekeyed IKEv2 SA PASSED
*May 24 19:14:10.504: IKEv2:(SA ID = 1):Completed SA init exchange
```

\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Check for EAP exchange  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Generate my authentication data  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):**Use preshared key for id 172.16.10.1,**  
key len 5  
\*May 24 19:14:10.504: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication  
data  
\*May 24 19:14:10.504: IKEv2:[Crypto Engine -> IKEv2] **IKEv2 authentication data**  
**generation PASSED**  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Get my authentication method  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):My authentication method is 'PSK'  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Check for EAP exchange  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Generating IKE\_AUTH message  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Constructing IDi payload: '172.16.10.1'  
of type 'IPv4 address'  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):**ESP Proposal: 1**, SPI size: 4  
(IPSec negotiation),  
**Num. transforms: 3**  
**AES-CBC SHA96 Don't use ESN**  
\*May 24 19:14:10.504: IKEv2:(SA ID = 1):Building packet for encryption.  
Payload contents:  
VID IDi AUTH SA TSi TSr NOTIFY(INITIAL\_CONTACT) NOTIFY(SET\_WINDOW\_SIZE)  
NOTIFY(ESP\_TFC\_NO\_SUPPORT) NOTIFY(NON\_FIRST\_FRAGS)  
  
\*May 24 19:14:10.505: IKEv2:(SA ID = 1):**Sending Packet**  
[To 172.16.10.2:500/From 172.16.10.1:500/VRF i0:f0]  
Initiator SPI : 9FFC38791FFEF212 - Responder SPI : 6CDC17F5B0B10C1A Message id: 1  
IKEv2 IKE\_AUTH Exchange REQUEST  
Payload contents:  
ENCR  
  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):**Received Packet**  
[From 172.16.10.2:500/To 172.16.10.1:500/VRF i0:f0]  
Initiator SPI : 9FFC38791FFEF212 - Responder SPI : 6CDC17F5B0B10C1A Message id: 1  
IKEv2 IKE\_AUTH Exchange RESPONSE  
Payload contents:  
IDr AUTH SA TSi TSr NOTIFY(Unknown - 16403)  
  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Process auth response notify  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Searching policy based on peer's  
identity '172.16.10.2' of type 'IPv4 address'  
\*May 24 19:14:10.522: IKEv2:Searching Policy with fvrf 0, local address 172.16.10.1  
\*May 24 19:14:10.522: IKEv2:Found Policy 'ikev2policy'  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Verify peer's policy  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Peer's policy verified  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Get peer's authentication method  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):**Get peer's preshared key for 172.16.10.2**  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Verify peer's authentication data  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Use preshared key for id 172.16.10.2, key len 5  
\*May 24 19:14:10.522: IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data  
\*May 24 19:14:10.522: IKEv2:[Crypto Engine -> IKEv2] **IKEv2 authentication data**  
**generation PASSED**  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):**Verification of peer's authentication data**  
**PASSED**  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Check for EAP exchange  
\*May 24 19:14:10.522: IKEv2:(SA ID = 1):Processing IKE\_AUTH message  
\*May 24 19:14:10.522: IKEv2:KMI/verify policy/sending to IPSec:  
prot: 3 txfm: 12 hmac 2 flags 8177 keysize 128 IDB 0x0  
\*May 24 19:14:10.522: IPSEC(validate\_proposal\_request): proposal part #1  
\*May 24 19:14:10.522: IPSEC(validate\_proposal\_request): proposal part #1,  
(key eng. msg.) INBOUND local= 172.16.10.1:0, remote= 172.16.10.2:0,  
**local\_proxy= 192.168.1.0/255.255.255.0/256/0,**  
**remote\_proxy= 192.168.2.0/255.255.255.0/256/0,**

```

protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 24 19:14:10.522: Crypto mapdb : proxy_match
    src addr      : 192.168.1.0
    dst addr      : 192.168.2.0
    protocol      : 0
    src port      : 0
    dst port      : 0
*May 24 19:14:10.522: IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database.
SA lifetime timer (86400 sec) started
*May 24 19:14:10.522: IKEv2:(SA ID = 1):Session with IKE ID PAIR
(172.16.10.2, 172.16.10.1) is UP
*May 24 19:14:10.522: IKEv2:IKEv2 MIB tunnel started, tunnel index 1
*May 24 19:14:10.522: IKEv2:(SA ID = 1):Load IPSEC key material
*May 24 19:14:10.522: IKEv2:(SA ID = 1):[IKEv2 -> IPsec] Create IPsec SA into
IPsec database
*May 24 19:14:10.522: IKEv2:(SA ID = 1):Asynchronous request queued

*May 24 19:14:10.522: IKEv2:(SA ID = 1):
*May 24 19:14:10.523: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*May 24 19:14:10.523: Crypto mapdb : proxy_match
    src addr      : 192.168.1.0
    dst addr      : 192.168.2.0
    protocol      : 256
    src port      : 0
    dst port      : 0
*May 24 19:14:10.523: IPSEC(crypto_ipsec_create_ipsec_sas): Map found cmap
*May 24 19:14:10.523: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and peer 172.16.10.2
*May 24 19:14:10.523: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
    sa_spi= 0xDF405365(3745534821),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 6
    sa_lifetime(k/sec)= (4608000/3600)
*May 24 19:14:10.523: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.10.2, sa_proto= 50,
    sa_spi= 0xC0CC116C(3234599276),
    sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 5
    sa_lifetime(k/sec)= (4608000/3600)
*May 24 19:14:10.523: IPSEC: Expand action denied, notify RP
*May 24 19:14:10.523: IKEv2:(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec
SA into IPsec database PASSED

```

保护192.168.1.0/24和192.168.2.0/24之间的流量的IKEv2会话启用，并且IPSec SA创建。

## Cisco IOS : 检查IPSec计数器

```

R1#show crypto session detail
Crypto session current status

```

```

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

```

```

Interface: Ethernet0/0
Uptime: 00:00:09
Session status: UP-ACTIVE
Peer: 172.16.10.2 port 500 fvrf: (none) ivrf: (none)
    Phase1_id: 172.16.10.2
    Desc: (none)
IKEv2 SA: local 172.16.10.1/500 remote 172.16.10.2/500 Active

```



```
Capabilities:(none) connid:1 lifetime:23:59:51
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4375820/3590
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4375820/3590
```

在100数据包以后发送：

```
R1#ping 192.168.2.1 source 192.168.1.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/5 ms
R1#
```

```
R1#show crypto session detail
Crypto session current status
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
Interface: Ethernet0/0
Uptime: 00:00:15
Session status: UP-ACTIVE
Peer: 172.16.10.2 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.2
Desc: (none)
IKEv2 SA: local 172.16.10.1/500 remote 172.16.10.2/500 Active
Capabilities:(none) connid:1 lifetime:23:59:45
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
Inbound:  #pkts dec'ed 100 drop 0 life (KB/Sec) 4375803/3585
Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4375803/3585
```

计数器由100增加。

## Cisco IOS : 验证IKEv2和IPSec参数

Cisco IOS有非常好的统计信息/详细信息IKEv2会话的：

```
R1#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA
```

Tunnel-id	Local	Remote	fvrf/ivrf	Status
1	172.16.10.1/500	172.16.10.2/500	none/none	READY
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/152 sec				
CE id: 1019, Session-id: 3				
Status Description: Negotiation done				
Local spi: 9FFC38791FFEF212		Remote spi: 6CDC17F5B0B10C1A		
Local id: 172.16.10.1				
Remote id: 172.16.10.2				
Local req msg id: 2		Remote req msg id: 0		
Local next msg id: 2		Remote next msg id: 0		
Local req queued: 2		Remote req queued: 0		
Local window: 5		Remote window: 1		
DPD configured for 0 seconds, retry 0				

Fragmentation not configured.  
Extended Authentication not configured.  
NAT-T is not detected  
Cisco Trust Security SGT is disabled  
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA

R1#show crypto ipsec sa

```
interface: Ethernet0/0
  Crypto map tag: cmap, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 172.16.10.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.10.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xC0CC116C(3234599276)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xDF405365(3745534821)
    transform: esp-aes esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: cmap
    sa timing: remaining key lifetime (k/sec): (4375803/3442)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xC0CC116C(3234599276)
    transform: esp-aes esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: cmap
    sa timing: remaining key lifetime (k/sec): (4375803/3442)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

strongSwan : 隧道建立

May 24 21:14:10 localhost charon: 08[NET] received packet: from 172.16.10.1[500]

```

to 172.16.10.2[500] (400 bytes)
May 24 21:14:10 localhost charon: 08[ENC] parsed IKE_SA_INIT request 0
[ SA KE No V V N(NATD_S_IP) N(NATD_D_IP) ]
May 24 21:14:10 localhost charon: 08[ENC] received unknown vendor
ID: 43:49:53:43:4f:2d:44:45:4c:45:54:45:2d:52:45:41:53:4f:4e
May 24 21:14:10 localhost charon: 08[ENC] received unknown vendor ID:
46:4c:45:58:56:50:4e:2d:53:55:50:50:4f:52:54:45:44
May 24 21:14:10 localhost charon: 08[IKE] 172.16.10.1 is initiating an IKE_SA
May 24 21:14:10 localhost charon: 08[IKE] 172.16.10.1 is initiating an IKE_SA
May 24 21:14:10 localhost charon: 08[ENC] generating IKE_SA_INIT response 0
[ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH) ]
May 24 21:14:10 localhost charon: 08[NET] sending packet: from 172.16.10.2[500]
to 172.16.10.1[500] (376 bytes)
May 24 21:14:10 localhost charon: 07[NET] received packet: from 172.16.10.1[500]
to 172.16.10.2[500] (284 bytes)
May 24 21:14:10 localhost charon: 07[ENC] parsed IKE_AUTH request 1 [ V IDi AUTH
SA TSi TSr N(INIT_CONTACT) N(SET_WINSIZE) N(ESP_TFC_PAD_N) N(NON_FIRST_FRAG) ]
May 24 21:14:10 localhost charon: 07[CFG] looking for peer configs matching
172.16.10.2[%any]...172.16.10.1[172.16.10.1]
May 24 21:14:10 localhost charon: 07[CFG] selected peer config 'ciscoios'
May 24 21:14:10 localhost charon: 07[IKE] authentication of '172.16.10.1' with
pre-shared key successful
May 24 21:14:10 localhost charon: 07[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED,
not using ESPv3 TFC padding
May 24 21:14:10 localhost charon: 07[IKE] authentication of '172.16.10.2' (myself)
with pre-shared key
May 24 21:14:10 localhost charon: 07[IKE] IKE_SA ciscoios[2] established between
172.16.10.2[172.16.10.2]...172.16.10.1[172.16.10.1]
May 24 21:14:10 localhost charon: 07[IKE] IKE_SA ciscoios[2] established between
172.16.10.2[172.16.10.2]...172.16.10.1[172.16.10.1]
May 24 21:14:10 localhost charon: 07[IKE] scheduling reauthentication in 3247s
May 24 21:14:10 localhost charon: 07[IKE] maximum IKE_SA lifetime 3427s
May 24 21:14:10 localhost charon: 07[IKE] CHILD_SA ciscoios{2} established with
SPIs c0cc116c_i df405365_o and TS 192.168.2.0/24 === 192.168.1.0/24
May 24 21:14:10 localhost charon: 07[IKE] CHILD_SA ciscoios{2} established with
SPIs c0cc116c_i df405365_o and TS 192.168.2.0/24 === 192.168.1.0/24
May 24 21:14:10 localhost vpn: + 172.16.10.1 192.168.1.0/24 == 172.16.10.1 --
172.16.10.2 == 192.168.2.0/24

```

隧道建立详细信息查找得有点类似于IKEv1。

## strongSwan : 验证IPSec连接状态

```

pluton ~ # ipsec statusall
Status of IKE charon daemon (strongSwan 5.0.4, Linux 3.2.12-gentoo, x86_64):
  uptime: 2 minutes, since May 24 21:13:27 2013
  malloc: sbrk 393216, mmap 0, used 274864, free 118352
  worker threads: 8 of 16 idle, 7/1/0/0 working, job queue: 0/0/0/0, scheduled: 4
  loaded plugins: charon mysql sqlite aes des sha1 sha2 md5 random nonce x509
  revocation constraints pubkey pkcs1 pkcs8 pgp dnskey pem openssl gcrypt
  fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default
  stroke updown eap-identity eap-sim eap-aka eap-aka-3gpp2 eap-simaka-pseudonym
  eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-radius xauth-generic
Listening IP addresses:
  10.0.0.100
  192.168.10.1
  192.168.2.1
  172.16.10.2
Connections:
  ciscoios: 172.16.10.2...172.16.10.1 IKEv2
  ciscoios: local: [172.16.10.2] uses pre-shared key authentication
  ciscoios: remote: [172.16.10.1] uses pre-shared key authentication

```

```

ciscoios:   child: 192.168.2.0/24 === 192.168.1.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
  ciscoios[2]: ESTABLISHED 116 seconds ago, 172.16.10.2[172.16.10.2]...
172.16.10.1[172.16.10.1]
  ciscoios[2]: IKEv2 SPIs: 12f2fe1f7938fc9f_i 1a0cblb0f517dc6c_r*,
pre-shared key reauthentication in 52 minutes
  ciscoios[2]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
  ciscoios{2}:  INSTALLED, TUNNEL, ESP SPIs: c0cc116c_i df405365_o
  ciscoios{2}:  AES_CBC_128/HMAC_SHA1_96, 10000 bytes_i (100 pkts, 102s ago),
10000 bytes_o (100 pkts, 102s ago), rekeying in 12 minutes
  ciscoios{2}:   192.168.2.0/24 === 192.168.1.0/24

```

## strongSwan : 验证IPSec策略

```

pluton ~ # ip -s xfrm policy
src 192.168.1.0/24 dst 192.168.2.0/24 uid 0
  dir fwd action allow index 1154 priority 1859 share any flag (0x00000000)
lifetime config:
  limit: soft (INF)(bytes), hard (INF)(bytes)
  limit: soft (INF)(packets), hard (INF)(packets)
  expire add: soft 0(sec), hard 0(sec)
  expire use: soft 0(sec), hard 0(sec)
lifetime current:
  0(bytes), 0(packets)
  add 2013-05-24 21:14:10 use -
tmpl src 172.16.10.1 dst 172.16.10.2
  proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
  level required share any
  enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff
src 192.168.1.0/24 dst 192.168.2.0/24 uid 0
  dir in action allow index 1144 priority 1859 share any flag (0x00000000)
lifetime config:
  limit: soft (INF)(bytes), hard (INF)(bytes)
  limit: soft (INF)(packets), hard (INF)(packets)
  expire add: soft 0(sec), hard 0(sec)
  expire use: soft 0(sec), hard 0(sec)
lifetime current:
  0(bytes), 0(packets)
  add 2013-05-24 21:14:10 use 2013-05-24 21:14:23
tmpl src 172.16.10.1 dst 172.16.10.2
  proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
  level required share any
  enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff
src 192.168.2.0/24 dst 192.168.1.0/24 uid 0
  dir out action allow index 1137 priority 1859 share any flag (0x00000000)
lifetime config:
  limit: soft (INF)(bytes), hard (INF)(bytes)
  limit: soft (INF)(packets), hard (INF)(packets)
  expire add: soft 0(sec), hard 0(sec)
  expire use: soft 0(sec), hard 0(sec)
lifetime current:
  0(bytes), 0(packets)
  add 2013-05-24 21:14:10 use 2013-05-24 21:14:23
tmpl src 172.16.10.2 dst 172.16.10.1
  proto esp spi 0x00000000(0) reqid 2(0x00000002) mode tunnel
  level required share any
  enc-mask ffffffff auth-mask ffffffff comp-mask ffffffff

```

## 相关信息

- [Openswan](#)
- [strongSwan用户文档](#)
- [FlexVPN和互联网密钥交换版本2配置指南， Cisco IOS版本15M&T](#)
- [技术支持和文档 - Cisco Systems](#)