使用PSK的站点到站点VPN的IOS IKEv2调试故障排除

目录

简介

先决条件

- 要求
- 使用的组件
- 规则

背景信息

核心问题

路由器配置

故障排除

- 路由器调试
- CHILD_SA调试

隧道验证

- ISAKMP
- IPsec

相关信息

简介

本文档介绍使用非共享密钥(PSK)时Cisco IOS®上的Internet密钥交换版本2(IKEv2)调试。

先决条件

要求

Cisco建议您了解IKEv2的数据包交换。有关详细信息，请参阅IKEv2数据包交换和协议级别调试。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Internet密钥交换版本2(IKEv2)
- Cisco IOS 15.1(1)T或更高版本

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。如果您的网络处于活动状态，请确保您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。

背景信息

本文档提供有关如何在配置中转换特定调试行的信息。

核心问题

IKEv2中的数据包交换与IKEv1中的数据包交换截然不同。在IKEv1中，有一个明确分界的phase1交换，包含六(6)个数据包，之后包含三(3)个数据包的阶段2交换；IKEv2交换是可变的。有关数据包交换的区别和说明的详细信息，请再次参阅IKEv2数据包交换和协议级别调试。

路由器配置

本节列出了本文档中使用的配置。

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

本文档中使用了以下debug命令：

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

Router 1(Initiator)消息说明	调试
路由器1收到与对等体ASA 10.0.0.2的加密acl匹配的数据包。启动SA创建	*11月11日20:28:34.003:IKEv2：从调度程序获取数据包 *11月11日20:28:34.003:IKEv2：处理pak队列中的项目 *11月11日19:30:34.811:IKEv2:%通过地址10.0.0.2获取预共享密钥 *11月11日19:30:34.811:IKEv2：将建议PHASE1-prop添加到工具包策略 *11月11日19:30:34.811:IKEv2:(1)：选择IKE配置文件IKEV2-SETUP *11月11日19:30:34.811:IKEv2：新的ikev2 sa请求已接受 *11月11日19:30:34.811:IKEv2：将传出协商服务计数增加1
第一对消息是IKE_SA_INIT交换。这些消息会协商加密算法、交换失效并执行Diffie-Hellman交换。 相关配置： `crypto ikev2 proposal PHASE1-prop encryption 3des aes-cbc-128 integrity sha1 group 2crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key local cisco pre-shared-key remote cisco`	*11月11日19:30:34.811:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000000 CurState：空闲事件：EV_INIT_SA *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000000 CurState: I_BLD_INIT事件：EV_GET_IKE_POLICY *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT Event:EV_SET_POLICY *11月11日19:30:34.811:IKEv2:(SA ID = 1)：设置配置的策略 *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT事件：EV_CHK_AUTH4PKI *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT Event:EV_GEN_DH_KEY *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT事件：EV_NO_EVENT *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT事件：EV_OK_RECD_DH_PUBKEY_RESP *11月11日19:30:34.811:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000000 CurState: I_BLD_INIT事件：EV_GET_CONFIG_MODE

	*11月11日19:30:34.811:IKEv2:IKEv2启动器 — 在IKE_SA_INIT交换中没有要送的配置数据 *11月11日19:30:34.811:IKEv2：没有要发送到工具包的配置数据： *11月11日19:30:34.811:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT事件：EV_BLD_MSG *11月11日19:30:34.811:IKEv2：构建供应商特定负载：DELETE-REASON *11月11日19:30:34.811:IKEv2：构建供应商特定负载：（自定义） *11月11日19:30:34.811:IKEv2：构建通知负载：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.811:IKEv2：构建通知负载：NAT_DETECTION_DESTINATION_IP
正在生成IKE_INIT_SA数据包的启动器。它包含：ISAKMP Header(SPI/version/flags)、SAi1（IKE发起方支持的加密算法）、KEi（发起方的DH公钥值）和N（发起方Nonce）。	*11月11日19:30:34.811: IKEv2:(SA ID = 1)：下一个负载：SA，版本：2.0交类型：IKE_SA_INIT，标志：INITIATOR消息ID:0，长度：344 负载内容： SA下一个负载：KE，保留：0x0，长度：56 最后一个建议：0x0，保留：0x0，长度：52 方案：1，协议ID:IKE，SPI大小：0,#trans：最后一个转换：0x3，保留：0x0：长度：8 类型：1，保留：0x0,id:3DES 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2 KE下一个负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 N下一个负载：VID，保留：0x0，长度：24 VID Next负载：VID，保留：0x0，长度：23 VID Next负载：NOTIFY，保留：0x0，长度：21 NOTIFY(NAT_DETECTION_SOURCE_IP)下一负载：NOTIFY，保留：0x0，长度：28 安全协议ID:IKE，spi大小：0，类型：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一负载：无，保留：0x0，长度：28 安全协议id:IKE，spi大小：0，类型：NAT_DETECTION_DESTINATION_
----------发起程序已发送IKE_INIT_SA ---------->	
	*11月11日19:30:34.814:IKEv2：从调度程序获取数据包 *11月11日19:30:34.814:IKEv2：处理pak队列中的项目 *11月11日19:30:34.814:IKEv2：新的ikev2 sa请求已接受 *11月11日19:30:34.814:IKEv2：将传入协商服务计数增加1

	*11月11日19:30:34.814: IKEv2：下一个负载：SA，版本：2.0交换类型：IKE_SA_INIT，标志：INITIATOR消息id:0，长度：344 负载内容： SA下一个负载：KE，保留：0x0，长度：56 最后一个建议：0x0，保留：0x0，长度：52 方案：1，协议ID:IKE，SPI大小：0,#trans：最后一个转换：0x3，保留：0x0：长度：8 类型：1，保留：0x0,id:3DES 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2 KE下一个负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 N下一个负载：VID，保留：0x0，长度：24 *11月11日19:30:34.814:IKEv2：解析供应商特定负载：CISCO-DELETE-REASON VID下一负载：VID，保留：0x0，长度：23 *11月11日19:30:34.814:IKEv2：解析供应商特定负载：（自定义）VID下一负载：通知，保留：0x0，长度：21 *11月11日19:30:34.814:IKEv2：解析通知负载：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP)下一负载：NOTIFY，保留：0x0，长度：28 安全协议ID:IKE，spi大小：0，类型：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.814:IKEv2：解析通知负载：NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一负载：无，保留：0x0，度：28 安全协议id:IKE，spi大小：0，类型：NAT_DETECTION_DESTINATION_
	*11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState：空闲事件：EV_RECV_INIT *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT Event:EV_VERIFY_MSG *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT Event:EV_INSERT_SA *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT事件：EV_GET_IKE_POLICY *11月11日19:30:34.814:IKEv2：将建议默认添加到工具包策略 *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT事件：EV_PROC_MSG *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT事件：EV_DETECT_NAT *11月11日19:30:34.814:IKEv2:(SA ID = 1)：处理NAT发现通知 *11月11日19:30:34.814:IKEv2:(SA ID = 1)：处理nat检测源通知 *11月11日19:30:34.814:IKEv2:(SA ID = 1)：远程地址匹配 *11月11日19:30:34.814:IKEv2:(SA ID = 1)：正在处理nat detect dst notify *11月11日19:30:34.814:IKEv2:(SA ID = 1)：本地地址匹配 *11月11日19:30:34.814:IKEv2:(SA ID = 1)：未找到NAT *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_INIT事件：EV_CHK_CONFIG_MODE *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件：EV_SET_POLICY *11月11日19:30:34.814:IKEv2:(SA ID = 1)：设置已配置的策略 *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件： EV_CHK_AUTH PKI *11月11日19:30:34.814:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件： EV_PKI_SESH打开 *11月11日19:30:34.814:IKEv2:(SA ID = 1)：打开PKI会话 *11月11日19:30:34.815:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT Event:EV_DH_GEN密钥(_K) *11月11日19:30:34.815:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件：EV_NO_EVENT *11月11日19:30:34.815:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT Event:EV_OK_RECECT D_DH_PUBKEY_RESP *11月11日19:30:34.815:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.815:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT Event:EV_DH_GEN密码(_S) *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =

	00000000 CurState:R_BLD_INIT事件：EV_NO_EVENT *11月11日19:30:34.822:IKEv2:%正在通过地址10.0.0.1获取预共享密钥 *11月11日19:30:34.822:IKEv2：将建议默认添加到工具包策略 *11月11日19:30:34.822:IKEv2:(2)：选择IKE配置文件IKEV2-SETUP *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件：EV_OK_RECD DH_SECRET_RESP *11月11日19:30:34.822:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT Event:EV_GEN_SGN密钥ID *11月11日19:30:34.822:IKEv2:(SA ID = 1)：生成密钥ID *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件： EV_GET_CONFIG模式 *11月11日19:30:34.822:IKEv2:IKEv2响应器 — 在IKE_SA_INIT交换中没有要 送的配置数据 *11月11日19:30:34.822:IKEv2：没有要发送到工具包的配置数据： *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件：EV_BLD *11月11日19:30:34.822:IKEv2：构建供应商特定负载：DELETE-REASON *11月11日19:30:34.822:IKEv2：构建供应商特定负载：（自定义） *11月11日19:30:34.822:IKEv2：构建通知负载 ：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.822:IKEv2：构建通知负载 ：NAT_DETECTION_DESTINATION_IP *11月11日19:30:34.822:IKEv2：构造通知负载 ：HTTP_CERT_LOOKUP_SUPPORTED
	*11月11日19:30:34.822:IKEv2:(SA ID = 1)：下一个负载：SA，版本：2.0交 类型：IKE_SA_INIT，标志：RESPONDER MSG-RESPONSE消息ID:0，长 ：449 负载内容： SA下一个负载：KE，保留：0x0，长度：48 最后一个建议：0x0，保留：0x0，长度：44 提议：1，协议ID:IKE，SPI大小：0,#trans:4上次转换：0x3，保留：0x0： 度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2

	KE下一个负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 N下一个负载：VID，保留：0x0，长度：24 VID Next负载：VID，保留：0x0，长度：23 VID Next负载：NOTIFY，保留：0x0，长度：21 NOTIFY(NAT_DETECTION_SOURCE_IP)下一负载：NOTIFY，保留：0x0，长度：28 安全协议ID:IKE，spi大小：0，类型：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一负载：CERTREQ，保：0x0，长度：28 安全协议id:IKE，spi大小：0，类型：NAT_DETECTION_DESTINATION_ CERTREQ下一个负载：NOTIFY，保留：0x0，长度：105 证书编码PKIX的散列和URL NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下一负载：无，保留：0x0，长度：8 安全协议ID:IKE，spi大小：0，类型：HTTP_CERT_LOOKUP_SUPPORTED	
	*11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:INIT_DONE事件：EV_DONE *11月11日19:30:34.822:IKEv2:(SA ID = 1)：思科DeleteReason Notify已启用 *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:INIT_DONE事件：EV_CHK4_ROLE *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:INIT_DONE事件：EV_START_TMR。 *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_WAIT_AUTH事件：EV_NO_EVENT *11月11日19:30:34.822:IKEv2：已接受新ikev2 sa请求 *11月11日19:30:34.822:IKEv2：将传出协商服务计数增加1	
<----------响应器已发送IKE_INIT_SA----------		
路由器1收到来自路由器2的IKE_SA_INIT响应数据包。	*11月11日19:30:34.823:IKEv2：从调度程序获取数据包 *11月11日19:30:34.823:IKEv2：从调度程序获取数据包 *11月11日19:30:34.823:IKEv2：处理pak队列中的项目	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000000 CurState: INIT_DONE Event:EV_START_TMR

Router1验证并处理响应：(1)计算发起方DH密钥，以及(2)也生成发起方DH密钥。	*11月11日19:30:34.823:IKEv2:(SA ID = 1)：下一个负载：SA，版本：2.0交 类型：IKE_SA_INIT，标志：RESPONDER MSG-RESPONSE Message id:0，长度：449 负载内容： SA下一个负载：KE，保留：0x0，长度：48 最后一个建议：0x0，保留：0x0，长度：44 提议：1，协议ID:IKE，SPI大小：0,#trans:4上次转换：0x3，保留：0x0： 度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2 KE下一个负载：N，保留：0x0，长度：136 DH组：2，保留：0x0 N下一个负载：VID，保留：0x0，长度：24 *11月11日19:30:34.823:IKEv2：解析供应商特定负载：CISCO-DELETE-REASON VID下一负载：VID，保留：0x0，长度：23 *11月11日19:30:34.823:IKEv2：解析供应商特定负载：（自定义）VID下一负载：NOTIFY，保留：0x0，长度：21 *11月11日19:30:34.823:IKEv2：解析通知负载 ：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP)下一负载：NOTIFY，保留 ：0x0，长度：28 安全协议ID:IKE，spi大小：0，类型：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.824:IKEv2：解析通知负载 ：NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一负载：CERTREQ，保 ：0x0，长度：28 安全协议id:IKE，spi大小：0，类型：NAT_DETECTION_DESTINATION_ CERTREQ下一个负载：NOTIFY，保留：0x0，长度：105 证书编码PKIX的散列和URL *11月11日19:30:34.824: IKEv2：解析通知负载 ：HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下一负载：无，保留 ：0x0，长度：8 安全协议ID:IKE，spi大小：0，类型 ：HTTP_CERT_LOOKUP_SUPPORTED

	*11月11日19:30:34.824:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_WAIT_INIT事件： EV_RECV_INIT *11月11日19:30:34.824:IKEv2:(SA ID = 1)：正在处理IKE_SA_INIT消息 *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_PROC_INIT事件：EV_CHK4_NOTIFY *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_PROC_INIT事件：EV_VERIFY_MSG *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_PROC_INIT事件：EV_PROC_MSG *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_PROC_INIT事件：EV_DETECT_NAT *11月11日19:30:34.824:IKEv2:(SA ID = 1)：处理NAT发现通知 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：处理nat detect src notify *11月11日19:30:34.824:IKEv2:(SA ID = 1)：远程地址匹配 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：正在处理nat detect dst notify *11月11日19:30:34.824:IKEv2:(SA ID = 1)：本地地址匹配 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：未找到NAT *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_PROC_INIT事件：EV_CHK_NAT T *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_CHK_CONFIG模式 *11月11日19:30:34.824:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:INIT_DONE事件：EV_GEN_DH_SECRET IP地址 *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件： EV_NO_EVENT *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:INIT_DONE事件：EV_OK_RECD_DH SECRET_RESP *11月11日19:30:34.831:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:INIT_DONE事件：EV_GEN_SKYID *11月11日19:30:34.831:IKEv2:(SA ID = 1)：生成密钥ID *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:INIT_DONE事件：EV_DONE

	*11月11日19:30:34.831:IKEv2:(SA ID = 1)：思科DeleteReason Notify已启用 *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:INIT_DONE事件：EV_CHK4_ROLE *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH事件：EV_GET_CONFIG模式 *11月11日19:30:34.831:IKEv2：将配置数据发送到工具包 *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH事件：EV_CHK EAP
发起方启动IKE_AUTH交换并生成身份验证负载。IKE_AUTH数据包包含：ISAKMP报头（SPI/版本/标志）、IDi（发起方身份）、AUTH负载、SAi2（发起类似于IKEv1中阶段2转换集交换的SA），以及TSi和TSr（发起方和响应方流量选择器）。它们分别包含用于转发/接收加密流量的发起方和响应方的源地址和目的地址。地址范围指定进出该范围的所有流量都通过隧道传输。如果响应方可以接受该建议，它将发送相同的TS有效负载。第一个CHILD_SA是为匹配触发数据包的proxy_ID对创建的。 相关配置： `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	*11月11日19:30:34.831:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH Event:EV_GEN_AUTH IP地址 *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH事件： EV_CHK类型 *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH事件：EV_OK_AUTH GEN *11月11日19:30:34.831:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState:I_BLD_AUTH事件：EV_SEND *11月11日19:30:34.831:IKEv2：构建供应商特定负载：思科 — 花岗岩 *11月11日19:30:34.831:IKEv2：构建通知负载：INITIAL_CONTACT *11月11日19:30:34.831:IKEv2：构造通知负载：SET_WINDOW_SIZE *11月11日19:30:34.831:IKEv2：构建通知负载：ESP_TFC_NO_SUPPORT *11月11日19:30:34.831:IKEv2：构造通知负载：NON_FIRST_FRAGS 负载内容： VID Next负载：IDi，保留：0x0，长度：20 IDi下一个负载：身份验证，保留：0x0，长度：12 Id类型：IPv4地址，保留：0x0 0x0 AUTH Next payload:CFG，reserved:0x0,length:28 身份验证方法PSK，保留： 0x0，保留0x0 CFG下一个负载：SA，保留：0x0，长度：309 cfg类型：CFG_REQUEST，保留：0x0，保留：0x0 *11月11日19:30:34.831:SA下一负载：TSi，保留：0x0，长度：40 最后一个建议：0x0，保留：0x0，长度：36 提议：1，协议ID:ESP，SPI大小：4,#trans：最后一个转换：0x3，保留：0x0：长度：8 类型：1，保留：0x0,id:3DES 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96

	上次转换：0x0，保留：0x0：长度：8 类型：5，保留：0x0,id：请勿使用ESN TSi下一个负载：TSr，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255 TSr下一个负载：NOTIFY，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255 NOTIFY(INITIAL_CONTACT)下一个负载：NOTIFY，保留：0x0，长度：8 安全协议ID:IKE，spi大小：0，类型：INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE)下一负载：NOTIFY，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型：SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT)下一负载：NOTIFY，保留：0x0，长度 安全协议ID:IKE，spi大小：0，类型：ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS)下一负载：无，保留：0x0，长度：8 安全协议ID:IKE，spi大小：0，类型：NON_FIRST_FRAGS *11月11日19:30:34.832:IKEv2:(SA ID = 1)：下一个负载：ENCR，版本：2.0 换类型：IKE_AUTH，标志：INITIATOR消息ID:1，长度：556 负载内容： ENCR下一个负载：VID，保留：0x0，长度：528 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 0000001 CurState: I_WAIT_AUTH事件:EV_NO_EVENT
----------发起方已发送IKE_AUTH ---------->	
	*11月11日19:30:34.832:IKEv2：从调度程序获取数据包 *11月11日19:30:34.832:IKEv2：处理pak队列中的项目 *11月11日19:30:34.832:IKEv2:(SA ID = 1)：请求具有mess_id 1；预期为1至 *11月11日19:30:34.832: IKEv2:(SA ID = 1)：下一个负载：ENCR，版本 ：2.0交换类型：IKE_AUTH，标志：INITIATOR消息ID:1，长度：556 负载内容： *11月11日19:30:34.832:IKEv2：解析供应商特定负载：（自定义）VID下一负 载：IDi，保留：0x0，长度：20 IDi下一个负载：身份验证，保留：0x0，长度：12 Id类型：IPv4地址，保留：0x0 0x0 AUTH下一个负载：CFG，保留：0x0，长度：28 身份验证方法PSK，保留： 0x0，保留0x0 CFG下一个负载：SA，保留：0x0，长度：309

	cfg类型：CFG_REQUEST，保留：0x0，保留：0x0 *11月11日19:30:34.832：属性类型：内部IP4 DNS，长度：0 *11月11日19:30:34.832：属性类型：内部IP4 DNS，长度：0 *11月11日19:30:34.832：属性类型：内部IP4 NBNS，长度：0 *11月11日19:30:34.832：属性类型：内部IP4 NBNS，长度：0 *11月11日19:30:34.832：属性类型：内部IP4子网，长度：0 *11月11日19:30:34.832：属性类型：应用版本，长度：257 属性类型：未知 — 28675，长度：0 *11月11日19:30:34.832：属性类型：未知 — 28672，长度：0 *11月11日19:30:34.832：属性类型：未知 — 28692，长度：0 *11月11日19:30:34.832：属性类型：未知 — 28681，长度：0 *11月11日19:30:34.832：属性类型：未知 — 28674，长度：0 *11月11日19:30:34.832: SA下一个负载：TSi，保留：0x0，长度：40 最后一个建议：0x0，保留：0x0，长度：36 提议：1，协议ID:ESP，SPI大小：4,#trans：最后一个转换：0x3，保留：0x0：长度：8 类型：1，保留：0x0,id:3DES 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：5，保留：0x0,id：请勿使用ESN TSi下一个负载：TSr，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255 TSr下一个负载：NOTIFY，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255
	*11月11日19:30:34.832:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_RECV *11月11日19:30:34.832:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_CHK_NAT t *11月11日19:30:34.832:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_PROC_ID *11月11日19:30:34.832:IKEv2:(SA ID = 1)：已收到进程ID中的有效参数 *11月11日19:30:34.832:IKEv2:(SA ID = 1):SM跟踪 — > SA: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 *11月11日19:30:34.832:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_GET_POLICY by_BY PEERID(_P) *11月11日19:30:34.833:IKEv2:(1)：选择IKE配置文件IKEV2-SETUP *11月11日19:30:34.833:IKEv2:%通过地址10.0.0.1获取预共享密钥 *11月11日19:30:34.833:IKEv2:%通过地址10.0.0.1获取预共享密钥 *11月11日19:30:34.833:IKEv2：将建议默认添加到工具包策略 *11月11日19:30:34.833:IKEv2:(SA ID = 1)：使用IKEv2配置文件“IKEV2-SETUP” *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_SET_POLICY *11月11日19:30:34.833:IKEv2:(SA ID = 1)：设置配置的策略 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_VERIFY_POLICY by_POLICY PEERID(_P) *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_CHK4AUTH EAP *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_WAIT_AUTH事件：EV_CHK_POLQREEAP IP地址 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件： EV_CHK_AUTH类型 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_GET_HR密钥 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件： EV_VERIFY *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_CHK4_IC *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_CHK_REDIRECT *11月11日19:30:34.833:IKEv2:(SA ID = 1)：不需要重定向检查，跳过该检查 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH Event: EV_NOTIONE IP地址 *11月11日19:30:34.833：未配置IKEv2:AAA组授权

	*11月11日19:30:34.833：未配置IKEv2:AAA用户授权 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_CHK_CONFIG模式 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_SET_RECD config_MODE *11月11日19:30:34.833:IKEv2：从工具包接收配置数据： *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件：EV_PROC_SA TS *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_VERIFY_AUTH事件： EV_GET_CONFIG_EVENT IP 址 *11月11日19:30:34.833：构造配置应答时出错 *11月11日19:30:34.833:IKEv2：没有要发送到工具包的配置数据： *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件： EV_MY_AUTH方法 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件： EV_GET_HR密钥 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件：EV_GEN *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件：EV_CHK4_SIGN *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件： EV_OK_AUTH GEN *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:R_BLD_AUTH事件：EV_SEND *11月11日19:30:34.833:IKEv2：构建供应商特定负载：思科 — 花岗岩 *11月11日19:30:34.833:IKEv2：构造通知负载：SET_WINDOW_SIZE *11月11日19:30:34.833:IKEv2：构建通知负载：ESP_TFC_NO_SUPPORT *11月11日19:30:34.833:IKEv2：构造通知负载 ：NON_FIRST_FRAGS
	*11月11日19:30:34.833:IKEv2:(SA ID = 1)：下一个负载：ENCR，版本：2.0 换类型： IKE_AUTH，标志：RESPONDER MSG-RESPONSE Message id:1，长度：252 负载内容：

	ENCR下一个负载：VID，保留：0x0，长度：224 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:AUTH_DONE事件：EV_OK *11月11日19:30:34.833:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:AUTH_DONE事件：EV_PKI_SESH_CLOSE *11月11日19:30:34.833:IKEv2:(SA ID = 1)：关闭PKI会话 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:AUTH_DONE事件：EV_UPDATE_CAC_STATS *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:AUTH_DONE事件：EV_INSERT_IKE *11月11日19:30:34.834:IKEv2：存储mib索引ikev2 1，平台60 *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState:AUTH_DONE事件：EV_GEN_LOAD_IPSEC *11月11日19:30:34.834:IKEv2:(SA ID = 1)：异步请求已排队 *11月11日19:30:34.834:IKEv2:(SA ID = 1): *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO	
<----------响应器已发送IKE_AUTH----------		
发起方从响应方接收响应。	*11月11日19:30:34.834:IKEv2：从调度程序获取数据包 *11月11日19:30:34.834:IKEv2：处理pak队列中的项目	*11月11日19:30:34.840:IKEv2:(SA I 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:AUTH_DONE 件：EV_OK_RECD_LOAD IPSEC *11月11日19:30:34.840:IKEv2:(SA I 1)：操作：Action_Null *11月11日19:30:34.840:IKEv2:(SA I 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:AUTH_DONE 件：EV_START_ACCT *11月11日19:30:34.840:IKEv2:(SA I 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:AUTH_DONE

		件：EV_CHECK_DUPE *11月11日19:30:34.840:IKEv2:(SA I 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:AUTH_DONE 件：EV_CHK4_ROLE
路由器1验证并处理此数据包中的身份验证数据。然后，路由器1将此SA插入其SAD。	*11月11日19:30:34.834: IKEv2:(SA ID = 1)：下一个负载：ENCR，版本：2.0交换类型：IKE_AUTH，标志：RESPONDER MSG-RESPONSE Message id:1，长度：252 负载内容： *11月11日19:30:34.834: IKEv2：解析供应商特定负载：（自定义）VID下一载：IDr.，保留：0x0，长度：20 IDr。下一个负载：身份验证，保留：0x0，长度：12 Id类型：IPv4地址，保留：0x0 0x0 AUTH Next payload:SA，reserved:0x0,length:28 身份验证方法PSK，保留： 0x0，保留0x0 SA下一个负载：TSi，保留：0x0，长度：40 最后一个建议：0x0，保留：0x0，长度：36 提议：1，协议ID:ESP，SPI大小：4,#trans：最后一个转换：0x3，保留：0x0：长度：8 类型：1，保留：0x0,id:3DES 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：5，保留：0x0,id：请勿使用ESN TSi下一个负载：TSr，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255 TSr下一个负载：NOTIFY，保留：0x0，长度：24 TS数量：1，保留0x0，保留0x0 TS类型：TS_IPV4_ADDR_RANGE，proto id:0，长度：16 起始端口：0，结束端口：65535 起始地址：0.0.0.0，结束地址：255.255.255.255 *11月11日19:30:34.834: IKEv2：解析通知负载：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一负载：NOTIFY，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型：SET_WINDOW_SIZE *11月11日19:30:34.834: IKEv2：解析通知负载：ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT)下一负载：NOTIFY，保留：0x0，长度	

	安全协议ID:IKE，spi大小：0，类型：ESP_TFC_NO_SUPPORT *11月11日19:30:34.834: IKEv2：解析通知负载：NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS)下一个负载：无，保留：0x0，长度：8 安全协议ID:IKE，spi大小：0，类型：NON_FIRST_FRAGS *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_WAIT_AUTH Event:EV_RECAUTH_RAUTH IP地址 *11月11日19:30:34.834:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH事件：EV_CHK4_NOTIFY *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH Event:EV_PROC消息 *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: 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 *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_GET_POLICY by_PEERID *11月11日19:30:34.834:IKEv2：将建议阶段1-prop添加到工具包策略 *11月11日19:30:34.834:IKEv2:(SA ID = 1)：使用IKEv2配置文件“IKEV2-SETUP” *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH事件：EV_VERIFY_POLICY by_PEERID *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_CHK_AUTH类型 *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_GET_HR密钥 *11月11日19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH Event:EV_AUTH_AUTH IP地址 *11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH事件：EV_CHK eap *11月11日19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:I_PROC_AUTH Event:EV_AUTH_AUTH完成(_D) *Nov 11 19:30:34.835：未配置IKEv2:AAA组授权

*11月11日19:30:34.835：未配置IKEv2:AAA用户授权
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:I_PROC_AUTH事件：EV_CHK_CONFIG模式
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:I_PROC_AUTH事件：EV_CHK4_IC
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:I_PROC_AUTH事件：EV_CHK_IKE仅
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:I_PROC_AUTH事件：EV_PROC_SA TS
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_OK
*11月11日19:30:34.835:IKEv2:(SA ID = 1)：操作：Action_Null
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_PKI_SESH_CLOSE
*11月11日19:30:34.835:IKEv2:(SA ID = 1)：关闭PKI会话
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_UPDATE_CAC_STATS
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_INSERT_IKE
*11月11日19:30:34.835:IKEv2：存储mib索引ikev2 1，平台60
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_GEN_LOAD_IPSEC
*11月11日19:30:34.835:IKEv2:(SA ID = 1)：异步请求已排队

*11月11日19:30:34.835:IKEv2:(SA ID = 1):
*11月11日19:30:34.835:IKEv2:(SA ID = 1):SM跟踪 — >
SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState:AUTH_DONE事件：EV_NO_EVENT
*11月11日19:30:34.835:IKEv2:KMI消息8已使用。未采取任何操作。
*11月11日19:30:34.835：已使用IKEv2:KMI消息12。未采取任何操作。
*11月11日19:30:34.835:IKEv2：在模式配置集中没有要发送的数据。
*11月11日19:30:34.841:IKEv2：添加与会话8的SPI 0x9506D414相关联的标
句柄0x80000002

*11月11日19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =

	00000001 CurState:AUTH_DONE事件：EV_OK_RECD_LOAD IPSEC *11月11日19:30:34.841:IKEv2:(SA ID = 1)：操作：Action_Null *11月11日19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:AUTH_DONE事件：EV_START_ACCT *11月11日19:30:34.841:IKEv2:(SA ID = 1)：无需记帐 *11月11日19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:AUTH_DONE事件：EV_CHECK_DUPE *11月11日19:30:34.841:IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: AUTH_DONE Event: EV_CHK_ROLE IP地址	
发起方上的隧道处于启用状态，且状态显示READY。	*11月11日19:30:34.841:IKEv2:(SA ID = 1):SM跟踪 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: READYEvent:EV_CHK_IKE_ONLY *11月11日19:30:34.841:IKEv2:(SA ID = 1):SM跟踪 — > SA: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 Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: READY Even EV_R_OK *11月11日19:30:34.840:IKEv2:(SA I 1):SM跟踪 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:READY事件 ：EV_NO_EVENT

CHILD_SA调试

此交换由单个请求/响应对组成，在IKEv1中称为第2阶段交换。初始交换完成后，IKE_SA的任一端均可发起此协议。

Router 1 CHILD_SA消息说明	调试	Router 2 CHILD_SA
路由器1启动CHILD_SA交换。这是CREATE_CHILD_SA请求。 CHILD_SA数据包通常包含： • SA HDR(version.flags/exchange type) • Nonce Ni（可选）：如果创建CHILD_SA作为初始交换的一部分，则不得发送第二个KE负载和nonce) • SA负载 • KEi(Key-	*11月11日19:31:35.873:IKEv2：从调度程序获取数据包 *11月11日19:31:35.873:IKEv2：处理pak队列中的项目 *11月11日19:31:35.873:IKEv2:(SA ID = 2)：请求具有mess_id 3；预期为3至7 *11月11日19:31:35.873:IKEv2:(SA ID	

optional):CREATE_CHILD_SA请求可以选择性包含用于附加DH交换的KE负载，从而为CHILD_SA启用更强的前向保密保证。如果SA提供包括不同的DH组，则KEi必须是发起方期望响应方接受的组的元素。如果它猜测错误，CREATE_CHILD_SA交换将失败，并且它可以使用不同的KEi重试 • N（通知负载 — 可选）。Notify Payload用于将信息数据（例如错误条件和状态转换）传输到IKE对等设备。通知负载可以出现在响应消息（通常它指定请求被拒绝的原因）、信息交换（报告不在IKE请求中的错误）或任何其他消息中，以指示发送方功能或修改请求的含义。如果此CREATE_CHILD_SA交换对除IKE_SA外的现有SA重新生成密钥，REKEY_SA类型的前N个负载必须标识要重新生成密钥的SA。如果此CREATE_CHILD_SA交换不对现有SA重新生成密钥，则必须省略N个负载。	= 2)：下一个负载：ENCR，版本：2.0交换类型：CREATE_CHILD_SA，标志：INITIATOR消息ID:3，长度：396 负载内容： SA下一个负载：N，保留：0x0，长度：152 最后一个建议：0x0，保留：0x0，长度：148 方案：1，协议ID:IKE，SPI大小：8,#trans：最后一次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA512 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA384 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA256 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:MD5 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA512 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA384 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA256 上次转换：0x3，保留：0x0：长度：8	

	类型：3，保留：0x0,id:SHA96 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:MD596 上次转换：0x3，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1536_MODP/组5 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2 N下一个负载：KE，保留：0x0，长度：24 KE下一个负载：NOTIFY，保留：0x0，长度：136 DH组：2，保留：0x0 *11月11日19:31:35.874:IKEv2：解析通知负载：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一负载：无，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型：SET_WINDOW_SIZE *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:READY事件：EV_RECV_CREATE_CHILD *11月11日19:31:35.874:IKEv2:(SA ID = 2)：操作：Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟踪 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_INIT事件：EV_RECV_CREATE_CHILD *11月11日19:31:35.874:IKEv2:(SA ID = 2)：操作：Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID =	

	2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 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 Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_INIT事件： EV_CHK_CC_TYPE *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_IKE事 件：EV_REKEY_IKESA *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_IKE事 件：EV_GET_IKE_POLICY *11月11日19:31:35.874:IKEv2:%正在 通过地址10.0.0.2获取预共享密钥 *11月11日19:31:35.874:IKEv2:%通过 地址10.0.0.2获取预共享密钥 *11月11日19:31:35.874:IKEv2：将建 议阶段1-prop添加到工具包策略 *11月11日19:31:35.874:IKEv2:(SA ID = 2)：使用IKEv2配置文件“IKEV2- SETUP” *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟踪 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_IKE事件： EV_PROC_MSG *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_IKE事	

	件：EV_SET_POLICY *11月11日19:31:35.874:IKEv2:(SA ID = 2)：设置已配置的策略 *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件：EV_GEN_DH密钥 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件：EV_NO_EVENT *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件：EV_OK_RECD DH_PUBKEY_RESP *11月11日19:31:35.874:IKEv2:(SA ID = 2)：操作：Action_Null *11月11日19:31:35.874:IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG Event:EV_DH_GEN密码(_S) *11月11日19:31:35.81:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件：EV_NO_EVENT *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003	

	CurState:CHILD_R_BLD_MSG事件：EV_OK_RECD DH_SECRET_RESP *11月11日19:31:35.882:IKEv2:(SA ID = 2)：操作：Action_Null *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件：EV_BLD_MSG *11月11日19:31:35.882:IKEv2：构建通知负载：SET_WINDOW_SIZE 负载内容： SA下一个负载：N，保留：0x0，长度：56 最后一个建议：0x0，保留：0x0，长度：52 提议：1，协议ID:IKE，SPI大小：8,#trans:4上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度：8 类型：4，保留：0x0,id:DH_GROUP_1024_MODP/组2 N下一个负载：KE，保留：0x0，长度：24 KE下一个负载：NOTIFY，保留：0x0，长度：136 DH组：2，保留：0x0 NOTIFY(SET_WINDOW_SIZE)下一负载：无，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型：SET_WINDOW_SIZE	
	*11月11日19:31:35.869:IKEv2:(SA ID = 2)：下一个负载：ENCR，版本：	此数据包由Router 2接收。

	2.0交换类型 ：CREATE_CHILD_SA，标志： INITIATOR消息id:2，长度：460 负载内容： ENCR下一个负载：SA，保留 ：0x0，长度：432 *11月11日19:31:35.873:IKEv2：构建 通知负载：SET_WINDOW_SIZE 负载内容： SA下一个负载：N，保留：0x0，长度 ：152 最后一个建议：0x0，保留：0x0，长度 ：148 方案：1，协议ID:IKE，SPI大小 ：8,#trans：最后一次转换：0x3，保留 ：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA512 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA384 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA256 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度：8 类型：2，保留：0x0,id:MD5 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA512 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA384 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA256 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:SHA96 上次转换：0x3，保留：0x0：长度：8 类型：3，保留：0x0,id:MD596 上次转换：0x3，保留：0x0：长度：8 类型：4，保留 ：0x0,id:DH_GROUP_1536_MODP/组 5	

	上次转换：0x0，保留：0x0：长度：8 类型：4，保留 ：0x0,id:DH_GROUP_1024_MODP/组2 N下一个负载：KE，保留：0x0，长度：24 KE下一个负载：NOTIFY，保留 ：0x0，长度：136 DH组：2，保留：0x0 NOTIFY(SET_WINDOW_SIZE)下一负载：无，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型 ：SET_WINDOW_SIZE	
	*11月11日19:31:35.882:IKEv2:(SA ID = 2)：下一个负载：ENCR，版本：2.0交换类型 ：CREATE_CHILD_SA，标志 ：RESPONDER MSG-RESPONSE消息id:3，长度：300 负载内容： SA下一个负载：N，保留：0x0，长度：56 最后一个建议：0x0，保留：0x0，长度：52 提议：1，协议ID:IKE，SPI大小 ：8,#trans:4上次转换：0x3，保留 ：0x0：长度：12 类型：1，保留：0x0,id:AES-CBC 上次转换：0x3，保留：0x0：长度 ：8 类型：2，保留：0x0,id:SHA1 上次转换：0x3，保留：0x0：长度 ：8 类型：3，保留：0x0,id:SHA96 上次转换：0x0，保留：0x0：长度 ：8 类型：4，保留 ：0x0,id:DH_GROUP_1024_MODP/组2 N下一个负载：KE，保留：0x0，长度：24 KE下一个负载：NOTIFY，保留 ：0x0，长度：136 DH组：2，保留：0x0	Router 2现在为CHILD_SA 答。这是CREATE_CHILD CHILD_SA数据包通常包含 • SA HDR(version.fla type) • Nonce Ni（可选）： CHILD_SA作为初始 分，则不得发送第二 nonce。 • SA负载 • KEi(Key- optional):CREATE_ 求可以选择性包含用 换的KE负载，从而为 CHILD_SA启用更强 保证。如果SA提供多 DH组，则KEi必须是 响应方接受的组的元 猜测错误，则 CREATE_CHILD_S ，并且必须使用其他 • N(Notify payload-op Payload用于将信息 错误条件和状态转换 IKE对等设备。通知 现在响应消息（通常 被拒绝的原因）、信 告不在IKE请求中的 何其他消息中，以指 能或修改请求的含义 CREATE_CHILD_S

	*11月11日19:31:35.882:IKEv2：解析通知负载：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一负载：无，保留：0x0，长度：12 安全协议ID:IKE，spi大小：0，类型：SET_WINDOW_SIZE *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_WAIT Event: EV_RECV_CREATE子项(_S) *11月11日19:31:35.882:IKEv2:(SA ID = 2)：操作：Action_Null *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC Event: EV_CHK4_NOTIFY *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件：EV_VERIFY_MSG *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件：EV_PROC_MSG *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件：EV_CHK4_PFS *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — >	成除IKE_SA以外的 钥，REKEY_SA类型 载必须标识重新生成 如果此CREATE_CH 不对现有SA重新生成 须省略N个负载。 路由器2发出响应，并完成 SA。

	SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件 ：EV_GEN_DH_SECRET *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件 ：EV_NO_EVENT *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件 ：EV_OK_RECD_DH secret_RESP *11月11日19:31:35.890:IKEv2:(SA ID = 2)：操作：Action_Null *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件 ：EV_CHK_IKE_REKEY *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_PROC事件 ：EV_GEN_SKEY *11月11日19:31:35.890:IKEv2:(SA ID = 2)：生成密钥ID *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_DONE Event: EV_ACTIVATE_NEW SA *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — >	

	SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_DONE事件：EV_UPDATE_CAC_STATS *11月11日19:31:35.890:IKEv2：激活新的ikev2 sa请求 *11月11日19:31:35.890:IKEv2：无法减少传出协商的计数 *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_DONE事件：EV_CHECK_DUPE *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState:CHILD_I_DONE事件：EV_OK *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState：退出事件：EV_CHK_PENDING *11月11日19:31:35.890:IKEv2:(SA ID = 2)：处理了消息ID为3的响应，请求可从范围4至8发送 *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState：退出事件：EV_NO事件(_E)	
路由器1收到来自路由器2的响应数据包并完成激活CHILD_SA。	*11月11日19:31:35.882:IKEv2:(SA ID = 2)：下一个负载：ENCR，版本：2.0交换类型：CREATE_CHILD_SA，标志：RESPONDER MSG-RESPONSE Message id:3，长度：300	

	负载内容： ENCR下一个负载：SA，保留 ：0x0，长度：272 *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件 ：EV_CHK IKE_REKEY *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_BLD_MSG事件： EV_GEN_SKEY *11月11日19:31:35.882:IKEv2:(SA ID = 2)：生成密钥ID *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_DONE事件 ：EV_ACTIVATE_NEW_SA *11月11日19:31:35.882:IKEv2：存储mib索引ikev2 3，平台62 *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_DONE事件 ：EV_UPDATE_CAC_STATS *11月11日19:31:35.882:IKEv2：激活新的ikev2 sa请求 *11月11日19:31:35.882:IKEv2：无法减少传入协商的计数 *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:	

	CHILD_R_DONE Event: EV_CHECK_DUPE *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_DONE事件：EV_OK *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState:CHILD_R_DONE事件：EV_START_DEL_NEG_TSTATE先生 *11月11日19:31:35.882:IKEv2:(SA ID = 2)：操作：Action_Null *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState：退出事件：EV_CHK_PENDING *11月11日19:31:35.882:IKEv2:(SA ID = 2)：已发送消息ID为3的响应，可以接受范围4至8的请求 *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟踪 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState：退出事件：EV_NO事件(_E)	

隧道验证

ISAKMP

命令

<#root>

show crypto ikev2 sa detailed

路由器1的输出

<#root>

```
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
```

路由器2的输出

<#root>

```
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

<#root>

show crypto ipsec sa

注意：与IKEv1不同，此输出中的PFS DH组值在第一次隧道协商期间显示为“PFS(Y/N):N，DH组：无”，但在重新生成密钥后，将显示正确的值。这不是Bug，即使Cisco Bug ID CSCug67056中描述了该行为。（只有注册的Cisco用户才能访问内部Cisco工具或信息。）IKEv1和IKEv2之间的区别在于，在后一种情况下，子SA是作为身份验证交换本身的一部分创建的。在加密映射下配置的DH组仅在重新生成密钥期间使用。因此，在第一次重新生成密钥之前，您将看到“PFS(Y/N): N， DH组：none”。
使用IKEv1时，您会看到不同的行为，因为子SA创建发生在快速模式期间，并且CREATE_CHILD_SA消息具有携带密钥交换有效负载的设置，该负载指定DH参数以派生新的共享密钥。

路由器1的输出

<#root>

```
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:
```

路由器2的输出

<#root>

```
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:
```

您还可以在两台路由器上检查show crypto session命令的输出；此输出将隧道会话状态显示为UP-ACTIVE。

<#root>

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数据包交换和协议级调试
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。