Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPsec e IKE (modalità aggressiva IKEv1)

Sommario

Introduzione

In questo documento vengono descritti i debug su Cisco Adaptive Security Appliance (ASA) quando si usano la modalità aggressiva e la chiave precondivisa (PSK). Viene inoltre descritta la conversione di alcune righe di debug nella configurazione. Cisco raccomanda una conoscenza di base di IPsec e IKE (Internet Key Exchange).

In questo documento non viene parlato del traffico di passaggio dopo la creazione del tunnel.

Problema principale

I debug IKE e IPsec a volte sono criptici, ma è possibile usarli per capire i problemi relativi alla definizione del tunnel VPN con IPsec.

Scenario

La modalità aggressiva viene in genere utilizzata in caso di Easy VPN (EzVPN) con client software (Cisco VPN Client) e hardware (Cisco ASA 5505 Adaptive Security Appliance o Cisco IOS? Router software), ma solo quando viene utilizzata una chiave già condivisa. A differenza della modalità principale, la modalità aggressiva è costituita da tre messaggi.

I debug vengono eseguiti da un'ASA con software versione 8.3.2 e funziona come server EzVPN.

Il client EzVPN è un client software.

Comandi di debug usati

Di seguito sono riportati i comandi di debug usati nel documento:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

Configurazione ASA

La configurazione ASA di questo esempio è strettamente di base; non vengono utilizzati server esterni.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

Debug

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Descrizione messaggio server	Debug		Descrizione messaggio client
	49711:28:30.28908/24/12Sev=Info/6IKE/0x6300003B Tentativo di stabilire una connessione con 64.102.156.88. 49811:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_INITIALEvent: INIZIATORE_EV 49911:28:30.29708/24/12Sev=Info/4IKE/0x63000001 Avvio della negoziazione IKE fase 1 50011:28:30.29708/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_GEN_DHKEY 50111:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_BLD_MSG 50211:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_START_RETRY_TMR 50311:28:30.30408/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_SND_MSG1Event: EV_SND_MSG		Inizia la modalità aggressiva. Costruire AM1. Questo processo include: - HDR ISAKMP - appliance di sicurezza (SA) che contiene tutti i payload di trasformazione e le proposte supportate dal client - Payload scambio chiave - ID iniziatore fase 1 - Nessuna
	50411:28:30.30408/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) al 64.102.156.88		Invia AM1.
	<========== Messaggio aggressivo 1 (AM1) ==========		
Ricevi AM1 dal client.	24 ago 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) con	50611:28:30.3308/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=0000000000000000CurState: AM_WAIT_MSG2Event: EV_NO_EVENT	Attendere la risposta del server.

	payload: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 849		

Elabora AM1. Confronta le proposte e le trasformazioni ricevute con quelle già configurate per le corrispondenze. Configurazione pertinente: ISAKMP è abilitato sull'interfaccia ed è definito almeno un criterio che corrisponda a quello inviato dal client:
 	
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre-share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
Gruppo di tunnel corrispondente al nome identità presente:
 	
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione del payload SA
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload chiave
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload ISA_KE in corso
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload nonce
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, payload ID elaborazione
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ricevuto xauth V6 VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ricevuto DPD VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Ricevuto VID frammentazione
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Peer IKE incluso flag funzionalità frammentazione IKE: Modalità principale:TrueAggressive Mode:False
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, Ricevuto NAT-Traversal ver. 02 VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, elaborazione payload VID
	24 ago 11:31:03 [IKEv1 DEBUG]IP = 64.102.156.87, ricevuto VID client Cisco Unity
	24 ago 11:31:03 [IKEv1]IP = 64.102.156.87,	

tunnel-group EZ ipsec-attributes pre-shared-key cisco	connessione terminata su tunnel_group ipsec 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload SA IKE 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1]Fase 1 non riuscita: tipi di attributi non corrispondenti per la classe Gruppo Descrizione:Ricezione: Gruppo 2Cfg'd: Gruppo 5 24 ago 11:31:03 [IKEv1 DEBUG]Gruppo = ipsec, IP = 64.102.156.87, Proposta SA IKE n. 1, Trasforma n. 5	

	accettabileCorrisponde alla voce IKE globale n. 1	
Costruire AM2. Questo processo include: - criteri scelti - Diffie-Hellman (DH) - ID risponditore -auth - Payload del rilevamento NAT (Network Address Translation)	24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload SA ISAKMP 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload della chiave 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload nonce Ago 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Generazione delle chiavi per il risponditore in corso... 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload ID 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload hash 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Hash di calcolo per ISAKMP 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload VID Cisco Unity 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload VID Xauth V6 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload dpd vid 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione di NAT-Traversal VID ver 02 payload 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload di individuazione NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, calcolo dell'hash di rilevamento NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload di individuazione NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, calcolo dell'hash di rilevamento NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione della frammentazione VID + payload delle funzionalità estese 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload VID 24 ago 11:31:03 [IKEv1 DEBUG]Gruppo = ipsec, IP = 64.102.156.87, Invia Altiga/Cisco VPN3000/Cisco ASA GW VID	
Invia AM2.	Ago 24 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=0) con payload: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + NAT-D (130) + NAT-D (130) + FORNITORE (13) + FORNITORE (13) + NONE (0) lunghezza totale: 444	
	========== Messaggio aggressivo 2 (AM2) ==========>	

	50711:28:30.40208/24/12Sev=Info/5IKE/0x6300002F Pacchetto ISAKMP ricevuto: peer = 64.102.156,8 50811:28:30.40308/24/12Sev=Info/4IKE/0x63000014 RICEZIONE DI <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID(Unity), VID(Xauth), VID(dpd), VID(Nat-T), NAT-D, NAT-D, VID(Frag), VID(?)) da 64.102.156.88 5101:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_RCVD_MSG	Ricevere AM2.
	5111:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer è un peer conforme a Cisco-Unity 51211:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Il peer supporta XAUTH 51311:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supporta DPD 51411:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Peer supporta NAT-T 51511:28:30.41208/24/12Sev=Info/5IKE/0x63000001 Il peer supporta payload di frammentazione IKE 51611:28:30.41208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_GEN_IDCHIAVE 51711:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.42208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_WAIT_MSG2Event: EV_CRITTOGRAFIA_ATTIVA	Elaborare AM 2.
	5201:28:30.4208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_BLD_MSG] 5211:28:30.42208/24/12Sev=Debug/8IKE/0x63000001 IOS Vendor ID: costruzione avviata 52211:28:30.42208/24/12Sev=Info/6IKE/0x63000001 IOS Vendor ID Creazione completata	Costruire AM3. Questo processo include l'autenticazione client. A questo punto tutti i dati rilevanti per la crittografia sono già stati scambiati.
	52311:28:30.42308/24/12Sev=Debug/7IKE/0x63000076	Inviare il messaggio AM3.

	NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: AM_SND_MSG3Evento: EV_SND_MSG 52411:28:30.42308/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D, VID(?), VID(Unity)) a 64.102.156.88	
	<========== Messaggio aggressivo 3 (AM3) ==========	
Ricevi AM3 dal client.	24 ago 11:31:03 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) lunghezza totale: 168	
Elaborare AM 3. Confermare l'utilizzo NAT traversal (NAT-T). Entrambe le parti sono ora pronte ad avviare la crittografia del traffico.	24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload hash 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Hash di calcolo per ISAKMP 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione del payload di notifica 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload NAT-Discovery 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, calcolo dell'hash di rilevamento NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload NAT-Discovery 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, calcolo dell'hash di rilevamento NAT 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload VID Aug 24 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Elaborazione payload ID fornitore IOS/PIX (versione: 1.0.0, funzionalità: 00000408) 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, elaborazione payload VID 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, ricevuto VID client Cisco Unity 24 ago 11:31:03 [IKEv1]Group = ipsec, IP = 64.102.156.87, Rilevamento NAT automatico Stato:estremità remotaISdietro a un dispositivo NATuesta estremità NON dietro un dispositivo NAT	
Avviare la fase 1.5 (XAUTH) e richiedere le credenziali dell'utente.	24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload hash vuoto 24 ago 11:31:03 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, costruzione del payload hash qm 24 ago 11:31:03 [IKEv1]IP = 64.102.156.87, messaggio di INVIO IKE_DECODE (msgid=fb709d4d) con payload: HDR + HASH (8) + ATTR (14) + NONE (0) lunghezza totale: 72	
	========== XAuth - Richiesta credenziali ==========>	
	53511:28:30.43008/24/12Sev=Info/4IKE/0x63000014	Ricevi richiesta

	RICEZIONE DI <<< ISAKMP OAK TRANS *(HASH, ATTR) DA 64.102.156.88 53611:28:30.43108/24/12Sev=Decode/11IKE/0x63000001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Tipo di cambio:Transazione Flag:(Crittografia) MessageID(Hex):FB709D4D Lunghezza:76 Hash payload Payload successivo: Attributi Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 Attributi payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 20 Tipo: RICHIESTA_CFG_ISAKMP Reserved: 00 Identificativo: 0000 Tipo XAUTH: Generico Nome utente XAUTH: (vuoto) Password utente XAUTH: (vuoto) 53711:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	di autenticazione. Il payload decrittografato mostra campi di nome utente e password vuoti.
	53811:28:30.43108/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQUESTvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQUESTvent: EV_START_RETRY_TMR 5401:28:30.43208/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4EVENTO UTENTE: EV_NO_EVENT 541 11:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4EVENTO UTENTE: EV_RCVD_INPUT_UTENTE	Avviare la fase 1.5 (XAUTH). Avviare il timer dei tentativi in attesa dell'input dell'utente. Quando il timer dei tentativi scade, la connessione viene automaticamente interrotta.
	54211:28:36.41508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState:	Dopo aver ricevuto l'input dell'utente,

	TM_WAIT_4EVENTO UTENTE: EV_SND_MSG 54311:28:36.41508/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88 54411:28:36.41508/24/12Sev=Decode/11IKE/0x63000001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Tipo di cambio:Transazione Flag:(Crittografia) MessageID(Hex):FB709D4D Lunghezza:85 Hash payload Payload successivo: Attributi Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 Attributi payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 33 Tipo: ISAKMP_CFG_REPLY Reserved: 00 Identificativo: 0000 Tipo XAUTH: Generico Nome utente XAUTH: (dati non visualizzati) Password utente XAUTH: (dati non visualizzati)	inviare le credenziali dell'utente al server. Il payload decrittografato mostra i campi di nome utente e password compilati (ma nascosti). Richiesta di configurazione della modalità di invio (vari attributi).
	<========== Xauth - Credenziali utente ==========	
Ricevi credenziali utente.	24 ago 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=fb709d4d) con payload: HDR + HASH (8) + ATTR (14) + NESSUNO (0) lunghezza totale: 85 24 ago 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, process_attr(): Inserire!	
Elabora credenziali utente. Verificare le credenziali e generare il payload di configurazione della modalità. Configurazione pertinente: `username cisco password cisco`	Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, IP = 64.102.156.87, Elaborazione attributi di risposta MODE_CFG. Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: DNS primario = 192.168.1.99 Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: DNS secondario = cancellato Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: WINS primario = cancellato Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec,	

	Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: WINS secondario = cancellato Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: split tunneling list = split Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: dominio predefinito = jyoungta-labdomain.cisco.com Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Compressione IP = disabilitata Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Criterio Tunneling Ripartito = Disabilitato Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Impostazione proxy browser = nessuna modifica Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKEGetUserAttributes: Ignora proxy browser locale = disattiva 24 ago 11:31:09 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Utente (user1) autenticato.	
Invia risultato xuath.	Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash vuoto 24 ago 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash qm 24 ago 11:31:09 [IKEv1]IP = 64.102.156.87, messaggio di INVIO IKE_DECODE (msgid=5b6910ff) con payload: HDR + HASH (8) + ATTR (14) + NONE (0) lunghezza totale: 64	
	========== XAuth - Risultato autorizzazione ==========>	
	54511:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=Info/5IKE/0x6300002F Pacchetto ISAKMP ricevuto: peer = 64.102.156.88 54811:28:36.42408/24/12Sev=Info/4IKE/0x63000014 RICEZIONE DI <<< ISAKMP OAK TRANS *(HASH, ATTR) DA 64.102.156.88 54911:28:36.42508/24/12Sev=Decode/11IKE/0x63000	Ricezione dei risultati di autenticazione ed elaborazione dei risultati.

	001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Tipo di cambio:Transazione Flag:(Crittografia) MessageID(Hex):5B6910FF Lunghezza:76 Hash payload Payload successivo: Attributi Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): 7DCF47827164198731639BFB7595F694C9DDFE85 Attributi payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 12 Tipo: SET_CFG_ISAKMP Reserved: 00 Identificativo: 0000 Stato XAUTH: Superato 55011:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 5511:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETTvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETTvent: RISULTATO_AUTH_EV	
	55311:28:36.42508/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88	Risultato ACK.
	<========== Xauth - Conferma ==========	
ricevere ed elaborare ACK; nessuna risposta dal server.	24 ago 11:31:09 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=5b6910ff) con payload: HDR + HASH (8) + ATTR (14) + NONE (0) lunghezza totale: 60 Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Inserire! Ago 24 11:31:09 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Elaborazione attributi ACK cfg	
	55511:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->TM:MsgID=5B6910FFCurState:	Generare la richiesta mode-config. Il payload

	TM_XAUTH_DONEEvent: EV_XAUTH_DONE_SUC 55611:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: RICHIESTA_TERMINI_EV 55811:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: _RIMUOVI 55911:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 5601:28:36.42608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 5611:28:38.40608/24/12Sev=Debug/8IKE/0x6300004C Avvio del timer DPD per IKE SA (I_Cookie=D56197780D7BE3E5) R_Cookie=1B301D2DE710EDA0) (sa->stato = 1, sa->dpd.CONCERN_freq(mSec) = 5000 56211:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=Info/5IKE/0x6300005E Il client invia una richiesta firewall al concentratore 56611:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_START_RETRY_TMR	decrittografato mostra i parametri richiesti dal server.
	56711:28:38.40908/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG	Invia richiesta mode-config.

	56811:28:38.40908/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK TRANS *(HASH, ATTR) to 64.102.156.88 56911:28:38.62708/24/12Sev=Decode/11IKE/0x63000001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Tipo di cambio:Transazione Flag:(Crittografia) MessageID(Hex):84B4B653 Lunghezza: 183 Hash payload Payload successivo: Attributi Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): 81BFBF6721A744A815D69A315EF4AAA571D6B687 Attributi payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 131 Tipo: RICHIESTA_CFG_ISAKMP Reserved: 00 Identificativo: 0000 Indirizzo IPv4: (vuoto) Netmask IPv4: (vuoto) DNS IPv4: (vuoto) WINS (IPv4 NBNS): (vuoto) Scadenza indirizzo: (vuoto) Estensione Cisco: Banner: (vuoto) Estensione Cisco: Salva PWD: (vuoto) Estensione Cisco: Nome dominio predefinito: (vuoto) Estensione Cisco: Includi divisione: (vuoto) Estensione Cisco: Nome DNS diviso: (vuoto) Estensione Cisco: Esegui PFS: (vuoto) Sconosciuto: (vuoto) Estensione Cisco: Server di backup: (vuoto) Estensione Cisco: Disconnessione rimozione smart card: (vuoto) Versione applicazione: Cisco Systems VPN Client 5.0.07.0290:WinNT Estensione Cisco: Tipo di firewall: (vuoto) Estensione Cisco: Nome host DNS dinamico: ATBASU-LABBOX	
	<========== Richiesta configurazione modalità ==========		
Ricevi richiesta di configurazione	24 ago 11:31:11	57011:28:38.62808/24/12Sev=Debug/7IKE/0x63000076	Attendere la risposta del

modalità.	[IKEv1]IP = 64.102.156.87, messaggio IKE_DECODE RICEVUTO (msgid=84b4b653) con payload: HDR + HASH (8) + ATTR (14) + NONE (0) lunghezza totale: 183 Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, process_attr(): Inserire!	NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	server.
Richiesta di configurazione modalità processo. Molti di questi valori sono in genere configurati nei Criteri di gruppo. Tuttavia, poiché il server in questo esempio ha una configurazione di base, non è possibile visualizzarla qui.	Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Elaborazione attributi richiesta cfg Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di indirizzo IPV4. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Ricevuta richiesta per la maschera di rete IPV4. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di indirizzo del server DNS. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di indirizzo del server WINS. Ago 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Received unsupported transaction mode attribute: 5 Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Richiesta banner ricevuta. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di impostazione Salva PW. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG:	

	È stata ricevuta una richiesta per il nome di dominio predefinito. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta per l'elenco di split tunnel. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di suddivisione del DNS. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di impostazione PFS. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di impostazione proxy del browser client. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta per l'elenco peer IP-sec di backup. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di impostazione di disconnessione per la rimozione della smart card client. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: È stata ricevuta una richiesta di versione dell'applicazione. Ago 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Tipo di client: Versione applicazione client WinNTC: 5.0.07.0290 Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: Ricevuta richiesta di FWTYPE. Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, MODE_CFG: La richiesta ricevuta per il nome host DHCP per DNS è: ATBASU-LABBOX!	
Costruire la risposta mode-config con tutti i valori configurati. Configurazione pertinente: In questo caso, all'utente viene sempre assegnato lo stesso indirizzo IP. `username cisco attributes` **`vpn-framed-ip-address 192.168.1.100 255.255.255.0`** `group-policy EZ internal`	Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Obived IP addr (192.168.1.100) before initiating Mode Cfg (XAuth abilitato) Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Invio subnet mask (255.255.255.0) al client remoto Ago 24 11:31:11 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Assegnato indirizzo IP privato 192.168.1.100 all'utente remoto Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash vuoto Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, constructct_cfg_set: dominio predefinito = jyoungta-	

group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network-list value split default-domain value jyoungta-labdomain.cisco.com	labdomain.cisco.com Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Client Browser Proxy Attributes! Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Browser Proxy impostato su No-Modify (Nessuna modifica). I dati proxy del browser NON verranno inclusi nella risposta mode-cfg Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Send Cisco Smartcard Removal Disconnect enable!! Ago 24 11:31:11 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash qm	
Invia risposta mode-config.	24 ago 11:31:11 [IKEv1]IP = 64.102.156.87, messaggio di INVIO IKE_DECODE (msgid=84b4b653) con payload: HDR + HASH (8) + ATTR (14) + NONE (0) lunghezza totale: 215	
	========== Risposta Mode-config ==========>	
	5711:28:38.63808/24/12Sev=Info/5IKE/0x6300002F Pacchetto ISAKMP ricevuto: peer = 64.102.156.88 57211:28:38.63808/24/12Sev=Info/4IKE/0x63000014 RICEZIONE DI <<< ISAKMP OAK TRANS *(HASH, ATTR) DA 64.102.156.88 57311:28:38.63908/24/12Sev=Decode/11IKE/0x63000001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Tipo di cambio:Transazione Flag:(Crittografia) MessageID(Hex):84B4B653 Lunghezza: 220 Hash payload Payload successivo: Attributi Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): 6DE2E70ACF6B1858846BC62E590C00A66745D14D Attributi payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 163 Tipo: ISAKMP_CFG_REPLY Reserved: 00 Identificativo: 0000 Indirizzo IPv4: 192.168.1.100 Netmask IPv4: 255.255.255.0 DNS IPv4: 192.168.1.99	Ricevere i valori dei parametri mode-config dal server.

	Estensione Cisco: Salva PWD: No Estensione Cisco: Nome dominio predefinito: jyoungta-labdomain.cisco.com Estensione Cisco: Esegui PFS: No Versione applicazione: Cisco Systems, Inc ASA5505 versione 8.4(4)1 costruita dai costruttori su Thu 14-Jun-12 11:20 Estensione Cisco: Disconnessione rimozione smart card: Sì		
La fase 1 viene completata sul server. Avviare il processo in modalità rapida (QM).	24 ago 11:31:13 [DECODIFICA IKEv1]IP = 64.102.156.87, QM iniziale del risponditore IKE: id messaggio = 0e83792e 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Elaborazione in modalità rapida ritardata, DSID Cert/Trans Exch/RM in corso 24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Gratuitous ARP inviato per 192.168.1.100 Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87,	57411:28:38.63908/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_RCVD_MSG 57511:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Attributo = INTERNAL_IPV4_ADDRESS:, valore = 192.168.1.100 57611:28:38.63908/24/12Sev=Info/5IKE/0x63000010 MODE_CFG_REPLY: Attributo = INTERNAL_IPV4_NETMASK:, valore = 255.255.255.0 57711:28:38.63908/24/12Sev= Info/5IKE/0x63000010 MODE_CFG_REPLY: Attributo = INTERNAL_IPV4_DNS(1): , valore = 192.168.1.99 57811:28:38.63908/24/12Sev=Info/5IKE/0x6300000D MODE_CFG_REPLY: Attributo = MODECFG_UNITY_SAVEPWD: , valore = 0x00000000 57911:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Attributo = DOMINIO_UNITÀ_MODECFG: , valore = jyoungta-labdomain.cisco.com 58011:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attributo = MODECFG_UNITY_PFS: , valore = 0x00000000 5811:28:38.63908/24/12Sev=Info/5IKE/0x6300000E MODE_CFG_REPLY: Attributo = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5505 versione 8.4(4)1 compilato da Costruttori su Thu 14-Jun-12 11:20	Elaborare i parametri e configurarsi di conseguenza.

	Riprendi elaborazione in modalità rapida, DSID Cert/Trans Exch/RM completato 24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, FASE 1 COMPLETATA	58211:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attributo = MODECFG_UNITY_SMARTCARD_REMOVAL_DISCONNECT: , valore = 0x00000001 58311:28:38.63908/24/12Sev= Info/5IKE/0x6300000D MODE_CFG_REPLY: Attributo = Ricevuto e utilizzo di NAT-T numero porta , valore = 0x00001194 58411:28:39.36708/24/12Sev= Debug/9IKE/0x63000093 Il valore del parametro INI EnableDNSRedirection è 1 58511:28:39.36708/24/12Sev= Debug/7IKE/0x63000076 NAV Trace->TM:MsgID=84B4B653CurState: TM_MODECFG_DONEEvent: EV_MODECFG_DONE_SUC	
Costruire e inviare DPD per il client.	24 ago 11:31:13 [IKEv1]IP = 64.102.156.87, tipo Keep-alive per questa connessione: DPD 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Avvio del timer di reimpostazione chiave P1: 82080 secondi. 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, invio messaggio di notifica Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash vuoto 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash qm Ago 24 11:31:13 [IKEv1]IP = 64.102.156.87, messaggio di INVIO IKE_DECODE (msgid=be8f7821) con payload: HDR + HASH (8) + NOTIFY (11) + NONE (0) lunghezza totale: 92	
	========== Rilevamento peer inattivi (DPD) ==========>		
	58811:28:39.79508/24/12Sev=Debug/7IKE/0x63000015 intf_data: lcl=0x0501A8C0, mask=0x00FFFFFF, bcast=0xFF01A8C0, bcast_vra=0xFF07070A 58911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=Info/4IKE/0x63000056 Richiesta chiave ricevuta dal driver: IP locale = 192.168.1.100, IP GW = 64.102.156.88, IP remoto =	Avviare QM, Fase 2. Costruire QM1. Questo processo include: - Hash - SA con tutte le proposte di fase 2 supportate dal client, tipo di tunnel e crittografia

	0.0.0.0 5911:28:39.79508/24/12Sev=Debug/7IKE/0x63000076 NAV Trace->SA:I_Cookie=D56197780D7BE3E5 R_Cookie=1B301D2DE710EDA0CurState: CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_INITIALEvent: INIZIATORE_EV 59311:28:39.79508/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: V_CHK_PFS 59411:28:39.79608/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_START_RETRY_TMR	- Nessuna - ID client - ID proxy
	59611:28:39.79608/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_SND_MSG1Event: EV_SND_MSG 59711:28:39.79608/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) a 64.102.156.88	Inviare QM1.
	<========== Messaggio in modalità rapida 1 (QM1) ==========	
Ricevere QM1.	Ago 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=e83792e) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) lunghezza totale: 1026	
Elaborare QM1. Configurazione pertinente: `crypto dynamic-map DYN 10 set transform-set TRA`	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, elaborazione payload hash 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, elaborazione del payload SA 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, elaborazione payload nonce Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, payload ID elaborazione Ago 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, ID_IPV4_ADDR ID ricevuto 192.168.1.100 Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Ricevuti dati host proxy remoto in ID Payload:Address 192.168.1.100, Protocol	

	0, Port 0 Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, payload ID elaborazione Ago 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, ID_IPV4_ADDR_SUBNET ID ricevuto—0.0.0—0.0.0 Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Ricevuti dati subnet proxy IP locale in ID Payload:Indirizzo 0.0.0.0, Maschera 0.0.0, Protocollo 0, Porta 0 Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, QM IsRekeyed old sa non trovato da addr 24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Controllo mappa crittografica statica, Controllo mappa = out-map, seq = 10... Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Controllo mappa crittografica statica ignorato: Voce mappa crittografica incompleta. 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, selezione solo delle modalità UDP-Encapsulated-Tunnel e UDP-Encapsulated-Transport definite da NAT-Traversal 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, selezione solo delle modalità UDP-Encapsulated-Tunnel e UDP-Encapsulated-Transport definite da NAT-Traversal Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE Remote Peer configurato per la mappa crittografica: out-dyn-map 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, elaborazione payload SA IPSec	
Costruire QM2. Configurazione pertinente: `tunnel-group EZ type` **`remote-access`** *`! (tunnel type ra = tunnel type remote-access)`* `crypto ipsec transform-set TRA` **`esp-aes esp-sha-hmac`** `crypto ipsec security-association` **`lifetime seconds 28800`** `crypto ipsec security-association lifetime`	ago 24 11:31:13 [IKEv1 DEBUG]Gruppo = ipsec, Nome utente = utente1, IP = 64.102.156.87, Proposta SA IPSec n. 12, Trasforma n. 1 accettabileCorrisponde alla voce SA IPSec globale n. 10 Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE: richiesta SPI! IPSEC Nuova associazione di sicurezza embrionale creata @ 0xcfdffc90, SCB 0xCFDFFB58, Direzione: in entrata SPI: 0x9E18ACB2 ID sessione: 0x00138000 Numero VPIF: 0x00000004 Tipo di tunnel: ra Protocollo: esp Durata: 240 secondi Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE ha	

kilobytes 4608000 **crypto dynamic-map DYN 10 set transform-set TRA** crypto map MAP 65000 ipsec-isakmp dynamic DYN crypto map MAP interface outside	ottenuto un SPI dal motore della chiave: SPI = 0x9e18acb2 Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, oakley costruendo modalità rapida Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash vuoto 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload SA IPSec 24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, ignorando la durata della rigenerazione delle chiavi IPSec dell'iniziatore da 2147483 a 86400 secondi Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload nonce IPSec Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione ID proxy Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, ID proxy di trasmissione: Host remoto: 192.168.1.100Protocollo 0Porta 0 Subnet locale:0.0.0.0maschera 0.0.0 Protocollo 0porta 0 Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Invio della notifica della durata del RESPONDER all'iniziatore 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, costruzione del payload hash qm	
Inviare QM2.	Ago 24 11:31:13 [IKEv1 DECODE]Group = ipsec, Username = user1, IP = 64.102.156.87, Il risponditore IKE invia il secondo pacchetto QM: id messaggio = 0e83792e Ago 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE SENDING Message (msgid=e83792e) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) lunghezza totale: 184	
	========== Messaggio in modalità rapida 2 (QM2) ==========>	
	60811:28:39.96208/24/12Sev=Info/4IKE/0x63000014 RICEZIONE <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) da 64.102.156.88	Ricevere QM2.
	60911:28:39.96408/24/12Sev=Decode/11IKE/0x63000001 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0	Elabora QM2. Il payload decrittografato mostra le proposte scelte.

	Payload successivo:Hash Ver (Hex):10 Exchange, Tipo:Modalità Rapida Flag:(Crittografia) MessageID(Hex):E83792E Lunghezza: 188 Hash payload Payload successivo: Associazione di protezione Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): CABF38A62C9B88D1691E81F3857D6189534B2EC0 Associazione di sicurezza payload Payload successivo: Nonce Reserved: 00 Lunghezza payload: 52 DOI: IPSec Situazione: (SIT_IDENTITY_ONLY) Proposta payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 40 Proposta n.: 1 ID protocollo: PROTO_IPSEC_ESP Dimensione SPI: 4 N. di trasformazioni: 1 SPI: 9E18ACB2 Trasformazione payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 28 Trasformazione n.: 1 ID trasformazione: ESP_3DES Riservato2: 0000 Tipo di vita: Secondi Durata (Esadecimale): 0020C49B Modalità incapsulamento: Tunnel UDP Algoritmo di autenticazione: SHA1 Nonce payload Payload successivo: Identificazione Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): 3A079B75DA512473706F235EA3FCA61F1D15D4CD Identificazione payload Payload successivo: Identificazione Reserved: 00 Lunghezza payload: 12 Tipo ID: Indirizzo IPv4 ID protocollo (UDP/TCP, ecc.): 0 Port: 0	

	ID &due punti; 192.168.1.100 Identificazione payload Payload successivo: Notifica Reserved: 00 Lunghezza payload: 16 Tipo ID: Subnet IPv4 ID protocollo (UDP/TCP, ecc.): 0 Port: 0 ID &due punti; 0.0.0.0/0.0.0.0 Notifica payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 28 DOI: IPSec ID protocollo: PROTO_IPSEC_ESP Dimensione spi: 4 Tipo di notifica: STATUS_RESP_LIFETIME SPI: 9E18ACB2 &Due punti dati; Tipo di vita: Secondi Durata (Esadecimale): 00015180	
	6101:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 6111:28:39.96508/24/12Sev=Info/5IKE/0x63000045 Il valore della notifica RESPONDER-LIFETIME è 86400 secondi 61211:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6 Traccia NAV->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: V_CHK_PFS 61311:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6	Elaborare QM2.
	Traccia NAV->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event: EV_BLD_MSG 61411:28:39.96508/24/12Sev=Debug/7IKE/0x6300007 6 Intestazione ISAKMP COOKIE iniziatore:D56197780D7BE3E5 COOKIE del risponditore:1B301D2DE710EDA0 Payload successivo:Hash Ver (Hex):10 Exchange, Tipo:Modalità Rapida Flag:(Crittografia) MessageID(Hex):E83792E Lunghezza:52 Hash payload Payload successivo: Nessuna Reserved: 00 Lunghezza payload: 24 Dati (Esadecimali): CDDC20D91EB4B568C826D6A5770A5CF020141236	Costruire QM3. Payload decriptato per QM3 mostrato di seguito. Questo processo include hash.

	61511:28:39.96508/24/12Sev=Debug/7IKE/0x63000076 Traccia NAV->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 61611:28:39.96508/24/12Sev=Info/4IKE/0x63000013 INVIO >>> ISAKMP OAK QM *(HASH) a 64.102.156.88	Inviare QM3. Il client è pronto per la crittografia e la decrittografia.
	<========== Messaggio 3 in modalità rapida (QM3) ==========	
Ricevere QM3.	Ago 24 11:31:13 [IKEv1]IP = 64.102.156.87, IKE_DECODE RECEIVED Message (msgid=e83792e) con payload: HDR + HASH (8) + NONE (0) lunghezza totale : 52	

Elaborare QM3. Creare gli indici dei parametri di sicurezza (SPI) in entrata e in uscita. Aggiungere la route statica per l'host. Configurazione pertinente:
 	
`crypto ipsec transform-set TRA esp-aes esp-sha-hmac`
`crypto ipsec security-association lifetime seconds 28800`
`crypto ipsec security-association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set transform-set TRA`
`crypto dynamic-map DYN 10` **`set reverse-route`**
	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, elaborazione payload hash
	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, caricamento di tutte le SA IPSEC
	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generazione della chiave in modalità rapida!
	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, regola di crittografia NP per la ricerca di ACL corrispondenti out-dyn-map della mappa crittografica 10 Sconosciuto: restituito
	cs_id=cc107410; rule=00000000
	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Generazione della chiave in modalità rapida!
	IPSEC Nuova SA embrionale creata @ 0xccc9ed60, SCB 0xCF7F59E0,
	Direzione: in uscita
	SPI: 0xC055290A
	ID sessione: 0x00138000
	Numero VPIF: 0x00000004
	Tipo di tunnel: ra
	Protocollo: esp
	Durata: 240 secondi
	IPSEC Aggiornamento OBSA host completato, SPI 0xC055290A
	IPSEC Creazione del contesto VPN in uscita, SPI 0xC055290A
	Flag: 0x00000025
	SA: 0xccc9ed60
	SPI: 0xC055290A
	MTU: 1500 byte
	VCID: 0x00000000
	Peer: 0x00000000
	SCB 0xA5922B6B
	Canale: 0xc82afb60
	IPSEC Contesto VPN in uscita completato, SPI	

	0xC055290A Handle VPN: 0x0015909c IPSEC Nuova regola di crittografia in uscita, SPI 0xC055290A Indirizzo origine: 0.0.0.0 Maschera origine: 0.0.0.0 Indirizzo destinazione: 192.168.1.100 Maschera distr.: 255.255.255.255 Porte Src Superiore: 0 Inferiore: 0 Operazione: ignorare Porte Dst Superiore: 0 Inferiore: 0 Operazione: ignorare Protocollo: 0 Protocollo di utilizzo: falso SPI: 0x00000000 Usa SPI: falso IPSEC Regola di crittografia in uscita completata, SPI 0xC055290A ID regola: 0xcb47a710 IPSEC Nuova regola di autorizzazione in uscita, SPI 0xC055290A Indirizzo origine: 64.102.156.88 Maschera origine: 255.255.255.255 Indirizzo destinazione: 64.102.156.87 Maschera distr.: 255.255.255.255 Porte Src Superiore: 4500 Inferiore: 4500 Operazione: uguale Porte Dst Superiore: 58506 Inferiore: 58506 Operazione: uguale Protocollo: 17 Protocollo di utilizzo: vero SPI: 0x00000000 Usa SPI: falso IPSEC Regola autorizzazioni in uscita completata, SPI 0xC055290A ID regola: 0xcdf3cfa0 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, regola di crittografia NP per la ricerca di ACL corrispondenti out-dyn-map della mappa crittografica 10 Sconosciuto: restituito cs_id=cc107410; rule=00000000 24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Negoziazione della sicurezza completata per l'utente (user1)Responder,	

	Inbound SPI = 0x9e18acb2, In uscita SPI = 0xc055290a 24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, IKE ricevuto messaggio KEY_ADD per SA: SPI = 0xc055290a IPSEC Aggiornamento IBSA host completato, SPI 0x9E18ACB2 IPSEC Creazione del contesto VPN in ingresso, SPI 0x9E18ACB2 Flag: 0x00000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 MTU: 0 byte VCID: 0x00000000 Peer: 0x0015909C SCB 0xA5672481 Canale: 0xc82afb60 IPSEC Contesto VPN in ingresso completato, SPI 0x9E18ACB2 Handle VPN: 0x0016219c IPSEC Aggiornamento del contesto VPN in uscita 0x0015909C, SPI 0xC05290A Flag: 0x00000025 SA: 0xccc9ed60 SPI: 0xC055290A MTU: 1500 byte VCID: 0x00000000 Peer: 0x0016219C SCB 0xA5922B6B Canale: 0xc82afb60 IPSEC Contesto VPN in uscita completato, SPI 0xC055290A Handle VPN: 0x0015909c IPSEC Regola interna in uscita completata, SPI 0xC055290A ID regola: 0xcb47a710 IPSEC Regola SPD esterno in uscita completata, SPI 0xC055290A ID regola: 0xcdf3cfa0 IPSEC Nuova regola di flusso del tunnel in entrata, SPI 0x9E18ACB2 Indirizzo origine: 192.168.1.100 Maschera origine: 255.255.255.255 Indirizzo destinazione: 0.0.0.0 Maschera distr.: 0.0.0.0 Porte Src Superiore: 0 Inferiore: 0 Operazione: ignorare Porte Dst Superiore: 0 Inferiore: 0	

	Operazione: ignorare Protocollo: 0 Protocollo di utilizzo: falso SPI: 0x00000000 Usa SPI: falso IPSEC Regola di flusso del tunnel in entrata completata. SPI 0x9E18ACB2 ID regola: 0xcdf15270 IPSEC Nuova regola di decrittografia in ingresso, SPI 0x9E18ACB2 Indirizzo origine: 64.102.156.87 Maschera origine: 255.255.255.255 Indirizzo destinazione: 64.102.156.88 Maschera distr.: 255.255.255.255 Porte Src Superiore: 58506 Inferiore: 58506 Operazione: uguale Porte Dst Superiore: 4500 Inferiore: 4500 Operazione: uguale Protocollo: 17 Protocollo di utilizzo: vero SPI: 0x00000000 Usa SPI: falso IPSEC Regola di decrittografia in ingresso completata. SPI 0x9E18ACB2 ID regola: 0xce03c2f8 IPSEC Nuova regola autorizzazioni in ingresso, SPI 0x9E18ACB2 Indirizzo origine: 64.102.156.87 Maschera origine: 255.255.255.255 Indirizzo destinazione: 64.102.156.88 Maschera distr.: 255.255.255.255 Porte Src Superiore: 58506 Inferiore: 58506 Operazione: uguale Porte Dst Superiore: 4500 Inferiore: 4500 Operazione: uguale Protocollo: 17 Protocollo di utilizzo: vero SPI: 0x00000000 Usa SPI: falso IPSEC Regola autorizzazioni in ingresso completata, SPI 0x9E18ACB2 ID regola: 0xcf6f58c0 Ago 24 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Pitcher: ricevuto KEY_UPDATE, spi 0x9e18acb2	

	24 ago 11:31:13 [IKEv1 DEBUG]Group = ipsec, Username = user1, IP = 64.102.156.87, Avvio del timer di reimpostazione chiave P2: 82080 secondi. Ago 24 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, Aggiunta della route statica per l'indirizzo del client: 192.168.1.100	
Fase 2 completata. Entrambe le parti stanno crittografando e decrittografando ora.	24 ago 11:31:13 [IKEv1]Group = ipsec, Username = user1, IP = 64.102.156.87, PHASE 2 COMPLETED (msgid=0e83792e)	
Per i client hardware, viene ricevuto un ulteriore messaggio in cui il client invia informazioni su se stesso. Se si osserva attentamente, è necessario individuare il nome host del client EzVPN, il software in esecuzione sul client e la posizione e il nome del software	24 ago 11:31:13 [IKEv1]: IP = 10.48.66.23, IKE_DECODE RECEIVED Message (msgid=91facca9) con payload: HDR + HASH (8) + NOTIFY (11) + NONE (0) lunghezza totale: 184 ago 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, elaborazione payload hash ago 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, elaborazione del payload di notifica ago 24 11:31:13 [IKEv1 DECODE]: DESCRITTORE OBSOLETO - INDICE 1 ago 24 11:31:13 [IKEv1 DECODE]: 0000: 00000000 7534000B 62736E73 2D383731 ....u4.**bsns-871** 0010: 2D332E75 32000943 6973636F 20383731 **-3**.u2.**Cisco 871** 0020: 7535000B 46484B30 3934341 32513675 u5.FHK094412Q6u 0030: 36000932 32383538 39353638 75390009 6,228589568u9. 0040: 31343532 3136331 32753300 2B666C61 145216312u3.+**fla** 0050: 73683A63 3837302D 6164769 70736572 **sh:c870-advisor** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.bin** ago 24 11:31:13 [IKEv1 DEBUG]: Group = EZ, Username = cisco, IP = 10.48.66.23, Hash PSK di elaborazione 24 ago 11:31:13 [IKEv1]: Gruppo = EZ, Nome utente = cisco, IP = 192.168.1.100, Dimensioni hash PSK incoerenti ago 24 11:31:13 [IKEv1 DEBUG]: Gruppo = EZ, Nome utente = cisco, IP = 10.48.66.23, Verifica hash PSK non riuscita.	

Verifica tunnel

ISAKMP

L'output del comando **sh cry isa det** è:

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPSec

Poiché per attivare il tunnel viene utilizzato il protocollo Internet Control Message Protocol (ICMP), è attiva solo un'associazione di protezione IPsec. Il protocollo 1 è ICMP. Si noti che i valori SPI sono diversi da quelli negoziati nei debug. Questo è, infatti, lo stesso tunnel dopo il reindirizzamento della fase 2.

L'output del comando **sh crypto ipsec sa** è:

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #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: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
```

```
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003F
outbound esp sas:
spi: 0xC4B9A77C (3300501372)
transform: esp-aes esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 425984, crypto-map: DYN
sa timing: remaining key lifetime (sec): 28714
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Informazioni correlate

- Articolo di Wikipedia su IPsec
- Risoluzione dei problemi IPSec: descrizione e uso dei comandi di debug
- Documentazione e supporto tecnico – Cisco Systems