# Debug a livello di protocollo e scambio pacchetti IKEv2

## Sommario



## Introduzione

In questo documento vengono descritti i vantaggi dell'ultima versione di Internet Key Exchange (IKE) e le differenze tra la versione 1 e la versione 2.

IKE è il protocollo utilizzato per configurare un'associazione di sicurezza (SA, Security Association) nella suite di protocolli IPsec. IKEv2 è la seconda e ultima versione del protocollo IKE. L'adozione di questo protocollo è iniziata nel 2006. La necessità e l'intento di una revisione del protocollo IKE è stato descritto nell'Appendice A del *protocollo IKEv2 (Internet Key Exchange)* nella RFC 4306.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

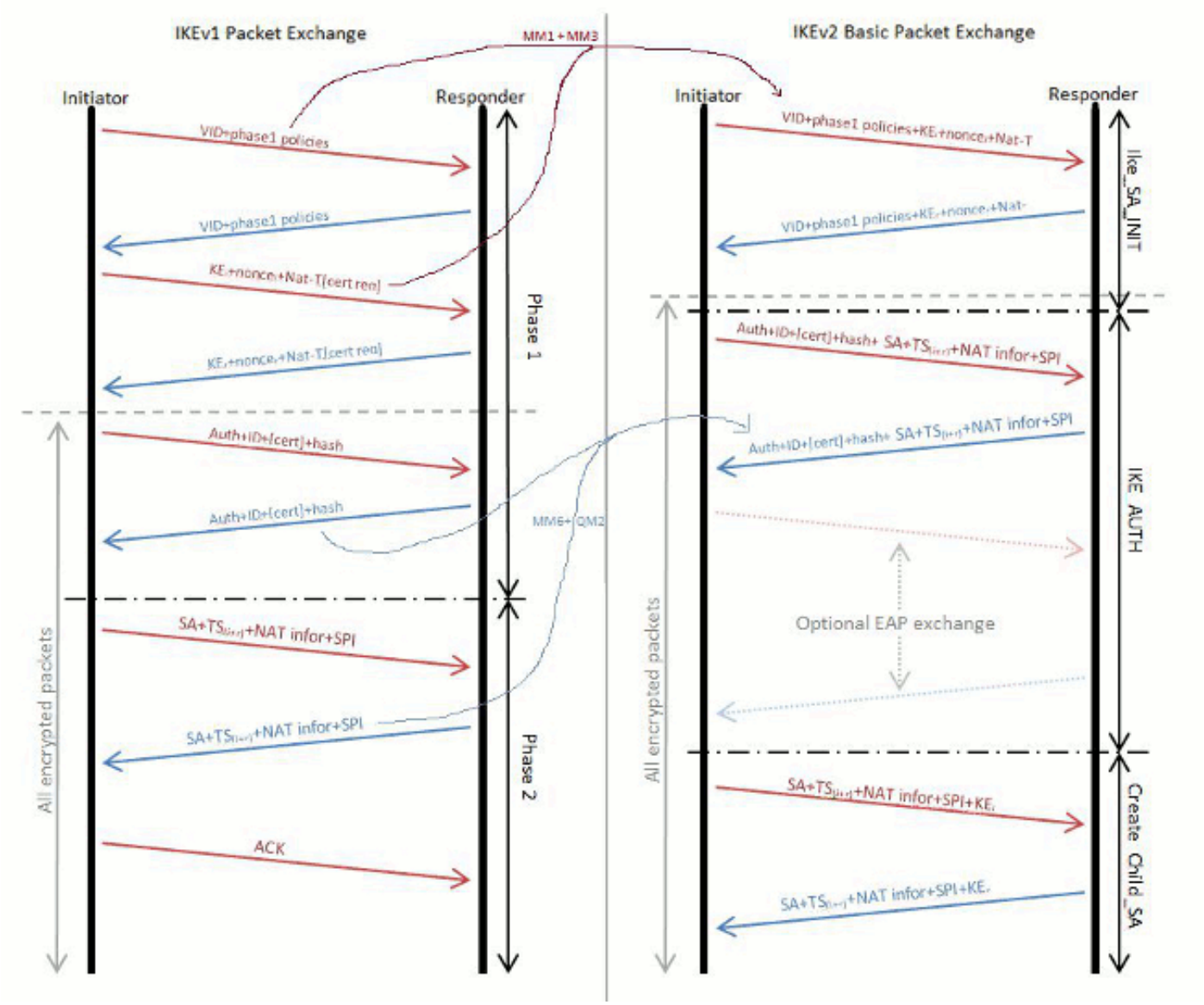
Il documento può essere consultato per tutte le versioni software o hardware.

### Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

# Differenze tra IKEv1 e IKEv2

Mentre il *protocollo IKEv2 (Internet Key Exchange)* nella RFC 4306 descrive in dettaglio i vantaggi di IKEv2 rispetto a IKEv1, è importante notare che l'intero scambio IKE è stato rivisto. Il diagramma fornisce un confronto dei due scambi:




Nel caso di IKEv1, lo scambio di fase 1 è stato chiaramente delimitato e contiene sei pacchetti, seguiti da uno scambio di fase 2 e composto da tre pacchetti; lo scambio IKEv2 è variabile. Nel migliore dei casi, può scambiare solo quattro pacchetti. Nella peggiore delle ipotesi, questo numero può aumentare fino a 30 pacchetti (se non di più), a seconda della complessità dell'autenticazione, del numero di attributi EAP (Extensible Authentication Protocol) utilizzati e del numero di associazioni di protezione formate. IKEv2 combina le informazioni della fase 2 in IKEv1 nello scambio IKE_AUTH e garantisce che, una volta completato lo scambio IKE_AUTH, entrambi i peer dispongano già di un'associazione di protezione e siano pronti a crittografare il traffico. Questa associazione di sicurezza viene creata solo per le identità proxy che corrispondono al pacchetto di trigger. Qualsiasi traffico successivo corrispondente ad altre identità proxy attiva lo scambio CREATE_CHILD_SA, che è l'equivalente dello scambio di fase 2 in IKEv1. Non è disponibile la modalità aggressiva o la modalità principale.

# Fasi iniziali in Exchange IKEv2

In effetti, IKEv2 ha solo due fasi iniziali di negoziazione:

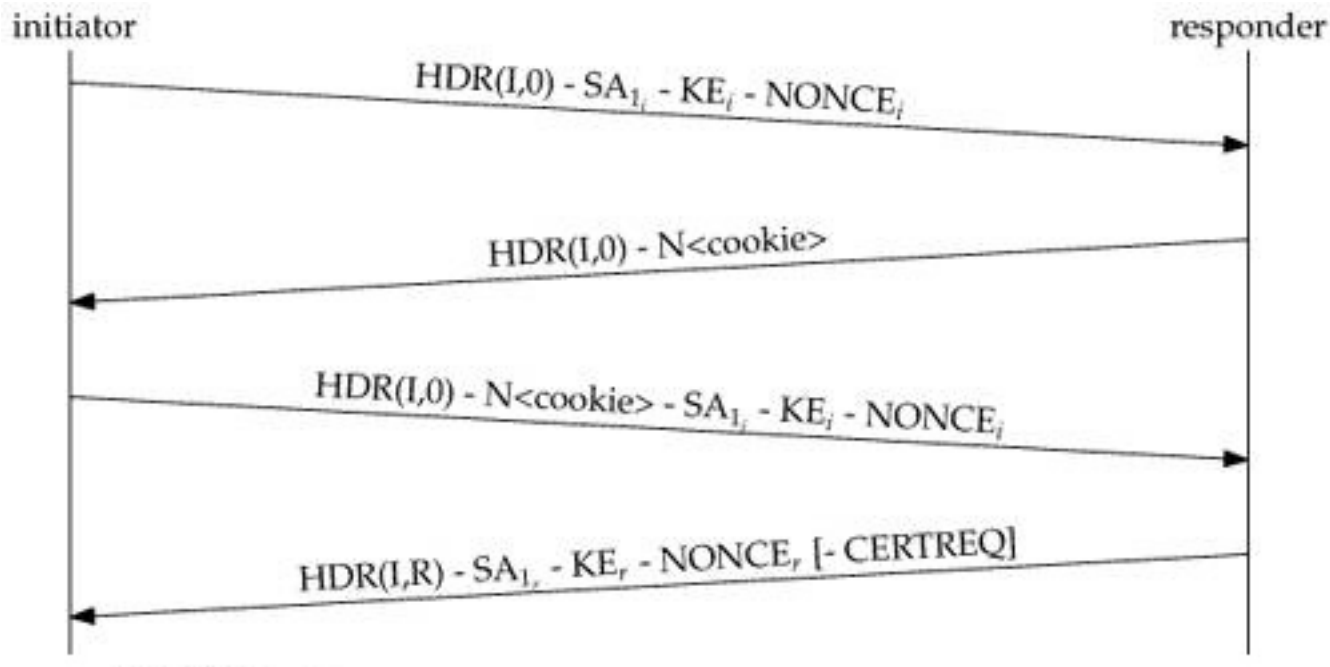
- IKE_SA_INIT Exchange
- Scambio IKE_AUTH

## IKE_SA_INIT Exchange

IKE_SA_INIT è lo scambio iniziale in cui i peer stabiliscono un canale sicuro. Dopo aver completato lo scambio iniziale, tutti gli altri scambi vengono crittografati. Gli scambi contengono solo due pacchetti perché combinano tutte le informazioni scambiate in MM1-4 in IKEv1. Di conseguenza, il responder è dispendioso dal punto di vista del calcolo per elaborare il pacchetto IKE_SA_INIT e può lasciare per elaborare il primo pacchetto; lascia il protocollo aperto a un attacco DOS da indirizzi falsificati.

Per proteggersi da questo tipo di attacchi, IKEv2 dispone di uno scambio opzionale all'interno di IKE_SA_INIT per prevenire attacchi di spoofing. Se viene raggiunta una determinata soglia di sessioni incomplete, il risponditore non elabora ulteriormente il pacchetto, ma invia una risposta all'iniziatore con un cookie. Per continuare la sessione, l'iniziatore deve inviare nuovamente il pacchetto IKE_SA_INIT e includere il cookie ricevuto.

L'iniziatore invia nuovamente il pacchetto iniziale insieme al payload di notifica dal risponditore, a dimostrazione che lo scambio originale non è stato oggetto di spoofing. Di seguito è riportato un diagramma dello scambio di IKE_SA_INIT con la richiesta di verifica dei cookie:




## Scambio IKE_AUTH

Al termine dello scambio IKE_SA_INIT, l'associazione di protezione IKEv2 viene crittografata. tuttavia, il peer remoto non è stato autenticato. Lo scambio IKE_AUTH viene utilizzato per autenticare il peer remoto e creare la prima associazione di protezione IPSec.

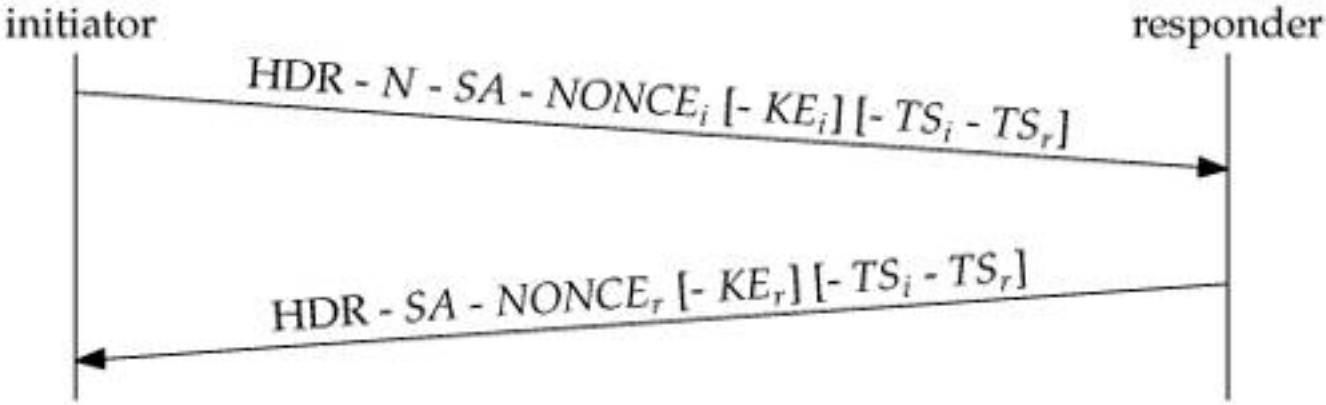
Lo scambio contiene l'ID ISAKMP (Internet Security Association and Key Management Protocol) e un payload di autenticazione. Il contenuto del payload di autenticazione dipende dal metodo di autenticazione, che può essere PSK (Pre-Shared Key), certificati RSA (RSA-SIG), certificati

ECDSA-SIG (Elliptic Curve Digital Signature Algorithm) o EAP. Oltre ai payload di autenticazione, lo scambio include i payload SA e Selettore traffico che descrivono l'associazione di protezione IPsec da creare.

## Scambi IKEv2 successivi

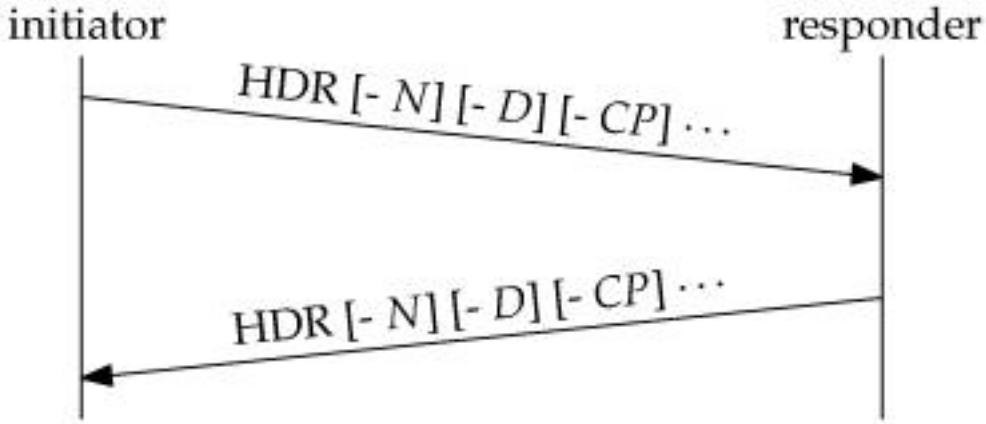
### Scambio CREATE_CHILD_SA

Se sono necessarie associazioni di protezione figlio aggiuntive o se è necessario reimpostare la chiave per l'associazione di protezione IKE o per una delle associazioni di protezione figlio, questa svolge la stessa funzione dello scambio in modalità rapida in IKEv1. Come illustrato nel diagramma, in questo scambio sono presenti solo due pacchetti. tuttavia, lo scambio si ripete per ogni nuova chiave o nuova associazione di protezione:




### SCAMBIO DI INFORMAZIONI

Come avviene in tutti gli scambi IKEv2, ogni richiesta di scambio DI INFORMAZIONI si aspetta una risposta. In uno scambio DI INFORMAZIONI Possono essere inclusi tre tipi di payload. È possibile includere qualsiasi combinazione di payload, come illustrato nel seguente diagramma:




- Il payload della notifica (N) è già stato visualizzato insieme ai cookie. Ci sono anche diversi altri tipi. Contengono informazioni di errore e sullo stato, come in IKEv1.
- Il payload Delete (D) informa il peer che il mittente ha eliminato una o più delle SA in arrivo. È previsto che il risponditore elimini tali associazioni di protezione e in genere includa nel messaggio di risposta i payload di eliminazione per le associazioni di protezione che corrispondono nella direzione opposta.
- Il payload di configurazione (CP) viene utilizzato per negoziare i dati di configurazione tra i

peer. Un utilizzo importante del PC è richiedere (richiedere) e assegnare (rispondere) un indirizzo in una rete protetta da un gateway di sicurezza. In genere, un host mobile stabilisce una rete VPN (Virtual Private Network) con un gateway di sicurezza nella rete domestica e richiede di ricevere un indirizzo IP nella rete domestica.**Nota:** questo elimina uno dei problemi che l'uso combinato del Layer 2 Tunneling Protocol (L2TP) e IPsec è destinato a risolvere.

## Informazioni correlate

- Nota tecnica sui debug ASA IKEv2 per la VPN da sito a sito con PSK
- Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPsec e IKE (modalità principale IKEv1)
- Note tecniche sulla risoluzione dei problemi relativi alla modalità principale IOS IPSec e IKE
- Debug ASA IPSec e IKE - Nota tecnica sulla modalità aggressiva IKEv1
- Cisco ASA serie 5500 Adaptive Security Appliance
- Download di software per appliance Cisco ASA serie 5500 Adaptive Security
- Negoziazione IPSec/protocolli IKE
- Cisco IOS Firewall
- Software Cisco IOS
- SSH (Secure Shell)
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems