站点到站点VPN的IOS IKEv2调试与排除故障TechNote的PSKs

目录

简介

本文描述互联网密钥交换在Cisco IOS的版本2 (IKEv2)调试，当使用预先共享密钥(PSK)时。另外，本文在配置里提供信息关于怎样翻译某些调试线路。

先决条件

要求

思科建议您有信息包交换的知识IKEv2的。欲知更多信息，参考IKEv2信息包交换和协议级调试。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 互联网密钥交换版本2 (IKEv2)
- Cisco IOS 15.1(1)T或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

核心问题

在IKEv2的信息包交换是完全不同的与在IKEv1的信息包交换。在IKEv1中有包括第2阶段交换跟随的六(6)数据包包括三(3)数据包的清楚地被标定的phase1交换;IKEv2交换可变。关于差异和信息包交换的说明的更多信息，参考IKEv2信息包交换和协议级调试。

路由器配置

此部分列出用于本文的配置。

路由器 1

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.101 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.2
tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 policy site-pol
proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
peer peer1
address 10.0.0.2 255.255.255.0
hostname host1
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
```

```
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

路由器 2

```
crypto ikev2 proposal PHASE1-prop
encryption 3des aes-cbc-128
integrity sha1
group 2
!
crypto ikev2 keyring KEYRNG
peer peer2
address 10.0.0.1 255.255.255.0
hostname host2
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile IKEV2-SETUP
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local KEYRNG
lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
set transform-set TS
set ikev2-profile IKEV2-SETUP
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
ip address 172.16.0.102 255.255.255.0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel destination 10.0.0.1
tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

故障排除

路由器调试

这些调试指令用于本文：

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

路由器1 (发起者)消息说明	调试	Router2 (响应方)消息说明
路由器1收到匹配对等体ASA的10.0.0.2加密ACL的数据包。启动SA创建	*Nov 11 20:28:34.003 ：IKEv2:Got从调度程序的一数据包 *Nov 11 20:28:34.003 ：IKEv2 ：处理朴队列的一个项目 *Nov 11 19:30:34.811 ：由地址10.0.0.2的IKEv2:%获得的预共享密匙 *Nov 11 19:30:34.811 ：对工具套件policyle的IKEv2:Adding建议PHASE1-prop *Nov 11 19:30:34.811 ：IKEv2:(1) ：选择IKE配置文件IKEV2-SETUP *Nov 11 19:30:34.811 ：IKEv2:New被承认的sa ikev2请求 *Nov 11 19:30:34.811 ：由一个的IKEv2:Incrementing流出的协商的sa计数 *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：IDLE事件：EV_INIT_SA *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：EV_GET_IKE_POLICY *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：**EV_SET_POLICY** *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):Setting已配置的策略 *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：EV_CHK_AUTH4PKI *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：**EV_GEN_DH_KEY** *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：EV_NO_EVENT *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：EV_OK_RECD_DH_PUBKEY_RESP *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):Action ：Action_Null *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000 (i) MsgID = 00000000 CurState ：I_BLD_INIT事件 ：EV_GET_CONFIG_MODE *Nov 11 19:30:34.811 ：IKEv2:IKEv2发起者-没有发送的设置数据在IKE_SA_INIT交换 *Nov 11 19:30:34.811 ：IKEv2:No发送的设置数据对工具套件： *Nov 11 19:30:34.811 ：IKEv2:(SA ID= 1):SM SA Trace->	
第一个对消息是IKE_SA_INIT交换。这些消息协商加密算法，交换目前，并且执行Diffie-Hellman交换。 **相关配置：** `crypto ikev2PHASE1-prop 3des aes-cbc-128 sha12crypto ikev2 KEYRNGpeer110.0.0.2 255.255.255.0host1 cisco`		

：I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000
(i) MsgID = 00000000 CurState ：I_BLD_INIT事件
：EV_BLD_MSG
*Nov 11 19:30:34.811 ：IKEv2:Construct卖方细节有效负载
：DELETE-REASON
*Nov 11 19:30:34.811 ：IKEv2:Construct卖方细节有效负载
：(自定义)
*Nov 11 19:30:34.811 ：IKEv2:Construct通知有效负载
：NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.811 ：IKEv2:Construct通知有效负载
：NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.811 ： **IKEv2:(SA ID= 1):Next**有效负载
：SA，版本：2.0 Exchange类型： **IKE_SA_INIT，**标志
： **发起者**消息ID ：0，长度：344
有效负载内容：
SA下有效负载：KE，保留：0x0，长度：56
最后建议：0x0，保留：0x0，长度：52
建议：1，协议ID ：IKE， SPI大小：0， #trans ：5最后转换：0x3，保留：0x0 ：长度：8
类型：1，保留：0x0， id ：3DES
最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
KE下有效负载：N，保留：0x0，长度：136
DH组：2，保留：0x0
N下有效负载：VID，保留：0x0，长度：24
VID下有效负载：VID，保留：0x0，长度：23
VID下有效负载：通知，保留：0x0，长度：21
NOTIFY(NAT_DETECTION_SOURCE_IP)下有效负载：通知，保留：0x0，长度：28
安全协议id ：IKE， spi大小：0，键入
：NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP)下有效负载：无，保留：0x0，长度：28
安全协议id ：IKE， spi大小：0，键入
：NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.814 ：IKEv2:Got从调度程序的一数据包
*Nov 11 19:30:34.814 ：IKEv2:Processing朴队列的一个项目
*Nov 11 19:30:34.814 ：IKEv2:New被承认的sa ikev2请求
*Nov 11 19:30:34.814 ：由一个的IKEv2:Incrementing流入协商的sa计数
*Nov 11 19:30:34.814 ：IKEv2:Next有效负载：SA，版本：2.0 Exchange类型：IKE_SA_INIT，标志：发起者消息ID：0，长度：344
有效负载内容：
SA下有效负载：KE，保留：0x0，长度：56

构件IKE_INIT_SA数据包的发起者。它包含：ISAKMP IKE发起者支持)的报头(SPI/version/flags)，SAi1 (加密算法，KEi (发起者的DH公共密钥值)和N (发起者目前)。

响应方接收IKE_INIT_SA。

响应方启动该对等体的SA创建。

最后建议：0x0，保留：0x0，长度：52
建议：1，协议ID ：IKE， SPI大小：0， #trans ：5最后转换：0x3，保留：0x0 ：长度：8
类型：1，保留：0x0， id ：3DES
最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
KE下有效负载：N，保留：0x0，长度：136
DH组：2，保留：0x0
N下有效负载：VID，保留：0x0，长度：24

*Nov 11 19:30:34.814 ：IKEv2:Parse卖方细节有效负载
：CISCO-DELETE-REASON VID下有效负载：VID，保留
：0x0，长度：23
*Nov 11 19:30:34.814 ：IKEv2:Parse卖方细节有效负载
：(自定义) VID下有效负载：通知，保留：0x0，长度：21
*Nov 11 19:30:34.814 ：IKEv2:Parse通知有效负载
：NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP)下有效负载：通知，保留：0x0，长度：28
安全协议id ：IKE， spi大小：0，键入
：NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.814 ：IKEv2:Parse通知有效负载
：NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP)下有效负载：无，保留：0x0，长度：28
安全协议id ：IKE， spi大小：0，键入
：NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：IDLE事件：**EV_RECV_INIT**
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：R_INIT事件：**EV_VERIFY_MSG**
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：R_INIT事件：**EV_INSERT_SA**
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：R_INIT事件：**EV_GET_IKE_POLICY**
*Nov 11 19:30:34.814 ：IKEv2:Adding对工具套件策略的建议默认
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->

响应方验证并且处理IKE_INIT消息：(1)从发起者提供的那些选择crypto套件， (2)计算其自己的DH密钥，并且(3)计算一个skeyid值，所有密钥可以为此IKE_SA派生。所有，除了跟随所有消息的报头加密并且验证。用于加密和完整性保护的密钥从SKEYID派生和叫作：SK_e (加密)，SK_a (验证)，SK_d派生并且使用进一步密钥材料的

：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_INIT事件：**EV_PROC_MSG**
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_INIT事件：EV_DETECT_NAT
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):Process NAT发现通知
*Nov 11 19:30:34.814 ：nat IKEv2:(SA的ID= 1):Processing检测src通知
*Nov 11 19:30:34.814 ：IKEv2:(SA匹配的ID= 1):Remote地址
*Nov 11 19:30:34.814 ：nat IKEv2:(SA的ID= 1):Processing检测dst通知
*Nov 11 19:30:34.814 ：IKEv2:(SA匹配的ID= 1):Local地址
*Nov 11 19:30:34.814 ：1):No NAT找到的IKEv2:(SA ID=
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_INIT事件：EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_SET_POLICY
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1) ：**设置已配置的策略**
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_CHK_AUTH4PKI
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_PKI_SESH_OPEN
*Nov 11 19:30:34.814 ：IKEv2:(SA ID= 1):Opening PKI会话
*Nov 11 19:30:34.815 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：**EV_GEN_DH_KEY**
*Nov 11 19:30:34.815 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_NO_EVENT
*Nov 11 19:30:34.815 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件
：**EV_OK_RECD_DH_PUBKEY_RESP**
*Nov 11 19:30:34.815 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.815 ：IKEv2:(SA ID= 1):SM SA Trace->

派生CHILD_SAs的，并且分开的SK_e和SK_a为每个方向被计算。

相关配置：

```
crypto ikev2PHASE1-prop 3des aes-cbc-128 sha12crypto ikev2 KEYRNGpeer210.0.0.1 255.255.255.0host2 cisco
```

：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：**EV_GEN_DH_SECRET**
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_NO_EVENT
*Nov 11 19:30:34.822 ：**由地址10.0.0.1的**IKEv2:%**获得的预共享密匙**
*Nov 11 19:30:34.822 ：IKEv2:Adding对工具套件策略的建议默认
*Nov 11 19:30:34.822 ：IKEv2:(2) ：选择IKE配置文件IKEV2-SETUP
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件
：EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：**EV_GEN_SKEYID**
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1) ：**生成skeyid**
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_GET_CONFIG_MODE
*Nov 11 19:30:34.822 ：IKEv2:IKEv2响应方-没有发送的设置数据在IKE_SA_INIT交换
*Nov 11 19:30:34.822 ：IKEv2:No发送的设置数据对工具套件：
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000
CurState ：R_BLD_INIT事件：EV_BLD_MSG
*Nov 11 19:30:34.822 ：IKEv2:Construct卖方细节有效负载：DELETE-REASON
*Nov 11 19:30:34.822 ：IKEv2:Construct卖方细节有效负载：(自定义)
*Nov 11 19:30:34.822 ：IKEv2:Construct通知有效负载：NAT_DETECTION_SOURCE_IP
*Nov 11 19:30:34.822 ：IKEv2:Construct通知有效负载：NAT_DETECTION_DESTINATION_IP
*Nov 11 19:30:34.822 ：IKEv2:Construct通知有效负载：HTTP_CERT_LOOKUP_SUPPORTED
*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):Next有效负载：SA，版本：2.0 Exchange类型： **IKE_SA_INIT，**标志： **响应方MSG-RESPONSE**消息ID ：0，长度：449
有效负载内容：
SA下有效负载：KE，保留：0x0，长度：48
最后建议：0x0，保留：0x0，长度：44

Router2建立IKE_SA_INIT交换的响应方消息，由ASA1接收。此数据包包含：ISAKMP报头

	建议：1，协议ID ：IKE， SPI大小：0， #trans ：4最后转换：0x3，保留：0x0 ：长度：12 类型：1，保留：0x0， id ：AES-CBC 最后转换：0x3，保留：0x0 ：长度：8 类型：2，保留：0x0， id ：SHA1 最后转换：0x3，保留：0x0 ：长度：8 类型：3，保留：0x0， id ：SHA96 最后转换：0x0，保留：0x0 ：长度：8 类型：4，保留：0x0， id ：DH_GROUP_1024_MODP/Group 2 KE下有效负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 N下有效负载：VID，保留：0x0，长度：24 VID下有效负载：VID，保留：0x0，长度：23 VID下有效负载：通知，保留：0x0，长度：21 NOTIFY(NAT_DETECTION_SOURCE_IP)下有效负载：通知，保留：0x0，长度：28 安全协议id ：IKE， spi大小：0，键入 ：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下有效负载：CERTREQ，保留：0x0，长度：28 安全协议id ：IKE， spi大小：0，键入 ：NAT_DETECTION_DESTINATION_IP CERTREQ下有效负载：通知，保留：0x0，长度：105 Cert编码PKIX哈希和URL NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下有效负载：无，保留：0x0，长度：8 安全协议id ：IKE， spi大小：0，键入 ：HTTP_CERT_LOOKUP_SUPPORTED *Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：INIT_DONE事件：EV_DONE *Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):Cisco DeleteReason Notify启用 *Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：INIT_DONE事件：EV_CHK4_ROLE		(SPI/版本/标志)，IKE响应方选择)，KEr的SAr1(cryptographic算法(响应方的DH公共密钥值)和响应方目前。
	*Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：INIT_DONE事件：**EV_START_TMR** *Nov 11 19:30:34.822 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000000 CurState ：R_WAIT_AUTH事件：EV_NO_EVENT *Nov 11 19:30:34.822 ：IKEv2 ：**被承认的新的sa ikev2请求** *Nov 11 19:30:34.822 ：IKEv2 ：**增加由一个的流出的协商的sa计数**		Router2派出响应方消息到路由器1。
路由器1收到从Router2的	*Nov 11 19:30:34.823 ：IKEv2:Got从调度程序的一	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C	响应方启动验证进程的计时器。

	数据包
IKE_SA_INIT响应数据包。	*Nov 11 19:30:34.823 ：IKEv2:Got从调度程序的一数据包 4 (r) MsgID = 00000000 CurState ：INIT_DONE事件 ：**EV_START_TMR** *Nov 11 19:30:34.823 ：IKEv2:Processing朴队列的一个项目 *Nov 11 19:30:34.823 ：IKEv2:(SA ID= 1):Next有效负载 ：SA，版本：2.0 Exchange类型：IKE_SA_INIT，标志 ： **响应方MSG-RESPONSE**消息ID ：0，长度：449 有效负载内容： **SA**下有效负载：KE，保留：0x0，长度：48 最后建议：0x0，保留：0x0，长度：44 建议：1，协议ID ：IKE， SPI大小：0， #trans ：4最后转换：0x3，保留：0x0 ：长度：12 类型：1，保留：0x0， id ：AES-CBC 最后转换：0x3，保留：0x0 ：长度：8 类型：2，保留：0x0， id ：SHA1 最后转换：0x3，保留：0x0 ：长度：8 类型：3，保留：0x0， id ：SHA96 最后转换：0x0，保留：0x0 ：长度：8 类型：4，保留：0x0， id ：DH_GROUP_1024_MODP/Group 2 **KE**下有效负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 **N**下有效负载：VID，保留：0x0，长度：24
Router1验证并且处理答复：(1)计算发起者DH密钥，并且(2)发起者skeyid也生成。	*Nov 11 19:30:34.823 ：IKEv2:Parse卖方细节有效负载 ：CISCO-DELETE-REASON VID下有效负载：VID，保留 ：0x0，长度：23 *Nov 11 19:30:34.823 ：IKEv2:Parse卖方细节有效负载 ：(自定义) VID下有效负载：通知，保留：0x0，长度：21 *Nov 11 19:30:34.823 ：IKEv2:Parse通知有效负载 ：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP)下有效负载：通知，保留：0x0，长度：28 安全协议id ：IKE， spi大小：0，键入 ：NAT_DETECTION_SOURCE_IP *Nov 11 19:30:34.824 ：IKEv2:Parse通知有效负载 ：NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下有效负载 ：CERTREQ，保留：0x0，长度：28 安全协议id ：IKE， spi大小：0，键入 ：NAT_DETECTION_DESTINATION_IP CERTREQ下有效负载：通知，保留：0x0，长度：105 Cert编码PKIX哈希和URL *Nov 11 19:30:34.824 ：IKEv2:Parse通知有效负载

：HTTP_CERT_LOOKUP_SUPPORTED
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下有效负载：无，保留：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：HTTP_CERT_LOOKUP_SUPPORTED
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_WAIT_INIT事件：EV_RECV_INIT
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):Processing
IKE_SA_INIT消息
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_CHK4_NOTIFY
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_VERIFY_MSG
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_PROC_MSG
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_DETECT_NAT
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):Process NAT发现通知
*Nov 11 19:30:34.824 ：nat IKEv2:(SA的ID=
1):Processing检测src通知
*Nov 11 19:30:34.824 ：IKEv2:(SA匹配的ID= 1):Remote地址
*Nov 11 19:30:34.824 ：nat IKEv2:(SA的ID=
1):Processing检测dst通知
*Nov 11 19:30:34.824 ：IKEv2:(SA匹配的ID= 1):Local地址
*Nov 11 19:30:34.824 ：1):No NAT找到的IKEv2:(SA ID=
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_CHK_NAT_T
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_PROC_INIT事件：EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.824 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件：EV_GEN_DH_SECRET
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件：EV_NO_EVENT

*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件
：EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件：**EV_GEN_SKEYID**
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1) ：**生成skeyid**
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件：EV_DONE
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):Cisco
DeleteReason Notify启用
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：INIT_DONE事件：EV_CHK4_ROLE
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：EV_GET_CONFIG_MODE
*Nov 11 19:30:34.831 ：IKEv2:Sending对工具套件的设置
数据
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：EV_CHK_EAP
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：**EV_GEN_AUTH**
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：EV_OK_AUTH_GEN
*Nov 11 19:30:34.831 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000000
CurState ：I_BLD_AUTH事件：EV_SEND_AUTH
*Nov 11 19:30:34.831 ：IKEv2:Construct卖方细节有效负载
：CISCO-GRANITE
*Nov 11 19:30:34.831 ：IKEv2:Construct通知有效负载
：INITIAL_CONTACT
*Nov 11 19:30:34.831 ：IKEv2:Construct通知有效负载

发起者开始IKE_AUTH交换并且生成验证有效负载。IKE_AUTH数据包包含：ISAKMP报头(SPI/版本/标志)，IDi (创始者的标识)，验证有效负载，SAi2(initiates SA类似于在IKEv1的第2阶段转换集合交换)和TSi和Tsr (发起者和响应方流量选择器)：包含发起者和响应方的源地址和目的地址分别转发的/接收加密流量的他们。地址范围指定到/从该范围的所有流量被以隧道

：SET_WINDOW_SIZE
*Nov 11 19:30:34.831 ：IKEv2:Construct通知有效负载
：ESP_TFC_NO_SUPPORT
*Nov 11 19:30:34.831 ：IKEv2:Construct通知有效负载
：NON_FIRST_FRAGS
有效负载内容：
VID下有效负载：IDi，保留：0x0，长度：20
IDi下有效负载：验证，保留：0x0，长度：12
Id类型：IPv4地址，保留：0x0 0x0
验证下有效负载：CFG，保留：0x0，长度：28
验证方法PSK，保留：0x0，保留0x0
CFG下有效负载：SA，保留：0x0，长度：309
cfg类型：CFG_REQUEST，保留：0x0，保留：0x0
*Nov 11 19:30:34.831 ： SA下有效负载： **TSi**，保留
：0x0，长度：40
最后建议：0x0，保留：0x0，长度：36
建议：1，协议ID ：ESP， SPI大小：4， #trans ：3最后转
换：0x3，保留：0x0 ：长度：8
类型：1，保留：0x0， id ：3DES
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：5，保留：0x0， id ：请勿使用ESN
TSi下有效负载：Tsr，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度：16
启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255
Tsr下有效负载：通知，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度：16
启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255
NOTIFY(INITIAL_CONTACT)下有效负载：通知，保留
：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：INITIAL_CONTACT
NOTIFY(SET_WINDOW_SIZE)下有效负载：通知，保留
：0x0，长度：12
安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT)下有效负载：通知，保
留：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS)下有效负载：无，保留
：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：NON_FIRST_FRAGS

*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):Next有效负载
：ENCR，版本：2.0 Exchange类型： **IKE_AUTH**，标志
： **发起者**消息ID ：1，长度：556

传输。如果建议是可接受对响应方，退还相同的TS有效载荷。第一个CHILD_SA为匹配触发数据包的proxy_ID对创建。

相关配置：

```
crypto ipsec transform-set TS esp-3des esp-sha-hmac
crypto ipsec profile phse2-prof
set transform-set TS
ikev2-profile IKEV2-SETUP
```

有效负载内容：
ENCR下有效负载：VID，保留：0x0，长度：528

*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID =
00000001 **CurState ：I_WAIT_AUTH**事件
：EV_NO_EVENT
*Nov 11 19:30:34.832 ：IKEv2:Got从调度程序的一数据包
*Nov 11 19:30:34.832 ：IKEv2:Processing朴队列的一个项
目
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):Request有
mess_id 1;预计1至1
*Nov 11 19:30:34.832 ： **IKEv2:(SA ID= 1):Next**有效负载
：ENCR，版本：2.0 Exchange类型： **IKE_AUTH**，标志
： **发起者**消息ID ：1，长度：556
有效负载内容：
*Nov 11 19:30:34.832 ：IKEv2:Parse卖方细节有效负载
：(自定义) VID下有效负载：IDi，保留：0x0，长度：20
IDi下有效负载：验证，保留：0x0，长度：12
Id类型：IPv4地址，保留：0x0 0x0
验证下有效负载：CFG，保留：0x0，长度：28
验证方法PSK，保留：0x0，保留0x0
CFG下有效负载：SA，保留：0x0，长度：309
cfg类型：CFG_REQUEST，保留：0x0，保留：0x0
*Nov 11 19:30:34.832 ： attrib类型：内部IP4 DNS，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：内部IP4 DNS，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：内部IP4 NBNS，长
度：0
*Nov 11 19:30:34.832 ： attrib类型：内部IP4 NBNS，长
度：0
*Nov 11 19:30:34.832 ： attrib类型：内部IP4子网，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：应用程序版本，长度
：257
attrib类型：未知- 28675，长度：0
*Nov 11 19:30:34.832 ： attrib类型：未知- 28672，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：未知- 28692，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：未知- 28681，长度
：0
*Nov 11 19:30:34.832 ： attrib类型：未知- 28674，长度
：0
*Nov 11 19:30:34.832 ： **SA**下有效负载：TSi，保留
：0x0，长度：40
最后建议：0x0，保留：0x0，长度：36
建议：1，协议ID ：ESP， SPI大小：4， #trans ：3最后
转换：0x3，保留：0x0 ：长度：8
类型：1，保留：0x0， id ：3DES
最后转换：0x3，保留：0x0 ：长度：8

Router2接收并且验证从路由器接收的身份验证数据1。
相关配置： `crypto ipsec ikev2ipsec AES256aes-256sha-1 md5`

类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：5，保留：0x0， id ：请勿使用ESN
TSi下有效负载：Tsr，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度：16
启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255
Tsr下有效负载：通知，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度：16
启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：R_WAIT_AUTH事件： EV_RECV_AUTH
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：R_WAIT_AUTH事件：EV_CHK_NAT_T
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：R_WAIT_AUTH事件：EV_PROC_ID
*Nov 11 19:30:34.832 ：在进程ID的IKEv2:(SA ID= 1):Received有效parameteres
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：R_WAIT_AUTH事件：EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
*Nov 11 19:30:34.832 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：R_WAIT_AUTH事件：EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.833 ：IKEv2:(1) ：选择IKE配置文件IKEV2-SETUP
*Nov 11 19:30:34.833 ：由地址10.0.0.1的IKEv2:%获得的预共享密匙
*Nov 11 19:30:34.833 ：由地址10.0.0.1的IKEv2:%获得的预共享密匙
*Nov 11 19:30:34.833 ：IKEv2:Adding对工具套件策略的建议默认
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Using IKEv2配置文件'IKEV2-SETUP
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001

Router2建立答复到该IKE_AUTH的数据包它从路由器1.接收。此响应数据包包含：ISAKMP报头(SPI/版本/标志)，IDr (响应方的标识)，验证有效负载，SAr2(initiates SA类似于在IKEv1的第2阶段转换集合交换)和TSi和Tsr (发起者和响应方流量选择器)。包含发起者和响应方的源地址和目的地址分别转发的/接收加密流量的他们。地址范围指定到/从该范围的所有流量被以隧道传输。这些参数是相同的到从ASA1接收的那个。

CurState ：R_WAIT_AUTH事件：EV_SET_POLICY
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Setting已配置的策略
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_WAIT_AUTH事件
：EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_WAIT_AUTH事件：EV_CHK_AUTH4EAP
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_WAIT_AUTH事件：EV_CHK_POLREQEAP
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件：EV_VERIFY_AUTH
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件：EV_CHK4_IC
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件：EV_CHK_REDIRECT
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Redirect检查不是需要的，跳过它
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_NOTIFY_AUTH_DONE
*Nov 11 19:30:34.833 ：IKEv2:AAA组授权没有配置
*Nov 11 19:30:34.833 ：IKEv2:AAA用户授权没有配置
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->

：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_SET_RECD_CONFIG_MODE
*Nov 11 19:30:34.833 ：IKEv2:Received从工具套件的设置数据：
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件：EV_PROC_SA_TS
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_VERIFY_AUTH事件
：EV_GET_CONFIG_MODE
*Nov 11 19:30:34.833 ：修建设置回复的IKEv2:Error
*Nov 11 19:30:34.833 ：IKEv2:No发送的设置数据对工具套件：
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_MY_AUTH_METHOD
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_GEN_AUTH
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_CHK4_SIGN
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_OK_AUTH_GEN
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：R_BLD_AUTH事件：EV_SEND_AUTH
*Nov 11 19:30:34.833 ：IKEv2:Construct卖方细节有效负载：CISCO-GRANITE
*Nov 11 19:30:34.833 ：IKEv2:Construct通知有效负载：SET_WINDOW_SIZE
*Nov 11 19:30:34.833 ：IKEv2:Construct通知有效负载：ESP_TFC_NO_SUPPORT
*Nov 11 19:30:34.833 ：IKEv2:Construct通知有效负载：NON_FIRST_FRAGS
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Next有效负载：ENCR，版本：2.0 Exchange类型： **IKE_AUTH**，标志： **响应方MSG-RESPONSE**消息ID ：1，长度：252

响应方发送IKE_AUTH的答复。

有效负载内容：
ENCR下有效负载：VID，保留：0x0，长度：224
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_OK
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_PKI_SESH_CLOSE
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):Closing PKI会话
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件
：EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.833 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_INSERT_IKE
*Nov 11 19:30:34.834 ：IKEv2:Store MIB索引ikev2 1，平台60
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_GEN_LOAD_IPSEC
*Nov 11 19:30:34.834 ：IKEv2:(SA排队的ID= 1):Asynchronous请求
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1) ：
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ： AUTH_DONE事件：EV_NO_EVENT

发起者从响应方的接收答复。

*Nov 11 19:30:34.834 ：IKEv2:Got从调度程序的一数据包

*Nov 11 19:30:34.834 ：IKEv2:Processing朴队列的一个项目

*Nov 11 19:30:34.840 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001
CurState ：AUTH_DONE事件
：EV_OK_RECD_LOAD_IPSEC
*Nov 11 19:30:34.840 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.840 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F

响应方插入条目到哀伤。

0B
R_SPI=F94020DD8CB4B9C
4 (r) MsgID = 00000001
CurState ：AUTH_DONE事
件：EV_START_ACCT
*Nov 11 19:30:34.840
：IKEv2:(SA ID= 1):SM SA
Trace->
：I_SPI=F074D8BBD5A59F
0B
R_SPI=F94020DD8CB4B9C
4 (r) MsgID = 00000001
CurState ：AUTH_DONE事
件：EV_CHECK_DUPE
*Nov 11 19:30:34.840
：IKEv2:(SA ID= 1):SM SA
Trace->
：I_SPI=F074D8BBD5A59F
0B
R_SPI=F94020DD8CB4B9C
4 (r) MsgID = 00000001
CurState ：AUTH_DONE事
件：EV_CHK4_ROLE

*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):Next有效负载
：ENCR，版本：2.0 Exchange类型： **IKE_AUTH**，标志
： **响应方MSG-RESPONSE**消息ID ：1，长度：252
有效负载内容：

*Nov 11 19:30:34.834 ：IKEv2:Parse卖方细节有效负载
：(自定义) VID下有效负载：IDr，保留：0x0，长度：20
IDr下有效负载：验证，保留：0x0，长度：12
Id类型：IPv4地址，保留：0x0 0x0
验证下有效负载：SA，保留：0x0，长度：28
验证方法PSK，保留：0x0，保留0x0
SA下有效负载：TSi，保留：0x0，长度：40
最后建议：0x0，保留：0x0，长度：36
建议：1，协议ID ：ESP， SPI大小：4， #trans ：3最后
转换：0x3，保留：0x0 ：长度：8
类型：1，保留：0x0， id ：3DES
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：5，保留：0x0， id ：请勿使用ESN
TSi下有效负载：Tsr，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度
：16
启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255
Tsr下有效负载：通知，保留：0x0，长度：24
数字时间分配系统：1，保留0x0，保留0x0
TS类型：TS_IPV4_ADDR_RANGE，原始id ：0，长度
：16

路由器1验证并且处理在此数据包的身份验证数据。路由器1然后插入此SA到其哀伤。

启动端口：0，末端端口：65535
起始地址：0.0.0.0，结尾地址：255.255.255.255

*Nov 11 19:30:34.834 ：IKEv2:Parse通知有效负载
：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下
有效负载：通知，保留：0x0，长度：12
安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE

*Nov 11 19:30:34.834 ：IKEv2:Parse通知有效负载
：ESP_TFC_NO_SUPPORT
NOTIFY(ESP_TFC_NO_SUPPORT)下有效负载：通知，保
留：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：ESP_TFC_NO_SUPPORT

*Nov 11 19:30:34.834 ：IKEv2:Parse通知有效负载
：NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS)下
有效负载：无，保留：0x0，长度：8
安全协议id ：IKE， spi大小：0，键入
：NON_FIRST_FRAGS

*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_WAIT_AUTH事件：EV_RECV_AUTH
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_CHK4_NOTIFY
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_PROC_MSG
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件
：EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_
FOR_PROF_SEL
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件
：EV_GET_POLICY_BY_PEERID
*Nov 11 19:30:34.834 ：对工具套件策略的IKEv2:Adding建
议PHASE1-prop
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):Using IKEv2配置
文件'IKEV2-SETUP
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B

R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件
：EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.834 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：**EV_VERIFY_AUTH**
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_CHK_EAP
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件
：**EV_NOTIFY_AUTH_DONE**
*Nov 11 19:30:34.835 ：IKEv2:AAA组授权没有配置
*Nov 11 19:30:34.835 ：IKEv2:AAA用户授权没有配置
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件
：EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_CHK4_IC
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：I_PROC_AUTH事件：EV_PROC_SA_TS
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_OK
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_PKI_SESH_CLOSE

*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):Closing PKI会话
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件
：EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_INSERT_IKE
*Nov 11 19:30:34.835 ：IKEv2:Store MIB索引ikev2 1，平台60
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_GEN_LOAD_IPSEC
*Nov 11 19:30:34.835 ：IKEv2:(SA排队的ID=
1):Asynchronous请求

*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1) ：
*Nov 11 19:30:34.835 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_NO_EVENT
*Nov 11 19:30:34.835 ：8被消耗的IKEv2:KMI消息。没有执行的操作。
*Nov 11 19:30:34.835 ：12被消耗的IKEv2:KMI消息。没有执行的操作。
*Nov 11 19:30:34.835 ：发送的IKEv2:No数据在模式配置集。
*Nov 11 19:30:34.841 ：IKEv2:Adding ident把柄
0x80000002关联与会话的8 SPI 0x9506D414

*Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件
：EV_OK_RECD_LOAD_IPSEC
*Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):Action
：Action_Null
*Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_START_ACCT
*Nov 11 19:30:34.841 ：1):Accounting没要求的IKEv2:(SA ID=
*Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001
CurState ：AUTH_DONE事件：EV_CHECK_DUPE
*Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace->
：I_SPI=F074D8BBD5A59F0B
R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001

通道是UP在发起者和状态showsREADY。	CurState ： **AUTH_DONE**事件：EV_CHK4_ROLE *Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState ： **READYEvent** ：EV_CHK_IKE_ONLY *Nov 11 19:30:34.841 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (i) MsgID = 00000001 CurState ：READY事件 ：EV_I_OK	***Nov** 11 19:30:34.840 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ： **READY**事件 ：EV_R_OK *Nov 11 19:30:34.840 ：IKEv2:(SA ID= 1):SM SA Trace-> ：I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (r) MsgID = 00000001 CurState ：READY事件 ：EV_NO_EVENT	通道是UP在响应方。响应方通道在发起者前通常出来。

CHILD_SA调试

此交换包括一个请求/响应对和指在IKEv1的第2阶段交换。在最初的交换完成后，它也许由IKE_SA的任一个结尾启动。

路由器1 CHILD_SA消息说明	**调试**	**Router2 CHILD_SA消息说明**
路由器1启动CHILD_SA交换。	*Nov 11 19:31:35.873 ：IKEv2:Got从调度程序的一数据包	
这是CREATE_CHILD_SA请求。	*Nov 11 19:31:35.873 ：IKEv2:Processing朴队列的一个项目	
CHILD_SA数据包典型地包含： • SA HDR (version.flags/交换类型) • 目前Ni (可选)：作为初始交换一部分，如果CHILD_SA创建，不能发送秒钟KE有效负载和目前) • SA有效负载 • KEi (KEY可选)：CREATE_CHILD_SA请求也许或者包含	*Nov 11 19:31:35.873 ：IKEv2:(SA ID= 2):Request有mess_id 3;预计3至7 *Nov 11 19:31:35.873 ：IKEv2:(SA ID= 2):Next有效负载：ENCR，版本：2.0 **Exchange类型：CREATE_CHILD_SA**，标志： **发起者**消息ID ：3，长度：396 有效负载内容： **SA**下有效负载：N，保留：0x0，长度：152 最后建议：0x0，保留：0x0，长度：148 建议：1，协议ID ：IKE， SPI大小：8， #trans ：15最后转换：0x3，保留：0x0 ：长度：12 类型：1，保留：0x0， id ：AES-CBC 最后转换：0x3，保留：0x0 ：长度：12 类型：1，保留：0x0， id ：AES-CBC 最后转换：0x3，保留：0x0 ：长度：12 类型：1，保留：0x0， id ：AES-CBC 最后转换：0x3，保留：0x0 ：长度：8 类型：2，保留：0x0， id ：SHA512	

另外的DH交换的一KE有效负载能启用向前秘密更加强的保证CHILD_SA的。如果SA提供包括不同的DH组，KEi必须是发起者盼望响应方接受组的元素。如果它错误猜测，CREATE_CHILD_SA交换发生故障，并且将必须再试与不同的KEi

- N (请通知有效负载可选)。通知有效负载，用于传送信息性数据，例如错误情况和状态转换，对IKE对等体。通知有效负载可能出现在响应消息(通常指定请求为什么拒绝)，在信息性Exchange (报告一个错误不在IKE请求)，或者在指示发送方功能或修改请求的含义的其他消息。除IKE_SA之外，如果此CREATE_CHILD_SA交换重新生成密钥现有SA，类型REKEY_SA主导的N有效负载必须识别重新

最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA384
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA256
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：MD5
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA512
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA384
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA256
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：MD596
最后转换：0x3，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1536_MODP/Group 5
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
N下有效负载：KE，保留：0x0，长度：24
KE下有效负载：通知，保留：0x0，长度：136
DH组：2，保留：0x0

*Nov 11 19:31:35.874 ：IKEv2:Parse通知有效负载
：SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)**下有效负载：无，保留：0x0，长度：12
安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE

*Nov 11 19:31:35.874 ：IKEv2 ：(**SA ID= 2):SM** SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：READY事件： **EV_RECV_CREATE_CHILD**
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_INIT事件
：EV_RECV_CREATE_CHILD
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_INIT事件：EV_VERIFY_MSG
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6

R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_INIT事件：EV_CHK_CC_TYPE
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_IKE事件： **EV_REKEY_IKESA**
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_IKE事件：EV_GET_IKE_POLICY
*Nov 11 19:31:35.874 ：**由地址10.0.0.2的**IKEv2:%**获得的预共享密匙**
*Nov 11 19:31:35.874 ：由地址10.0.0.2的IKEv2:%获得的预共享密匙
*Nov 11 19:31:35.874 ：对工具套件策略的IKEv2:Adding建议PHASE1-prop
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):Using IKEv2配置文件'IKEV2-SETUP
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_IKE事件：EV_PROC_MSG
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_IKE事件：EV_SET_POLICY
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2) ：**设置已配置的策略**
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件：EV_GEN_DH_KEY
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件：EV_NO_EVENT
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件
：EV_OK_RECD_DH_PUBKEY_RESP
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.874 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件
：**EV_GEN_DH_SECRET**
*Nov 11 19:31:35.881 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件：EV_NO_EVENT
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->

生成密钥的SA。如果此CREATE_CHILD_SA交换不重新生成密钥现有SA，必须省略N有效负载。

：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件
：EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件：EV_BLD_MSG
*Nov 11 19:31:35.882 ： **IKEv2:Construct通知有效负载**
：SET_WINDOW_SIZE
有效负载内容：
SA下有效负载：N，保留：0x0，长度：56
最后建议：0x0，保留：0x0，长度：52
建议：1，协议ID ：IKE， SPI大小：8， #trans ：4最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
N下有效负载：KE，保留：0x0，长度：24
KE下有效负载：通知，保留：0x0，长度：136
DH组：2，保留：0x0
NOTIFY(SET_WINDOW_SIZE)下有效负载：无，保留：0x0，长度：12
安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE
*Nov 11 19:31:35.869 ：IKEv2 ：(**SA ID= 2):Next**有效负载：ENCR，版本：2.0 Exchange类型
： **CREATE_CHILD_SA**，标志： **发起者**消息ID ：2，长度：460
有效负载内容：
ENCR下有效负载：SA，保留：0x0，长度：432
*Nov 11 19:31:35.873 ：IKEv2:Construct通知有效负载
：SET_WINDOW_SIZE
有效负载内容：
SA下有效负载：N，保留：0x0，长度：152
最后建议：0x0，保留：0x0，长度：148
建议：1，协议ID ：IKE， SPI大小：8， #trans ：15最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA512
最后转换：0x3，保留：0x0 ：长度：8

此数据包由Router2接收。

类型：2，保留：0x0， id ：SHA384
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA256
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：MD5
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA512
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA384
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA256
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：MD596
最后转换：0x3，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1536_MODP/Group 5
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
N下有效负载：KE，保留：0x0，长度：24
KE下有效负载：通知，保留：0x0，长度：136
DH组：2，保留：0x0
NOTIFY(SET_WINDOW_SIZE)下有效负载：无，保留
：0x0，长度：12
安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE
*Nov 11 19:31:35.882 ：IKEv2 ：(**SA ID= 2):Next**有效负载
：ENCR，版本：2.0 Exchange类型
： **CREATE_CHILD_SA，**标志： **响应方MSG-RESPONSE**消息ID ：3，长度：300
有效负载内容：
SA下有效负载：N，保留：0x0，长度：56
最后建议：0x0，保留：0x0，长度：52
建议：1，协议ID ：IKE， SPI大小：8， #trans ：4最后转换：0x3，保留：0x0 ：长度：12
类型：1，保留：0x0， id ：AES-CBC
最后转换：0x3，保留：0x0 ：长度：8
类型：2，保留：0x0， id ：SHA1
最后转换：0x3，保留：0x0 ：长度：8
类型：3，保留：0x0， id ：SHA96
最后转换：0x0，保留：0x0 ：长度：8
类型：4，保留：0x0， id
：DH_GROUP_1024_MODP/Group 2
N下有效负载：KE，保留：0x0，长度：24
KE下有效负载：通知，保留：0x0，长度：136
DH组：2，保留：0x0

*Nov 11 19:31:35.882 ：IKEv2:Parse通知有效负载
：SET_WINDOW_SIZE **NOTIFY(SET_WINDOW_SIZE)**下

Router2当前建立CHILD_SA交换的回复。这是CREATE_CHILD_SA答复。
CHILD_SA数据包典型地包含：

- SA HDR (version.flags/交换类型)
- 目前Ni(optional)：作为初始交换一部分，如果CHILD_SA创建，不能发送秒钟KE有效负载和目前。
- SA有效负载
- KEi (KEY可选)：CREATE_CHILD_SA请求

有效负载：无，保留：0x0，长度：12
  安全协议id ：IKE， spi大小：0，键入
：SET_WINDOW_SIZE

*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ： **CHILD_I_WAIT事件**
： **EV_RECV_CREATE_CHILD**
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ： **CHILD_I_PROC事件**：EV_CHK4_NOTIFY
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件： **EV_VERIFY_MSG**
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_PROC_MSG
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_CHK4_PFS
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_GEN_DH_SECRET
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_NO_EVENT
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件
：EV_OK_RECD_DH_SECRET_RESP
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_CHK_IKE_REKEY
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_PROC事件：EV_GEN_SKEYID
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):Generate skeyid
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6

也许或者包含另外的DH交换的一KE有效负载能启用向前秘密更加强的保证CHILD_SA的。如果SA提供包括不同的DH组，KEi必须是发起者盼望响应方接受组的元素。如果它错误猜测，CREATE_CHILD_SA交换发生故障，并且必须再试与不同的KEi。

- N (请通知有效负载可选)：通知有效负载用于传送信息性数据，例如错误情况和状态转换，对IKE对等体。通知有效负载也许出现在响应消息(通常指定请求为什么拒绝)，在信息性交换(报告一个错误不在IKE请求)，或者在指示发送方功能或修改请求的含义的其他消息。除IKE_SA之外，如果此CREATE_CHILD_SA交换重新生成密钥现有SA，类型REKEY_SA主导的N有效负载必须识别重新

R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ： **CHILD_I_DONE事件**
： **EV_ACTIVATE_NEW_SA**
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_DONE事件
：EV_UPDATE_CAC_STATS
*Nov 11 19:31:35.890 ：IKEv2:New激活的sa ikev2请求
*Nov 11 19:31:35.890 ：减少流出的协商的计数的
IKEv2:Failed
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_DONE事件：EV_CHECK_DUPE
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：CHILD_I_DONE事件：EV_OK
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID = 00000003
CurState ：退出事件：EV_CHK_PENDING
*Nov 11 19:31:35.890 ：IKEv2:(SA与消息ID 3的ID=
2):Processed答复，请求可以是发送的从范围4到8
*Nov 11 19:31:35.890 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (i) MsgID =
00000003 **CurState ：退出事件**：EV_NO_EVENT
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):Next有效负载
：ENCR，版本：2.0 Exchange类型
： **CREATE_CHILD_SA**，标志： **响应方MSG-RESPONSE**消息ID ：3，长度：300
有效负载内容：
ENCR下有效负载：SA，保留：0x0，长度：272

生成密钥的SA。如果此CREATE_CHILD_SA交换不重新生成密钥现有SA，必须省略N有效负载。Router2发送答复并且完成激活新的孩子SA。

*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件
：**EV_CHK_IKE_REKEY**
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_BLD_MSG事件：EV_GEN_SKEYID
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2) ：**生成skeyid**
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_DONE事件
：**EV_ACTIVATE_NEW_SA**
*Nov 11 19:31:35.882 ：IKEv2:Store MIB索引ikev2 3，平台62

路由器1收到从Router2的响应数据包并且完成激活CHILD_SA。

*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_DONE事件
：EV_UPDATE_CAC_STATS
*Nov 11 19:31:35.882 ：IKEv2:New激活的sa ikev2请求
*Nov 11 19:31:35.882 ：减少流入协商的计数的
IKEv2:Failed
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ： **CHILD_R_DONE事件**：EV_CHECK_DUPE
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_DONE事件：EV_OK
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：CHILD_R_DONE事件
：EV_START_DEL_NEG_TMR
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):Action
：Action_Null
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID = 00000003
CurState ：退出事件：EV_CHK_PENDING
*Nov 11 19:31:35.882 ：IKEv2:(SA与消息ID 3的ID=
2):Sent答复，请求可以是接受的从范围4到8
*Nov 11 19:31:35.882 ：IKEv2:(SA ID= 2):SM SA Trace->
：I_SPI=0C33DB40DBAAADE6
R_SPI=F14E2BBA78024DE3 (r) MsgID =
00000003 **CurState ：退出事件**：EV_NO_EVENT

通道验证

ISAKMP

命令

show crypto ikev2 sa detailed

1输出的路由器

```
Router1#show crypto ikev2 sa  detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.0.1/500 10.0.0.2/500 none/none READY
Encr: AES-CBC, keysize: 128,
Hash: SHA96, DH Grp:2,
Auth sign: PSK, Auth verify: PSK
```

```
Life/Active Time: 120/10 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: E58F925107F8B73F Remote spi: AFD098F4147869DA
Local id: 10.0.0.1
Remote id: 10.0.0.2
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: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

Router2输出

```
Router2#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.0.2/500 10.0.0.1/500 none/none READY
Encr: AES-CBC, keysize: 128, Hash: SHA96,
DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 120/37 sec
CE id: 1006, Session-id: 4
Status Description: Negotiation done
Local spi: AFD098F4147869DA Remote spi: E58F925107F8B73F
Local id: 10.0.0.2
Remote id: 10.0.0.1
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

IPsec

命令

show crypto ipsec sa

> **注意**：在此输出中，不同于在IKEv1， PFS DH组的值出现作为“PFS是/否：N， DH组：什么都”在第一隧道协商时，但是，在重新生成密钥发生后，正确的值没出现。这不是bug，即使行为在Cisco Bug ID CSCug67056描述。
>
> 在IKEv1和IKEv2之间的区别是作为验证交换一部分，在后者，孩子SAS创建。DH组配置在加密映射下仅会使用在期间重新生成密钥。因此，您会看到‘PFS是/否：N， DH组：什么都’直到第一不重新生成密钥。
>
> 使用IKEv1，您看到一种不同的行为，在快速模式期间，因为SA儿童创建发生，并且CREATE_CHILD_SA消息有指定DH参数派生一新建的共享机密的提供传送密钥交换有效负载。

1输出的路由器

```
Router1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port):
(0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt:
10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt:
10, #pkts verify: 10
#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.: 10.0.0.1,
remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xF6083ADD(4127734493)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec):
(4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4276853/3592)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Router2输出

```
Router2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
current_peer 10.0.0.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#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.: 10.0.0.2,
remote crypto endpt.: 10.0.0.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x6B74CB79(1802816377)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xF6083ADD(4127734493)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 17, flow_id: SW:17,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime
(k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x6B74CB79(1802816377)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 18, flow_id: SW:18,
sibling_flags 80000040,
crypto map: Tunnel0-head-0
sa timing: remaining key
lifetime (k/sec): (4347479/3584)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

您能也检查输出**显示crypto session命令**在两路由器;此输出显示隧道会话状态作为启动-激活。

```
Router1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
```

```
Peer: 10.0.0.2 port 500
IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map

Router2#show cry session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

相关信息

- IKEv2信息包交换和协议级调试
- 技术支持和文档 - Cisco Systems