了解 IPsec IKEv1 协议

目录

简介

先决条件

- 要求
- 使用的组件
- 背景信息

IPsec

IKE协议

- IKE阶段

IKE模式（第1阶段）

- 主模式
- 积极模式

IPsec模式（第2阶段）

- 快速模式

IKE词汇表

主模式数据包交换

- 主模式1 (MM1)
- 确定两个同时进行的协商
- 主模式2 (MM2)
- 主模式3和4 (MM3-MM4)
- 主模式5和6 (MM5-MM6)

快速模式（QM1、QM2和QM3）

主动模式数据包交换

主模式与主动模式

IKEv2与IKEv1数据包交换

基于策略与基于路由

- 基于策略的VPN
- 基于路由的VPN

无法通过VPN接收流量的常见问题

- ISP阻止UDP 500/4500
- ISP阻止ESP

相关信息

简介

本文档介绍建立虚拟专用网络(VPN)的互联网密钥交换(IKEv1)协议过程。

先决条件

要求

Cisco建议您了解基本的安全概念：

- 身份验证
- 机密性
- 完整性
- IPsec

使用的组件

本文档不限于特定的软件和硬件版本。

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。

背景信息

用于建立虚拟专用网络(VPN)的互联网密钥交换(IKEv1)协议流程对于了解数据包交换非常重要，有助于简化任何类型的IKEv1互联网协议安全(IPsec)问题的故障排除。

IPsec

IPsec是在IP层为Internet通信提供安全保护的一组协议。目前IPsec最常见的用途是在两个位置之间（网关到网关）或在远程用户与企业网络（主机到网关）之间提供虚拟专用网络(VPN)。

IKE协议

IPsec使用IKE协议协商并建立安全的站点到站点或远程访问虚拟专用网络(VPN)隧道。IKE协议也称为互联网安全关联和密钥管理协议(ISAKMP)（仅在思科提供）。

IKE有两个版本：

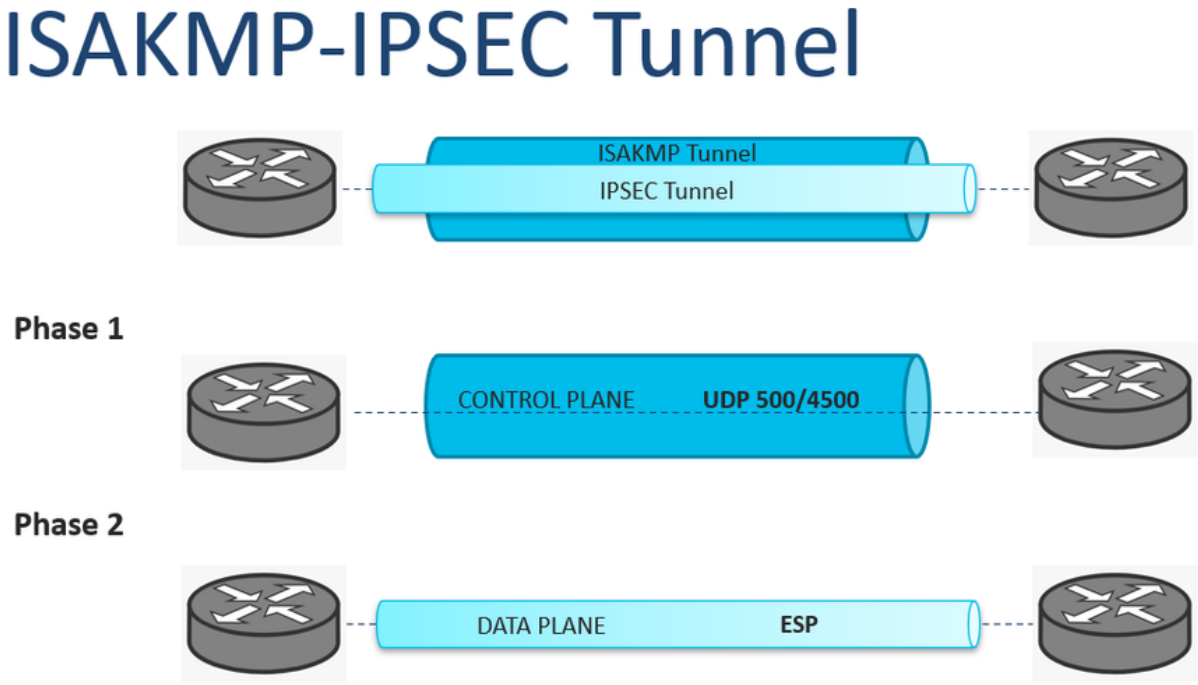
- IKEv1：在RFC 2409（互联网密钥交换）中定义
- IKE第2版(IKEv2)：在RFC 4306互联网密钥交换(IKEv2)协议中定义

IKE阶段

ISAKMP将协商分为两个阶段：

- 第1阶段：两个ISAKMP对等体建立经过身份验证的安全隧道，保护ISAKMP协商消息。此隧道称为ISAKMP SA。ISAKMP定义了两种模式：主模式(MM)和主动模式。
- 第2阶段：协商要通过IPsec隧道传输的数据加密(SA)的关键材料和算法。此阶段称为快速模式。

为了实现所有抽象概念，第1阶段隧道是父隧道，第2阶段是子隧道。下图以隧道形式说明两个阶段：



注意：第1阶段(ISAKMP)隧道保护两个网关之间的控制平面VPN流量。控制平面流量可以是协商数据包、信息包、DPD、keepalive、重新生成密钥等。ISAKMP协商使用UDP 500和4500端口建立安全信道。

注意：第2阶段(IPsec)隧道可保护在两个网关之间通过VPN的数据平面流量。用于保护数据的算法在第2阶段配置，并且独立于第1阶段中指定的算法。
用于封装和加密这些数据包的协议是封装安全负载(ESP)。

IKE模式（第1阶段）

主模式

发起方向响应方发送建议或建议时，IKE会话开始。节点间的第一次交换建立基本的安全策略；发起方提出加密和认证算法供使用。响应方选择适当的建议书（假设已选择建议书）并将其发送给发起方。下一个交换传递Diffie-Hellman公钥和其他数据。所有进一步协商在IKE SA内加密。第三个交换机会验证ISAKMP会话。一旦建立IKE SA，IPSec协商（快速模式）就会开始。

积极模式

主动模式将IKE SA协商压缩成三个数据包，SA所需的所有数据都由发起方通过。响应方发送建议、密钥材料和ID，并在下一个数据包中验证会话。发起方回复并验证会话。协商速度更快，且发起方和响应方ID传递清晰。

IPsec模式（第2阶段）

快速模式

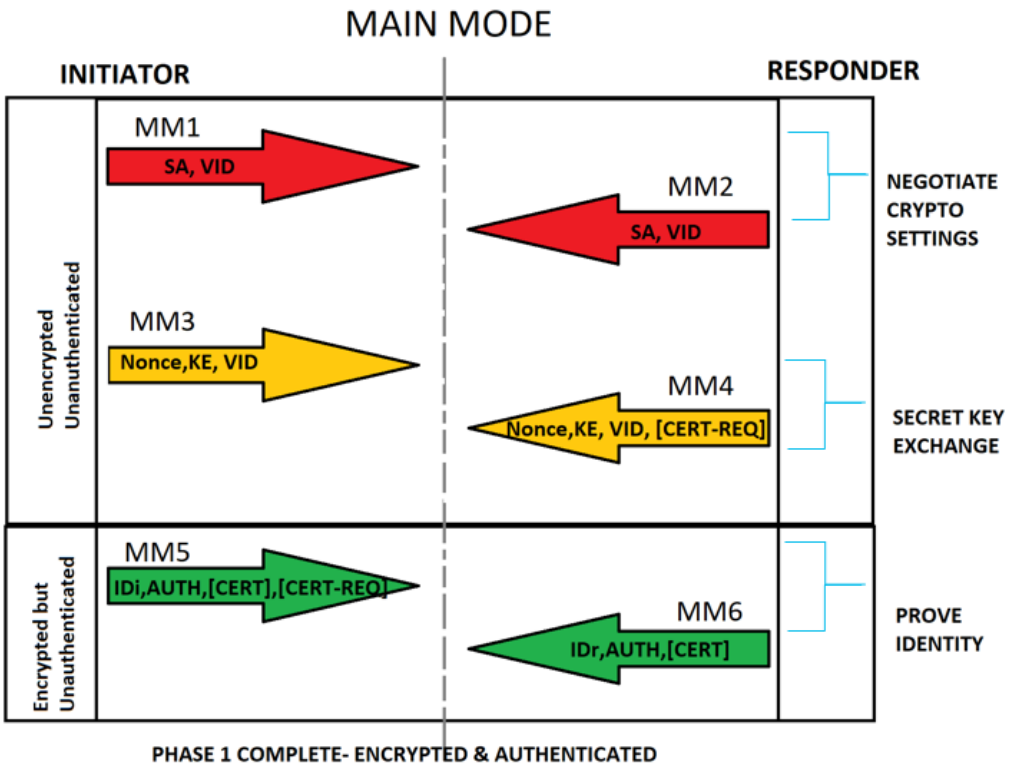
IPSec协商（或快速模式）类似于主动模式 IKE协商，但协商必须在IKE SA中保护。快速模式协商用于数据加密的SA，并管理该IPSec SA的密钥交换。

IKE词汇表

- 安全关联(SA)是在两个网络实体之间建立共享安全属性以支持安全通信。SA包括加密算法和模式等属性；流量加密密钥；以及用于要通过连接传递的网络数据的参数。
- 处理供应商ID (VID)以确定对等体是否支持NAT穿越、失效对等体检测功能和分段等。
- 随机数：发起方发送的随机生成的数字。此随机数连同使用商定密钥的其他项目一起散列并发送回。发起方会检查cookie和nonce，并拒绝没有正确nonce的任何消息。这有助于防止重播，因为没有任何第三方能够预测随机生成的随机随机事件是什么。
- Diffie-Hellman (DH)安全密钥交换过程的密钥交换(KE)信息。
- 身份发起方/响应方(IDi/IDr.)用于向对等体发送身份验证信息。此信息在公用共享密钥的保护下传输。
- Diffie-Hellman (DH)密钥交换是在公共信道上安全交换加密算法的方法。
- IPSec共享密钥可以派生，DH可以再次使用，以确保完全向前保密(PFS)或原始DH交换刷新为先前派生的共享密钥。

主模式数据包交换

每个ISAKMP数据包都包含用于建立隧道的负载信息。IKE词汇表将IKE缩写说明为主模式的数据包交换的负载内容的一部分，如下图所示。

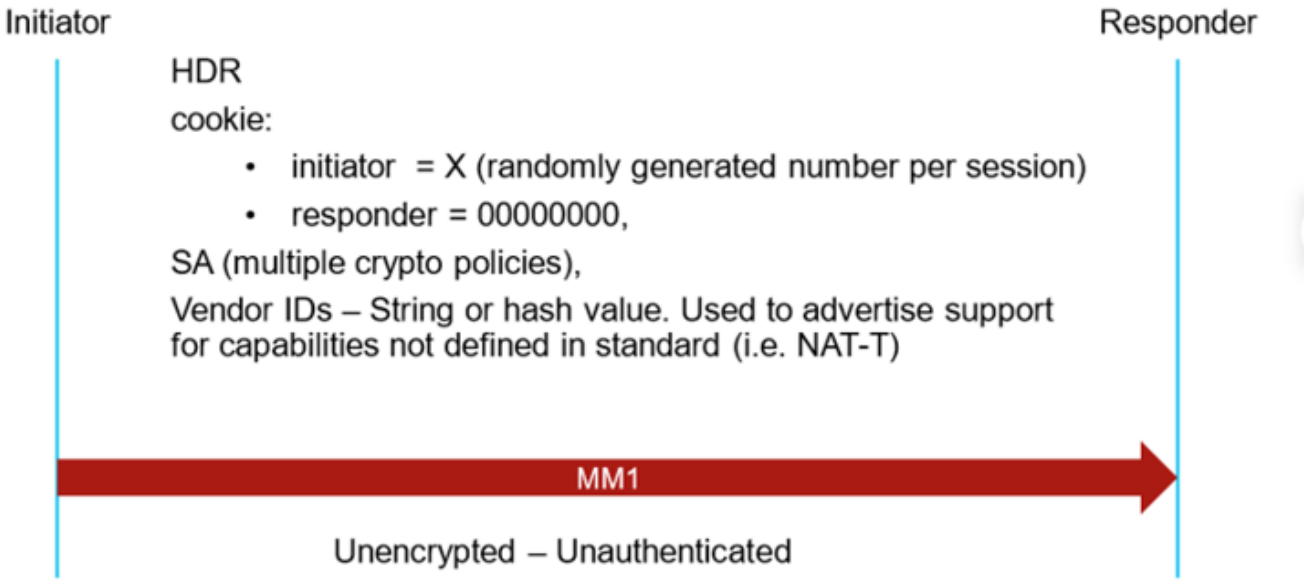


主模式1 (MM1)

要设置ISAKMP协商的条款，您需要创建ISAKMP策略，包括：

- 一种身份验证方法，用于确保对等体的身份。
- 一种加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码(HMAC)方法，用于确保发送方的身份，并确保消息在传输过程中未被修改。
- Diffie-Hellman组，用于确定加密密钥确定算法的强度。安全设备使用此算法获取加密密钥和散列密钥。
- 对安全设备在更换加密密钥之前使用加密密钥的时间的限制。

第一个数据包由IKE协商的发起方发送，如图所示：



注意：主模式1是IKE协商的第一个数据包。因此，当响应方SPI设置为0时，发起方SPI设置为随机值。在第二个数据包(MM2)中，响应方SPI必须使用新值进行响应，并且整个协商保持相同的SPI值。

如果捕获MM1并使用Wireshark网络协议分析器，则SPI值在Internet安全连接和密钥管理协议内容中，如图所示：

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
```

注意：如果路径中MM1数据包丢失或没有MM2应答，则IKE协商会保留MM1重新传输，直到达到最大重新传输次数为止。此时，发起方保持相同的SPI，直到再次触发下一次协商。

提示：识别发起方和响应方SPI对于识别同一VPN的多个协商以及缩小某些协商问题的范围非常有用。

确定两个同时进行的协商

在Cisco IOS® XE平台上，可以使用配置的远程IP地址的条件按隧道过滤调试。但是，同步协商会显示在日志中，并且无法对其进行过滤。需要手动执行。如前所述，整个协商为发起方和响应方保留相同的SPI值。如果从同一对等体IP地址收到数据包，但SPI与协商达到最大重新传输次数之前跟踪的上一个值不匹配，则这是同一对等体的另一个协商，如图所示：

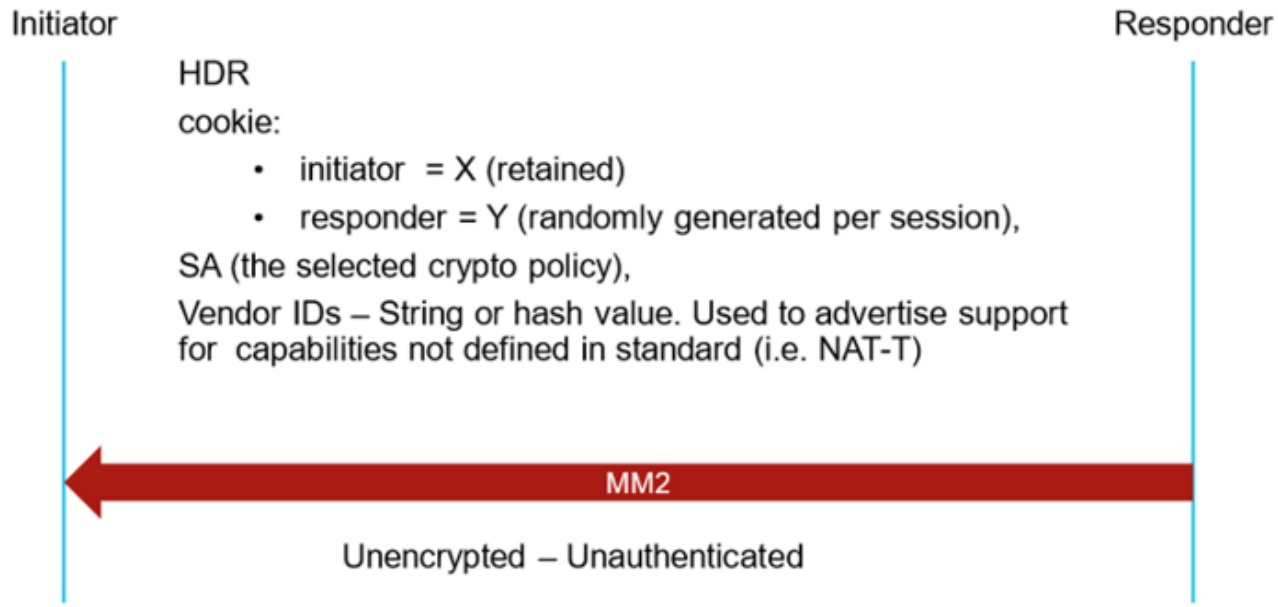
```
ISR4451
****************************************
                2A8F14E40D648E28
*Apr 29 16:57:40.944: IKEv2:(SESSION ID = 27621,SA ID = 1):Sending Packet [To 198.19.252.1:500/From 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 2A8F14E40D648E28 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) VID

*Apr 29 16:57:42.200: IPSEC:(SESSION ID = 27621) (key_engine) request timer fired: count = 1,
  (identity) local= 10.11.6.2:0, remote= 198.19.252.1:0,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Apr 29 16:57:42.200: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.11.6.2:500, remote= 198.19.252.1:500,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0,
    protocol= ESP, transform= esp-aes 256 esp-sha-hmac  (Tunnel),
    lifedur= 28800s and 4294967295kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
omr2-site1#     5638222923EA3C5A
*Apr 29 16:57:53.763: IKEv2:Received Packet [From 198.19.252.1:500/To 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 5638222923EA3C5A - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) NOTIFY(Unknown - 16431) NOTIFY(REDIRECT_SUPPORTED)
```

注意：该示例显示协商中的第一个数据包(MM1)的同时协商。但是，这可以在任何协商点发生。所有后续数据包必须在响应方SPI上包含与0不同的值。

主模式2 (MM2)

在主模式2数据包中，响应方为匹配的提议发送所选策略，并且响应方SPI设置为随机值。整个协商保持相同的SPI值。MM2回复MM1，SPI响应器设置为与0不同的值，如图所示：



如果捕获MM2并使用Wireshark网络协议分析器，则发起方SPI和响应方SPI值在Internet安全连接和密钥管理协议内容中，如图所示：

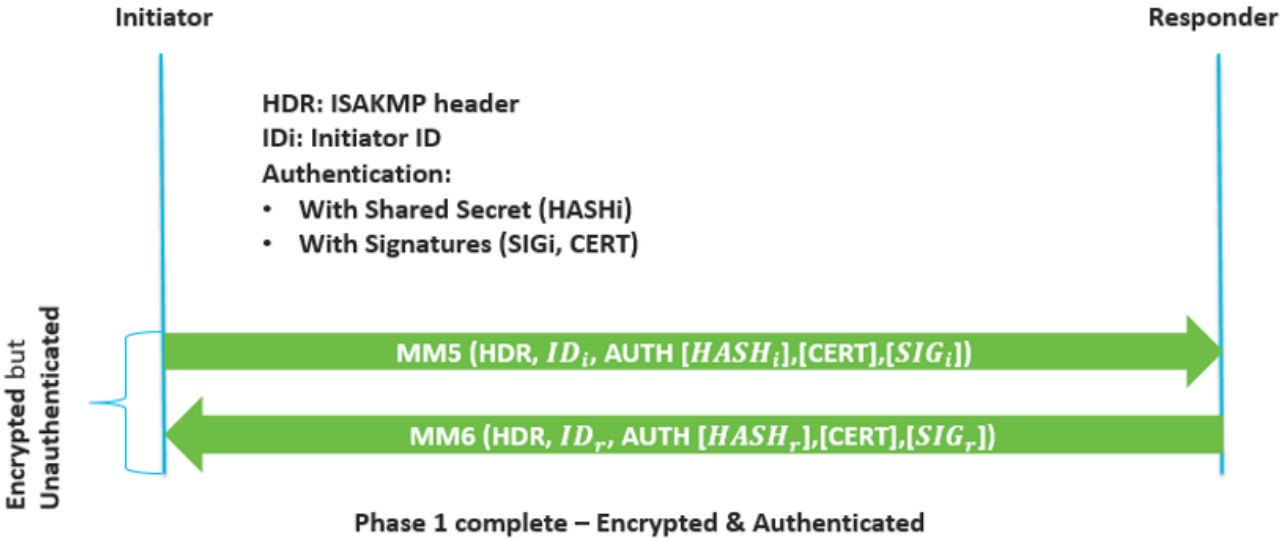
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 2bc06438c94e88dc
    Next payload: Security Association (33)
```

主模式3和4 (MM3-MM4)

MM3和MM4数据包仍未加密且未经身份验证，并且会进行密钥交换。MM3和MM4如图所示：

主模式5和6 (MM5-MM6)

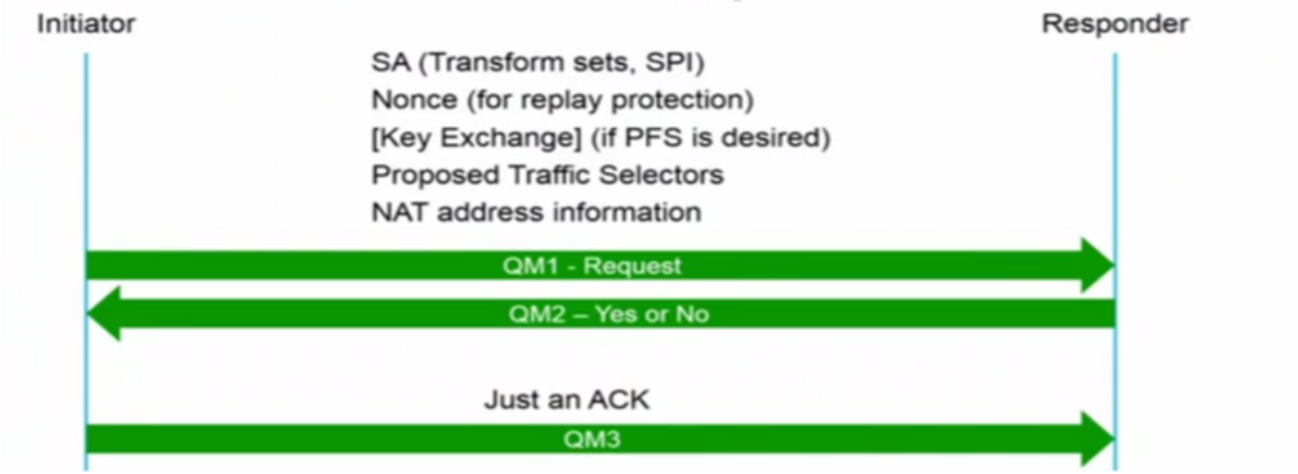
MM5和MM6数据包已加密，但仍未经身份验证。在这些数据包上，身份验证按图中所示进行：



快速模式（QM1、QM2和QM3）

在主节点和IKE在第1阶段建立安全隧道后出现快速模式。快速模式协商共享IPSec策略，用于IPSec安全算法，并管理IPSec SA建立的密钥交换。随机数用于生成新的共享密钥材料，并防止来自生成的伪造SA的重播攻击。

如图所示，在此阶段交换三个数据包：

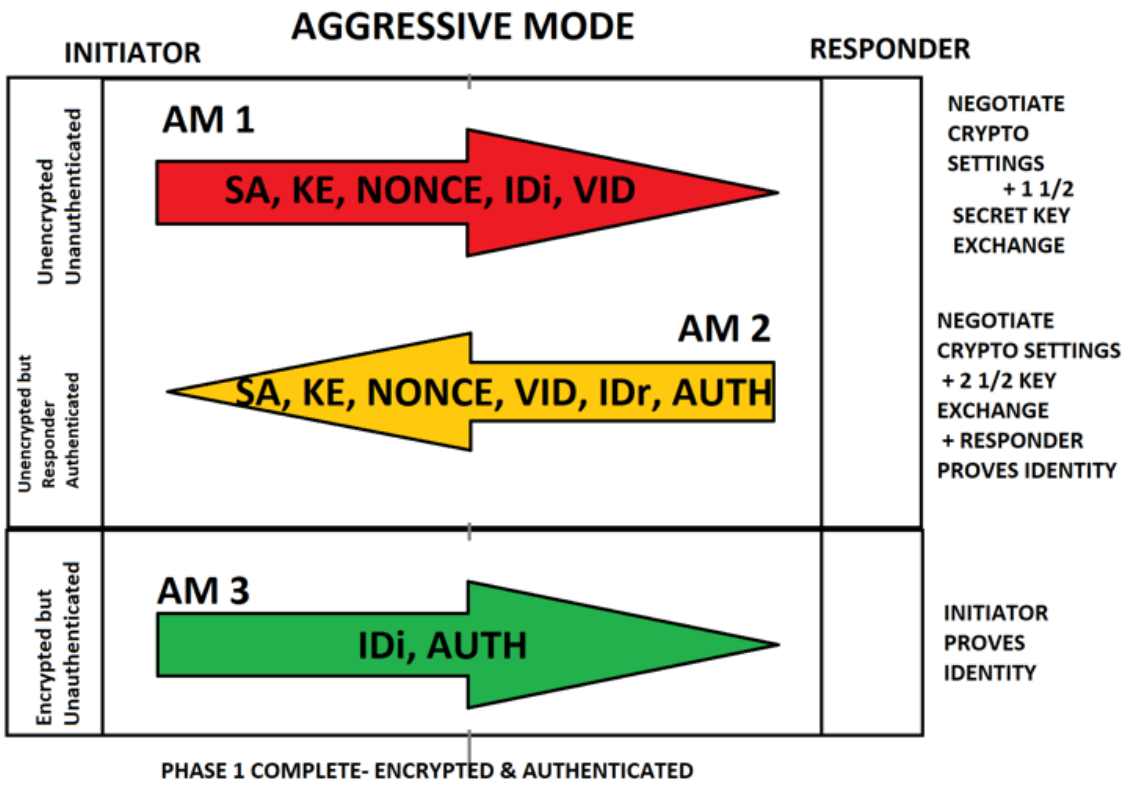


主动模式数据包交换

主动模式将IKE SA协商压缩为三个数据包，SA所需的所有数据都由发起方通过。

- 响应方发送建议、密钥材料和ID，并在下一个数据包中验证会话。
- 发起方回复并验证会话。
- 协商速度更快，且发起方和响应方ID传递清晰。

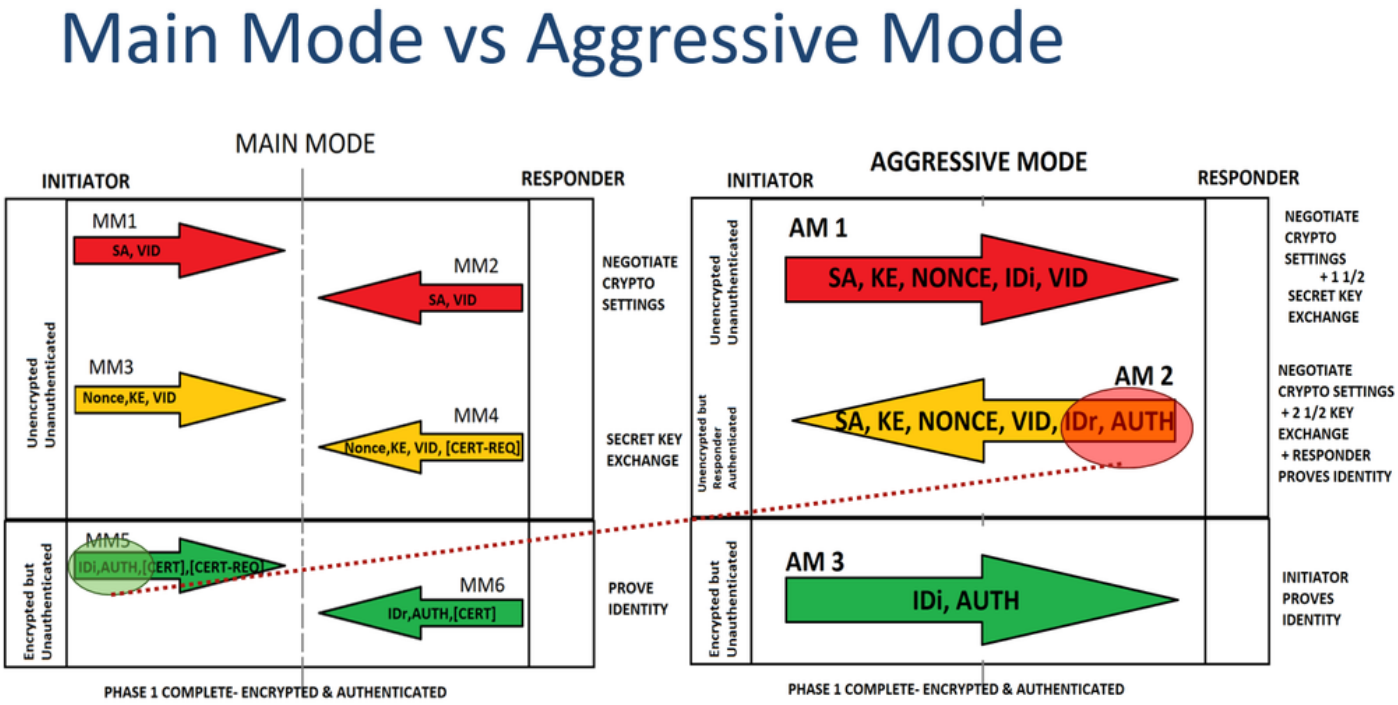
下图显示在主动模式下交换的三个数据包的负载内容：



主模式与主动模式

与主模式相比，主动模式可分为三个包：

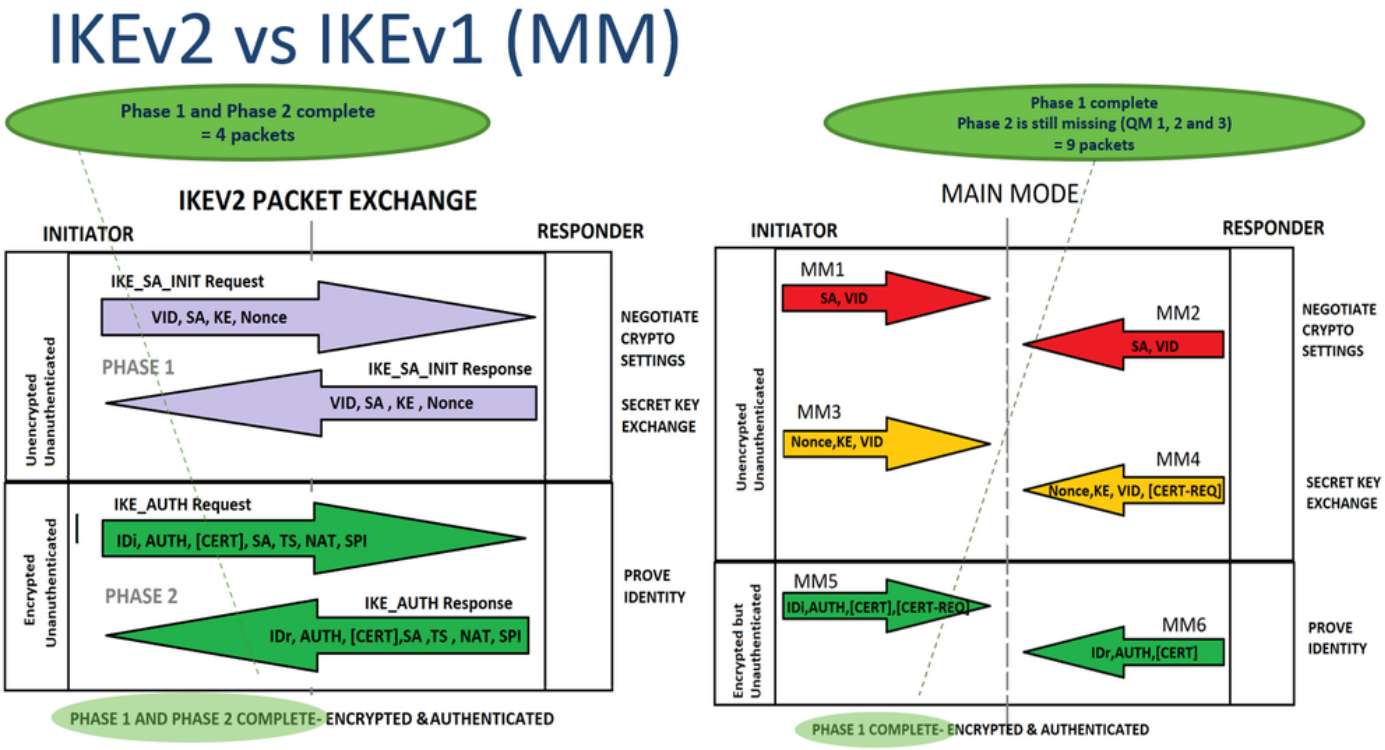
- AM 1吸收MM1和MM3。
- AM 2吸收MM2、MM4和MM6的一部分。这就是攻击性模式的漏洞的来源。AM 2组成ID和身份验证未加密。与主模式不同，此信息是加密的。
- AM 3提供ID和身份验证。这些值已加密。



IKEv2与IKEv1数据包交换

在IKEv2协商中，为建立隧道而交换的消息更少。IKEv2使用四个消息；IKEv1使用六个消息（在主模式下）或三个消息（在主动模式下）。

IKEv2消息类型定义为请求和响应对。下图显示了IKEv2与IKEv1的数据包比较和负载内容：



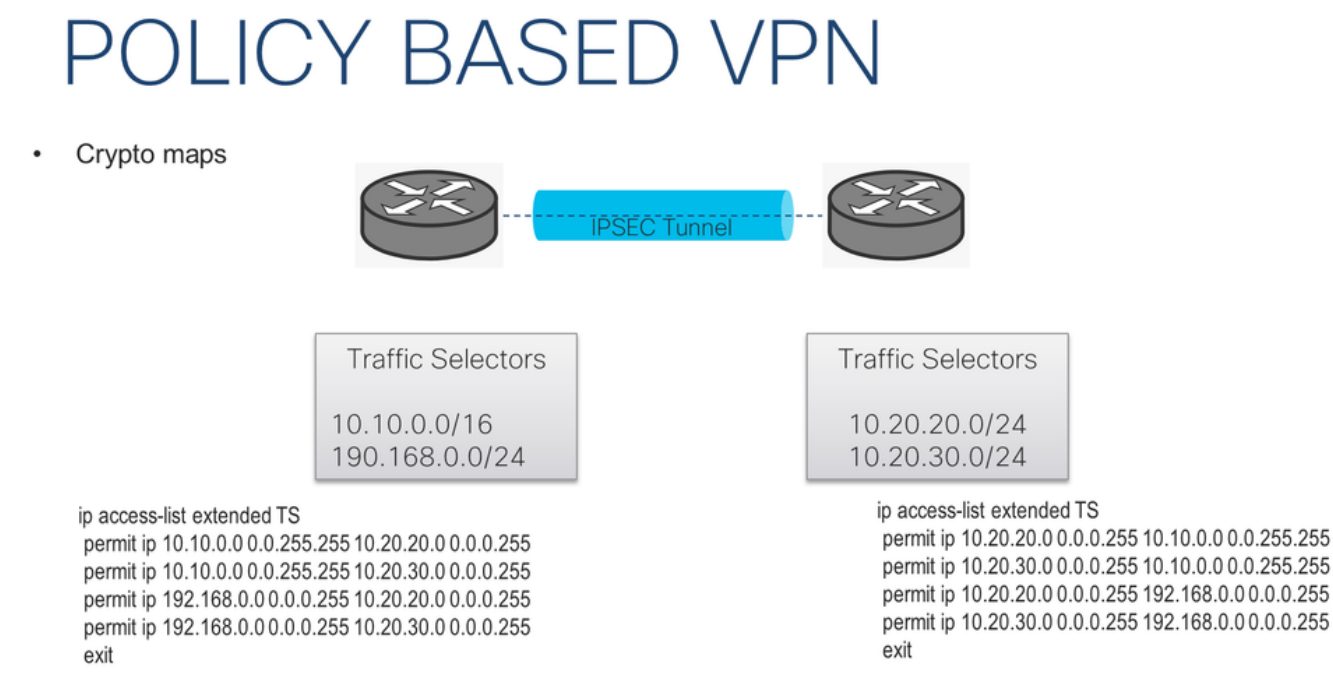
注意：本文档不深入探讨IKEv2数据包交换。有关更多参考，请导航到[IKEv2数据包交换和协议级别调试]。

基于策略与基于路由

基于策略的VPN

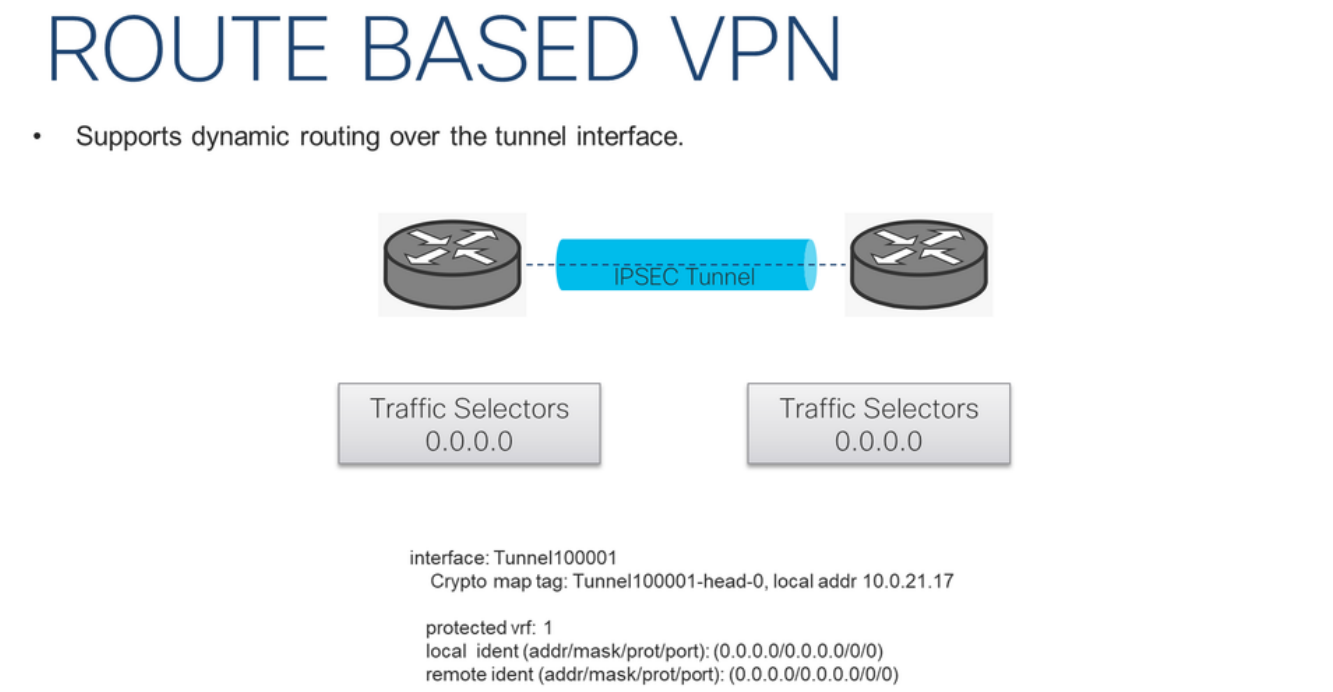
如名称所述，基于策略的VPN是IPsec VPN隧道，对符合策略匹配条件的传输流量执行策略操作。对于Cisco设备，会配置访问列表(ACL)并将其附加到加密映射，以指定要重定向到VPN并加密的流量。

流量选择器是在策略中指定的子网或主机，如图所示：



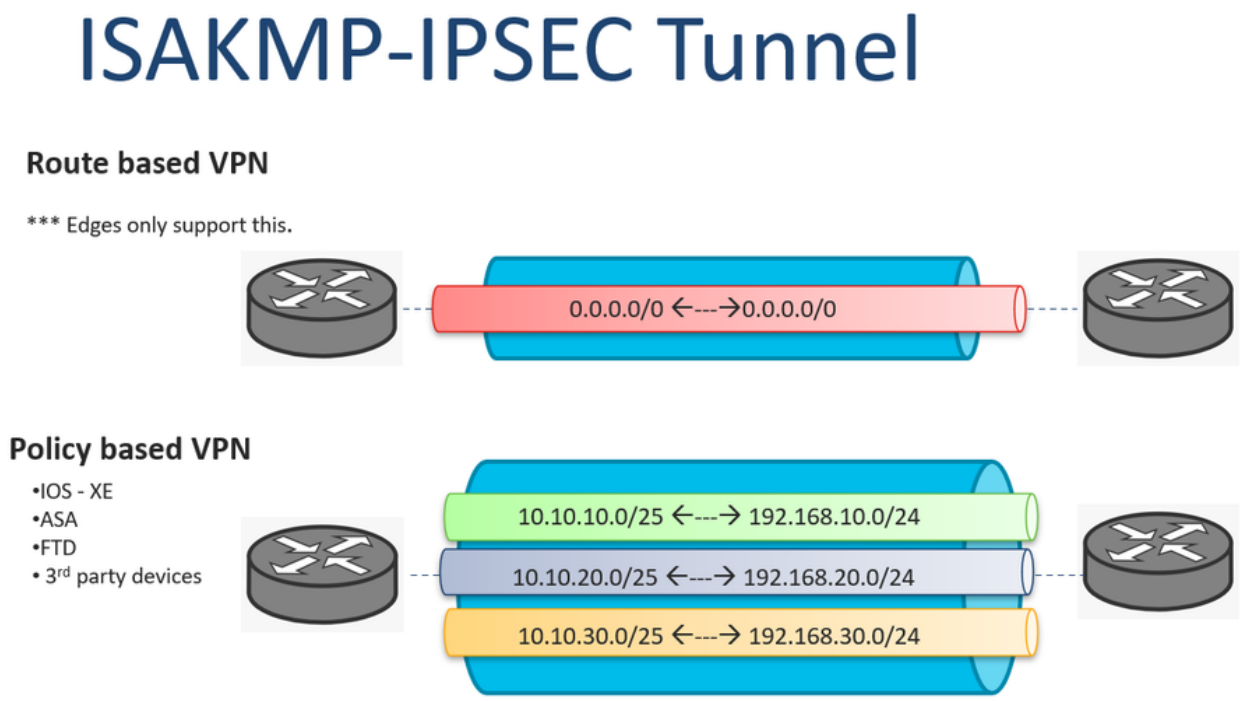
基于路由的VPN

不需要策略。流量被重定向到具有路由的隧道，并支持通过隧道接口进行动态路由。默认情况下，流量选择器（通过VPN加密的流量）为0.0.0.0到0.0.0.0，如图所示：



注意：由于流量选择器为0.0.0.0，因此中包含任何主机或子网。因此，仅创建一个SA。动态隧道例外。本文档不介绍动态隧道。

基于策略和路由的VPN可以具体化，如图所示：



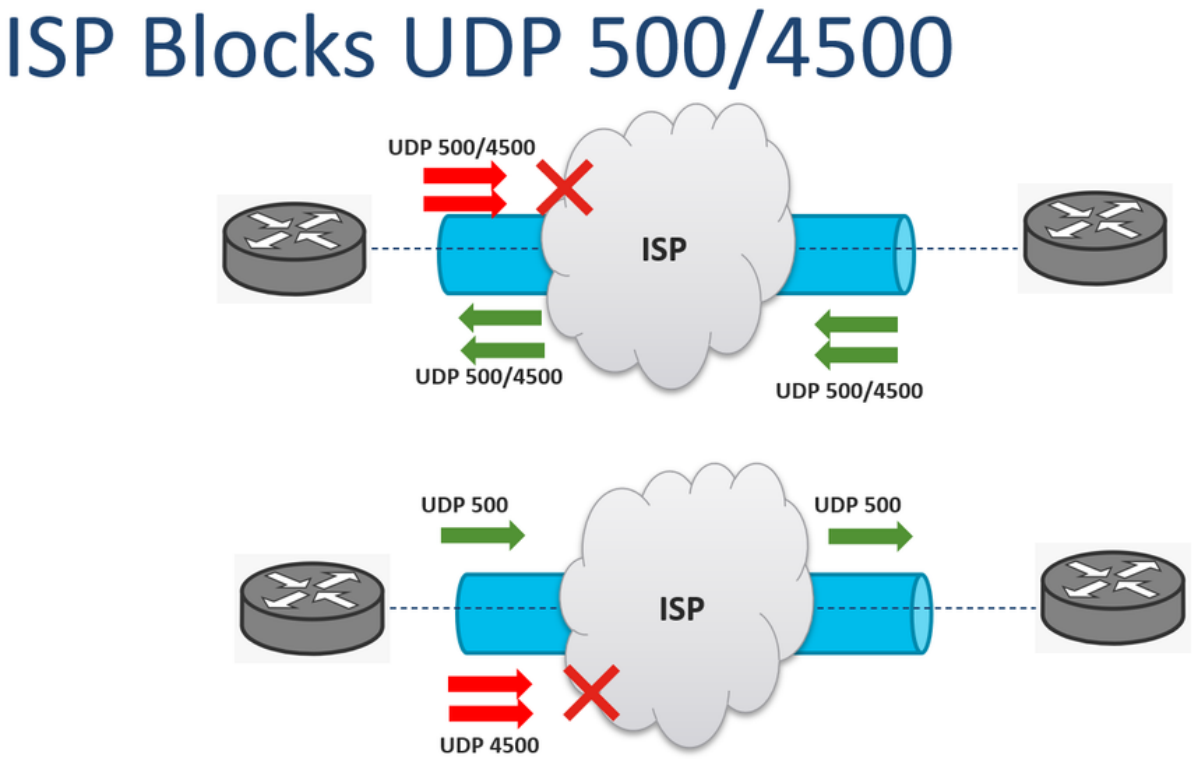
注意：与仅创建一个SA的基于路由的VPN不同，基于策略的VPN可以创建多个SA。配置ACL后，ACL上的每条语句（如果它们不同）都会创建子隧道。

无法通过VPN接收流量的常见问题

ISP阻止UDP 500/4500

互联网服务提供商(ISP)阻止UDP 500/4500端口是一个非常常见的问题。对于IPsec隧道的建立，可以采用两个不同的ISP。其中一个可以阻塞端口，另一个允许阻塞。

下图显示了ISP只能在一个方向上阻止UDP 500/4500端口的两个场景：

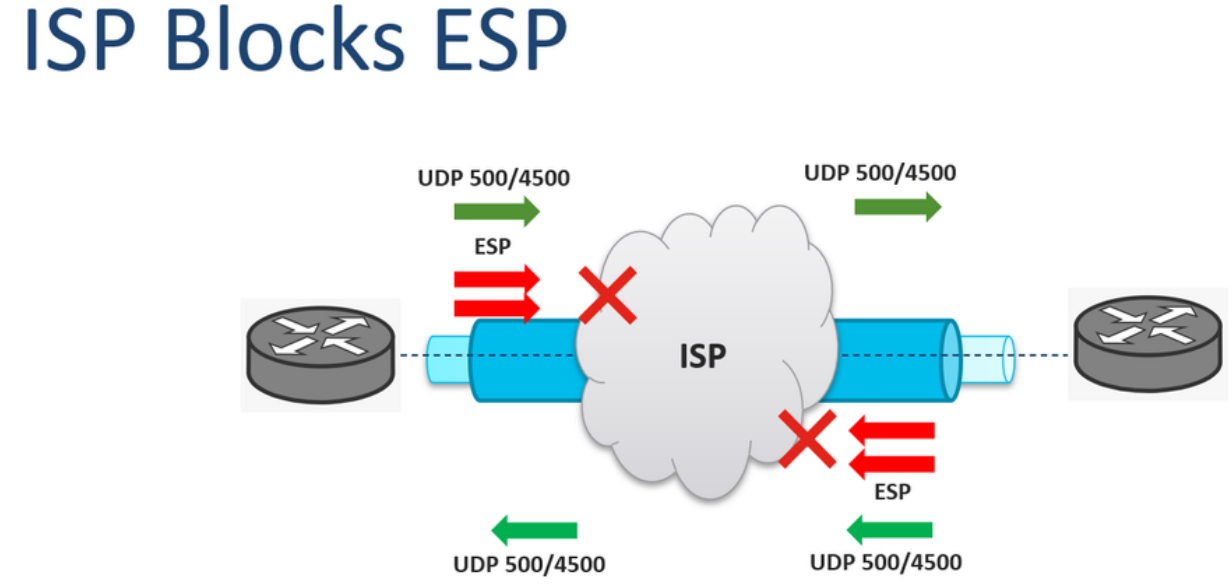


注意：互联网密钥交换(IKE)使用端口UDP 500建立安全VPN隧道。当NAT存在于一个VPN终端中时，使用UDP 4500。

注意：当ISP阻止UDP 500/4500时，IPsec隧道建立会受到影响，它不会启动。

ISP阻止ESP

IPsec隧道的另一个非常常见的问题是ISP阻止ESP流量；但它允许UDP 500/4500端口。例如，允许UDP 500/4500端口双向传输。因此，隧道已成功建立，但ISP或ISP在两个方向上都阻止了ESP数据包。这会导致通过VPN的加密流量失败，如图所示：



注意：当ISP阻止ESP数据包时，IPsec隧道建立是成功的，但已加密的流量将受到影响。VPN启动时可以反映这一点，但流量无法通过该接口工作。

提示：ESP流量仅在一个方向被阻止的场景也可能出现。症状相同，但使用隧道统计信息、封装、解封计数器或RX和TX计数器可以轻松找到它。

相关信息

- KEv2数据包交换和协议级调试
- 互联网密钥交换(IKE) - RFC 2409
- 互联网密钥交换(IKEv2)协议
- 技术支持和文档 - Cisco Systems

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）。