Informazioni sul protocollo IPsec IKEv1

Sommario

Introduzione

In questo documento viene descritto il processo del protocollo IKEv1 (Internet Key Exchange) per una rete privata virtuale (VPN).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei concetti base relativi alla sicurezza:

- Autenticazione
- Riservatezza
- Integrità
- IPSec

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il processo del protocollo IKEv1 (Internet Key Exchange) per una rete VPN (Virtual Private Network) è importante per comprendere lo scambio di pacchetti e semplificare la risoluzione di qualsiasi problema di IPsec (Internet Protocol Security) con IKEv1.

IPSec

IPsec è una suite di protocolli che fornisce protezione alle comunicazioni Internet a livello IP. Attualmente IPsec viene comunemente utilizzato per fornire una rete VPN (Virtual Private Network) tra due postazioni, ovvero da gateway a gateway, oppure tra un utente remoto e una rete aziendale, ovvero da host a gateway.

Protocollo IKE

IPsec utilizza il protocollo IKE per negoziare e stabilire tunnel VPN (Virtual Private Network) ad accesso remoto o da sito a sito protetti. Il protocollo IKE è noto anche come ISAKMP (Internet Security Association and Key Management Protocol) (solo in Cisco).

IKE è disponibile in due versioni:

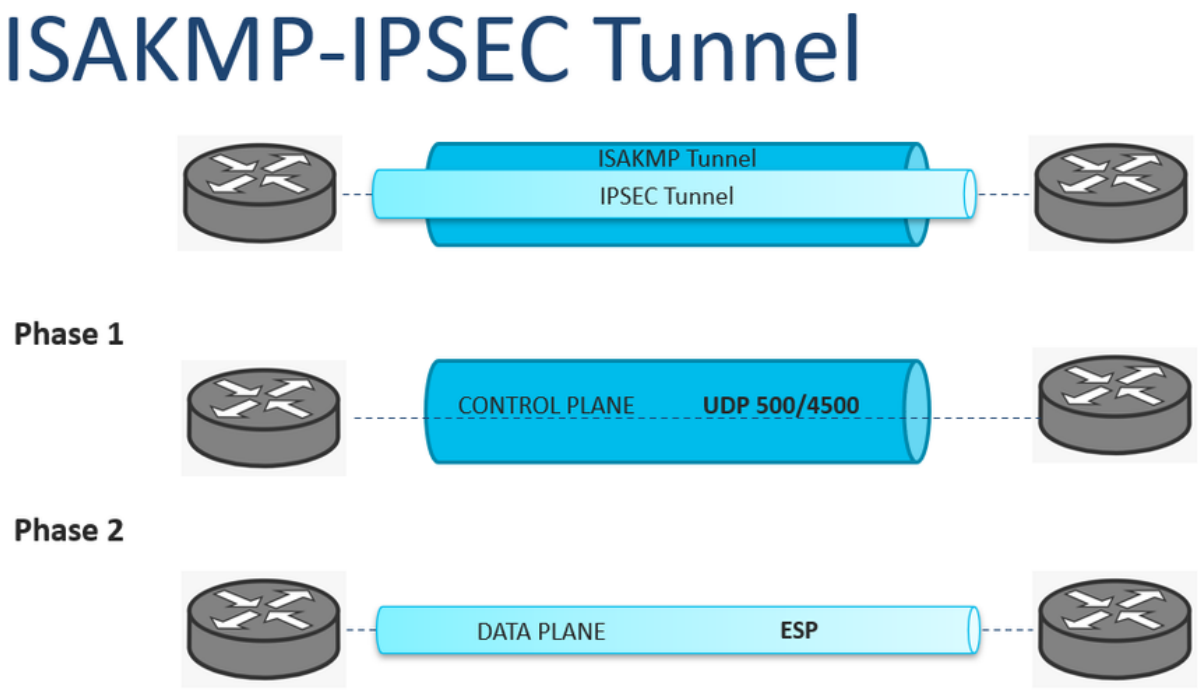
- IKEv1: definito nella RFC 2409, The Internet Key Exchange
- IKE versione 2 (IKEv2): definito nella RFC 4306, Internet Key Exchange (IKEv2) Protocol

Fasi IKE

ISAKMP separa la negoziazione in due fasi:

- Fase 1: i due peer ISAKMP stabiliscono un tunnel sicuro e autenticato, che protegge i messaggi di negoziazione ISAKMP. Questo tunnel è noto come SA ISAKMP. ISAKMP definisce due modalità: Modalità principale (MM) e Modalità aggressiva.
- Fase 2: negoziare i materiali e gli algoritmi chiave per la crittografia (SA) dei dati da trasferire sul tunnel IPsec. Questa fase è denominata Modalità rapida.

Per materializzare tutti i concetti astratti, il tunnel della fase 1 è il tunnel padre e la fase 2 è un tunnel secondario. Nell'immagine vengono mostrate le due fasi come tunnel:



Nota: la fase 1 (ISAKMP) del tunnel protegge il traffico VPN Control Plant tra i due gateway. Il traffico Control Plane può essere costituito da pacchetti di negoziazione, pacchetti di informazioni, DPD, keepalive, rekey e così via. La negoziazione ISAKMP utilizza le porte UDP 500 e 4500 per stabilire un canale sicuro.

Nota: il tunnel della fase 2 (IPsec) protegge il traffico del Data Plane che passa attraverso la VPN tra i due gateway. Gli algoritmi utilizzati per proteggere i dati sono configurati nella fase 2 e sono indipendenti da quelli specificati nella fase 1.
Il protocollo usato per incapsulare e crittografare questi pacchetti è Encapsulation Security Payload (ESP).

Modalità IKE (fase 1)

Modalità principale

Una sessione IKE inizia quando il promotore invia una proposta o una proposta al risponditore. Il primo scambio tra i nodi stabilisce i criteri di sicurezza di base; l'iniziatore propone gli algoritmi di crittografia e autenticazione da utilizzare. Il risponditore sceglie la proposta appropriata (supponendo che sia stata scelta una proposta) e la invia al promotore. Lo scambio successivo passa le chiavi pubbliche Diffie-Hellman e altri dati. Tutte le ulteriori negoziazioni vengono crittografate all'interno dell'associazione di sicurezza IKE. Il terzo scambio autentica la sessione ISAKMP. Dopo aver stabilito l'associazione di protezione IKE, ha inizio la negoziazione IPSec (modalità rapida).

Modalità aggressiva

La modalità aggressiva comprime la negoziazione SA IKE in tre pacchetti, con tutti i dati necessari per l'associazione di protezione passati dall'iniziatore. Il responder invia la proposta, il materiale chiave e l'ID e autentica la sessione nel pacchetto successivo. L'iniziatore risponde e autentica la sessione. La negoziazione è più rapida e l'ID dell'iniziatore e del risponditore viene passato in chiaro.

Modalità IPsec (fase 2)

Modalità rapida

La negoziazione IPSec, o modalità rapida, è simile alla negoziazione IKE in modalità aggressiva, ad eccezione della negoziazione, che deve essere protetta all'interno di un'associazione di protezione IKE. La modalità rapida negozia l'associazione di protezione per la crittografia dei dati e gestisce lo scambio di chiavi per tale associazione di protezione IPSec.

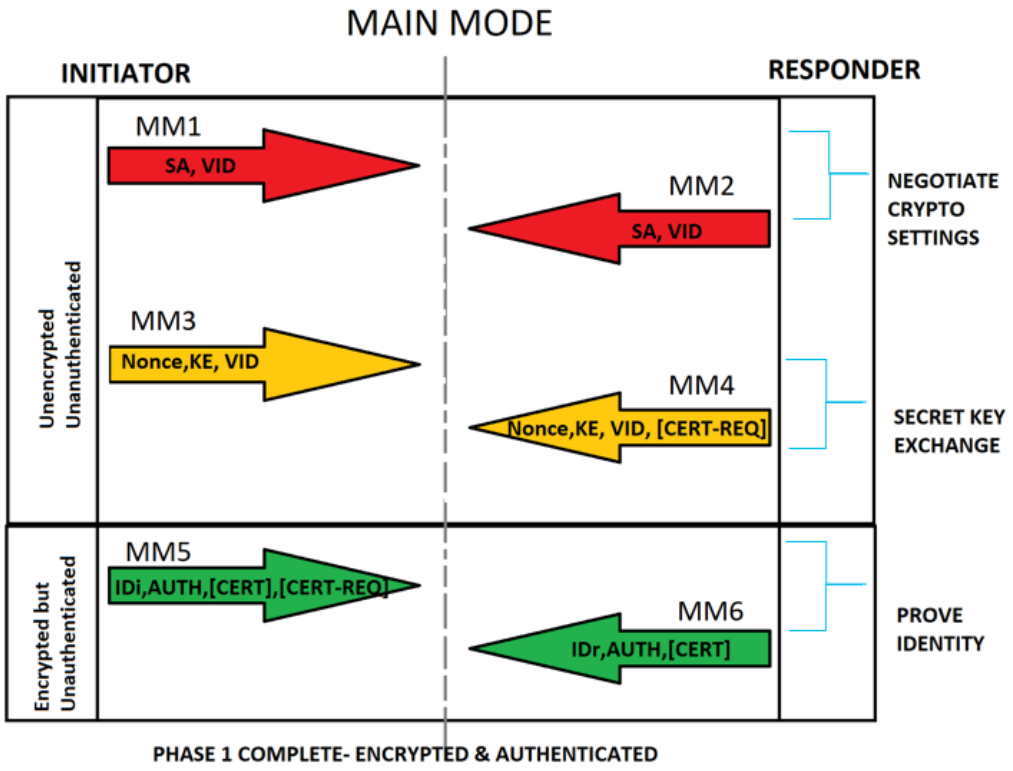
Glossario IKE

- Un'associazione di protezione (SA, Security Association) è la definizione di attributi di protezione condivisi tra due entità di rete per supportare la comunicazione protetta. Un'associazione di protezione include attributi quali l'algoritmo e la modalità di crittografia, la chiave di crittografia del traffico e i parametri per i dati di rete da passare attraverso la connessione.
- Gli ID fornitore (VID) vengono elaborati per determinare se il peer supporta NAT-Traversal, Dead Peer Detection, Fragmentation e così via.
- Nonce: numero generato in modo casuale inviato dall'iniziatore. Questo nonce viene hash insieme agli altri elementi con la chiave concordata utilizzata e viene restituito. L'iniziatore controlla il cookie e il nonce e rifiuta tutti i messaggi che non hanno il nonce corretto. In questo modo è possibile evitare la ripetizione poiché nessuna terza parte è in grado di prevedere il nonce generato in modo casuale.
- Informazioni KE (Key Exchange) per il processo di scambio sicuro delle chiavi Diffie-Hellman (DH).
- Identity Initiator/responder (IDi/IDr.) viene utilizzato per inviare informazioni di autenticazione al peer. Queste informazioni vengono trasmesse sotto la protezione del segreto condiviso comune.

- Lo scambio di chiavi Diffie-Hellman (DH) è un metodo per lo scambio sicuro di algoritmi crittografici su un canale pubblico.
- La chiave condivisa IPSec può essere derivata con il DH utilizzato di nuovo per garantire la funzionalità PFS (Perfect Forward Secrecy) o con lo scambio DH originale aggiornato al segreto condiviso derivato in precedenza.

Modalità principale Packet Exchange

Ogni pacchetto ISAKMP contiene le informazioni sul payload per la definizione del tunnel. Il glossario IKE illustra le abbreviazioni IKE come parte del contenuto del payload per lo scambio di pacchetti in modalità principale, come mostrato nell'immagine.



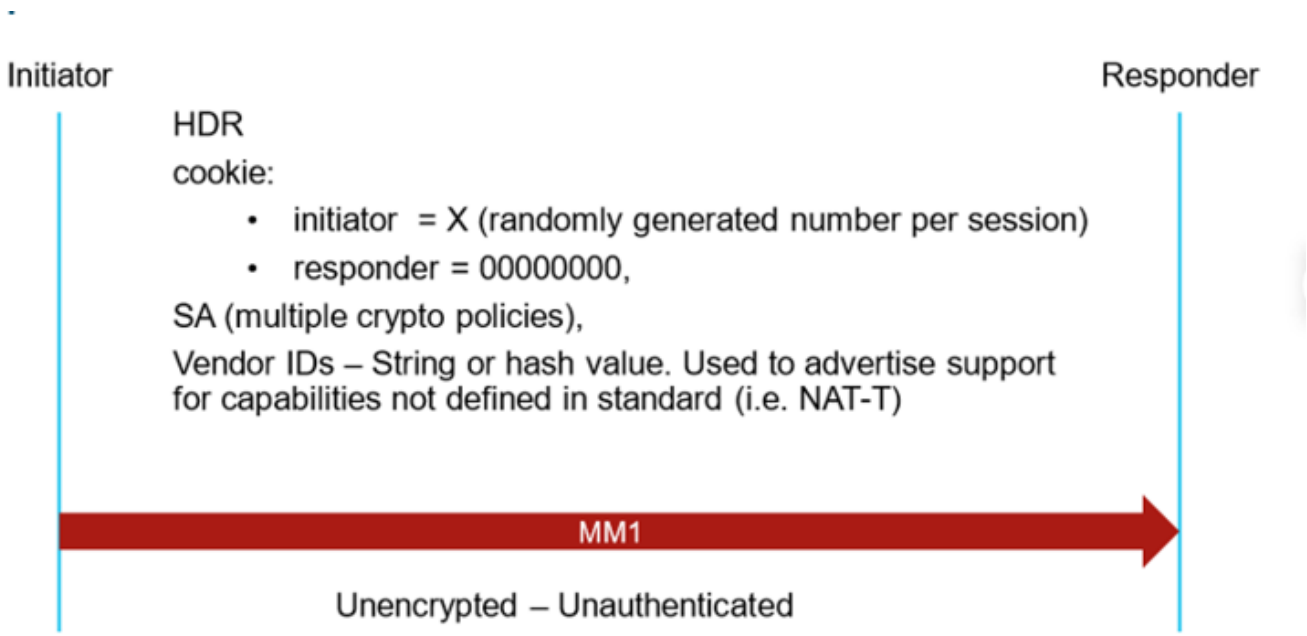
Modalità principale 1 (MM1)

Per impostare i termini delle negoziazioni ISAKMP, creare una policy ISAKMP che include:

- Un metodo di autenticazione per garantire l'identità dei peer.
- Un metodo di crittografia per proteggere i dati e garantire la privacy.
- Un metodo HMAC (Hashed Message Authentication Codes) per garantire l'identità del mittente e che il messaggio non sia stato modificato durante la trasmissione.
- Gruppo Diffie-Hellman per determinare la forza dell'algoritmo di cifratura e determinazione delle chiavi. L'accessorio di protezione utilizza questo algoritmo per derivare le chiavi di crittografia e hash.
- Limitazione del tempo di utilizzo di una chiave di crittografia da parte dell'accessorio di

protezione prima della sostituzione.

Il primo pacchetto viene inviato dall'iniziatore della negoziazione IKE, come mostrato nell'immagine:



Nota: la modalità principale 1 è il primo pacchetto della negoziazione IKE. Pertanto, l'indice SPI iniziatore è impostato su un valore casuale mentre l'indice SPI risponditore è impostato su 0. Nel secondo pacchetto (MM2) è necessario rispondere all'SPI del risponditore con un nuovo valore e l'intera negoziazione mantiene gli stessi valori SPI.

Se si acquisisce MM1 e si utilizza Wireshark Network Protocol Analyzer, il valore SPI è compreso nel contenuto di Internet Security Association e Key Management Protocol, come mostrato nell'immagine:

```
> 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)
```

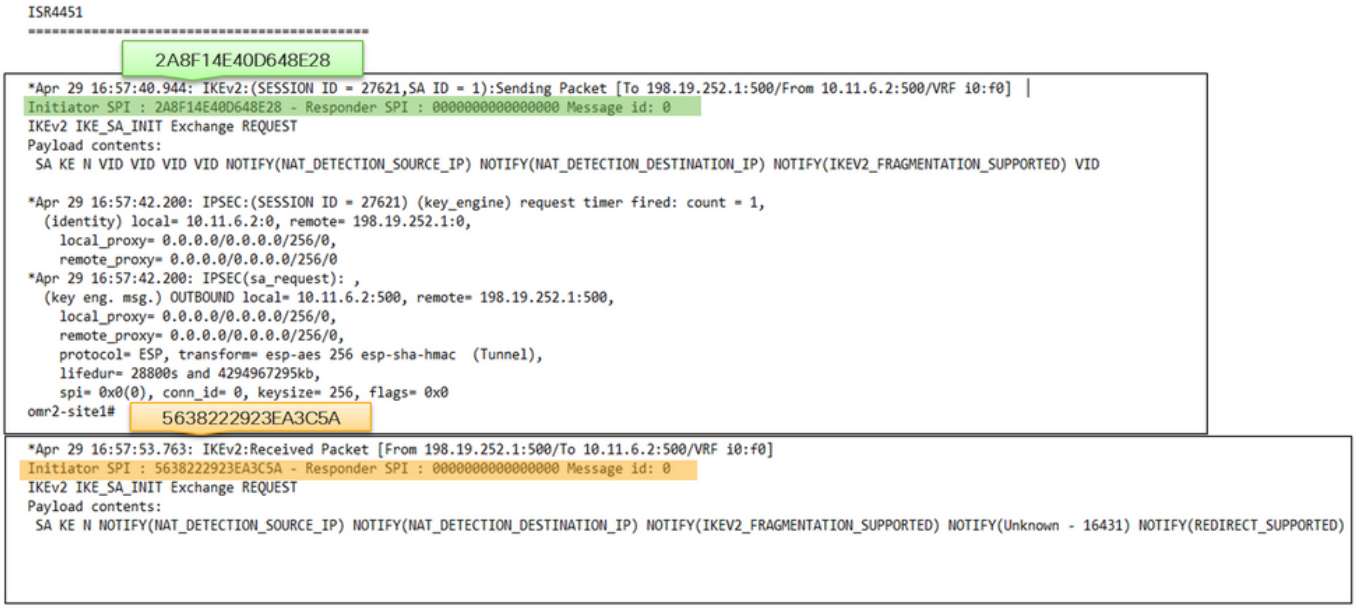
Nota: nel caso in cui il pacchetto MM1 venga perso nel percorso o non vi sia alcuna risposta MM2, la negoziazione IKE mantiene le ritrasmissioni MM1 finché non viene raggiunto il numero massimo di ritrasmissioni. A questo punto, l'iniziatore mantiene lo stesso SPI fino a quando non viene attivata di nuovo la negoziazione successiva.

Suggerimento: l'identificazione degli SPI dell'iniziatore e del risponditore è molto utile per

identificare più negoziazioni per la stessa VPN e restringere alcuni problemi di negoziazione.

Identificare due negoziazioni simultanee

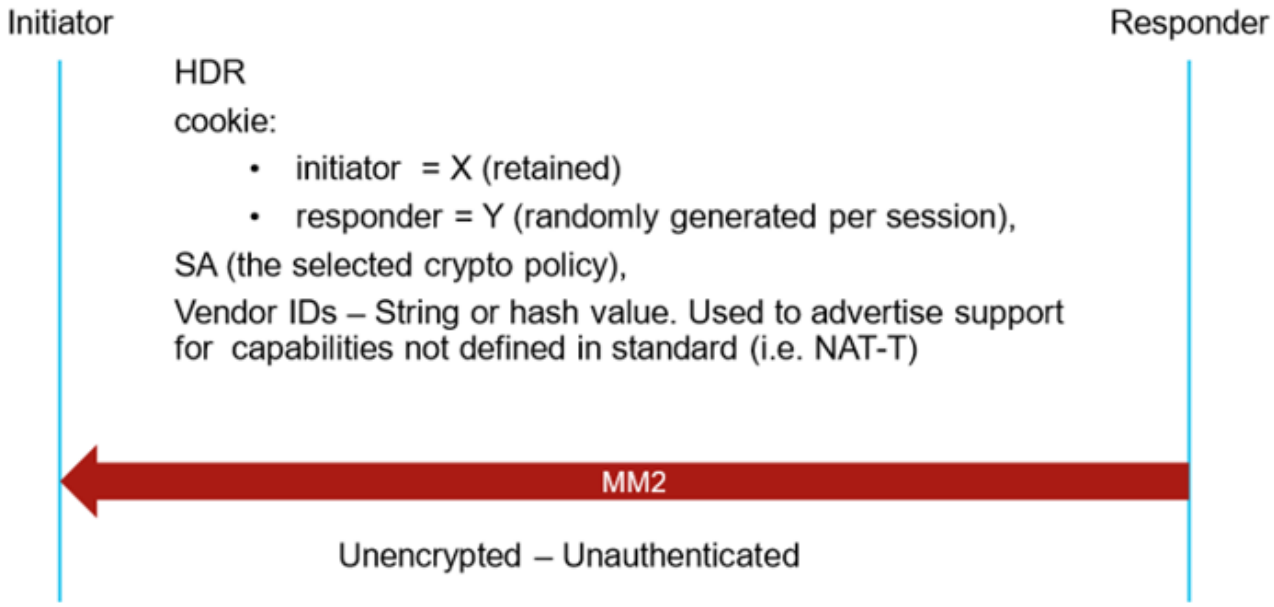
Sulle piattaforme Cisco IOS® XE, i debug possono essere filtrati per tunnel con una condizione per l'indirizzo IP remoto configurato. Le negoziazioni simultanee vengono tuttavia visualizzate nei registri e non è possibile filtrarle. È necessario farlo manualmente. Come accennato in precedenza, l'intera negoziazione mantiene gli stessi valori SPI per Iniziatore e Risponditore. Se un pacchetto viene ricevuto dallo stesso indirizzo IP peer ma l'SPI non corrisponde al valore precedente rilevato prima che la negoziazione raggiunga il numero massimo di ritrasmissioni, si tratta di un'altra negoziazione per lo stesso peer come mostrato nell'immagine:



Nota: nell'esempio viene mostrata la negoziazione simultanea per il primo pacchetto della negoziazione (MM1). Tuttavia, ciò può avvenire in qualsiasi momento della negoziazione. Tutti i pacchetti successivi devono includere un valore diverso da 0 in SPI risponditore.

Modalità principale 2 (MM2)

Nel pacchetto della modalità principale 2, il risponditore invia il criterio selezionato per le proposte con corrispondenza e l'indice SPI del risponditore viene impostato su un valore casuale. L'intera negoziazione mantiene gli stessi valori SPI. L'MM2 risponde a MM1 e il risponditore SPI è impostato su un valore diverso da 0, come mostrato nell'immagine:



Se si acquisisce MM2 e si utilizza Wireshark Network Protocol Analyzer, i valori SPI Initiator e SPI Responder si trovano all'interno del contenuto di Internet Security Association e Key Management Protocol, come mostrato nell'immagine:

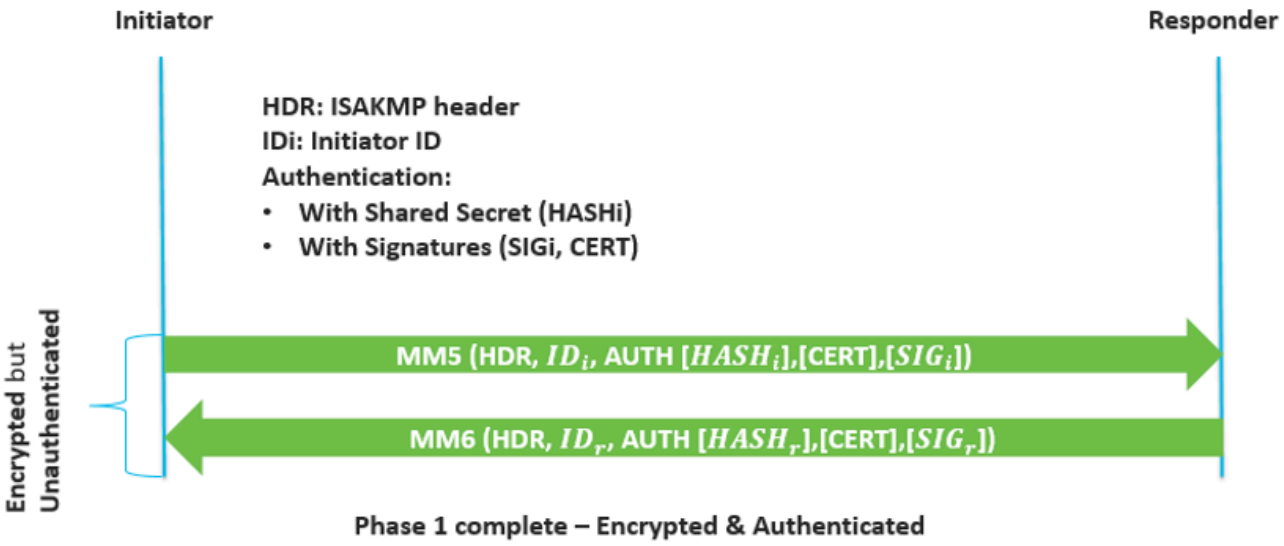
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Modalità principale 3 e 4 (MM3-MM4)

I pacchetti M3 e M4 non sono ancora crittografati e non autenticati e viene eseguito lo scambio di chiave segreta. I formati MM3 e MM4 sono mostrati nell'immagine:

Modalità principale 5 e 6 (MM5-MM6)

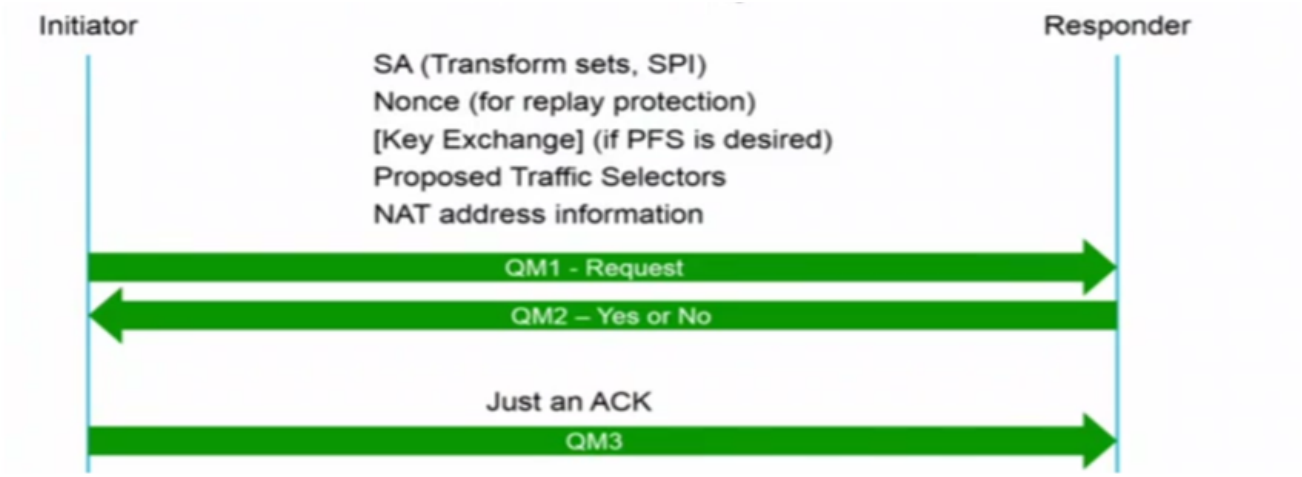
I pacchetti MM5 e MM6 sono già crittografati ma non autenticati. Su questi pacchetti, l'autenticazione ha luogo come mostrato nell'immagine:



Modalità rapida (QM1, QM2 e QM3)

La modalità rapida si verifica dopo che il modem principale e IKE hanno stabilito il tunnel protetto nella fase 1. La modalità rapida consente di negoziare i criteri IPSec condivisi per gli algoritmi di protezione IPSec e di gestire lo scambio di chiavi per la definizione dell'associazione di protezione IPSec. Il nonce viene utilizzato per generare nuovo materiale di chiave segreta condivisa e impedire attacchi di tipo replay da parte di associazioni di protezione false generate.

In questa fase vengono scambiati tre pacchetti, come mostrato nell'immagine:



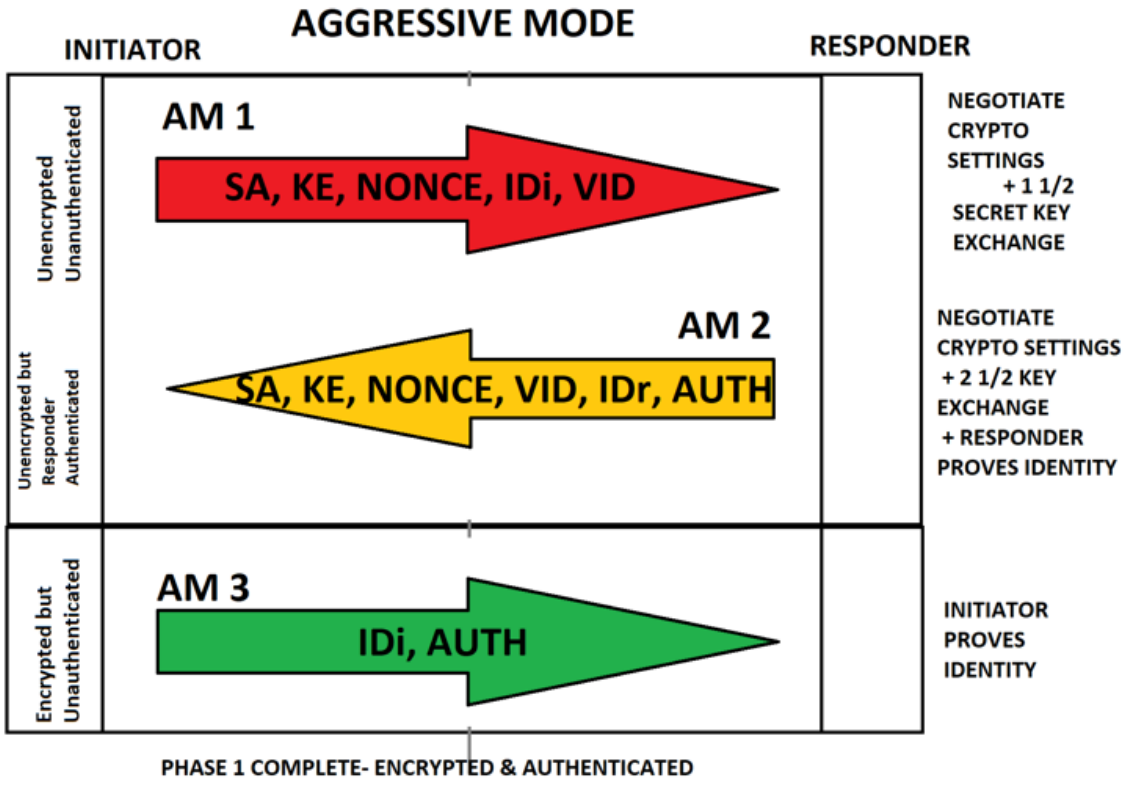
Packet Exchange in modalità aggressiva

La modalità aggressiva comprime la negoziazione SA IKE in tre pacchetti, con tutti i dati richiesti per l'associazione di protezione passati dall'iniziatore.

- Il responder invia la proposta, il materiale chiave e l'ID e autentica la sessione nel pacchetto successivo.
- L'iniziatore risponde e autentica la sessione.

- La negoziazione è più rapida e l'ID dell'iniziatore e del risponditore viene passato in chiaro.

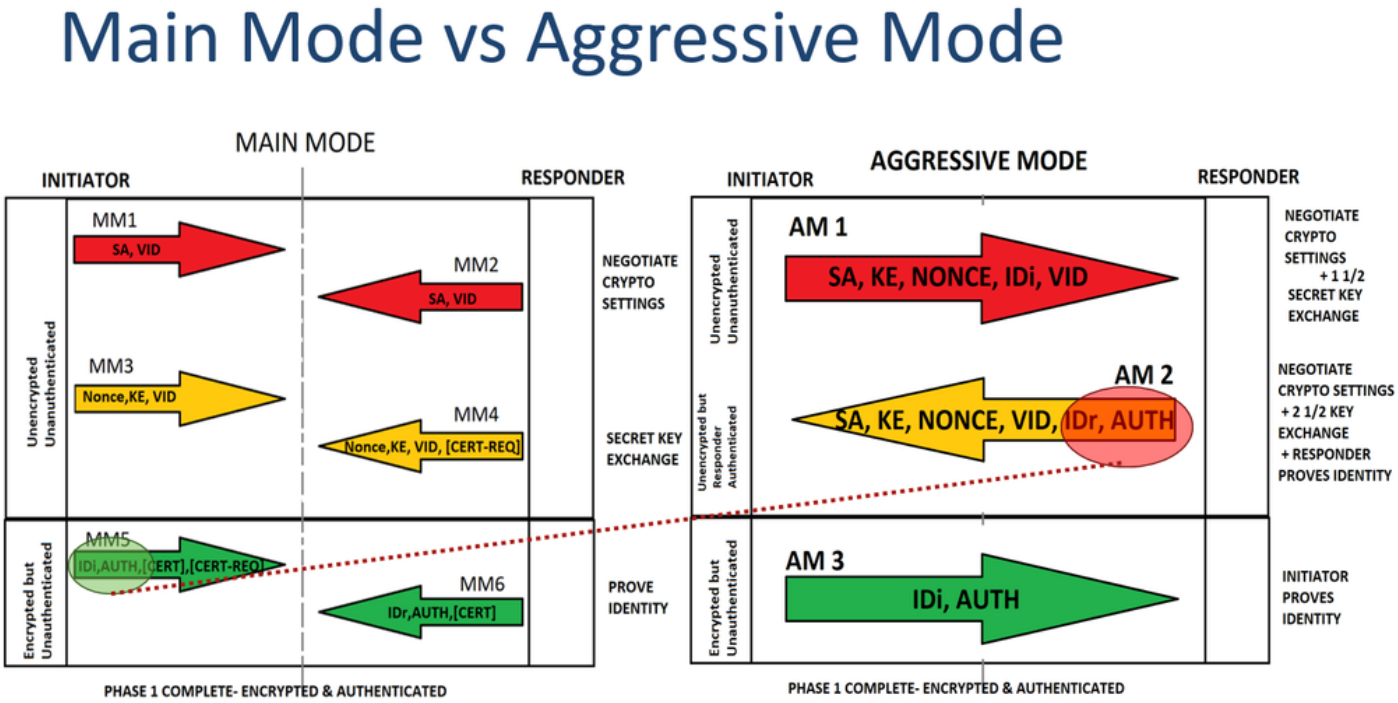
L'immagine mostra il contenuto del payload per i tre pacchetti scambiati in modalità aggressiva:



Modalità principale e modalità aggressiva

Rispetto alla modalità principale, la modalità aggressiva si riduce a tre pacchetti:

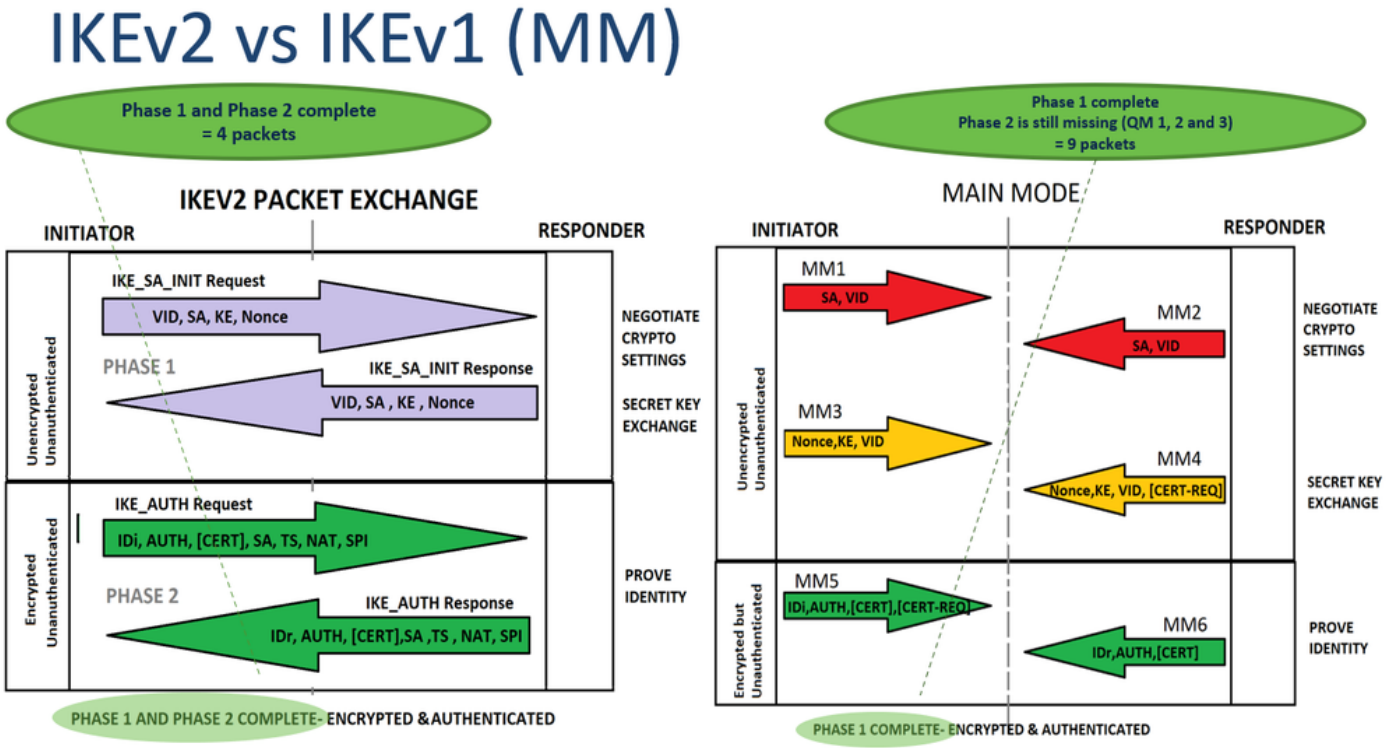
- AM 1 assorbe MM1 e MM3.
- AM 2 assorbe MM2, MM4 e parte di MM6. Da qui deriva la vulnerabilità della Modalità Aggressiva. La versione AM 2 comprende IDr. e Authentication unencrypted. A differenza della modalità principale, queste informazioni sono crittografate.
- AM 3 fornisce l'IDi e l'autenticazione. Tali valori sono crittografati.



Confronto tra IKEv2 e IKEv1 Package Exchange

Nella negoziazione IKEv2, viene scambiato un numero inferiore di messaggi per stabilire un tunnel. IKEv2 utilizza quattro messaggi; IKEv1 utilizza sei messaggi (nella modalità principale) o tre messaggi (in modalità aggressiva).

I tipi di messaggi IKEv2 sono definiti come coppie Richiesta e Risposta. Nell'immagine viene mostrato il confronto dei pacchetti e il contenuto del payload di IKEv2 rispetto a IKEv1:



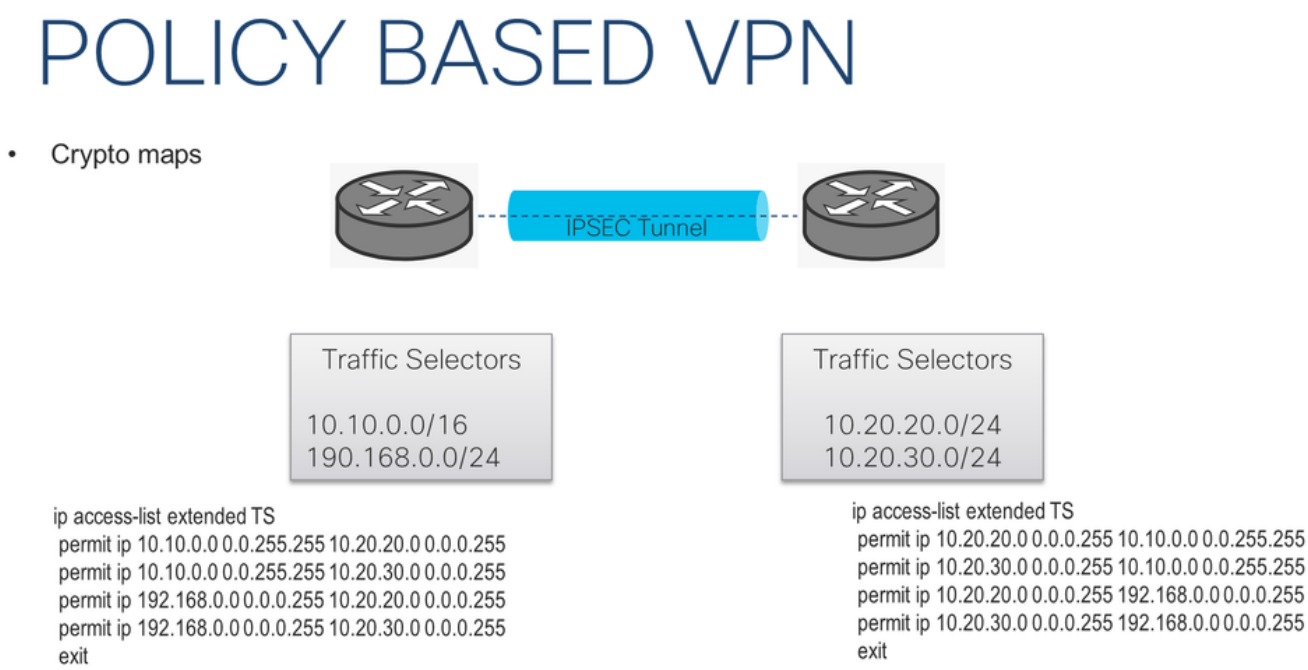
Nota: questo documento non approfondisce la questione dello scambio di pacchetti IKEv2. Per ulteriori riferimenti, passare a Packet Exchange IKEv2 e debug a livello di protocollo.

Basato su regole e basato su route

VPN basata su criteri

Come indica il nome, una VPN basata su criteri è un tunnel VPN IPsec con un'azione criterio per il traffico di transito che soddisfa i criteri di corrispondenza del criterio. Nel caso di dispositivi Cisco, viene configurato un elenco degli accessi (ACL) che viene collegato a una mappa crittografica per specificare il traffico da reindirizzare alla VPN e crittografare.

I selettori di traffico sono le subnet o gli host specificati nel criterio, come mostrato nell'immagine:

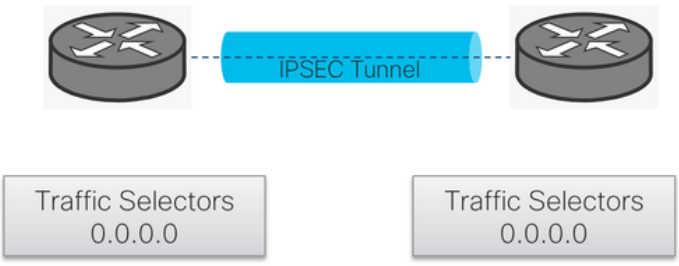


VPN basata su route

Non è necessaria una politica. Il traffico viene reindirizzato ai tunnel con percorsi e supporta il routing dinamico sull'interfaccia del tunnel. I selettori del traffico (traffico crittografato tramite VPN) sono da 0.0.0.0 a 0.0.0.0 per impostazione predefinita, come mostrato nell'immagine:

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.

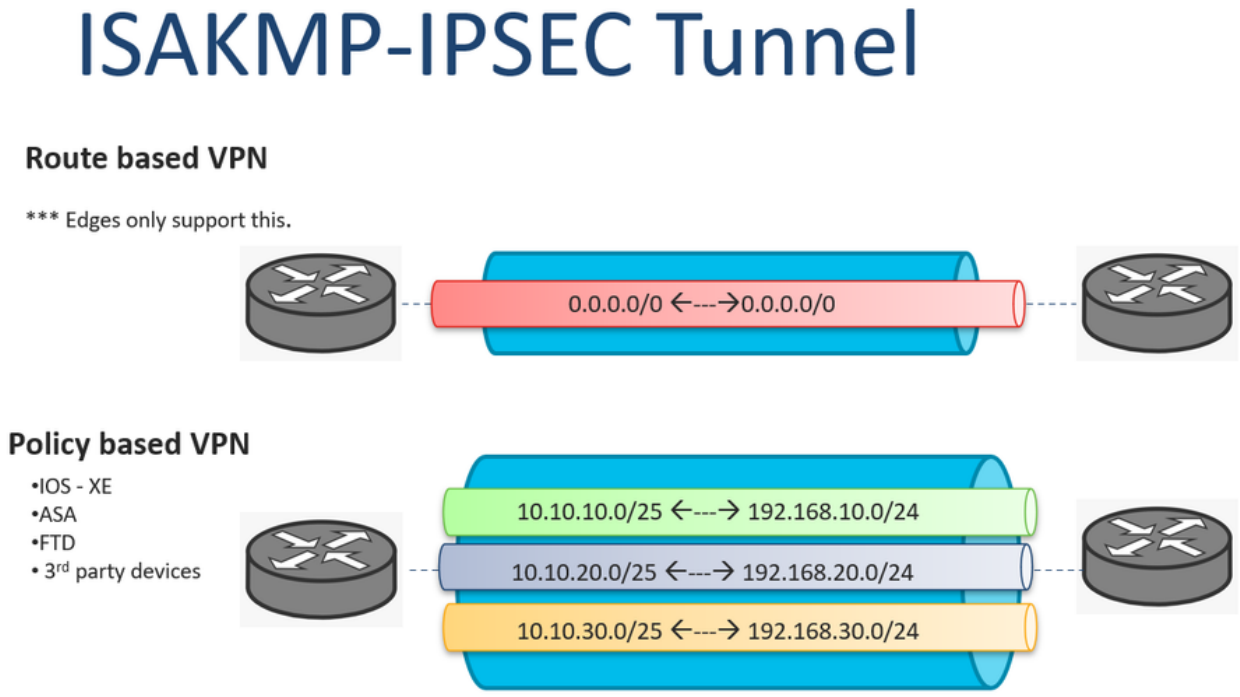



```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  protected vrf:  1
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

Nota: poiché i selettori Traffic sono 0.0.0.0, qualsiasi host o subnet viene incluso in. Viene pertanto creata una sola associazione di protezione. Eccezione per il tunnel dinamico. Questo documento non descrive i tunnel dinamici.

La VPN basata su criteri e route può essere materializzata come mostrato nell'immagine:



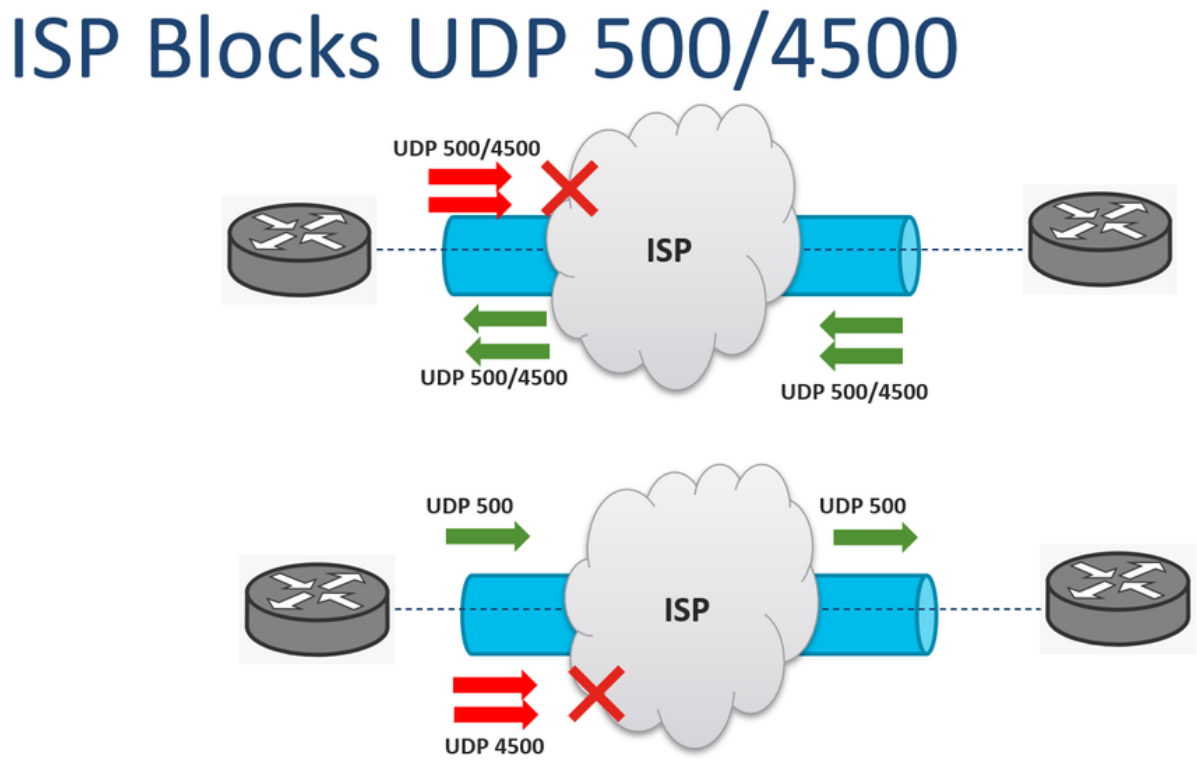
Nota: a differenza della VPN basata su route con una sola SA creata, la VPN basata su criteri può creare più SA. Quando si configura un ACL, ciascuna istruzione sull'ACL (se sono diverse tra loro) crea un sub-tunnel.

I problemi comuni per il traffico non ricevono tramite VPN

ISP blocca UDP 500/4500

È un problema molto comune che il provider di servizi Internet (ISP) blocchi le porte UDP 500/4500. Per stabilire un tunnel IPsec, è possibile utilizzare due diversi ISP. Una può bloccare le porte, l'altra lo consente.

Nell'immagine vengono mostrati due scenari in cui un ISP può bloccare le porte UDP 500/4500 in una sola direzione:

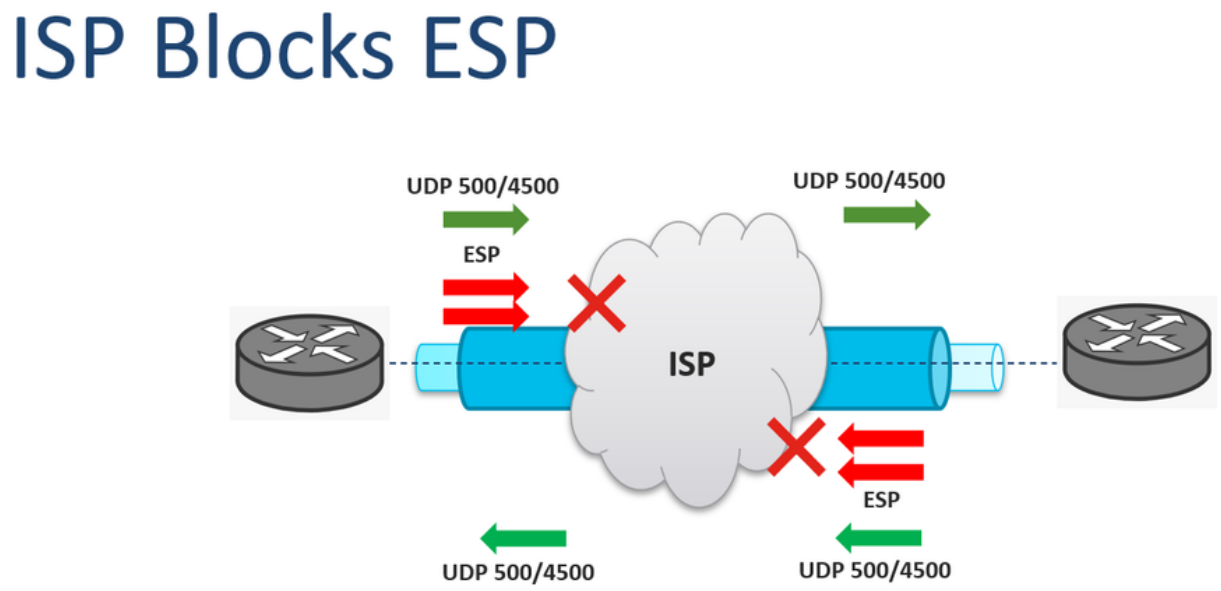


Nota: la porta UDP 500 viene utilizzata dall'IKE (Internet Key Exchange) per la creazione di tunnel VPN sicuri. UDP 4500 viene utilizzato quando NAT è presente in un endpoint VPN.

Nota: quando l'ISP blocca UDP 500/4500, la configurazione del tunnel IPsec viene compromessa e non si riattiva.

ISP Blocks ESP

Un altro problema molto comune sui tunnel IPsec è che l'ISP blocca il traffico ESP; tuttavia, permette le porte UDP 500/4500. Ad esempio, le porte UDP 500/4500 sono consentite in modo bidirezionale. Pertanto, il tunnel è stato stabilito correttamente, ma i pacchetti ESP sono bloccati dall'ISP o dagli ISP in entrambe le direzioni. In questo modo, il traffico crittografato attraverso la VPN non riesce, come mostrato nell'immagine:



Nota: quando l'ISP blocca i pacchetti ESP, il tunnel IPSec viene stabilito correttamente, ma il traffico crittografato viene influenzato. Può essere riflessa con la VPN attiva, ma il traffico non vi funziona sopra.

Suggerimento: può essere presente anche lo scenario in cui il traffico ESP viene bloccato solo in una direzione. I sintomi sono gli stessi, ma è possibile trovarli facilmente con le informazioni statistiche del tunnel, i contatori di incapsulamento e decapsulamento o i contatori RX e TX.

Informazioni correlate

- Debug a livello di protocollo e scambio pacchetti KEv2
- IKE (Internet Key Exchange) - RFC 2409
- Protocollo IKEv2 (Internet Key Exchange)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).