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

Sommario

Introduzione

In questo documento vengono descritti i debug su Adaptive Security Appliance (ASA) quando si usano sia la modalità principale sia la chiave precondivisa (PSK). Viene inoltre descritta la conversione di alcune righe di debug nella configurazione.

Gli argomenti non trattati in questo documento includono il traffico di passaggio dopo la definizione del tunnel e i concetti base di IPsec o IKE (Internet Key Exchange).

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti.

- PSK
- IKE

Componenti usati

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

- Cisco ASA 9.3.2
- Router con Cisco IOS® 12.4T

Problema principale

I debug IKE e IPsec a volte sono crittografati, ma è possibile utilizzarli per capire dove si è verificato un problema di creazione del tunnel VPN IPsec.

Scenario

La modalità principale viene in genere utilizzata tra tunnel da LAN a LAN oppure, nel caso dell'accesso remoto (EzVPN), quando i certificati vengono utilizzati per l'autenticazione.

I debug vengono eseguiti da due appliance ASA con software versione 9.3.2. I due dispositivi formeranno un tunnel LAN-LAN.

Vengono descritti due scenari principali:

- ASA come iniziatore per IKE
- ASA che risponde a IKE

Comandi di debug usati

debug crypto ikev1 127

debug crypto ipsec 127

Configurazione ASA

Configurazione IPSec:

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

Configurazione IP:

```
ciscoasa#

show ip
```

```
System IP Addresses:
Interface                  Name      IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
Current IP Addresses:
Interface                  Name       IP address      Subnet mask      Method
GigabitEthernet0/0       inside     192.168.1.1    255.255.255.0   manual
GigabitEthernet0/1       outside   10.0.0.1          255.255.255.0   manual
```

Configurazione NAT:

```
object network INSIDE-RANGE
 subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
 subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

Debug

Descrizione messaggio iniziatore	Debug	Descrizione messaggio risponditore
Inizio scambio modalità principale; non sono stati condivisi criteri e i peer sono ancora in MM_NO_STATE. Come iniziatore, l'ASA inizia a costruire il payload.	[DEBUG IKEv1]: Caraffa: ricevuto messaggio di acquisizione chiave, spi 0x0 IPSEC(crypto_map_check)-3: Ricerca corrispondenza mappa crittografica per 5 tuple: Port=1, saddr=192.168.1.2, sport=2816, daddr=192.168.2.1, dport=2816 IPSEC(crypto_map_check)-3: Controllo della mappa crittografica MAP 10: corrispondente. [IKEv1]: IP = 10.0.0.2, iniziatore IKE: Nuova fase 1, Intf inside, peer IKE 10.0.0.2 indirizzo proxy locale 192.168.1.0, indirizzo proxy remoto 192.168.2.0, mappa crittografica (MAP) [DEBUG IKEv1]: IP = 10.0.0.2, creazione del **payload SA ISAKMP**	
Costruzione MM1 Questo processo èInclude iProposta iniziale per IKE e sfornitori NAT-T supportati.	[DEBUG IKEv1]: IP = 10.0.0.2, costruzione di NAT-Traversal VID ver 02 payload [DEBUG IKEv1]: IP = 10.0.0.2, costruzione di NAT-Traversal VID ver 03 payload [DEBUG IKEv1]: IP = 10.0.0.2, costruzione del VID NAT-Traversal rispetto al payload RFC [DEBUG IKEv1]: IP = 10.0.0.2, creazione del VID di frammentazione + payload di funzionalità estese	
Inviare MM1.	[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + SA (1) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 168	
	========== ====>	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + SA (1) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 164	MM1 ricevuto dall'iniziatore.
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione del payload SA	Elaborare MM1.
	[DEBUG IKEv1]: IP = 10.0.0.2, la proposta Oakley è accettabile	Inizia il confronto tra
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID	le policy
	[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto VID RFC NAT-Traversal	ISAKMP/IKE.
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID	Il peer remoto
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID	annuncia di poter
	[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto NAT-Traversal over 03 VID	utilizzare NAT-T.
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID	Configurazione
	[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto NAT-Traversal over 02 VID	correlata:
	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload SA IKE	*crypto isakmp policy*
	[DEBUG IKEv1]: IP = 10.0.0.2, proposta SA IKE n. 1, trasformazione n. 1	*10*

	accettabile Corrisponde alla voce IKE globale n. 2	*pre-condivisione di autenticazione* *crittografia 3des* *hash sha* *gruppo 2* *life 86400*
	[DEBUG IKEv1]: IP = 10.0.0.2, costruzione del payload SA ISAKMP [DEBUG IKEv1]: IP = 10.0.0.2, costruzione di NAT-Traversal VID ver 02 payload [DEBUG IKEv1]: IP = 10.0.0.2, creazione del VID di frammentazione + payload di funzionalità estese	Costruzione MM2 In questo messaggio il risponditore seleziona le impostazioni dei criteri isakmp da utilizzare. Inoltre, annuncia le versioni NAT-T che può utilizzare.
	[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE(0) lunghezza totale: 128	Invia MM2.
	<==========MM2==========	
MM2 ricevuto da responder.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + SA (1) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 104	
Elaborazione MM2.	[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione del payload SA [DEBUG IKEv1]: IP = 10.0.0.2, la proposta Oakley è accettabile [DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID [DEBUG IKEv1]: IP = 10.0.0.2, ricevuto VID RFC NAT-Traversal	
Costruire MM3. Questo processo èIncludepayload di rilevamento NAT, Diffie- Hellman (DH) e Supporto DPD.	Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload della chiave Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload nonce Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload VID di Cisco Unity Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, costruzione del payload VID Xauth V6 Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, Invia IOS VID Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload ID fornitore IOS di spoofing ASA (versione: 1.0.0, funzionalità: 20000001) Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, costruzione del payload VID Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, inviare il VID GW Altiga/Cisco VPN3000/Cisco ASA Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload di individuazione NAT Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, creazione del payload di individuazione NAT Nov 30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT	(i)nitator include g, p e A per rispondere),
Invia MM3.	[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) lunghezza totale: 304	
	========== =>	
	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) lunghezza totale: 284	MM3 ricevuto dall'iniziatore.
	[DEBUG IKEv1]: IP = 10.0.0.2, payload chiave di elaborazione [DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload ISA_KE [DEBUG IKEv1]: IP = 10.0.0.2, elaborazione del payload nonce [DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID	Elaborazione di MM3. Da payload NAT-D il risponditore è in grado di determinare

[DEBUG IKEv1]: IP = 10.0.0.2, DPD VID ricevuto
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload ID fornitore IOS/PIX (versione: 1.0.0, funzionalità: 00000f6f)
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto Xauth V6 VID
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload NAT-Discovery
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload NAT-Discovery
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload della chiave
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload nonce
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload VID di Cisco Unity
[DEBUG IKEv1]: IP = 10.0.0.2, costruzione del payload VID xauth V6
[DEBUG IKEv1]: IP = 10.0.0.2, Invia IOS VID
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload ID fornitore IOS di spoofing ASA (versione: 1.0.0, funzionalità: 20000001)
[DEBUG IKEv1]: IP = 10.0.0.2, costruzione del payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, Invio di Altiga/Cisco VPN3000/Cisco ASA GW VID
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload di individuazione NAT
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT
[DEBUG IKEv1]: IP = 10.0.0.2, creazione del payload di individuazione NAT
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT

se l'iniziatore è dietro NAT e se il responder è dietro NAT.
Dal DH KE, il risponditore del payload ottiene i valori di p, g e A.

Costruire MM4. Questo processo èInclude payload di rilevamento NAT, DH KE rIl risponder genera "B" e "s" (restituisce "B" all'iniziatore), e DPD VIDEO

[IKEv1]: IP = 10.0.0.2, connessione terminata sul gruppo di tunnel 10.0.0.2
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione delle chiavi per il risponditore in corso...

Il peer viene associato al gruppo di tunnel L2L 10.0.0.2 e le chiavi di crittografia e hash vengono generate dalla "s" sopra riportata e dalla chiave già condivisa.

[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) lunghezza totale: 304

Invia MM4.

<==========
======

MM4 ricevuto dal risponditore.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) lunghezza totale: 304

Elabora MM4.
Dai payload NAT-D, l'iniziatore è ora in grado di determinare se il l'iniziatore è dietro NAT e se il responder è dietro NAT.

[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione come payload
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload ISA_KE
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione del payload nonce
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto VID client Cisco Unity
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, DPD VID ricevuto
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload ID fornitore IOS/PIX (versione: 1.0.0, funzionalità: 00000f7f)
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload VID
[DEBUG IKEv1]: IP = 10.0.0.2, ricevuto Xauth V6 VID
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload NAT-Discovery
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione payload NAT-Discovery
[DEBUG IKEv1]: IP = 10.0.0.2, elaborazione dell'hash di rilevamento NAT

Dal DH KE, iL'iniziatore riceve "B" e può ora generare "s".

[IKEv1]: IP = 10.0.0.2, connessione terminata sul gruppo di tunnel 10.0.0.2
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione delle chiavi per l'iniziatore in corso...

Il peer è associato al gruppo di tunnel L2L 10.0.0.2 e l'iniziatore genera chiavi di

crittografia e hash utilizzando "s" sopra e la chiave precondivisa.			
	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, creazione payload ID [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash		
Costruire MM5. Configurazione correlata: crypto isakmp identity auto	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Hash di calcolo per ISAKMP [DEBUG IKEv1]: IP = 10.0.0.2, Costruzione del payload keep-alive IOS: proposta=32767/32767 sec. [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload dpd vid		
Invio MM5	[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 96		
	========== ===>		
Responder non è dietro alcun NAT. NAT-T non richiesto.	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Stato rilevamento NAT automatico: L'estremità remota NON è dietro un dispositivo NAT Questa estremità NON è dietro un dispositivo NAT	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + ID (5) + HASH (8) + NONE (0) lunghezza totale : 64	MM5 ricevuto dall'iniziatore. Questo processo èInclude ridentità peer remota (ID) e catterraggio della connessione su un particolare gruppo di tunnel.
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione	Elaborare MM5. L'autenticazione con chiavi già condivise inizia ora. L'autenticazione viene eseguita su entrambi i peer; verranno pertanto visualizzati due set di processi di autenticazione corrispondenti. Configurazione correlata: tunnel group 10.0.0.2 tipo ipsec-l2l No NAT-T richiesto in questo caso.
		[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID ricevuto 10.0.0.2	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload hash	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Hash di calcolo per ISAKMP	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione del payload di notifica	
		[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2,NAT automatico	
		[IKEv1]: IP = 10.0.0.2, connessione terminata sul gruppo di tunnel 10.0.0.2	
		Stato rilevamento: L'estremità remota NON è dietro un dispositivo NAT	
		Questa estremità NON è dietro un dispositivo NAT	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, creazione payload ID	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash	Costruire MM6. Invia identità include i tempi di rigenerazione delle chiavi avviati e l'identità inviata al peer remoto.
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Hash di calcolo per ISAKMP	
		[DEBUG IKEv1]: IP = 10.0.0.2, Costruzione del payload keep-alive IOS: proposta=32767/32767 sec.	
		[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload dpd vid	
		[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=0) con payload: HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + FORNITORE (13) + NESSUNO (0) lunghezza totale: 96	Invia MM6.
		<==========	
MM6 ricevuto dal risponditore.	[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=0) con payload: HDR + ID (5) + HASH (8) + NONE (0) lunghezza totale : 64	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, FASE 1 COMPLETATA [IKEv1]: IP = 10.0.0.2, tipo Keep-alive per questa connessione: DPD [DEBUG IKEv1]: Gruppo = 10.0.0.2,	Fase 1 completata. Avviare il timer di reimpostazione chiavi isakmp. Configurazione

		correlata: crypto isakmp policy 10 pre-condivisione di autenticazione crittografia 3des hash sha gruppo 2 life 86400 cisco asa# sh esegui tutte le mappe crittografiche crypto isakmp identity auto
	IP = 10.0.0.2, Avvio del timer di reimpostazione chiave P1: 64800 secondi.	
Elabora MM6. Questo processo èInclude ridentità remota inviata da peer e fDecisione finale relativa al gruppo di tunnel da selezionare.	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione [DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID ricevuto 10.0.0.2 [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload hash [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Hash di calcolo per ISAKMP [IKEv1]: IP = 10.0.0.2, connessione terminata sul gruppo di tunnel 10.0.0.2 [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Oakley inizia modalità rapida [DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, QM iniziale iniziatore IKE: id messaggio = 7b80c2b0	
Fase 1 completata. Avviare il timer di reimpostazione chiavi ISAKMP.		
C correlataConfigurazione: tunnel group 10.0.0.2 tipo ipsec-l2l gruppo di tunnel 10.0.0.2 ipsec-attributes cisco pre-shared-key	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, FASE 1 COMPLETATA [IKEv1]: IP = 10.0.0.2, tipo Keep-alive per questa connessione: DPD La DPD è stata negoziata ed è stata completata la fase 1. [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Avvio del timer di reimpostazione chiave P1: 82080 secondi.	
Inizia la fase 2 (modalità rapida).	IPSEC Nuova SA embrionale creata @ 0x53FC3C00, SCB 0x53F90A00 Direzione: in entrata SPI: 0xFD2D851F ID sessione: 0x00006000 Numero VPIF: 0x00000003 Tipo di tunnel: l2l Protocollo: esp Durata: 240 secondi	
Costruire QM1. Questo processo include ID proxy e IPsec politiche. Configurazione correlata: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac access-list VPN	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, IKE ha ottenuto SPI dal motore della chiave: SPI = 0xfd2d851f [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, modalità rapida di costruzione oakley [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash vuoto [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload SA IPSec [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload nonce IPSec [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione ID proxy	

	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID proxy di trasmissione: Subnet locale: Maschera 192.168.1.0 Maschera 255.255.255.0 Protocollo 1 Porta 0	
extended allow icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0	Subnet remota: 192.168.2.0 Maschera 255.255.255.0 Protocollo 1 Porta 0 Invio della subnet locale (192.168.1.0/24) e della subnet remota prevista (192.168.2.0/24) in corso [DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Invio del contatto iniziale da parte dell'iniziatore IKE [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash qm [DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Iniziatore IKE che invia il primo pacchetto QM: id messaggio = 7b80c2b0	
Invio QM1	[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) lunghezza totale: 200 ==========QM1==========>	
	[DECODIFICA IKEv1]: IP = 10.0.0.2, QM iniziale del risponditore IKE: messaggio id = 52481cf5 [IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=52481cf5) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) lunghezza totale: 172	QM1 ricevuto dall'iniziatore. Il risponditore inizia la fase 2 (QM).
		Elaborare QM1. Questo processo confronta i proxy remoti con quelli locali e seleziona IP accettabilesec policy.
	[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload hash [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload SA [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload nonce [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione	Configurazione correlata: crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac access-list VPN extended allow icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0 mappa crittografica MAP 10 corrispondente all'indirizzo VPN
	[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ricevuto—192.168.2.0—255.255.255.0[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Ricevuti dati subnet proxy IP remoto nel payload ID: Indirizzo 192.168.2.0, Maschera 255.255.255.0, Protocollo 1, Porta 0 [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione [DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ricevuto—192.168.1.0—255.255.255.0 [IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Ricevuti dati subnet proxy IP locale nel payload ID: Indirizzo 192.168.1.0, Maschera 255.255.255.0, Protocollo 1, Porta 0	Vengono ricevute le subnet remote e locali (192.168.2.0/24 e 192.168.1.0/24).
	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed old sa non trovato da addr	
	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, controllo mappa crittografica statica, controllo mappa = MAP, seq = 10... [IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, controllo mappa crittografica statica, mappa MAP, seq = 10 è una corrispondenza corretta	Trovata una voce di crittografia statica corrispondente.
	[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, peer remoto IKE configurato per	

la mappa crittografica: MAPPA
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione del payload SA IPSec
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, IPSec SA Proposta n. 1, Trasformazione n. 1 corrispondenza accettabile Corrispondenza globale SA IPSec voce n. 10
[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, IKE: richiesta SPI!
IPSEC Nuova SA embrionale creata @ 0x53FC3698, SCB 0x53FC2998
Direzione: in entrata
SPI: 0x1698CAC7
ID sessione: 0x00004000
Numero VPIF: 0x00000003
Tipo di tunnel: l2l
Protocollo: esp
Durata: 240 secondi
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, IKE ha ottenuto SPI dal motore della chiave: SPI = 0x1698cac7
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, modalità rapida di costruzione oakley
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash vuoto
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload SA IPSec
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload nonce IPSec
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione ID proxy
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID proxy di trasmissione:
Subnet remota: 192.168.2.0 Maschera 255.255.255.0 Protocollo 1 Porta 0
Subnet locale: Maschera 192.168.1.0 Maschera 255.255.255.0 Protocollo 1 Porta 0
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, costruzione del payload hash qm
[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, il risponditore IKE invia il secondo pacchetto QM: id messaggio = 52481cf5
[IKEv1]: IP = 10.0.0.2, messaggio di invio IKE_DECODE (msgid=52481cf5) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) lunghezza totale: 172

Costruire QM2. Questo processo èInclude cconferma delle identità proxy, del tipo di tunnel e di viene eseguita la verifica degli ACL di crittografia con mirroring.

Inviare QM2.

<=============================QM2==========================

QM2 ricevuto dal risponditore.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=7b80c2b0) con payload: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) lunghezza totale: 200
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload hash
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload SA
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload nonce

Elaborare QM2. In questo processo, rl'estremità remota invia i parametri e vengono selezionate le durate di fase 2 proposte più brevi.

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione
[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ricevuto—192.168.1.0—255.255.255.0
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, payload ID elaborazione
[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID ricevuto—192.168.2.0—255.255.255.0
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione del payload di notifica
[DECODIFICA IKEv1]: Di seguito è riportata la decodifica della durata del risponditore (outb SPI[4]lattributes):
[DECODIFICA IKEv1]: 0000: DDE50931 80010001 00020004 00000E10 ...1.....

[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, il risponditore impone la modifica della durata della rigenerazione delle chiavi IPSec da 2800 a 3600 secondi
in base alla risposta del peer, l'ASA sta modificando alcuni attributi IPSEC. In questo caso, l'intervallo di reimpostazione delle chiavi
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, caricamento di tutte le associazioni di protezione IPSEC
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione della chiave in modalità rapida!

Trovata la mappa crittografica "MAP" e la voce 10 corrispondenti e la relativa corrispondenza con la "VPN" dell'elenco degli accessi.

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, la regola di crittografia NP cerca la mappa crittografica MAP 10 corrispondente alla VPN ACL: restituito cs_id=53f11198; rule=53f11a90

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione della chiave in modalità rapida!
IPSEC Nuova SA embrionale creata @ 0x53FC3698,
SCB 0x53F910F0
Direzione: in uscita
SPI: 0xDDE50931
ID sessione: 0x00006000
Numero VPIF: 0x00000003
Tipo di tunnel: l2l
Protocollo: esp
Durata: 240 secondi
IPSEC Aggiornamento OBSA host completato, SPI 0xDDE50931
IPSEC Creazione del contesto VPN in uscita, SPI 0xDDE50931
Flag: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 byte
VCID: 0x00000000
Peer: 0x00000000
SCB: 0x01CF218F
Canale: 0x4C69CB80
IPSEC Contesto VPN in uscita completato, SPI 0xDDE50931
Handle VPN: 0x000161A4
IPSEC Nuova regola di crittografia in uscita, SPI 0xDDE50931
Indirizzo origine: 192.168.1.0
Maschera origine: 255.255.255.0
Indirizzo destinazione: 192.168.2.0
Dst mask: 255.255.255.0
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 1
Protocollo di utilizzo: vero
SPI: 0x00000000
Usa SPI: falso
IPSEC Regola di crittografia in uscita completata, SPI 0xDDE50931
ID regola: 0x53FC3AD8
IPSEC Nuova regola di autorizzazione in uscita, SPI 0xDDE50931
Indirizzo origine: 10.0.0.1
Maschera origine: 255.255.255.255
Indirizzo destinazione: 10.0.0.2
Dst mask: 255.255.255.255

L'accessorio ha generato gli SPI 0xfd2d851f e 0xdde50931 rispettivamente per il traffico in entrata e in uscita.

Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 50
Protocollo di utilizzo: vero
SPI: 0xDDE50931
Usa SPI: vero
IPSEC Regola autorizzazioni in uscita completata, SPI 0xDDE50931
ID regola: 0x53F91538
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, la regola di crittografia NP cerca la mappa crittografica MAP 10 corrispondente alla VPN ACL: restituito cs_id=53f11198; rule=53f11a90
[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, negoziazione della sicurezza completata per l'iniziatore gruppo LAN-LAN (10.0.0.2), SPI in entrata = 0xfd2d851f, SPI in uscita = 0xdde50931
IPSEC Aggiornamento IBSA host completato, SPI 0xFD2D851F
IPSEC Creazione del contesto VPN in ingresso, SPI 0xFD2D851F
Flag: 0x00000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: 0 byte
VCID: 0x00000000
Peer: 0x000161A4
SCB: 0x01CEA8EF
Canale: 0x4C69CB80
IPSEC Contesto VPN in ingresso completato, SPI 0xFD2D851F
Handle VPN: 0x00018BBC
IPSEC Aggiornamento del contesto VPN in uscita 0x000161A4, SPI 0xDDE50931
Flag: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500 byte
VCID: 0x00000000
Peer: 0x00018BBC
SCB: 0x01CF218F
Canale: 0x4C69CB80
IPSEC Contesto VPN in uscita completato, SPI 0xDDE50931
Handle VPN: 0x000161A4
IPSEC Regola interna in uscita completata, SPI 0xDDE50931
ID regola: 0x53FC3AD8
IPSEC Regola SPD esterno in uscita completata, SPI 0xDDE50931
ID regola: 0x53F91538
IPSEC Nuova regola flusso tunnel in ingresso, SPI 0xFD2D851F
Indirizzo origine: 192.168.2.0
Maschera origine: 255.255.255.0
Indirizzo destinazione: 192.168.1.0
Dst mask: 255.255.255.0
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 1
Protocollo di utilizzo: vero
SPI: 0x00000000

Costruire QM3. Conferma tutti gli SPI creati nel peer remoto.

Usa SPI: falso
IPSEC Regola di flusso del tunnel in entrata completata. SPI 0xFD2D851F
ID regola: 0x53F91970
IPSEC Nuova regola di decrittografia in ingresso, SPI 0xFD2D851F
Indirizzo origine: 10.0.0.2
Maschera origine: 255.255.255.255
Indirizzo destinazione: 10.0.0.1
Dst mask: 255.255.255.255
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 50
Protocollo di utilizzo: vero
SPI: 0xFD2D851F
Usa SPI: vero
IPSEC Regola di decrittografia in ingresso completata. SPI 0xFD2D851F
ID regola: 0x53F91A08
IPSEC Nuova regola permessi in ingresso, SPI 0xFD2D851F
Indirizzo origine: 10.0.0.2
Maschera origine: 255.255.255.255
Indirizzo destinazione: 10.0.0.1
Dst mask: 255.255.255.255
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 50
Protocollo di utilizzo: vero
SPI: 0xFD2D851F
Usa SPI: vero
IPSEC Regola autorizzazioni in ingresso completata, SPI 0xFD2D851F
ID regola: 0x53F91AA0

Inviare QM3.

[DECODIFICA IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Iniziatore IKE che invia il terzo pacchetto QM: id messaggio = 7b80c2b0

==========QM3==========>

[IKEv1]: IP = 10.0.0.2, IKE_DECODE SENDING Message (msgid=7b80c2b0) con payload: HDR + HASH (8) + NONE (0) lunghezza totale: 76

[IKEv1]: IP = 10.0.0.2, IKE_DECODE RECEIVED Message (msgid=52481cf5) con payload: HDR + HASH (8) + NONE (0) lunghezza totale : 52

QM3 ricevuto dall'iniziatore.

[DEBUG IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, IKE ha ricevuto un messaggio KEY_ADD per SA: SPI = 0xdde50931

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, lanciatore: ricevuto KEY_UPDATE, spi 0xfd2d851f

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Avvio del timer di reimpostazione chiave P2: 3.060 secondi.

[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETATA (msgid=7b80c2b0)

Fase 2 completata. L'iniziatore è ora pronto a crittografare e decrittografare i pacchetti utilizzando questi valori SPI.

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, elaborazione payload hash

Elaborare QM3. Le chiavi di crittografia vengono generate per le associazioni di

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, caricamento di tutte le associazioni di protezione IPSEC

[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione della

chiave in modalità rapida!
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, la regola di crittografia
NP cerca la mappa crittografica MAP 10 corrispondente alla VPN ACL:
restituito cs_id=53f11198; rule=53f11a90
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Generazione della
chiave in modalità rapida!
IPSEC Nuova SA embrionale creata @ 0x53F18B00,
SCB 0x53F8A1C0
Direzione: in uscita
SPI: 0xDB680406
ID sessione: 0x00004000
Numero VPIF: 0x00000003
Tipo di tunnel: l2l
Protocollo: esp
Durata: 240 secondi
IPSEC Aggiornamento OBSA host completato, SPI 0xDB680406
IPSEC Creazione del contesto VPN in uscita, SPI 0xDB680406
Flag: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 byte
VCID: 0x00000000
Peer: 0x00000000
SCB: 0x005E4849
Canale: 0x4C69CB80
IPSEC Contesto VPN in uscita completato, SPI 0xDB680406
Handle VPN: 0x0000E9B4
IPSEC Nuova regola di crittografia in uscita, SPI 0xDB680406
Indirizzo origine: 192.168.1.0
Maschera origine: 255.255.255.0
Indirizzo destinazione: 192.168.2.0
Dst mask: 255.255.255.0
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 1
Protocollo di utilizzo: vero
SPI: 0x00000000
Usa SPI: falso
IPSEC Regola di crittografia in uscita completata, SPI 0xDB680406
ID regola: 0x53F89160
IPSEC Nuova regola di autorizzazione in uscita, SPI 0xDB680406
Indirizzo origine: 10.0.0.1
Maschera origine: 255.255.255.255
Indirizzo destinazione: 10.0.0.2
Dst mask: 255.255.255.255
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 50
Protocollo di utilizzo: vero
SPI: 0xDB680406
Usa SPI: vero
IPSEC Regola autorizzazioni in uscita completata, SPI 0xDB680406

protezione dei dati. Durante questo processo, Gli SPI vengono impostati per consentire il passaggio del traffico.

ID regola: 0x53E47E88
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, la regola di crittografia NP cerca la mappa crittografica MAP 10 corrispondente alla VPN ACL: restituito cs_id=53f11198; rule=53f11a90
[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, negoziazione della sicurezza completata per il risponditore LAN-to-LAN (10.0.0.2), SPI in entrata = 0x1698cac7, SPI in uscita = 0xdb680406
[DEBUG IKEv1]: Group = 10.0.0.2, IP = 10.0.0.2, IKE ha ricevuto un messaggio KEY_ADD per SA: SPI = 0xdb680406
IPSEC Aggiornamento IBSA host completato, SPI 0x1698CAC7
IPSEC Creazione del contesto VPN in ingresso, SPI 0x1698CAC7
Flag: 0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: 0 byte
VCID: 0x00000000
Peer: 0x0000E9B4
SCB: 0x005DAE51
Canale: 0x4C69CB80
IPSEC Contesto VPN in ingresso completato, SPI 0x1698CAC7
Handle VPN: 0x00011A8C
IPSEC Aggiornamento del contesto VPN in uscita 0x0000E9B4, SPI 0xDB680406
Flag: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500 byte
VCID: 0x00000000
Peer: 0x00011A8C
SCB: 0x005E4849
Canale: 0x4C69CB80
IPSEC Contesto VPN in uscita completato, SPI 0xDB680406
Handle VPN: 0x0000E9B4
IPSEC Regola interna in uscita completata, SPI 0xDB680406
ID regola: 0x53F89160
IPSEC Regola SPD esterno in uscita completata, SPI 0xDB680406
ID regola: 0x53E47E88
IPSEC Nuova regola di flusso del tunnel in entrata, SPI 0x1698CAC7
Indirizzo origine: 192.168.2.0
Maschera origine: 255.255.255.0
Indirizzo destinazione: 192.168.1.0
Dst mask: 255.255.255.0
Porte Src
Superiore: 0
Inferiore: 0
Operazione: ignorare
Porte Dst
Superiore: 0
Inferiore: 0
Operazione: ignorare
Protocollo: 1
Protocollo di utilizzo: vero
SPI: 0x00000000
Usa SPI: falso
IPSEC Regola di flusso del tunnel in entrata completata, SPI 0x1698CAC7
ID regola: 0x53FC3E80
IPSEC Nuova regola di decrittografia in ingresso, SPI 0x1698CAC7
Indirizzo origine: 10.0.0.2
Maschera origine: 255.255.255.255
Indirizzo destinazione: 10.0.0.1
Dst mask: 255.255.255.255
Porte Src
Superiore: 0
Inferiore: 0

Gli SPI vengono assegnati alle associazioni di protezione dei dati.

Operazione: ignorare Porte Dst Superiore: 0 Inferiore: 0 Operazione: ignorare Protocollo: 50 Protocollo di utilizzo: vero SPI: 0x1698CAC7 Usa SPI: vero IPSEC Regola di decrittografia in ingresso completata, SPI 0x1698CAC7 ID regola: 0x53FC3F18 IPSEC Nuova regola di autorizzazione per connessioni in entrata, SPI 0x1698CAC7 Indirizzo origine: 10.0.0.2 Maschera origine: 255.255.255.255 Indirizzo destinazione: 10.0.0.1 Dst mask: 255.255.255.255 Porte Src Superiore: 0 Inferiore: 0 Operazione: ignorare Porte Dst Superiore: 0 Inferiore: 0 Operazione: ignorare Protocollo: 50 Protocollo di utilizzo: vero SPI: 0x1698CAC7 Usa SPI: vero IPSEC Regola di autorizzazione in ingresso completata, SPI 0x1698CAC7 ID regola: 0x53F8AEA8 [DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, lanciatore: ricevuto KEY_UPDATE, spi 0x1698cac7	
[DEBUG IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, Avvio del timer di reimpostazione chiave P2: 3.060 secondi.	Avviare i tempi di rigenerazione delle chiavi IPsec.
[IKEv1]: Gruppo = 10.0.0.2, IP = 10.0.0.2, FASE 2 COMPLETATA (msgid=52481cf5)	Fase 2 completata. Sia il risponditore che l'iniziatore sono in grado di crittografare/decrittografare il traffico.

Verifica tunnel

Nota: Poiché per attivare il tunnel viene utilizzato ICMP, è attiva una sola associazione di protezione IPSec. Protocollo 1 = ICMP.

```
show crypto ipsec sa
```

```
interface: outside
  Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
   access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/
```

```
1
```

```
/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/
```

1

```
/0)
   current_peer: 10.0.0.2
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 4, #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.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
   path mtu 1500, ipsec overhead 74, media mtu 1500
   current outbound spi: DB680406
   current inbound spi : 1698CAC7
  inbound esp sas:
   spi: 0x
```

1698CAC7

```
 (379112135)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000001F
  outbound esp sas:
   spi: 0xDB680406 (3681027078)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001
```

show crypto isakmp sa

```
  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: 10.0.0.2
   Type    :
```

L2L

```
             Role    :
```

responder

```
   Rekey   : no              State   :
```

MM_ACTIVE

Informazioni correlate

- Un buon punto di partenza è articolo di wikipedia su IPSec. Standard and references contiene molte informazioni utili
- Risoluzione dei problemi IPSec: descrizione e uso dei comandi di debug
- **Documentazione e supporto tecnico – Cisco Systems**