瞭解 IPsec IKEv1 通訊協定

目錄

簡介

本檔案介紹建立虛擬私人網路(VPN)的網際網路金鑰交換(IKEv1)通訊協定程式。

必要條件

需求

思科建議您瞭解基本的安全概念：

- 驗證
- 機密性
- 完整性
- IPsec

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

建立虛擬私人網路(VPN)的網際網路金鑰交換(IKEv1)通訊協定程式對於了解封包交換非常重要，可讓您更輕鬆地疑難排解IKEv1的任何型別網際網路通訊協定安全(IPsec)問題。

IPsec

IPsec是在IP層為Internet通訊提供安全保護的一組協定。IPsec當前最常用的用途是在兩個位置之間（網關到網關）或在遠端使用者與企業網路之間（主機到網關）提供虛擬專用網路(VPN)。

IKE通訊協定

IPsec使用IKE協定協商並建立安全的站點到站點或遠端訪問虛擬專用網路(VPN)隧道。IKE協定也稱為網際網路安全連線和金鑰管理協定(ISAKMP)（僅在思科提供）。

IKE有兩個版本：

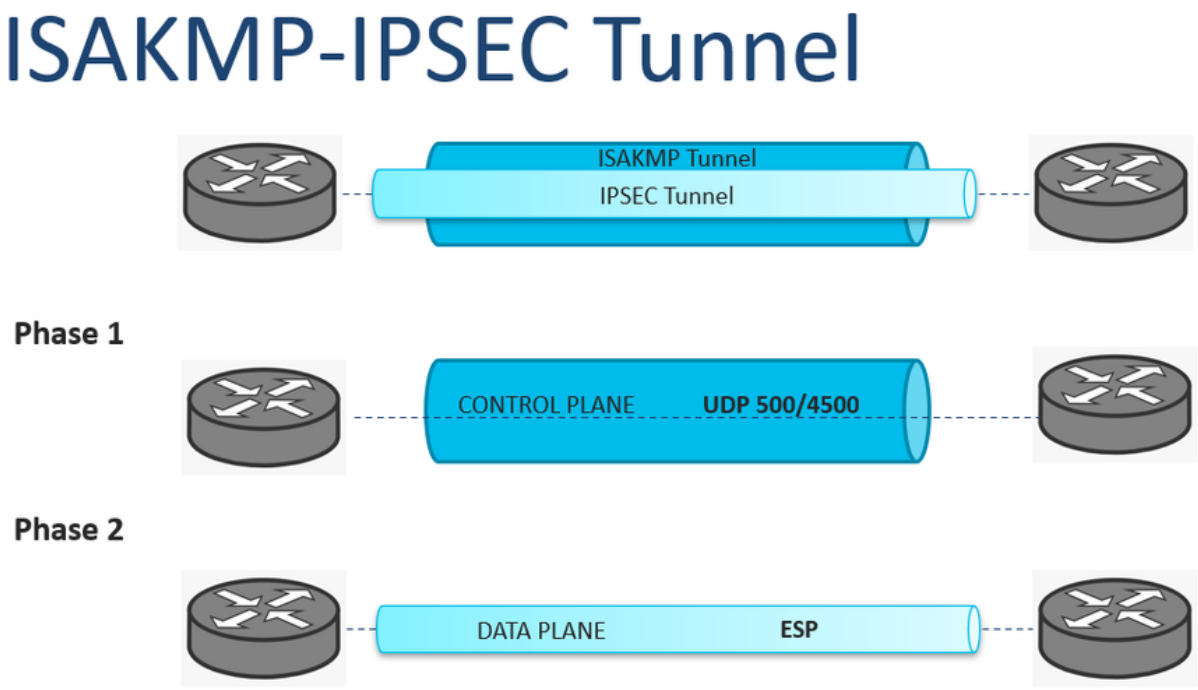
- IKEv1：在RFC 2409，網際網路金鑰交換
- IKE第2版(IKEv2)：在RFC 4306中定義，網際網路金鑰交換(IKEv2)協定

IKE階段

ISAKMP將協商分為兩個階段：

- 第1階段：兩個ISAKMP對等體建立一個安全且經過身份驗證的隧道，用於保護ISAKMP協商消息。此隧道稱為ISAKMP SA。ISAKMP定義了兩種模式：主模式(MM)和主動模式。
- 第2階段：它協商要透過IPSec隧道傳輸的資料加密(SA)的關鍵材料和演算法。此階段稱為快速模式。

為了體現所有抽象概念，階段1隧道是父隧道，階段2是子隧道。下圖說明了作為隧道的兩個階段：



注意：第1階段(ISAKMP)隧道可保護兩個網關之間的控制板VPN流量。控制平面流量可以是協商資料包、資訊包、DPD、keepalive和rekey等。ISAKMP協商使用UDP 500和4500埠建立安全通道。

注意：階段2 (IPsec)隧道可保護在兩個網關之間透過VPN的資料平面流量。用於保護資料的演算法是在階段2中配置的，獨立於階段1中指定的演算法。
用於封裝和加密這些封包的通訊協定是封裝安全負載(ESP)。

IKE模式（第1階段）

主模式

當發起方向響應方傳送提議或提議時，IKE會話開始。節點之間的第一次交換建立基本安全策略；發起方提出要使用的加密和驗證演算法。響應方選擇適當的方案（假設已選擇方案）並將其傳送給啟動方。下一次交換將傳遞Diffie-Hellman公鑰和其他資料。所有進一步的協商在IKE SA內都會被加密。第三個交換對ISAKMP會話進行身份驗證。一旦建立IKE SA，IPSec協商（快速模式）就會開始。

主動模式

主動模式將IKE SA協商壓縮為三個資料包，由發起方傳遞SA所需的所有資料。響應方傳送建議、金鑰材料和ID，並在下一個資料包中驗證會話。發起方回覆並驗證會話。協商更快，且發起方和響應方ID以明文形式傳遞。

IPsec模式（第2階段）

快速模式

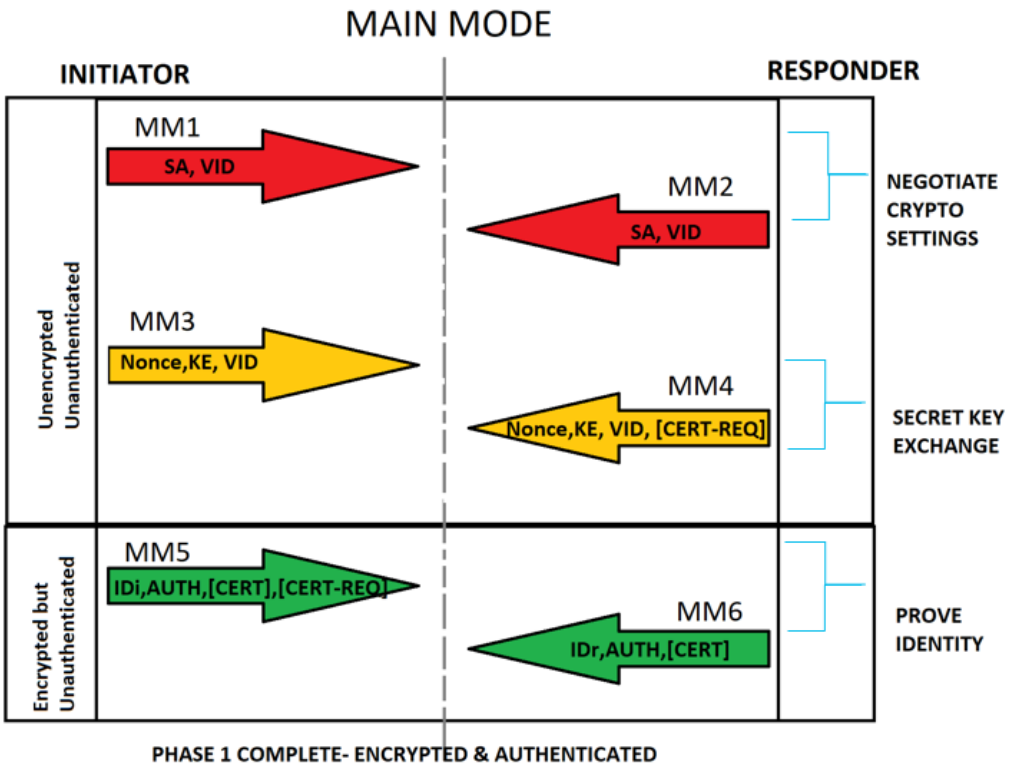
IPSec協商（或快速模式）類似於主動模式 IKE協商，但協商除外，它必須在IKE SA中受到保護。快速模式會協商SA以進行資料加密，並管理該IPSec SA的金鑰交換。

IKE辭彙表

- 安全關聯(SA)是在兩個網路實體之間建立共用的安全屬性以支援安全通訊。SA包括諸如加密演算法和模式的屬性；流量加密金鑰；以及用於要透過連線傳遞的網路資料的引數。
- 處理供應商ID (VID)以確定對等體是否支援NAT遍歷、失效對等體檢測功能、分段等。
- Nonce：發起方傳送的隨機生成的編號。此隨機數會與其他使用協定金鑰的專案一起雜湊，並傳回。初始器會檢查Cookie和Nonce，並拒絕任何沒有正確Nonce的消息。這有助於防止重播，因為沒有任何第三方能夠預測隨機生成的隨機事件是什麼。
- Diffie-Hellman (DH)安全金鑰交換過程的金鑰交換(KE)資訊。
- 身份發起方/響應方(IDi/IDr.)用於向對等方傳送身份驗證資訊。此資訊在共同共用金鑰的保護下傳輸。
- Diffie-Hellman (DH)金鑰交換是一種在公共通道上安全交換加密演算法的方法。
- IPSec共用金鑰可衍生為DH，DH可再次使用以確保完全正向保密(PFS)或原始DH交換更新為先前衍生的共用金鑰。

主模式資料包交換

每個ISAKMP資料包都包含用於建立隧道的負載資訊。IKE辭彙表將IKE縮寫解釋為主模式上資料包交換的負載內容的一部分，如下圖所示。

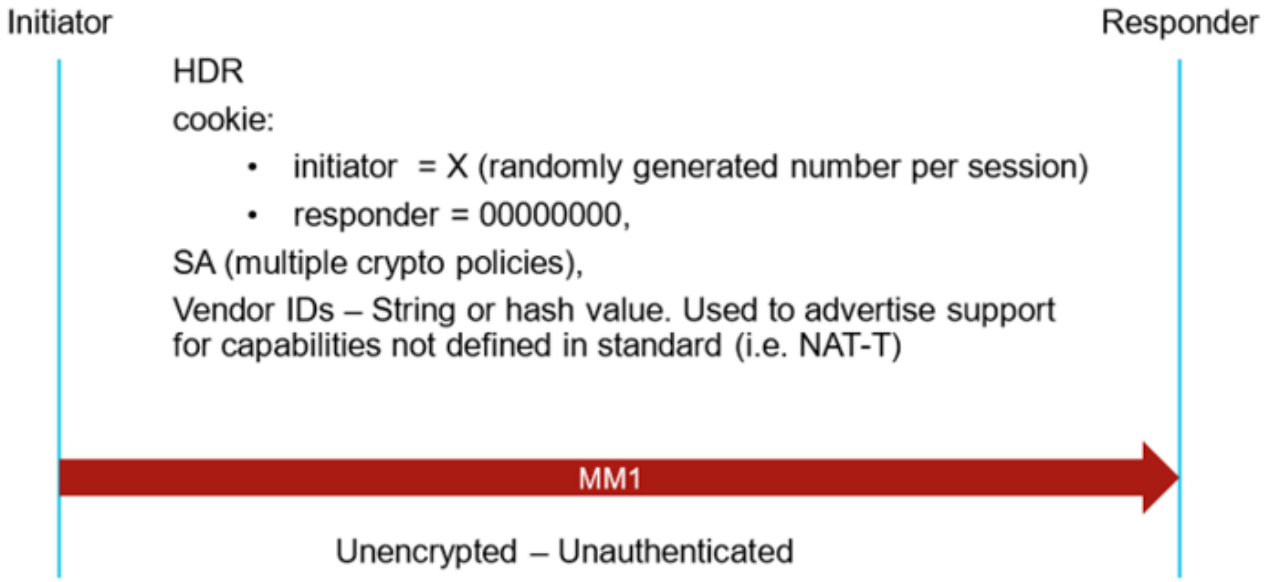


主模式1 (MM1)

要設定ISAKMP協商的條件，您需要建立一個ISAKMP策略，包括：

- 一種身份驗證方法，用於確保對等體的身份。
- 一種加密方法，用於保護資料並確保隱私。
- 雜湊消息驗證代碼(HMAC)方法，用於確保傳送方的身份，並確保消息在傳輸過程中未被修改。
- 用於確定加密金鑰確定演算法強度的Diffie-Hellman組。安全裝置使用此演算法導出加密金鑰和雜湊金鑰。
- 安全裝置在金鑰被替換之前使用加密金鑰的時間限制。

第一個資料包由IKE協商的發起方傳送，如圖所示：



注意：主模式1是IKE協商的第一個資料包。因此，啟動器SPI設定為隨機值，而響應器SPI設定為0。在第二個資料包(MM2)中，必須使用新值來響應方SPI，並且整個協商保持相同的SPI值。

如果捕獲MM1並使用Wireshark網路協定分析器，則SPI值位於Internet安全連線和金鑰管理協定內容中，如圖所示：

```
> 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：在這種情況下，MM1資料包在路徑中丟失或者沒有MM2應答，IKE協商會保留MM1的重傳，直到達到最大重傳次數為止。此時，發起方將保持相同的SPI，直到再次觸發下一個協商。

提示：標識發起方和響應方SPI對於標識同一VPN的多個協商以及縮小某些協商問題範圍非常有用。

確定兩個同時進行的協商

在Cisco IOS® XE平台上，可以透過配置遠端IP地址的條件為每個隧道過濾調試。但是，同步協商會顯示在日誌中，並且無法對其進行過濾。需要手動執行。如前所述，整個協商會保持發起方和響應方的SPI值相同。如果從同一對等體IP地址收到資料包，但SPI與協商達到最大重傳次數之前跟蹤的上一個值不匹配，則這是同一對等體的另一個協商，如下圖所示：

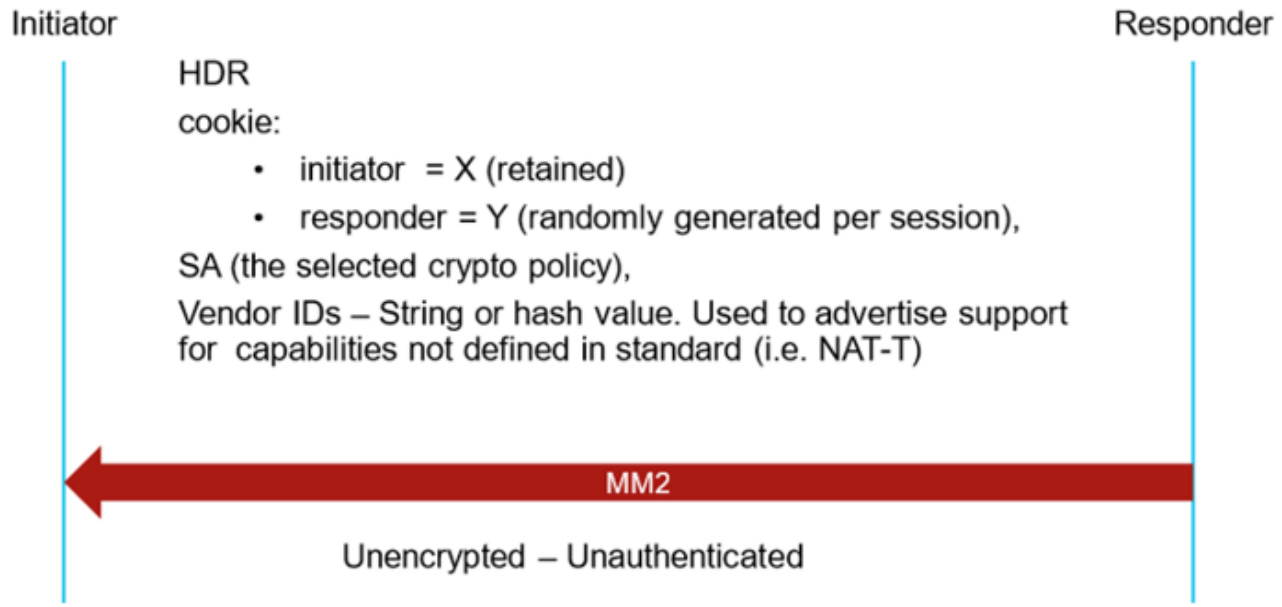
```
ISR4451
****************************************
2A8F14E40D648E28
*Apr 29 16:57:40.944: IKEv2:(SESSION ID = 27621,SA ID = 1):Sending Packet [To 198.19.252.1:500/From 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 2A8F14E40D648E28 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange 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：此範例顯示交涉中(MM1)第一個封包的同時交涉。但是，這可以在任何協商點發生。所有後續資料包必須包含與響應方SPI上的0不同的值。

主模式2 (MM2)

在Main Mode 2資料包中，響應方為匹配的建議傳送選定的策略，並且響應方SPI設定為隨機值。整個協商會保持相同的SPI值。MM2回覆MM1，SPI響應器設定為與0不同的值，如圖所示：



如果捕獲MM2並使用Wireshark網路協定分析器，則啟動器SPI和響應器SPI值位於Internet安全連線和金鑰管理協定內容中，如圖所示：

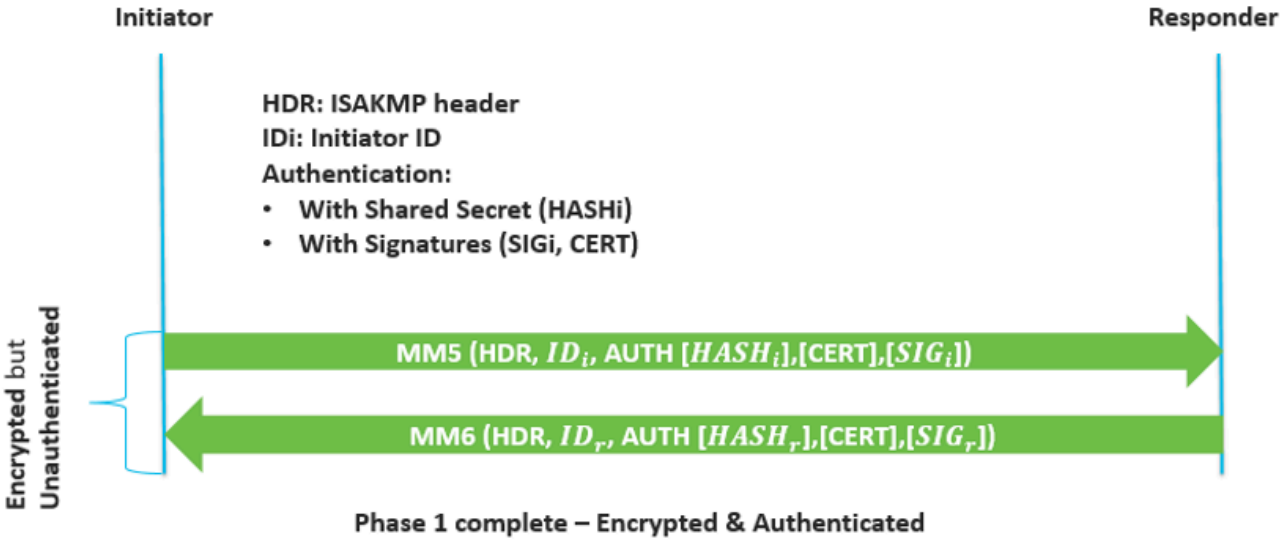
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

主模式3和4 (MM3-MM4)

MM3和MM4資料包仍然未加密且未經身份驗證，並且發生金鑰交換。MM3和MM4如下圖所示：

主模式5和6 (MM5-MM6)

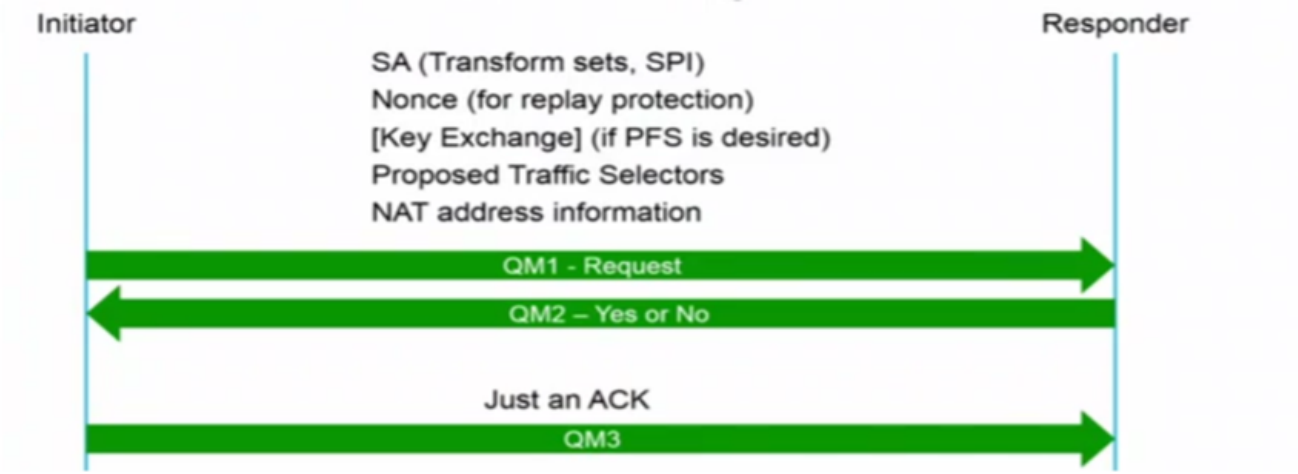
MM5和MM6資料包已加密，但仍未經身份驗證。在這些封包上，會進行驗證，如下圖所示：



快速模式（QM1、QM2和QM3）

快速模式發生在主節點和IKE在第1階段建立安全隧道之後。快速模式會針對IPSec安全演算法協商共用IPSec策略，並管理IPSec SA建立的金鑰交換。這些nonce用於生成新的共用金鑰材料，並防止來自生成的偽造SA的重播攻擊。

此階段會交換三個封包，如下圖所示：

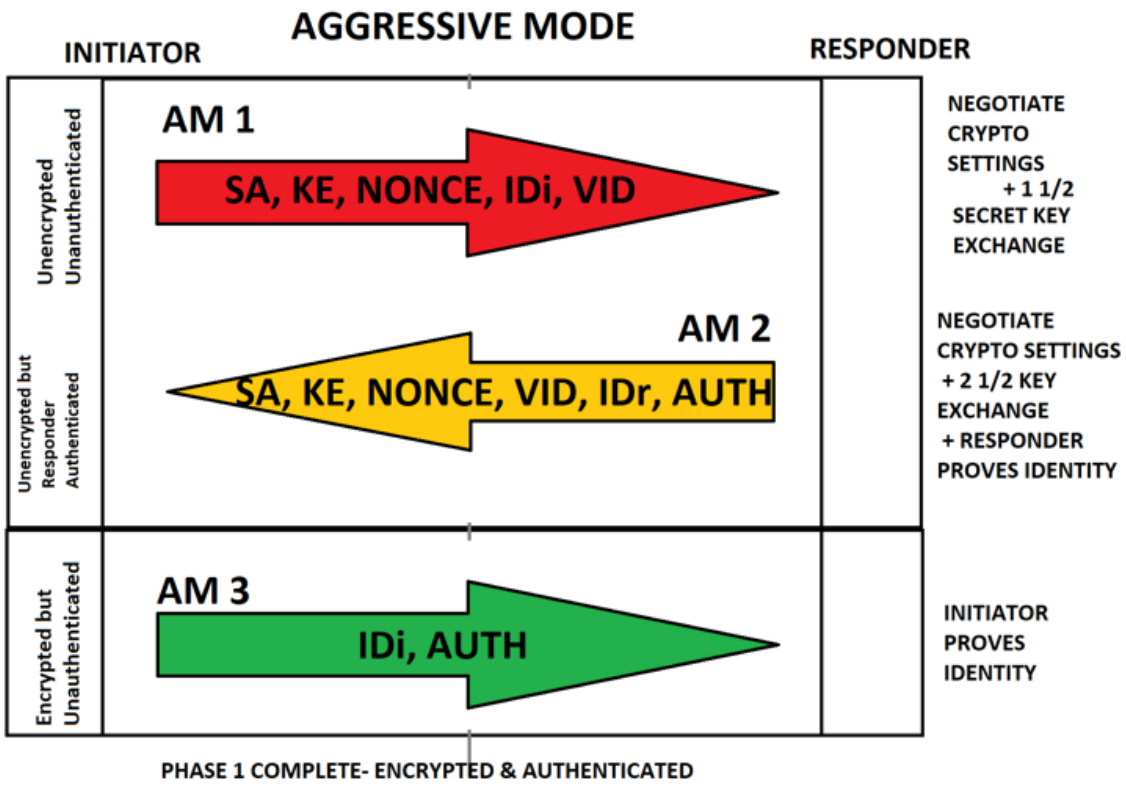


主動模式封包交換

主動模式將IKE SA協商壓縮為三個資料包，SA所需的所有資料由發起方傳遞。

- 響應方傳送建議、金鑰材料和ID，並在下一個資料包中驗證會話。
- 發起方回覆並驗證會話。
- 協商更快，且發起方和響應方ID以明文形式傳遞。

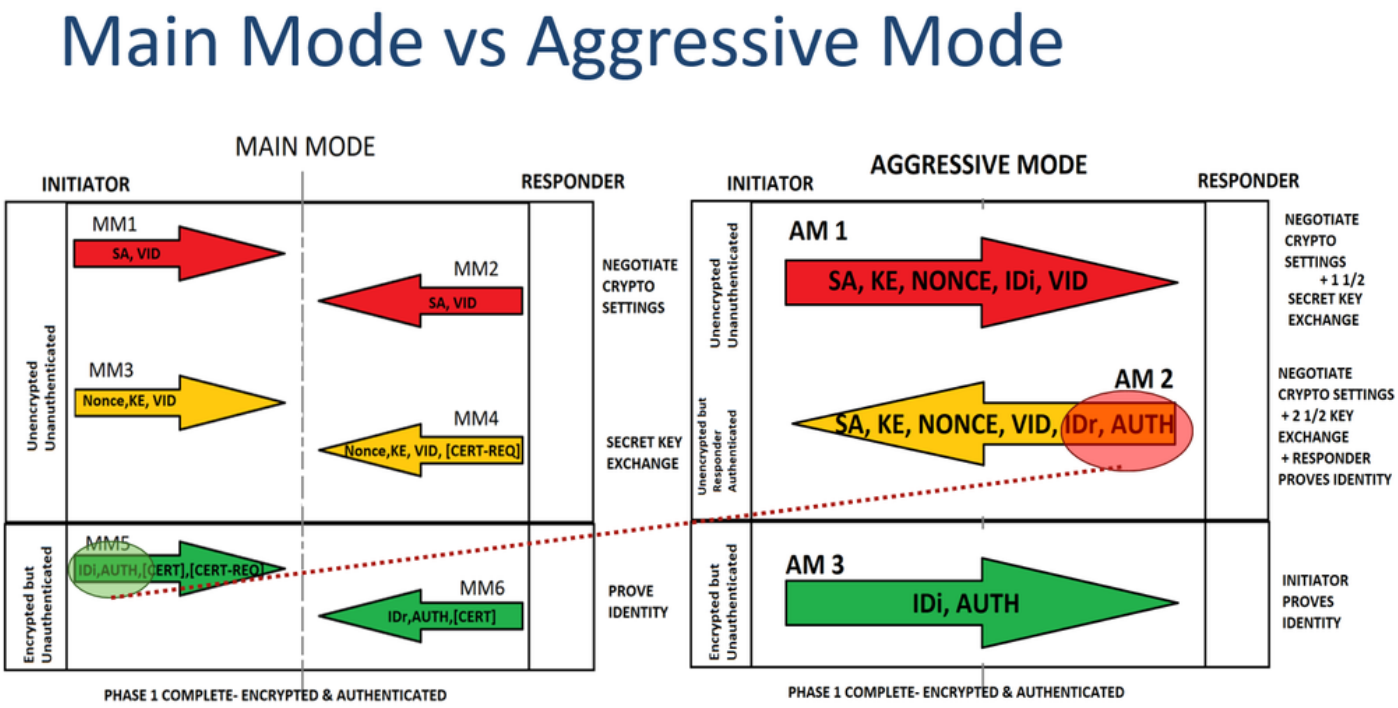
該圖顯示在主動模式下交換的三個資料包的負載內容：



主模式與主動模式

與主模式相比，主動模式可分為三個套件：

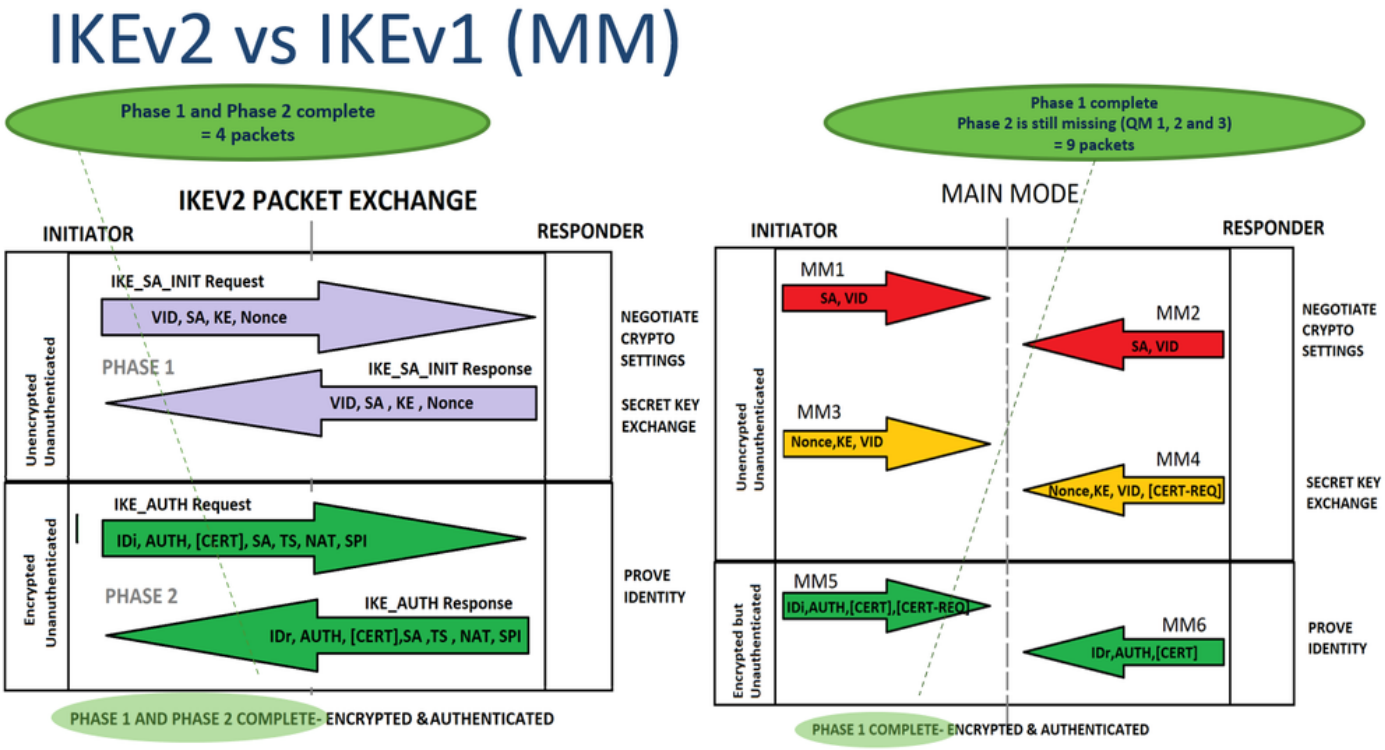
- AM 1吸收MM1和MM3。
- AM 2吸收MM2、MM4和MM6的一部分。攻擊模式漏洞的來源就是此。AM 2組成IDr和身份驗證未加密。與主模式不同，此資訊是加密的。
- AM 3提供ID和身份驗證。這些值已加密。



IKEv2與IKEv1封包交換

在IKEv2協商中，為建立隧道而交換的消息較少。IKEv2使用四條消息；IKEv1使用六條消息（在主模式下）或三條消息（在主動模式下）。

IKEv2消息型別定義為請求和響應對。下圖顯示了IKEv2與IKEv1的資料包比較和負載內容：



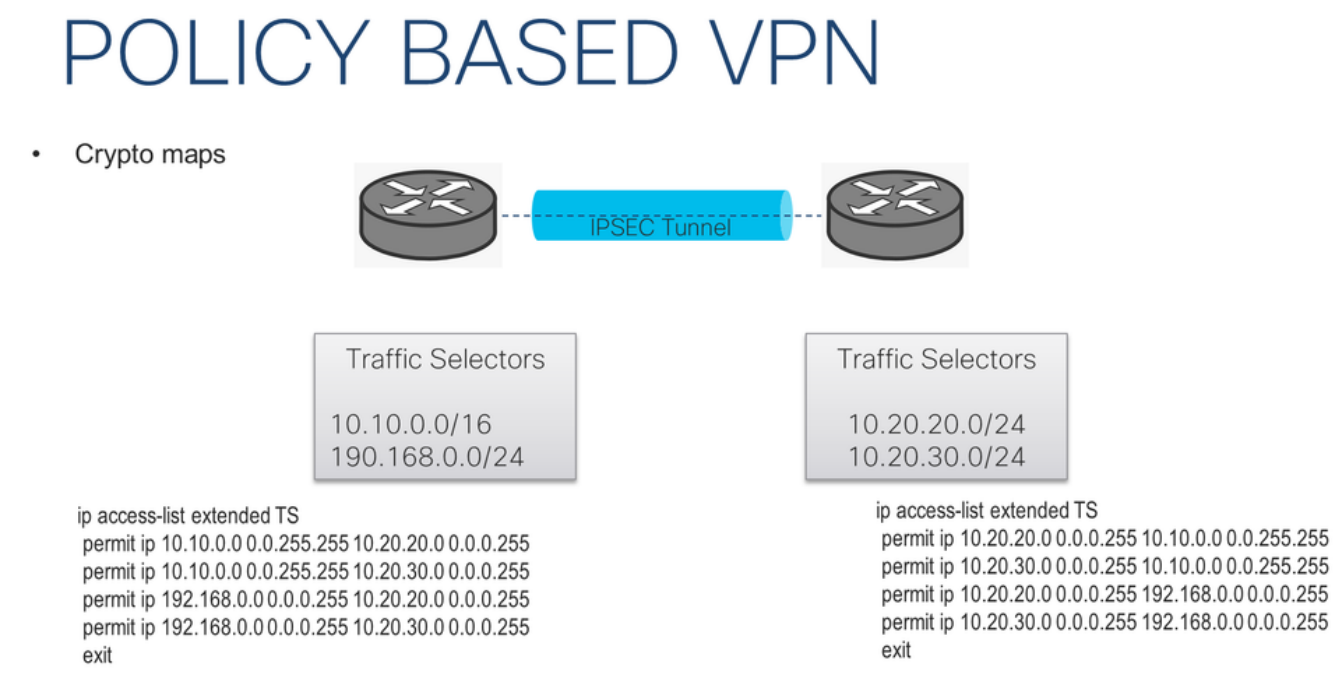
注意：本文檔不深入探討IKEv2資料包交換。有關更多參考，請導航到IKEv2資料包交換和協定級別調試。

基於策略與基於路由

基於策略的VPN

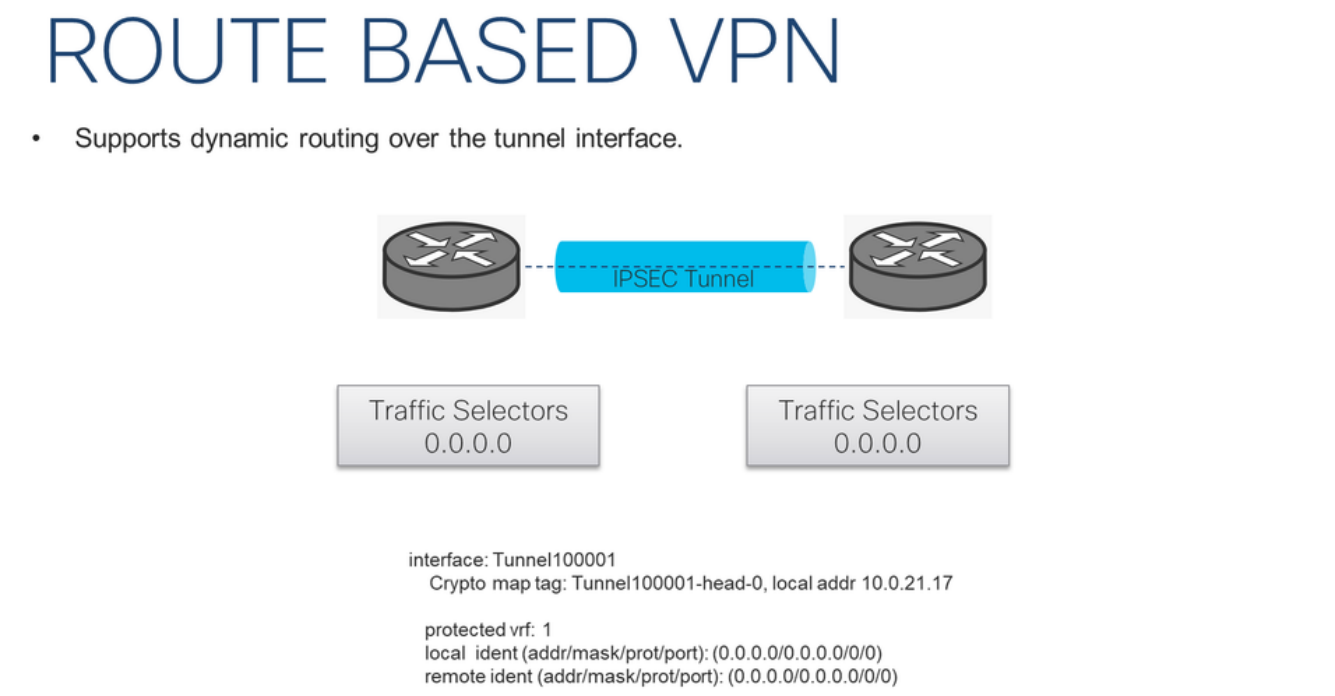
如名稱所述，基於策略的VPN是一條IPsec VPN隧道，其策略操作用於符合策略匹配條件的傳輸流量。就Cisco裝置而言，會設定存取清單(ACL)並將其附加至密碼編譯對應，以指定要重新導向到VPN並加密的流量。

流量選擇器是在策略上指定的子網或主機，如圖所示：



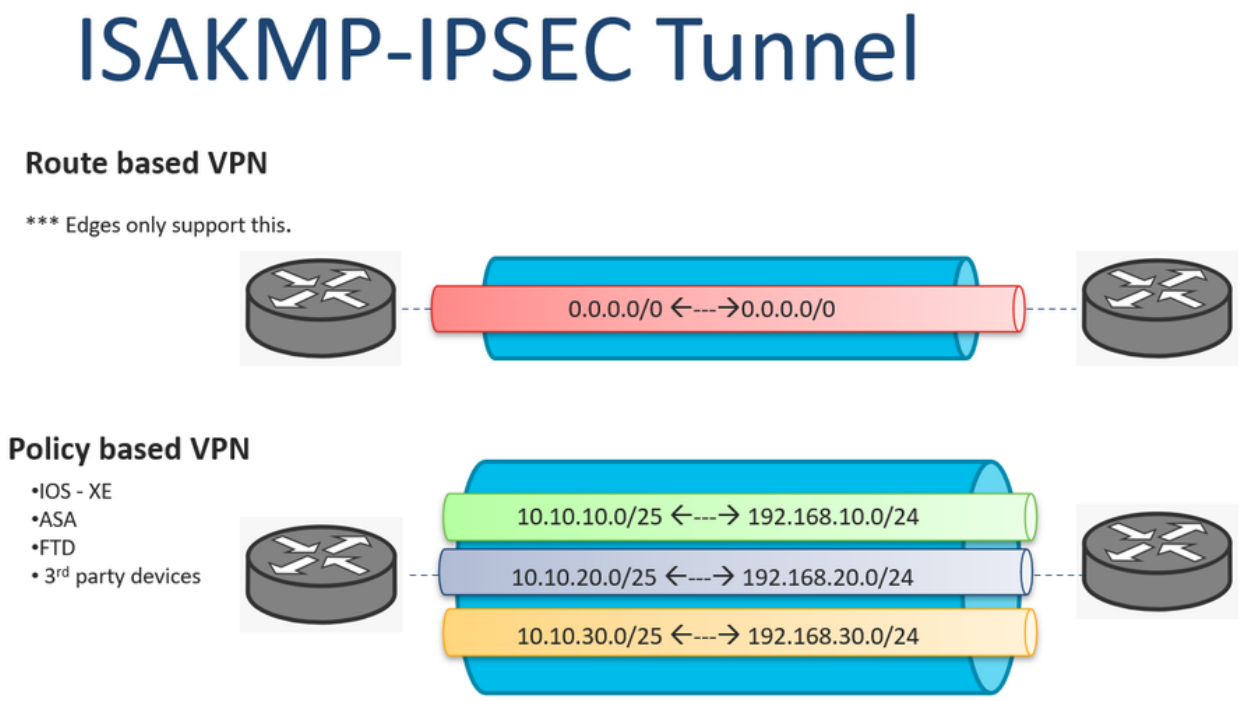
基於路由的VPN

不需要策略。流量被重定向到具有路由的隧道，並支援透過隧道介面進行動態路由。預設情況下，流量選擇器（透過VPN加密的流量）是從0.0.0.0到0.0.0.0，如圖所示：



注意：由於流量選擇器是0.0.0.0，因此中包含任何主機或子網。因此，僅建立一個SA。動態通道有一個例外。本文檔不介紹動態隧道。

策略和基於路由的VPN可以具體化，如圖所示：



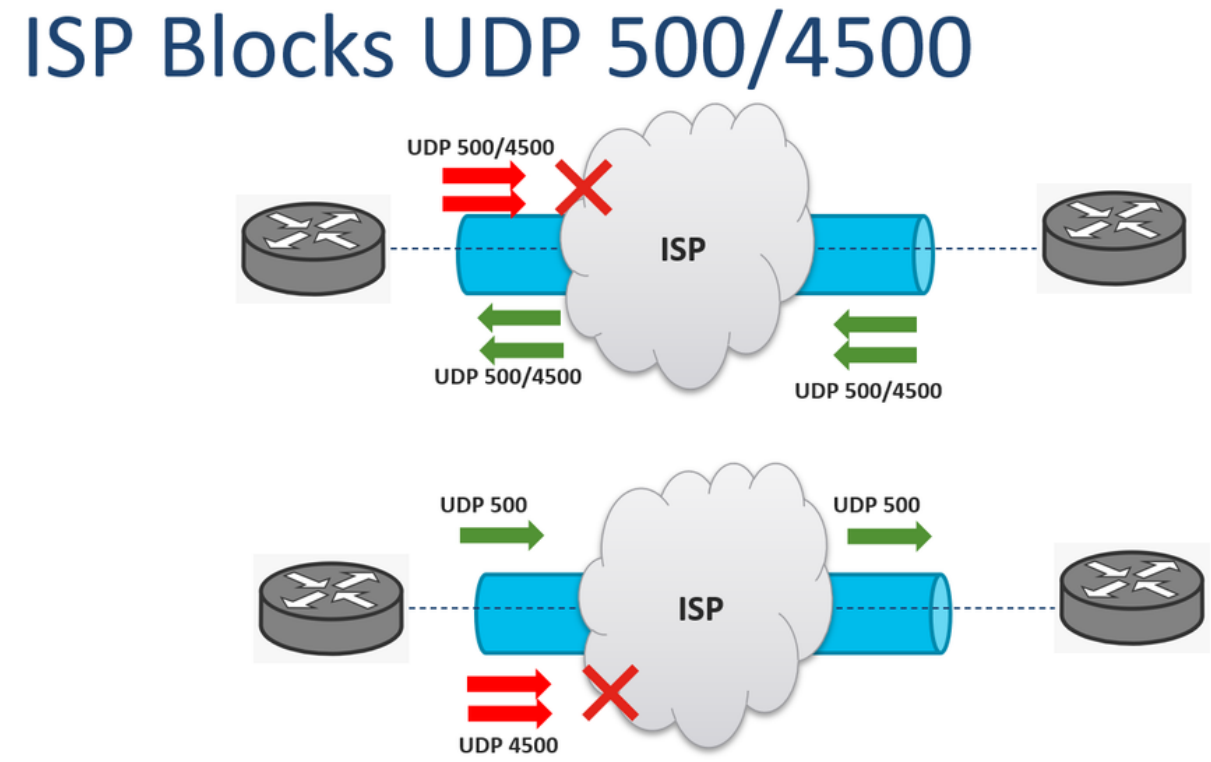
注意：與只建立一個SA的基於路由的VPN不同，基於策略的VPN可以建立多個SA。配置ACL後，ACL上的每條語句（如果它們之間不同）都會建立一個子隧道。

無法通過VPN接收流量的常見問題

ISP阻止UDP 500/4500

網際網路服務提供商(ISP)阻止UDP 500/4500埠是一個非常常見的問題。對於IPSec隧道建立，可以採用兩個不同的ISP。其中一個可以封鎖連線埠，另一個允許使用。

下圖顯示了ISP只能在一個方向上阻止UDP 500/4500埠的兩個場景：

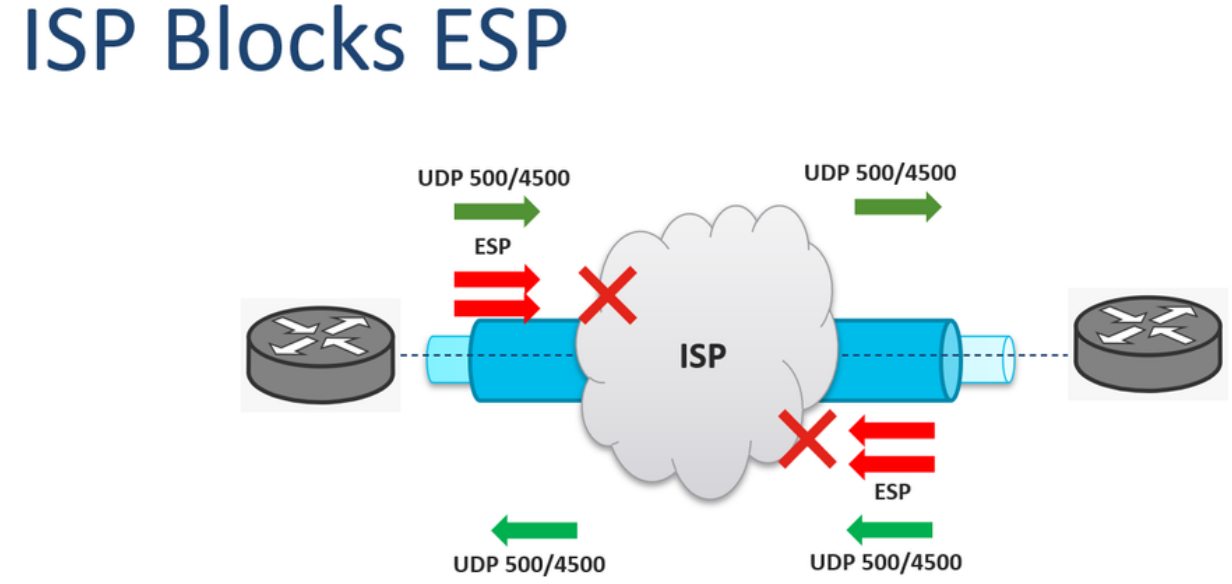


注意：網際網路金鑰交換(IKE)使用埠UDP 500建立安全VPN隧道。當NAT存在於一個VPN端點中時，使用UDP 4500。

注意：當ISP阻止UDP 500/4500時，IPSec隧道建立會受到影響，它不會啟動。

ISP阻止ESP

IPsec隧道的另一個非常常見的問題是ISP阻止ESP流量；但它允許UDP 500/4500埠。例如，允許UDP 500/4500埠採用雙向方式。因此，隧道已成功建立，但ISP或ISP在兩個方向上都阻止了ESP資料包。這會導致透過VPN的加密流量失敗，如圖所示：



注意：當ISP阻止ESP資料包時，IPsec隧道建立成功，但加密的資料流會受到影響。它可以在VPN啟動時反映出來，但流量無法通過該埠工作。

提示：也可能會出現ESP流量僅在一個方向被阻止的情況。症狀相同，但可透過隧道統計資訊、封裝、解封計數器或RX和TX計數器輕鬆找到。

相關資訊

- KEv2資料包交換和協定級調試
- 網際網路金鑰交換(IKE) - RFC 2409
- 網際網路金鑰交換(IKEv2)協定
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。