Risoluzione dei problemi di debug IOS IKEv2 per la VPN da sito a sito con PSK

Sommario

Introduzione

In questo documento viene descritto il debug di Internet Key Exchange versione 2 (IKEv2) su Cisco IOS® quando si usa una chiave non condivisa (PSK).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dello scambio di pacchetti per IKEv2. Per ulteriori informazioni, fare riferimento a Debug a livello di protocollo e di scambio pacchetti IKEv2.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- IKEv2 (Internet Key Exchange versione 2)
- Cisco IOS 15.1(1)T o versioni successive

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.

Convenzioni

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

Premesse

Questo documento offre informazioni su come tradurre alcune righe di debug in una configurazione.

Problema principale

Lo scambio di pacchetti in IKEv2 è radicalmente diverso dallo scambio di pacchetti in IKEv1. In IKEv1 c'è stato uno scambio fase 1 chiaramente delimitato che consisteva di sei (6) pacchetti con uno scambio fase 2 successivo che consisteva di tre (3) pacchetti; lo scambio IKEv2 è variabile. Per ulteriori informazioni sulle differenze e una spiegazione sullo scambio dei pacchetti, consultare di nuovo Packet Exchange IKEv2 e Debug a livello di protocollo.

Configurazione del router

In questa sezione vengono elencate le configurazioni utilizzate nel documento.

Router 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
```

Router 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
```

Risoluzione dei problemi

Debug del router

Nel presente documento vengono usati i seguenti comandi di debug:

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

Descrizione messaggio router 1 (iniziatore)	Debug	Descrizione messaggio router 2 (risponditore)
Il router 1 riceve un pacchetto che corrisponde all'acl crittografico per l'appliance ASA 10.0.0.2 peer. Avvia la creazione dell'associazione di sicurezza	*11 nov 20:28:34.003: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 20:28:34.003: IKEv2:Elaborazione di un elemento dalla coda pak *11 nov 19:30:34.811: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.2 *11 nov 19:30:34.811: IKEv2:aggiunta della proposta di fase 1 al profilo del kit utensili *11 nov 19:30:34.811: IKEv2:(1): Scelta del profilo IKE IKEV2-SETUP *11 nov 19:30:34.811: IKEv2: nuova richiesta ikev2 sa ammessa *11 nov 19:30:34.811: IKEv2: incremento di un'unità della negoziazione in uscita come conteggio	
La prima coppia di messaggi è lo scambio IKE_SA_INIT. Questi messaggi negoziano algoritmi di	*Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: IDLE Evento: EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento: EV_GET_IKE _CRITERIO *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=00000000000000 (I)	

crittografia, scambiano nonce ed eseguono uno scambio Diffie-Hellman. Configurazione pertinente: `crypto ikev2 proposta PHASE1-prop crittografia 3des aes-cbc-128 integrità sha1 gruppo 2crypto ikev2 keyring peer KEYRNG indirizzo 10.0.0.2 255.255.255.0 hostname1 pre-shared-key local cisco pre-shared-key remote cisco`	MsgID = 0000000 CurState: I_BLD_INIT Event:EV_INIT _CRITERIO *11 nov 19:30:34.811: IKEv2:(ID SA = 1):Impostazione dei criteri configurati *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=00000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento: AUTEV_CHK H4PKI *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=00000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Event:EV_IT TASTO_DH *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento: EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento: EV_OK_RECD DH_PUBKEY_RESP *11 nov 19:30:34.811: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento CONFIG: MOD_G *11 nov 19:30:34.811: iniziatore IKEv2:IKEv2 - nessun dato di configurazione da inviare nello scambio IKE_SA_INIT *11 nov 19:30:34.811: IKEv2:Nessun dato di configurazione da inviare al kit utensili: *Nov 11 19:30:34.811: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MsgID = 0000000 CurState: I_BLD_INIT Evento MSEV_BLD G *11 nov 19:30:34.811: IKEv2: costruzione payload specifico del fornitore: DELETE-REASON *11 nov 19:30:34.811: IKEv2:Costruzione payload specifico del fornitore: (PERSONALIZZATO) *11 nov 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11 nov 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	
Iniziatore che crea il pacchetto IKE_INIT_SA. Contiene: ISAKMP Header (SPI/version/flags),	*Nov 11 19:30:34.811: IKEv2:(ID SA = 1):Payload successivo: SA, versione: 2.0 Tipo di scambio: IKE_SA_INIT, flag: INITIATOR ID messaggio: 0, lunghezza: 344 Contenuto payload: SA Payload successivo: KE, riservato: 0x0, lunghezza: 56	

SAi1 (algoritmo di crittografia supportato dall'iniziatore IKE), KEi (valore DH della chiave pubblica dell'iniziatore) e N (nonce iniziatore).	ultima proposta: 0x0, riservata: 0x0, lunghezza: 52 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 0, #trans: 5 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 1, riservato: 0x0, id: 3DES ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 Payload successivo KE: N, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 N Payload successivo: VID, riservato: 0x0, lunghezza: 24 VID Payload successivo: VID, riservato: 0x0, lunghezza: 23 Payload successivo VID: NOTIFY, riservato: 0x0, lunghezza: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Successivo payload: NOTIFY, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Payload successivo: NONE, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	
—L'iniziatore ha inviato IKE_INIT_SA —>		
	*11 nov 19:30:34.814: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:30:34.814: IKEv2:Elaborazione di un elemento dalla coda pak *11 nov 19:30:34.814: IKEv2: nuova richiesta ikev2 sa ammessa *11 nov. 19:30:34.814: IKEv2: incremento della negoziazione in entrata come conteggio di uno	Il risponditore riceve IKE_INIT_SA.
	*Nov 11 19:30:34.814: IKEv2:Next payload: SA, versione: 2.0 Tipo di scambio: IKE_SA_INIT, flag: INITIATOR ID messaggio: 0, lunghezza: 344 Contenuto payload: Carico utile successivo SA: KE, riservato: 0x0, lunghezza: 56 ultima proposta: 0x0, riservata: 0x0, lunghezza: 52	Il risponditore avvia la creazione dell'associazione di sicurezza per il peer.

	Proposta: 1, ID protocollo: IKE, dimensioni SPI: 0, #trans: 5 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 1, riservato: 0x0, id: 3DES ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 Payload successivo KE: N, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 N Payload successivo: VID, riservato: 0x0, lunghezza: 24 *11 nov 19:30:34.814: IKEv2:Analisi payload specifico del fornitore: CISCO-DELETE-REASON VID Payload successivo: VID, riservato: 0x0, lunghezza: 23 *11 nov 19:30:34.814: IKEv2:Analisi payload specifico del fornitore: (CUSTOM) VID Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 21 *11 nov 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY (NAT_DETECTION_SOURCE_IP) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_SOURCE_IP *11 nov 19:30:34.814: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY (NAT_DETECTION_DESTINATION_IP) Payload successivo: NONE, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_DESTINATION_IP	
	*Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: Evento IDLE:EV_RECV_INIT *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: Evento R_INIT:EV_VERIFY_MSG *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4	Il risponditore verifica ed elabora il messaggio IKE_INIT: (1) sceglie la suite di crittografia da quelle offerte dall'iniziatore, (2) calcola la propria chiave segreta DH

	(R) MsgID = 00000000 CurState: Evento R_INIT:EV_INSERT_SA *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: Evento R_INIT:EV_GET_IKE_POLICY *11 nov 19:30:34.814: IKEv2:aggiunta del valore predefinito della proposta alla policy del kit utensili *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: Evento R_INIT:EV_PROC_MSG *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_INIT: EV_DETECT_NAT *11 nov 19:30:34.814: IKEv2:(ID SA = 1):Notifica rilevamento NAT processo *11 nov 19:30:34.814: IKEv2:(ID SA = 1):Elaborazione della notifica nat detect src *11 nov 19:30:34.814: IKEv2:(ID SA = 1):Indirizzo remoto corrispondente *11 nov. 19:30:34.814: IKEv2:(ID SA = 1):Elaborazione della notifica di rilevamento nat *11 nov 19:30:34.814: IKEv2:(ID SA = 1):Indirizzo locale corrispondente *11 nov 19:30:34.814: IKEv2:(ID SA = 1):No NAT trovato *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Evento R_INIT: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento: EV_SET_POLICY *11 nov 19:30:34.814: IKEv2:(ID SA = 1):Impostazione dei criteri configurati *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento: EV_CHK_AUTH4PKI *Nov 11 19:30:34.814: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento: EV_PKI_SESH_OPEN	e (3) calcola un valore skeyid, dal quale è possibile derivare tutte le chiavi per questa IKE_SA. Tutte le intestazioni dei messaggi successivi, ad eccezione delle intestazioni, vengono crittografate e autenticate. Le chiavi utilizzate per la crittografia e la protezione dell'integrità sono derivate da SKEYID e sono note come: SK_e (crittografia), SK_a (autenticazione), SK_d è derivato e utilizzato per la derivazione di ulteriore materiale per le chiavi per CHILD_SA, mentre SK_e e SK_a separati sono calcolati per ciascuna direzione. Configurazione pertinente: `crypto ikev2 proposta PHASE1-prop crittografia 3des aes-cbc-128 integrità sha1 gruppo 2 crypto ikev2 keyring peer2 indirizzo 10.0.0.1`

	*11 nov 19:30:34.814: IKEv2:(ID SA = 1):Apertura di una sessione PKI *Nov 11 19:30:34.815: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento:EV_GEN_DH_KEY *Nov 11 19:30:34.815: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT *Nov 11 19:30:34.815: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento:EV_OK_RECD_DH_PUBKEY *11 nov 19:30:34.815: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.815: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento:EV_GEN_DH_SECRET *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_NO_EVENT *11 nov 19:30:34.822: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.1 *11 nov 19:30:34.822: IKEv2:aggiunta del valore predefinito della proposta alla policy del kit utensili *11 nov 19:30:34.822: IKEv2:(2): Scelta del profilo IKE IKEV2-SETUP *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:30:34.822: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento:EV_GEN_SKEYID *11 nov 19:30:34.822: IKEv2:(ID SA = 1):Generare skeyid *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: R_BLD_INIT Evento: EV_GET_CONFIG_MODE *11 nov 19:30:34.822: risponditore IKEv2:IKEv2 - nessun dato di configurazione da inviare nello scambio IKE_SA_INIT	255.255.255.0 hostname2 pre-shared-key locale cisco pre-shared-key remoto cisco

	*11 nov 19:30:34.822: IKEv2:Nessun dato di configurazione da inviare al kit utensili: *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_BLD_INIT Evento: EV_BLD_MSG *11 nov 19:30:34.822: IKEv2: costruzione payload specifico del fornitore: DELETE-REASON *11 nov 19:30:34.822: IKEv2:Costruzione payload specifico del fornitore: (PERSONALIZZATO) *11 nov 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *11 nov 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *11 nov 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*11 nov 19:30:34.822: IKEv2:(ID SA = 1):Payload successivo: SA, versione: 2.0 Tipo di scambio: IKE_SA_INIT, flag: RESPONDER MSG-RESPONSE ID messaggio: 0, lunghezza: 449 Contenuto payload: SA Payload successivo: KE, riservato: 0x0, lunghezza: 48 ultima proposta: 0x0, riservata: 0x0, lunghezza: 44 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 0, #trans: 4 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 Payload successivo KE: N, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 N Payload successivo: VID, riservato: 0x0, lunghezza: 24 VID Payload successivo: VID, riservato: 0x0, lunghezza: 23 Payload successivo VID: NOTIFY, riservato: 0x0, lunghezza: 21 NOTIFY(NAT_DETECTION_SOURCE_IP) Successivo payload: NOTIFY, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP) Payload	Il router 2 genera il messaggio del risponditore per lo scambio IKE_SA_INIT, ricevuto da ASA1. Il pacchetto contiene: ISAKMP Header (SPI/versione/flag), SAr1 (algoritmo di crittografia scelto dal risponditore IKE), KEr (valore di chiave pubblica DH del risponditore) e Responder Nonce.

	successivo: CERTREQ, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_DESTINATION_IP Payload successivo CERTREQ: NOTIFY, riservato: 0x0, lunghezza: 105 Hash di codifica del certificato e URL di PKIX NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Payload successivo: NONE, riservato: 0x0, lunghezza: 8 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED		
	*Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 nov 19:30:34.822: IKEv2:(ID SA = 1):Cisco DeleteReason Notify è abilitato *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: INIT_DONE Evento:EV_START_TMR. *Nov 11 19:30:34.822: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: R_WAIT_AUTH Evento: EV_NO_EVENT *11 nov 19:30:34.822: IKEv2:Richiesta nuova ikev2 sa ammessa *11 nov 19:30:34.822: IKEv2:incremento del conteggio SA di negoziazione in uscita di uno		Il router2 invia il messaggio del risponditore al router 1.
<—Il risponditore ha inviato IKE_INIT_SA —			
Il router 1 riceve il pacchetto di risposta IKE_SA_INIT dal router 2.	*11 nov 19:30:34.823: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:30:34.823: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:30:34.823:	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000000 CurState: Init_DONE Evento:EV_START_TMR	Il risponditore avvia il timer per il processo di autenticazione.

	IKEv2:Elaborazione di un elemento dalla coda pak		
Router1 verifica ed elabora la risposta: (1) viene calcolata la chiave segreta DH dell'iniziatore e (2) viene generato anche l'ID utente dell'iniziatore.	*11 nov 19:30:34.823: IKEv2:(ID SA = 1):Payload successivo: SA, versione: 2.0 Tipo di scambio: IKE_SA_INIT, flag: RESPONDER MSG-RESPONSE ID messaggio: 0, lunghezza: 449 Contenuto payload: SA Payload successivo: KE, riservato: 0x0, lunghezza: 48 ultima proposta: 0x0, riservata: 0x0, lunghezza: 44 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 0, #trans: 4 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 Payload successivo KE: N, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 N Payload successivo: VID, riservato: 0x0, lunghezza: 24 *11 nov 19:30:34.823: IKEv2:Analisi payload specifico del fornitore: CISCO-DELETE-REASON VID Payload successivo: VID, riservato: 0x0, lunghezza: 23 *11 nov 19:30:34.823: IKEv2:Analisi payload specifico del fornitore: (CUSTOM) VID Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 21 *11 nov 19:30:34.823: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP NOTIFY (NAT_DETECTION_SOURCE_IP) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_SOURCE_IP *11 nov 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP NOTIFY (NAT_DETECTION_DESTINATION_IP) Payload successivo: CERTREQ, riservato: 0x0, lunghezza: 28 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NAT_DETECTION_DESTINATION_IP		

	Payload successivo CERTREQ: NOTIFY, riservato: 0x0, lunghezza: 105 Hash di codifica del certificato e URL di PKIX *11 nov 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) Payload successivo: NONE, riservato: 0x0, lunghezza: 8 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: HTTP_CERT_LOOKUP_SUPPORTED *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_WAIT_INIT Evento: EV_RECV_INIT *11 nov 19:30:34.824: IKEv2:(ID SA = 1):Elaborazione del messaggio IKE_SA_INIT *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_PROC_INIT Evento: EV_CHK4_NOTIFY *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_PROC_INIT Evento: EV_VERIFY_MSG *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_PROC_INIT Evento: EV_PROC_MSG *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_PROC_INIT Evento: EV_DETECT_NAT *11 nov 19:30:34.824: IKEv2:(ID SA = 1):Notifica rilevamento NAT processo *11 nov 19:30:34.824: IKEv2:(ID SA = 1):Elaborazione della notifica nat detect src *11 nov 19:30:34.824: IKEv2:(ID SA = 1):Indirizzo remoto corrispondente *11 nov. 19:30:34.824: IKEv2:(ID SA = 1):Elaborazione della notifica di rilevamento nat *11 nov 19:30:34.824: IKEv2:(ID SA = 1):Indirizzo locale corrispondente *11 nov 19:30:34.824: IKEv2:(ID SA = 1):No NAT trovato *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4	

	(I) MsgID = 0000000 CurState: I_PROC_INIT Evento: EV_CHK_NAT_T *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: I_PROC_INIT Evento: EV_CHK_CONFIG_MODE *Nov 11 19:30:34.824: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: INIT_DONE Evento:EV_GEN_DH_SECRET *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_NO_EVENT *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:30:34.831: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: INIT_DONE Evento:EV_GEN_SKEYID *11 nov 19:30:34.831: IKEv2:(ID SA = 1):Generare skeyid *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_DONE *11 nov 19:30:34.831: IKEv2:(ID SA = 1):Cisco DeleteReason Notify è abilitato *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000000 CurState: INIT_DONE Evento: EV_CHK4_ROLE *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento: EV_GET_CONFIG_MODE *11 nov 19:30:34.831: IKEv2:Invio dei dati di configurazione al kit utensili *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento: EV_CHK_EAP	

L'iniziatore avvia lo scambio IKE_AUTH e genera il payload di autenticazione. Il pacchetto IKE_AUTH contiene: intestazione ISAKMP (SPI/versione/flag), IDi (identità iniziatore), payload AUTH, SAi2 (avvia l'associazione di protezione simile allo scambio di set di trasformazioni di fase 2 in IKEv1), TSi e TSr (selettori del traffico iniziatore e risponditore). Contengono rispettivamente l'indirizzo di origine e l'indirizzo di destinazione dell'iniziatore e del risponditore per l'inoltro/la ricezione del traffico crittografato. L'intervallo di indirizzi specifica che tutto il traffico da e verso l'intervallo è tunneling. Se la proposta è accettabile per il risponditore, verranno restituiti payload di Servizi terminal identici.	*Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento:EV_GEN_AUTH *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento: EV_CHK_AUTH_TYPE *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento: EV_OK_AUTH_GEN *Nov 11 19:30:34.831: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000000 CurState: I_BLD_AUTH Evento: EV_SEND_AUTH *11 nov 19:30:34.831: IKEv2: costruzione payload specifico del fornitore: CISCO-GRANITE *11 nov 19:30:34.831: IKEv2:Construct Notify Payload: CONTATTO_INIZIALE *11 nov 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11 nov 19:30:34.831: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11 nov 19:30:34.831: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS Contenuto payload: Payload successivo VID: IDi, riservato: 0x0, lunghezza: 20 IDi Payload successivo: AUTH, riservato: 0x0, lunghezza: 12 Tipo di ID: indirizzo IPv4, riservato: 0x0 0x0 AUTH Payload successivo: CFG, riservato: 0x0, lunghezza: 28 Metodo di autenticazione PSK, riservato: 0x0, riservato 0x0 CFG Payload successivo: SA, riservato: 0x0, lunghezza: 309 tipo cfg: CFG_REQUEST, riservato: 0x0, riservato: 0x0 *11 nov 19:30:34.831: SA Payload successivo: TSi, riservato: 0x0, lunghezza: 40 ultima proposta: 0x0, riservata: 0x0, lunghezza: 36 Proposta: 1, ID protocollo: ESP, dimensione SPI: 4, #trans: 3 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 1, riservato: 0x0, id: 3DES ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96	

La prima associazione di sicurezza CHILD_SA viene creata per la coppia proxy_ID che corrisponde al pacchetto di trigger.
 	
Configurazione pertinente: `crypto ipsec transform-set TS esp-3des esp-sha-hmac`
`crypto ipsec profilo phse2-prof`
`set transform-set TS`
`set ikev2-profilo IKEV2-SETUP`
	ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8
	tipo: 5, riservato: 0x0, id: Do not use ESN
	TSi Payload successivo: TSr, riservato: 0x0, lunghezza: 24
	Numero di TS: 1, riservato 0x0, riservato 0x0
	Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
	porta iniziale: 0, porta finale: 65535
	start addr: 0.0.0.0, end addr: 255.255.255.255
	TSr Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 24
	Numero di TS: 1, riservato 0x0, riservato 0x0
	Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
	porta iniziale: 0, porta finale: 65535
	start addr: 0.0.0.0, end addr: 255.255.255.255
	
	NOTIFY(INITIAL_CONTACT) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 8
	ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: INITIAL_CONTACT
	NOTIFY(SET_WINDOW_SIZE) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 12
	ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: SET_WINDOW_SIZE
	NOTIFY(ESP_TFC_NO_SUPPORT) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 8
	ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: ESP_TFC_NO_SUPPORT
	NOTIFY(NON_FIRST_FRAGS) Successivo payload: NONE, riservato: 0x0, lunghezza: 8
	ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NON_FIRST_FRAGS
	
	*11 nov 19:30:34.832: IKEv2:(ID SA = 1):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: IKE_AUTH, flag: INITIATOR ID messaggio: 1, lunghezza: 556
	Contenuto payload:
	Carico utile successivo ENCR: VID, riservato: 0x0, lunghezza: 528
	
	*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_WAIT_AUTH Evento: EV_NO_EVENT	

—Initiator ha inviato IKE_AUTH —>		

	*11 nov 19:30:34.832: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:30:34.832: IKEv2:Elaborazione di un elemento dalla coda pak *11 nov 19:30:34.832: IKEv2:(ID SA = 1):La richiesta ha valore mess_id 1; sono previsti da 1 a 1 *11 nov 19:30:34.832: IKEv2:(ID SA = 1):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: IKE_AUTH, flag: INITIATOR ID messaggio: 1, lunghezza: 556 Contenuto payload: *11 nov 19:30:34.832: IKEv2:Analisi payload specifico del fornitore: (CUSTOM) VID Payload successivo: IDi, riservato: 0x0, lunghezza: 20 IDi Payload successivo: AUTH, riservato: 0x0, lunghezza: 12 Tipo di ID: indirizzo IPv4, riservato: 0x0 0x0 AUTH Payload successivo: CFG, riservato: 0x0, lunghezza: 28 Metodo di autenticazione PSK, riservato: 0x0, riservato 0x0 CFG Payload successivo: SA, riservato: 0x0, lunghezza: 309 tipo cfg: CFG_REQUEST, riservato: 0x0, riservato: 0x0 *11 nov 19:30:34.832: tipo di attributo: DNS IP4 interno, lunghezza: 0 *11 nov 19:30:34.832: tipo di attributo: DNS IP4 interno, lunghezza: 0 *11 nov. 19:30:34.832: tipo attrib: IP4 NBNS interno, lunghezza: 0 *11 nov. 19:30:34.832: tipo attrib: IP4 NBNS interno, lunghezza: 0 *11 nov. 19:30:34.832: tipo attrib: subnet IP4 interna, lunghezza: 0 *Nov 11 19:30:34.832: tipo di matrice: versione applicazione, lunghezza: 257 tipo di attributo: sconosciuto - 28675, lunghezza: 0 *11 nov. 19:30:34.832: tipo attrib: sconosciuto - 28672, lunghezza: 0 *11 nov. 19:30:34.832: tipo attrib: sconosciuto - 28692, lunghezza: 0 *11 nov 19:30:34.832: tipo di matrice: sconosciuto - 28681, lunghezza: 0 *11 nov 19:30:34.832: tipo di matrice: sconosciuto - 28674, lunghezza: 0 *11 nov 19:30:34.832: SA Payload successivo: TSi,	Il router 2 riceve e verifica i dati di autenticazione ricevuti dal router 1. Configurazione pertinente: `crypto ipsec ikev2 ipsec-proposta protocollo AES256 esp crittografia aes-256 protocollo esp integrità sha-1 md5`

	riservato: 0x0, lunghezza: 40 ultima proposta: 0x0, riservata: 0x0, lunghezza: 36 Proposta: 1, ID protocollo: ESP, dimensione SPI: 4, #trans: 3 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 1, riservato: 0x0, id: 3DES ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 5, riservato: 0x0, id: Do not use ESN TSi Payload successivo: TSr, riservato: 0x0, lunghezza: 24 Numero di TS: 1, riservato 0x0, riservato 0x0 Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16 porta iniziale: 0, porta finale: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 TSr Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 24 Numero di TS: 1, riservato 0x0, riservato 0x0 Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16 porta iniziale: 0, porta finale: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255	
	*Nov 11 19:30:34.832: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_WAIT_AUTH Evento: EV_RECV_AUTH *Nov 11 19:30:34.832: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_NAT_T *Nov 11 19:30:34.832: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_WAIT_AUTH Evento: EV_PROC_ID *11 nov 19:30:34.832: IKEv2:(ID SA = 1):Ricevuti parametri validi nell'ID processo *Nov 11 19:30:34.832: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE FETCHED_FOR_PROF_SEL *Nov 11 19:30:34.832: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento:	Il router 2 genera la risposta al pacchetto IKE_AUTH ricevuto dal router 1. Il pacchetto di risposta contiene: ISAKMP Header (SPI/versione/flag), IDr. (identità del risponditore), AUTH Payload, SAr2 (avvia l'associazione di protezione simile allo scambio di set di trasformazioni di fase 2 in IKEv1), TSi e TSr (selettori del traffico dell'iniziatore e del risponditore). Contengono

	EV_GET_POLICY_BY_PEERID *11 nov 19:30:34.833: IKEv2:(1): Scelta del profilo IKE IKEV2-SETUP *11 nov 19:30:34.833: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.1 *11 nov 19:30:34.833: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.1 *11 nov 19:30:34.833: IKEv2:aggiunta del valore predefinito della proposta alla policy del kit utensili *11 nov 19:30:34.833: IKEv2:(ID SA = 1):Uso del profilo IKEv2 'IKEV2-SETUP' *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_WAIT_AUTH Evento: EV_SET_POLICY *11 nov 19:30:34.833: IKEv2:(ID SA = 1):Impostazione dei criteri configurati *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_AUTH4EAP *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_WAIT_AUTH Evento: EV_CHK_POLREQEAP *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_VERIFY_AUTH Evento: EV_CHK_AUTH_TYPE *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_PRESHR_KEY *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_VERIFY_AUTH Evento: EV_VERIFY_AUTH *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_VERIFY_AUTH Evento: EV_CHK4_IC	rispettivamente l'indirizzo di origine e l'indirizzo di destinazione dell'iniziatore e del risponditore per l'inoltro/la ricezione del traffico crittografato. L'intervallo di indirizzi specifica che tutto il traffico da e verso l'intervallo è tunneling. Questi parametri sono identici a quelli ricevuti da ASA1.

*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_REDIRECT
*11 nov 19:30:34.833: IKEv2:(ID SA = 1):Il controllo di reindirizzamento non è necessario, ignorandolo
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_NOTIFY_AUTH_DONE
*11 nov 19:30:34.833: IKEv2: l'autorizzazione del gruppo AAA non è configurata
*11 nov 19:30:34.833: IKEv2:l'autorizzazione utente AAA non è configurata
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_SET_RECD_CONFIG_MODE
*11 nov 19:30:34.833: IKEv2:Ricevuti dati di configurazione dal kit utensili:
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_PROC_SA_TS
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_VERIFY_AUTH Evento: EV_GET_CONFIG_MODE
*11 nov 19:30:34.833: IKEv2: errore durante la costruzione della risposta di configurazione
*11 nov 19:30:34.833: IKEv2:Nessun dato di configurazione da inviare al kit utensili:
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_MY_AUTH_METHOD
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_BLD_AUTH Evento: EV_GEN_AUTH *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_CHK4_SIGN *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: R_BLD_AUTH Evento: EV_OK_AUTH_GEN *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: R_BLD_AUTH Evento: EV_SEND_AUTH *11 nov 19:30:34.833: IKEv2:Costruzione payload specifico del fornitore: CISCO-GRANITE *11 nov 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *11 nov 19:30:34.833: IKEv2:Construct Notify Payload: ESP_TFC_NO_SUPPORT *11 nov 19:30:34.833: IKEv2:Construct Notify Payload: NON_FIRST_FRAGS	
	*11 nov 19:30:34.833: IKEv2:(ID SA = 1):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: IKE_AUTH, flag: RESPONDER MSG-RESPONSE ID messaggio: 1, lunghezza: 252 Contenuto payload: ENCR Payload successivo: VID, riservato: 0x0, lunghezza: 224 *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK *11 nov 19:30:34.833: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_PKI_SESH_CLOSE *11 nov 19:30:34.833: IKEv2:(ID SA = 1):Chiusura della sessione PKI *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000001 CurState: AUTH_DONE Evento:	Il risponditore invia la risposta per IKE_AUTH.

	EV_UPDATE_CAC_STATS *Nov 11 19:30:34.833: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento:EV_INSERT_IKE *11 nov 19:30:34.834: IKEv2:Indicizzazione mib archivio ikev2 1, piattaforma 60 *Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000001 CurState: AUTH_DONE Evento: EV_GEN_LOAD_IPSEC *11 nov 19:30:34.834: IKEv2:(ID SA = 1):Richiesta asincrona in coda *11 nov 19:30:34.834: IKEv2:(ID SA = 1): *Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_NO_EVENT		
<—Il risponditore ha inviato IKE_AUTH—			
L'iniziatore riceve una risposta dal risponditore.	*11 nov 19:30:34.834: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:30:34.834: IKEv2:Elaborazione di un elemento dalla coda pak	*Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 Stato corrente: AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC *11 nov 19:30:34.840: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4	Il risponditore inserisce una voce nel DAU.

		(R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHK4_ROLE	
Il router 1 verifica ed elabora i dati di autenticazione in questo pacchetto. Il router 1 inserisce quindi questa SA nel relativo SAD.	*11 nov 19:30:34.834: IKEv2:(ID SA = 1):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: IKE_AUTH, flag: RESPONDER MSG-RESPONSE ID messaggio: 1, lunghezza: 252 Contenuto payload: *11 nov 19:30:34.834: IKEv2:Analisi payload specifico del fornitore: (CUSTOM) VID Payload successivo: IDr., riservato: 0x0, lunghezza: 20 IDr. Payload successivo: AUTH, riservato: 0x0, lunghezza: 12 Tipo di ID: indirizzo IPv4, riservato: 0x0 0x0 AUTH Payload successivo: SA, riservato: 0x0, lunghezza: 28 Metodo di autenticazione PSK, riservato: 0x0, riservato 0x0 SA Payload successivo: TSi, riservato: 0x0, lunghezza: 40 ultima proposta: 0x0, riservata: 0x0, lunghezza: 36 Proposta: 1, ID protocollo: ESP, dimensione SPI: 4, #trans: 3 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 1, riservato: 0x0, id: 3DES ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 5, riservato: 0x0, id: Do not use ESN TSi Payload successivo: TSr, riservato: 0x0, lunghezza: 24 Numero di TS: 1, riservato 0x0, riservato 0x0 Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16 porta iniziale: 0, porta finale: 65535 start addr: 0.0.0.0, end addr: 255.255.255.255 TSr Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 24	

Numero di TS: 1, riservato 0x0, riservato 0x0
Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
porta iniziale: 0, porta finale: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255

*11 nov 19:30:34.834: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY (SET_WINDOW_SIZE) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 12
ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: SET_WINDOW_SIZE

*11 nov 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT NOTIFY (ESP_TFC_NO_SUPPORT) Payload successivo: NOTIFY, riservato: 0x0, lunghezza: 8
ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: ESP_TFC_NO_SUPPORT

*11 nov 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS NOTIFY (NON_FIRST_FRAGS) Payload successivo: NONE, riservato: 0x0, lunghezza: 8
ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: NON_FIRST_FRAGS

*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState: I_WAIT_AUTH Evento:EV_RECV_AUTH
*11 nov 19:30:34.834: IKEv2:(ID SA = 1):Azione: Action_Null
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_NOTIFY
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:EV_PROC_MSG
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_IF_PEER_CERT_NEEDS_TO FETCHED_FOR_PROF_SEL
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4

(I) MsgID = 0000001 CurState: I_PROC_AUTH Evento: EV_GET_POLICY_BY_PEERID
*11 nov 19:30:34.834: IKEv2:aggiunta della proposta di fase 1 alla policy del kit utensili
*11 nov 19:30:34.834: IKEv2:(ID SA = 1):Uso del profilo IKEv2 'IKEV2-SETUP'
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Stato corrente: I_PROC_AUTH Evento: EV_VERIFY_POLICY_BY_PEERID
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_AUTH_TYPE
*Nov 11 19:30:34.834: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_GET_PRESHR_KEY
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState: I_PROC_AUTH Evento:EV_VERIFY_AUTH
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Stato corrente: I_PROC_AUTH Evento: EV_CHK_EAP
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento:EV_NOTIFY_AUTH_DONE
*11 nov 19:30:34.835: IKEv2: l'autorizzazione del gruppo AAA non è configurata
*11 nov 19:30:34.835: IKEv2:l'autorizzazione utente AAA non è configurata
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState: I_PROC_AUTH Evento:

EV_CHK_IKE_ONLY
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: I_PROC_AUTH Evento: EV_PROC_SA_TS
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_OK
*11 nov 19:30:34.835: IKEv2:(ID SA = 1):Azione: Action_Null
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_PKI_SESH_CLOSE
*11 nov 19:30:34.835: IKEv2:(ID SA = 1):Chiusura della sessione PKI
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState: AUTH_DONE Evento: EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_INSERT_IKE
*11 nov 19:30:34.835: IKEv2:Indicizzazione mib archivio ikev2 1, piattaforma 60
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 0000001 CurState: AUTH_DONE Evento: EV_GEN_LOAD_IPSEC
*11 nov 19:30:34.835: IKEv2:(ID SA = 1):Richiesta asincrona in coda

*11 nov 19:30:34.835: IKEv2:(ID SA = 1):
*Nov 11 19:30:34.835: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_NO_EVENT
*11 nov 19:30:34.835: consumo messaggio IKEv2:KMI 8. Nessuna azione intrapresa.
*11 nov 19:30:34.835: messaggio IKEv2:KMI 12 consumato. Nessuna azione intrapresa.
*Nov 11 19:30:34.835: IKEv2:Nessun dato da inviare nel set di configurazione del modo.
*11 nov 19:30:34.841: IKEv2:aggiunta del manico di rientro

	0x80000002 associato a SPI 0x9506D414 per la sessione 8 *Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 Stato corrente: AUTH_DONE Evento: EV_OK_RECD_LOAD_IPSEC *11 nov 19:30:34.841: IKEv2:(ID SA = 1):Azione: Action_Null *Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_START_ACCT *11 nov 19:30:34.841: IKEv2:(ID SA = 1):Contabilità non richiesta *Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHECK_DUPE *Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: AUTH_DONE Evento: EV_CHK4_ROLE		
Il tunnel è attivo sull'iniziatore e lo stato mostra READY.	*Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: READYEvent: EV_CHK_IKE_ONLY *Nov 11 19:30:34.841: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MsgID = 00000001 CurState: Evento READY: EV_I_OK	*Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000001 CurState: READY Evento: EV_R_OK *Nov 11 19:30:34.840: IKEv2:(ID SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 00000001 CurState: Evento READY: EV_NO_EVENT	Tunnel attivo sul risponditore. Il tunnel del risponditore in genere viene visualizzato prima dell'iniziatore.

Debug CHILD_SA

Questo scambio è costituito da una singola coppia richiesta/risposta ed è stato definito come scambio di fase 2 in IKEv1. Può essere avviata da una delle estremità di IKE_SA una volta completati gli scambi iniziali.

Descrizione messaggio CHILD_SA Router 1	Debug	Descrizione del messaggio CHILD_SA del router 2
Il router 1 avvia lo scambio CHILD_SA. Richiesta CREATE_CHILD_SA. Il pacchetto CHILD_SA contiene in genere: • HDR SA (version.flags/exchange type) • Nonce Ni (facoltativo): se CHILD_SA viene creato come parte dello scambio iniziale, non è necessario inviare un secondo payload KE e nonce • Payload SA • KEi (Key-optional): la richiesta CREATE_CHILD_SA può facoltativamente contenere un payload KE per uno scambio DH aggiuntivo per consentire maggiori garanzie di segretezza di inoltro per CHILD_SA. Se l'associazione di protezione include gruppi DH diversi, KEi deve essere un elemento del gruppo che l'iniziatore si aspetta che il risponditore accetti. Se non è corretto, lo scambio CREATE_CHILD_SA ha esito negativo e può riprovare con una chiave KEi diversa • N (Notifica payload - facoltativo). Il payload	*11 nov 19:31:35.873: IKEv2:Ricevuto un pacchetto dal dispatcher *11 nov 19:31:35.873: IKEv2:Elaborazione di un elemento dalla coda pak *11 nov 19:31:35.873: IKEv2:(ID SA = 2):La richiesta ha mess_id 3; sono previsti da 3 a 7 *11 nov 19:31:35.873: IKEv2:(ID SA = 2):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: CREATE_CHILD_SA, flag: INITIATOR ID messaggio: 3, lunghezza: 396 Contenuto payload: SA Payload successivo: N, riservato: 0x0, lunghezza: 152 ultima proposta: 0x0, riservata: 0x0, lunghezza: 148 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 8, #trans: 15 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA512 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA384	

di notifica viene utilizzato per trasmettere dati informativi, ad esempio condizioni di errore e transizioni di stato, a un peer IKE. Un payload di notifica può essere visualizzato in un messaggio di risposta (in genere specifica il motivo per cui una richiesta è stata rifiutata), in uno scambio DI INFORMAZIONI (per segnalare un errore non in una richiesta IKE) o in qualsiasi altro messaggio per indicare le capacità del mittente o per modificare il significato della richiesta.Se questo scambio CREATE_CHILD_SA sta rieseguendo una chiave di un'associazione di protezione esistente diversa da IKE_SA, il payload N iniziale di tipo REKEY_SA DEVE identificare l'associazione di protezione sottoposta a reimpostazione della chiave. Se lo scambio CREATE_CHILD_SA non comporta la rigenerazione di una SA esistente, il payload N DEVE essere omesso.	ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA256 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: MD5 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA512 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA384 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA256 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: MD596 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1536_MODP/Group 5 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 N Payload successivo: KE, riservato: 0x0, lunghezza: 24 Payload successivo KE: NOTIFY, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 *11 nov 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Payload successivo: NONE, riservato: 0x0, lunghezza: 12 ID protocollo di sicurezza: IKE,	

	dimensioni spi: 0, tipo: SET_WINDOW_SIZE *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: Evento READY: EV_RECV_CREATE_CHILD *11 nov 19:31:35.874: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_INIT Evento: EV_RECV_CREATE_CHILD *11 nov 19:31:35.874: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_INIT Evento: EV_VERIFY_MSG *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 Stato corrente: CHILD_R_INIT Evento: EV_CHK_CC_TYPE *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_IKE Evento: EV_REKEY_IKESA *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6	

	R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_IKE Evento: EV_GET_IKE_POLICY *11 nov 19:31:35.874: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.2 *11 nov 19:31:35.874: IKEv2:% Recupero della chiave già condivisa dall'indirizzo 10.0.0.2 *11 nov 19:31:35.874: IKEv2:aggiunta della proposta di fase 1 alla policy del kit utensili *11 nov 19:31:35.874: IKEv2:(ID SA = 2):Uso del profilo IKEv2 'IKEV2-SETUP' *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_IKE Evento: EV_PROC_MSG *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_IKE Evento: EV_SET_POLICY *11 nov 19:31:35.874: IKEv2:(ID SA = 2):Impostazione dei criteri configurati *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_GEN_DH_KEY *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState:	

	CHILD_R_BLD_MSG Evento: EV_NO_EVENT *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_OK_RECD_DH_PUBKEY_RESP *11 nov 19:31:35.874: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.874: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento:EV_GEN_DH_SECRET *Nov 11 19:31:35.881: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_NO_EVENT *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:31:35.882: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_BLD_MSG *11 nov 19:31:35.882: IKEv2:ConstructNotify Payload: SET_WINDOW_SIZE Contenuto payload:	

	SA Payload successivo: N, riservato: 0x0, lunghezza: 56 ultima proposta: 0x0, riservata: 0x0, lunghezza: 52 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 8, #trans: 4 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 N Payload successivo: KE, riservato: 0x0, lunghezza: 24 Payload successivo KE: NOTIFY, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 NOTIFY(SET_WINDOW_SIZE) Payload successivo: NONE, riservato: 0x0, lunghezza: 12 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: SET_WINDOW_SIZE	
	*11 nov 19:31:35.869: IKEv2:(ID SA = 2):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: CREATE_CHILD_SA, flag: INITIATOR ID messaggio: 2, lunghezza: 460 Contenuto payload: ENCR Payload successivo: SA, riservato: 0x0, lunghezza: 432 *11 nov 19:31:35.873: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE	Questo pacchetto viene ricevuto dal router 2.

	Contenuto payload: SA Payload successivo: N, riservato: 0x0, lunghezza: 152 ultima proposta: 0x0, riservata: 0x0, lunghezza: 148 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 8, #trans: 15 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA512 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA384 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA256 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: MD5 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA512 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA384 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA256 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8	

	tipo: 3, riservato: 0x0, id: MD596 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1536_MODP/Group 5 ultima trasformazione: 0x0, riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 N Payload successivo: KE, riservato: 0x0, lunghezza: 24 Payload successivo KE: NOTIFY, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 NOTIFY(SET_WINDOW_SIZE) Payload successivo: NONE, riservato: 0x0, lunghezza: 12 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: SET_WINDOW_SIZE	
	*11 nov 19:31:35.882: IKEv2:(ID SA = 2):Payload successivo: ENCR, versione: 2.0 Tipo di scambio: CREATE_CHILD_SA, flag: RESPONDER MSG-RESPONSE ID messaggio: 3, lunghezza: 300 Contenuto payload: SA Payload successivo: N, riservato: 0x0, lunghezza: 56 ultima proposta: 0x0, riservata: 0x0, lunghezza: 52 Proposta: 1, ID protocollo: IKE, dimensioni SPI: 8, #trans: 4 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 12 tipo: 1, riservato: 0x0, id: AES-CBC ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 2, riservato: 0x0, id: SHA1 ultima trasformazione: 0x3, riservata: 0x0: lunghezza: 8 tipo: 3, riservato: 0x0, id: SHA96 ultima trasformazione: 0x0,	Il router 2 ora genera la risposta per lo scambio CHILD_SA. Questa è la risposta CREATE_CHILD_SA. Il pacchetto CHILD_SA contiene in genere: • HDR SA (version.flags/exchange type) • Nonce Ni(facoltativo): se CHILD_SA viene creato come parte dello scambio iniziale, non è necessario inviare un secondo payload KE e nonce. • Payload SA • KEi (Key-optional): la richiesta CREATE_CHILD_SA può facoltativamente contenere un payload KE per uno scambio

	riservata: 0x0: lunghezza: 8 tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MODP/Group 2 N Payload successivo: KE, riservato: 0x0, lunghezza: 24 Payload successivo KE: NOTIFY, riservato: 0x0, lunghezza: 136 Gruppo DH: 2, riservato: 0x0 *Nov 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) Payload successivo: NONE, riservato: 0x0, lunghezza: 12 ID protocollo di sicurezza: IKE, dimensioni spi: 0, tipo: SET_WINDOW_SIZE *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_WAIT Evento: EV_RECV_CREATE_CHILD *11 nov 19:31:35.882: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_VERIFY_MSG *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6	DH aggiuntivo per consentire maggiori garanzie di segretezza di inoltro per CHILD_SA. Se l'associazione di protezione include gruppi DH diversi, KEi deve essere un elemento del gruppo che l'iniziatore si aspetta che il risponditore accetti. Se non è corretto, lo scambio CREATE_CHILD_SA non riesce e deve essere eseguito un nuovo tentativo con un KEi diverso. • N (Notifica payload - facoltativo): il payload di notifica viene utilizzato per trasmettere dati informativi, ad esempio condizioni di errore e transizioni di stato, a un peer IKE. Un payload di notifica può essere visualizzato in un messaggio di risposta (in genere specifica il motivo per cui una richiesta è stata rifiutata), in uno scambio di informazioni (per segnalare un errore non in una richiesta IKE) o in qualsiasi altro messaggio per indicare le capacità del mittente o per modificare il significato della

	R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_PROC_MSG *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_CHK4_PFS *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_GEN_DH_SECRET *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_NO_EVENT *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_OK_RECD_DH_SECRET_RESP *11 nov 19:31:35.890: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_CHK_IKE_REKEY *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I)	richiesta. Se lo scambio CREATE_CHILD_SA sta rieseguendo la chiave di un'associazione di protezione esistente diversa da IKE_SA, il payload N iniziale di tipo REKEY_SA deve identificare l'associazione di protezione che viene rieseguita la chiave. Se lo scambio di CREATE_CHILD_SA non comporta la rigenerazione di una SA esistente, è necessario omettere il payload N. Il router 2 invia la risposta e completa l'attivazione della nuova associazione di protezione figlio.

	MsgID = 0000003 CurState: CHILD_I_PROC Evento: EV_GEN_SKEYID *11 nov 19:31:35.890: IKEv2:(ID SA = 2):Generazione skeyid *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_DONE Evento: EV_ACTIVATE_NEW_SA *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_DONE Evento: EV_UPDATE_CAC_STATS *11 nov. 19:31:35.890: IKEv2: richiesta attivazione nuova ikev2 *11 nov 19:31:35.890: IKEv2: impossibile ridurre il conteggio per la negoziazione in uscita *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_DONE Evento: EV_CHECK_DUPE *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: CHILD_I_DONE Evento: EV_OK *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 0000003 CurState: Evento EXIT: EV_CHK_PENDING *11 nov 19:31:35.890: IKEv2:(ID SA = 2):Risposta elaborata con ID	

	messaggio 3, le richieste possono essere inviate dall'intervallo 4 all'intervallo 8 *Nov 11 19:31:35.890: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MsgID = 00000003 CurState: EXIT Evento: EV_NO_EVENT	
Il router 1 riceve il pacchetto di risposta dal router 2 e completa l'attivazione di CHILD_SA.	*Nov 11 19:31:35.882: IKEv2:(ID SA = 2):Next payload: ENCR, versione: 2.0 Tipo di scambio: CREATE_CHILD_SA, flag: RESPONDER MSG-RESPONSE ID messaggio: 3, lunghezza: 300 Contenuto payload: ENCR Payload successivo: SA, riservato: 0x0, lunghezza: 272 *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento:EV_CHK_IKE_REKEY *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_BLD_MSG Evento: EV_GEN_SKEYID *11 nov 19:31:35.882: IKEv2:(ID SA = 2):Generare skeyid *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_DONE Evento:EV_ACTIVATE_NEW_SA *11 nov. 19:31:35.882: IKEv2:Indicizzazione mib archivio	

	ikev2 3, piattaforma 62 *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_DONE Evento: EV_UPDATE_CAC_STATS *11 nov 19:31:35.882: IKEv2:Richiesta di attivazione nuova impostazione ikev2 *11 nov 19:31:35.882: IKEv2: impossibile diminuire il conteggio per la negoziazione in entrata *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_DONE Evento: EV_CHECK_DUPE *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_DONE Evento: EV_OK *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: CHILD_R_DONE Evento: EV_START_DEL_NEG_TMR. *11 nov 19:31:35.882: IKEv2:(ID SA = 2):Azione: Action_Null *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 0000003 CurState: Evento EXIT: EV_CHK_PENDING *11 nov 19:31:35.882: IKEv2:(ID SA = 2):Risposta inviata con ID messaggio 3, le richieste possono	

	essere accettate dall'intervallo 4 all'intervallo 8 *Nov 11 19:31:35.882: IKEv2:(ID SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MsgID = 00000003 CurState: EXIT Evento: EV_NO_EVENT	

Verifica tunnel

ISAKMP

Comando

<#root>

show crypto ikev2 sa detailed

Uscita Router 1

<#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
```

Uscita Router 2

<#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

Comando

<#root>

show crypto ipsec sa

Nota: in questo output, a differenza di IKEv1, il valore del gruppo DH PFS viene visualizzato come "PFS (Y/N): N, gruppo DH: nessuno" durante la prima negoziazione del tunnel, ma, dopo una reimpostazione della chiave, vengono visualizzati i valori corretti. Non si tratta di un bug, anche se il comportamento è descritto nell'ID bug Cisco CSCug67056. (Solo gli utenti Cisco registrati possono accedere agli strumenti o alle informazioni Cisco interne.) La differenza tra IKEv1 e IKEv2 consiste nel fatto che, in quest'ultimo caso, le associazioni di protezione figlio vengono create come parte dello scambio AUTH. Il gruppo DH configurato nella mappa crittografica verrebbe utilizzato solo durante la reimpostazione della chiave. Verrà quindi visualizzato 'PFS (S/N): N, gruppo DH: nessuno' fino alla prima reimpostazione della chiave.

Con IKEv1, si verifica un comportamento diverso, in quanto la creazione di associazioni di protezione figlio avviene durante la modalità rapida e il messaggio CREATE_CHILD_SA dispone di un provisioning per il payload di scambio chiave che specifica i parametri DH per derivare un nuovo segreto condiviso.

Uscita Router 1

<#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:
```

Uscita Router 2

<#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:
```

È possibile anche controllare l'output del comando show crypto session su entrambi i router; questo output mostra lo stato della sessione tunnel come 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
```

Informazioni correlate

- Debug a livello di protocollo e scambio pacchetti IKEv2
- Supporto tecnico Cisco e download

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).