Debug di ASA IKEv2 per la risoluzione dei problemi della VPN di accesso remoto

Sommario

Introduzione

In questo documento viene illustrato come interpretare i debug su Cisco Adaptive Security Appliance (ASA) quando si usa Internet Key Exchange versione 2 (IKEv2) con un client Cisco AnyConnect Secure Mobility. In questo documento viene spiegato anche come convertire alcune righe di debug in una configurazione ASA.

Questo documento non descrive come passare il traffico dopo aver stabilito un tunnel VPN all'appliance ASA, né include concetti base di IPSec o IKE.

Prerequisiti

Requisiti

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

Componenti usati

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

- IKEv2 (Internet Key Exchange versione 2)
- Cisco Adaptive Security Appliance (ASA) versione 8.4 o successive

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

Problema principale

Il Cisco Technical Assistance Center (TAC) utilizza spesso i comandi IKE e IPSec debug per capire dove si è verificato un problema con la creazione del tunnel VPN IPSec, ma i comandi possono essere crittografati.

Scenario

Comandi debug

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

Configurazione ASA

Questa configurazione ASA è strettamente base e non prevede l'utilizzo di server esterni.

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure
```

```
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 2
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
 anyconnect modules value dart
 anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

File XML

```
<ServerList>
       <HostEntry>
               <HostName>Anu-IKEV2</HostName>
               <HostAddress>10.0.0.1</HostAddress>
               <UserGroup>ASA-IKEV2</UserGroup>
               <PrimaryProtocol>IPsec</PrimaryProtocol>
       </HostEntry>
</ServerList>
```

Nota: Il nome del gruppo di utenti nel profilo client XML deve essere uguale al nome del gruppo di tunnel sull'appliance ASA. In caso contrario, viene visualizzato il messaggio di errore 'Invalid Host Entry. Sul client AnyConnect viene visualizzato il messaggio "Reimmettere".

Descrizioni e log di debug

Nota: Poiché i log di Strumento di diagnostica e report (DART, Diagnostics and Reporting

Tool) sono in genere molto chiacchierati, in questo esempio alcuni log DART sono stati omessi per insignificanza.

Descrizione messaggio server	Debug
	Data: 04/23/2013 Ora: 16:24:55 Tipo: Informazioni Origine: acvpnui Descrizione: Funzione: IfcBaseClient::connect File: .\IfcBaseClient.cpp Riga: 964 **È stata richiesta una connessione VPN ad Anu-IKEV2.** ********** Data: 04/23/2013 Ora: 16:24:55 Tipo: Informazioni Origine: acvpnui Descrizione: Informazioni sul tipo di messaggio inviate all'utente: Contattare Anu-IKEV2. ********** Data: 04/23/2013 Ora: 16:24:55 Tipo: Informazioni Origine: acvpnui Descrizione: Funzione: ApiCert::getCertList File: .\ApiCert.cpp Riga: 259 Numero di certificati trovati: 0 ********** Data: 04/23/2013 Ora: 16:25:00 Tipo: Informazioni Origine: acvpnui Descrizione: **Avvio della connessione VPN al gateway sicuro https://10.0.0.1/ASA-IKEV2** ********** Data: 04/23/2013 Ora: 16:25:00 Tipo: Informazioni Origine: acvpnagent Descrizione: Tunnel avviato dal client GUI. ********** Data: 04/23/2013 Ora: 16:25:02 Tipo: Informazioni Origine: acvpnagent

Descrizione: Funzione: Protocollo IPSec::connectTransport
File: .\IPsecProtocol.cpp
Riga: 1629
Socket IKE aperto da 192.168.1.1:25170 a 10.0.0.1:500
****

—Inizio scambio IKE_SA_INIT—

L'appliance ASA riceve il messaggio IKE_SA_INIT dal client.

IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1]:50
InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000 MID=000000
IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0

La prima coppia di messaggi è lo scambio IKE_SA_INIT. Questi messaggi negoziano algoritmi di crittografia, scambiano nonce ed eseguono uno scambio Diffie-Hellman (DH).

IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: 0000000000000000]
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - rspi: 0000000000000000**
IKEv2-PROTO-4: Payload successivo: SA, **versione: 2.0**
IKEv2-PROTO-4: Tipo di scambio: IKE_SA_INIT, **flag: INIZIATORE**
IKEv2-PROTO-4: ID messaggio: 0x0, lunghezza: 528

Il messaggio IKE_SA_INIT ricevuto dal client contiene i seguenti campi:

1. **Intestazione ISAKMP** - SPI/versione/flag.
2. **SAi1** - Algoritmo di crittografia supportato dall'iniziatore IKE.
3. **KEi** - Valore della chiave pubblica DH dell'iniziatore.
4. **N** - Iniziatore Nonce.

Payload successivo **SA**: Chiave, riservata: 0x0, lunghezza: 168
IKEv2-PROTO-4: ultima proposta: 0x0, riservato: 0x0, lunghezza: 164
Proposta: 1, ID protocollo: IKE, dimensione SPI: 0, #trans: 18
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 1, riservato: 0x0, id: 3DES
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 1, riservato: 0x0, id: DES
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: SHA512
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: SHA384
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: SHA256
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: SHA1
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: MD5
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA512
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA384
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA256
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA96
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: MD596
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 4, riservato: 0x0, id: DH_GROUP_1536_MOP/Gruppo 5

IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 4, riservato: 0x0, id: DH_GROUP_1024_MOP/Gruppo 2
IKEv2-PROTO-4: ultima trasformazione: 0x0, riservato: 0x0: lunghezza: 8
tipo: 4, riservato: 0x0, id: DH_GROUP_768_MOP/Gruppo 1

Payload successivo **KE**: N, riservato: 0x0, lunghezza: 104
Gruppo DH: 1, Riservato: 0x0

eb 5e 29 fe cb 2e d1 28 ed 4a 54 b1 13 7c b8 89
f7 62 13 6b df 95 88 28 b5 97 ba 52 ef e4 1d 28
ca 06 d1 36 b6 67 32 9a c2 dd 4e d8 c7 80 de 20
36 34 c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5 ed 5f
ba ba 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
N Payload successivo: VID, riservato: 0x0, lunghezza: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b b b4
IKEv2-PROTO-5: Analisi payload specifico del fornitore: CISCO-DELETE-REASON VID Payload successivo: VID, riservato: 0x0, lunghezza: 23

L'ASA verifica ed elabora Messaggio IKE_INIT. L'appliance ASA:

1. Seleziona la suite di crittografia da quelli offerti dal promotore.
2. Calcola la propria chiave privata DH.
3. Calcola un valore SKEYID da per cui è possibile derivare tutte le chiavi questo IKE_SA. Le intestazioni di tutti i messaggi successivi sono crittografati e autenticati. OSPF (Open Shortest Path First) chiavi utilizzate per la crittografia e protezione dell'integrità derivata da SKEYID e sono noti come:

   SK_e - Crittografia.**SK_a** -

Pacchetto decrittografato:dati: 528 byte
IKEv2-PLAT-3: Elabora payload VID personalizzati
IKEv2-PLAT-3: VID copyright Cisco ricevuto da peer
IKEv2-PLAT-3: VID AnyConnect EAP ricevuto dal peer
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IDLE: **V_RECV_INIT**
IKEv2-PROTO-3: 6) Verifica individuazione NAT
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IDLE: V_CHK_REDIRECT
IKEv2-PROTO-5: 6) Controllo reindirizzamento non necessario. Verrà ignorat
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IDLE: V_CHK_CAC
IKEv2-PLAT-5: **Nuova richiesta sa ikev2 ammessa**
IKEv2-PLAT-5: Aumento di un conteggio SA per la negoziazione in ingresso
IKEv2-PLAT-5: HANDLE PSH NON VALIDO
IKEv2-PLAT-5: HANDLE PSH NON VALIDO
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IDLE: EV_CHK_COOKIE
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IDLE: EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: **EV_VERIFY_MSG**
IKEv2-PROTO-3: 6) **Verifica messaggio di inizializzazione SA**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: EV_INSERISCI_SA
IKEv2-PROTO-3: 6) Inserisci SA

Autenticazione.**SK_d** - Derivato e utilizzato per derivare ulteriori materiale per le chiavi SA_FIGLIO.SK_e e SK_a separati sono per ogni direzione.

Configurazione pertinente:

```
crypto ikev2 policy 10
 encryption aes-192
integrity
sha group 2  prf sha
lifetime
seconds 86400
crypto ikev2 enable outside
```

IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: EV_GET_IKE_POLICY
IKEv2-PROTO-3: 6) **Recupero dei criteri configurati**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: **PROC_EV_MSG**
IKEv2-PROTO-2: 6) Elaborazione messaggio iniziale in corso
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: EV_DETECT_NAT
IKEv2-PROTO-3: 6) Elabora notifica individuazione NAT
IKEv2-PROTO-5: 6) Elaborazione della notifica nat detect src
IKEv2-PROTO-5: 6) Indirizzo remoto non corrispondente
IKEv2-PROTO-5: 6) Elaborazione della notifica DST di rilevamento NAT in corso
IKEv2-PROTO-5: 6) Indirizzo locale corrispondente
IKEv2-PROTO-5: 6) L'host si trova all'esterno di NAT
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: MODALITÀ_CONFIG_CHK_EV
IKEv2-PROTO-3: 6) Ricevuti dati validi in modalità di configurazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_INIT: EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: 6) Imposta dati modalità di configurazione ricevuti
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_SET_POLICY
IKEv2-PROTO-3: 6) **Impostazione dei criteri configurati**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_PKI_SESH_OPEN
IKEv2-PROTO-3: 6) Apertura di una sessione PKI
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_DH_KEY
IKEv2-PROTO-3: 6) **Calcolo della chiave pubblica DH**
IKEv2-PROTO-3: 6)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: 6) Azione: Azione_Null
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_DH_SECRET
IKEv2-PROTO-3: 6) **Calcolo della chiave privata DH**

IKEv2-PROTO-3: 6)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: 6) Azione: Azione_Null
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_IDCHIAVE
IKEv2-PROTO-3: 6) **Genera skeyid**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GET_CONFIG_MODE

L'ASA costruisce il messaggio di risposta per lo scambio IKE_SA_INIT. Il pacchetto contiene:

1. **Intestazione ISAKMP** - SPI/versione/flag.
2. **SAr1** - Algoritmo di crittografia scelto dal risponditore IKE.
3. **KEr** - Valore della chiave pubblica DH del responder.
4. **N** - Risponditore Nonce.

IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_BLD_MSG**
IKEv2-PROTO-2: 6) **Invio messaggio iniziale**
IKEv2-PROTO-3: Proposta IKE: 1, dimensione SPI: 0 (negoziazione iniziale N. trasformazioni: 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Gruppo 1
IKEv2-PROTO-5: Crea payload specifico del fornitore: DELETE-REASONv2-PROTO-5: Crea payload specifico del fornitore: (PERSONALIZZATO)IKEv2-PROTO-5: Crea payload specifico del fornitore: (PERSONALIZZATO)IKEv2-PROTO-5: Payload notifica costruzione: NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Payload notifica costruzione: NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2: Non è stat possibile recuperare gli hash delle autorità di certificazione attendibili o non è disponibile alcun hash
IKEv2-PROTO-5: Crea payload specifico del fornitore: FRAMMENTAZIONIKEv2-PROTO-3: Tx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0
IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F**
IKEv2-PROTO-4: Payload successivo: SA, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_SA_INIT, **flag: RISPOSTA MSG RESPONDER**
IKEv2-PROTO-4: ID messaggio: 0x0, lunghezza: 386
Payload successivo **SA**: Chiave, riservata: 0x0, lunghezza: 48
IKEv2-PROTO-4: ultima proposta: 0x0, riservato: 0x0, lunghezza: 44
Proposta: 1, ID protocollo: IKE, dimensione SPI: 0, #trans: 4
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 2, riservato: 0x0, id: SHA1
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA96
IKEv2-PROTO-4: ultima trasformazione: 0x0, riservato: 0x0: lunghezza: 8
tipo: 4, riservato: 0x0, id: DH_GROUP_768_MOP/Gruppo 1

Payload successivo **KE**: N, riservato: 0x0, lunghezza: 104

Gruppo DH: 1, Riservato: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
e1 ce b4 a4 3c f2 8b 74 4e 20 59 b4 0b a1 ff 65
37 88 cc c4 a4 b6 fa 4a 63 03 93 89 e1 7e bd 6a
64 9a 38 24 e2 a8 40 f5 a3 d6 ef f7 1a df 33 cc
a1 8e fa dc 9c 34 45 79 1a 7c 29 05 87 8a ac 02
98 2e 7d cb 41 51 d6 fe fc c7 76 83 1d 03 b0 d7

N Payload successivo: VID, riservato: 0x0, lunghezza: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 ec 97 b8 67
d5 e7 c2 f5

Payload successivo VID: VID, riservato: 0x0, lunghezza: 23

L'ASA invia il messaggio di risposta per lo scambio IKE_SA_INIT. Scambio IKE_SA_INIT completato. L'appliance ASA avvia il timer per il processo di autenticazione.

IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [10.0.0.1]:500->[192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000000
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_FINE
IKEv2-PROTO-3: 6) Frammentazione abilitata
IKEv2-PROTO-3: 6) Cisco DeleteReason Notify è abilitato
IKEv2-PROTO-3: 6) Completamento scambio inizializzazione SA
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: V_CHK4_RUOLO
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: V_INIZIO_TMR
IKEv2-PROTO-3: 6) Avvio del timer in attesa del messaggio di autenticazione (30 sec)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_WAIT_AUTH: EV_NO_EVENT
—IKE_SA_INIT completato—
— Inizio IKE_AUTH —
****
Data: 04/23/2013
Ora: 16:25:00
Tipo: Informazioni
Origine: acvpnagent

****
Data: 04/23/2013
Ora: 16:25:02
Tipo: Informazioni
Origine: acvpnagent

Descrizione: Funzione: Protocollo IPSec::initiateTunne
File: .\IPsecProtocol.cpp
Riga: 345
Avvio del tunnel IPsec in corso
****

	Descrizione: Parametri Secure Gateway: Indirizzo IP: 10.0.0.1 Port: 443 URL: "10.0.0.1 " Metodo di autenticazione: **IKE - EAP-AnyConnect** **Identità IKE:** ********** Data: 04/23/2013 Ora: 16:25:00 Tipo: Informazioni Origine: acvpnagent Descrizione: **Avvio della connessione di Cisco AnyConnect Secure Mobility Client, versione 3.0.1047** ********** Data: 04/23/2013 Ora: 16:25:02 Tipo: Informazioni Origine: acvpnagent Descrizione: Funzione: log_ikev2 File: .\ikev2_anyconnect_osal.cpp Riga: 2730 **Ricevuta richiesta di creazione di un tunnel IPsec. local traffic selector = Intervallo indirizzi: 0.0.0.0-255.255.255.255 Protocollo: Intervallo porte 0: 0-65535 ; remote traffic selector = Intervallo indirizzi: 0.0.0.0-255.255.255.255 Protocollo: Intervallo porte 0: 0-65535** ********** Data: 04/23/2013 Ora: 16:25:02 Tipo: Informazioni Origine: acvpnagent Descrizione: Funzione: Protocollo IPSec::connectTransport File: .\IPsecProtocol.cpp Riga: 1629 **Socket IKE aperto da 192.168.1.1:25171 a 10.0.0.1:4500** **********
L'autenticazione viene eseguita con EAP. In una conversazione EAP è consentito un solo metodo di autenticazione EAP. L'appliance ASA riceve il messaggio IKE_AUTH dal client.	IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:**4500** InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000001 IKEv2-PROTO-3: **Rx** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x1
Quando il client include un payload IDi ma non un payload AUTH, indica il client ha dichiarato un'identità ma	IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6B94D7F] IKEv2-PROTO-4: IKEV2 **HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F** IKEv2-PROTO-4: Payload successivo: ENCR, **versione: 2.0** IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, **flag: INIZIATORE** IKEv2-PROTO-4: ID messaggio: 0x1, lunghezza: 540

non provarlo. Nei debug, l'opzione AUTH payload non presente in IKE_AUTH pacchetto inviato dal client. Il cliente invia il payload AUTH solo dopo Scambio EAP riuscito. Se l'appliance ASA è disposto a utilizzare un metodo di autenticazione, inserisce un EAP payload nel messaggio 4 e rinvia l'invio SAr2, TSi e TSr fino all'iniziatore autenticazione completata in un successivo scambio IKE_AUTH.

Il pacchetto dell'iniziatore IKE_AUTH contiene:

1. **Intestazione ISAKMP** - SPI/versione/flag.
2. **IDi** - Nome del gruppo di tunnel che il client desidera connettersi a può essere consegnato dall'IDi payload di tipo ID_KEY_ID in il messaggio iniziale del Scambio IKE_AUTH. Questo si verifica quando il profilo client* è preconfigurato con un nome di gruppo o, dopo un precedente autenticazione, il client ha il nome del gruppo è stato inserito nella cache preferenze.

IKEv2-PROTO-5: 6) La richiesta ha mess_id 1; previsto da 1 a 1
Pacchetto decrittografato REAL:Dati: 465 byte
IKEv2-PROTO-5: Analisi payload specifico del fornitore: Payload VID successivo (PERSONALIZZATO): IDi, riservato: 0x0, lunghezza: 20

58 af f6 11 52 8d b0 2c b8 da 30 46 be 91 56 fa
IDi Payload successivo: CERTREQ, riservato: 0x0, lunghezza: 28
Tipo ID: Nome gruppo, riservato: 0x0 0x0

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
Payload successivo **CERTREQ**: CFG, riservato: 0x0, lunghezza: 25
Codifica certificato X.509 - firma
&Due punti dati CertReq; 20 byte
Payload successivo **CFG**: SA, riservato: 0x0, lunghezza: 196
tipo cfg: **CFG_REQUEST**, riservata: 0x0, riservato: 0x0

tipo di attributo: indirizzo IPv4 interno, lunghezza: 0

tipo di attributo: netmask IP4 interna, lunghezza: 0

tipo di attributo: DNS IP4 interno, lunghezza: 0

tipo di attributo: NBNS IP4 interni, lunghezza: 0

tipo di attributo: scadenza indirizzo interno, lunghezza: 0

tipo di attributo: versione applicazione, lunghezza: 27

41 6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
tipo di attributo: indirizzo IP6 interno, lunghezza: 0

tipo di attributo: subnet IP4 interna, lunghezza: 0

tipo di attributo: Sconosciuto - 28682, lunghezza: 15

77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65
tipo di attributo: Sconosciuto - 28704, lunghezza: 0

tipo di attributo: Sconosciuto - 28705, lunghezza: 0

tipo di attributo: Sconosciuto - 28706, lunghezza: 0

tipo di attributo: Sconosciuto - 28707, lunghezza: 0

tipo di attributo: Sconosciuto - 28708, lunghezza: 0

tipo di attributo: Sconosciuto - 28709, lunghezza: 0

tipo di attributo: Sconosciuto - 28710, lunghezza: 0

tipo di attributo: Sconosciuto - 28672, lunghezza: 0

L'appliance ASA cerca di trovare una corrispondenza con un gruppo di tunnel nome con il contenuto di IKE Payload IDi. Dopo la prima la VPN IPSec riuscita è stabilito, il client memorizza nella cache nome gruppo (alias gruppo) a cui utente autenticato. Questo gruppo viene recapitato in IDi payload della connessione successiva tentare di indicare la gruppo probabile desiderato dal utente. Quando l'autenticazione EAP è specificato o implicito dal client e il profilo non contengono la <IKEIdentity> , il client invia un Payload ID_GROUP di tipo IDi con la stringa fissa *$AnyConnectClient$ *.

tipo di attributo: Sconosciuto - 28684, lunghezza: 0
tipo di attributo: Sconosciuto - 28711, lunghezza: 2
05 7e
tipo di attributo: Sconosciuto - 28674, lunghezza: 0
tipo di attributo: Sconosciuto - 28712, lunghezza: 0
tipo di attributo: Sconosciuto - 28675, lunghezza: 0
tipo di attributo: Sconosciuto - 28679, lunghezza: 0
tipo di attributo: Sconosciuto - 28683, lunghezza: 0
tipo di attributo: Sconosciuto - 28717, lunghezza: 0
tipo di attributo: Sconosciuto - 28718, lunghezza: 0
tipo di attributo: Sconosciuto - 28719, lunghezza: 0
tipo di attributo: Sconosciuto - 28720, lunghezza: 0
tipo di attributo: Sconosciuto - 28721, lunghezza: 0
tipo di attributo: Sconosciuto - 28722, lunghezza: 0
tipo di attributo: Sconosciuto - 28723, lunghezza: 0
tipo di attributo: Sconosciuto - 28724, lunghezza: 0
tipo di attributo: Sconosciuto - 28725, lunghezza: 0
tipo di attributo: Sconosciuto - 28726, lunghezza: 0
tipo di attributo: Sconosciuto - 28727, lunghezza: 0
tipo di attributo: Sconosciuto - 28729, lunghezza: 0

3. **CERTREQ** - Il client è richiesta di un'appliance ASA certificato preferito. Certificato è possibile includere i payload della richiesta in uno scambio

Payload successivo **SA**: TSi, riservato: 0x0, lunghezza: 124
IKEv2-PROTO-4: ultima proposta: 0x0, riservato: 0x0, lunghezza: 120
Proposta: 1, ID protocollo: ESP, dimensione SPI: 4, #trans: 12
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 1, riservato: 0x0, id: 3DES
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 1, riservato: 0x0, id: DES

quando il mittente deve ottenere il certificato del ricevitore. La richiesta di certificato payload elaborato da ispezione della 'Codifica certificato' per determinare se il processore certificati di questo tipo. In caso affermativo, la Il campo 'Autorità di certificazione' è ispezionati per determinare se il processore dispone di certificati che possono essere convalidati fino a uno dei la certificazione specificata autorità. Può trattarsi di una catena di certificati.

IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 1, riservato: 0x0, id: NULL
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA512
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA384
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA256
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA96
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: MD596
IKEv2-PROTO-4: ultima trasformazione: 0x0, riservato: 0x0: lunghezza: 8
tipo: 5, riservato: 0x0, id:

Payload successivo **TSi**: TSr, riservato: 0x0, lunghezza: 24
Numero di TS: 1, riservato 0x0, riservato 0x0
Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
start port: 0, porta finale: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
Payload successivo **TSr**: NOTIFY, riservato: 0x0, lunghezza: 24
Numero di TS: 1, riservato 0x0, riservato 0x0
Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
start port: 0, porta finale: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255

4. **CFG** - RICHIESTA_CFG/ CFG_REPLY consente un IKE endpoint per richiedere informazioni dall'altro. Se un attributo in Configurazione CFG_REQUEST payload non di lunghezza zero, è considerato un suggerimento al riguardo attributo.CFG_REPLY il payload di configurazione può restituire

o un nuovo valore. Può aggiungi anche nuovi attributi e non includerne alcuni richiesti. Richiedenti che ignorano i risultati restituiti attributi non disponibili riconoscere. In questi debug, il il client richiede il tunnel configurazione in RICHIESTA_CFG. L'appliance ASA risponde e invia il tunnel attributi di configurazione solo dopo scambio EAP riuscito.
5. **SAi2** - SAi2 avvia l'associazione di protezione, simile alla fase 2 scambio set di trasformazioni in IKEv1.
6. **TSi** e **TSr** - Iniziatore e risponditore, selettori traffico contengono, rispettivamente, l'origine e l'indirizzo di destinazione iniziatore e risponditore per inoltro e ricezione crittografati traffico. Intervallo di indirizzi specifica che tutto il

traffico da e verso l'intervallo è tunneling. Se il proposta è accettabile per la risponditore, invia un TS identico di ritorno.	

Attributi che il client deve fornire per l'autenticazione di gruppo è archiviata in un File del profilo AnyConnect.
***Configurazione profilo rilevante:**
 	
`<ServerList>`
`<HostEntry>`
`<HostName>Anu-IKEV2`
`</HostName>`
`<HostAddress>10.0.0.1`
`</HostAddress>`
 	
`<PrimaryProtocol>IPsec`
`</PrimaryProtocol>`
`</HostEntry>`
`</ServerList>`	

L'appliance ASA genera una risposta al messaggio IKE_AUTH e si prepara ad autenticarsi sul client.	**Pacchetto decriptato:**Data: 540 byte IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_RECV_AUTH IKEv2-PROTO-3: 6) Interruzione del timer in attesa del messaggio di autenticazione IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: V_CHK_NAT_T IKEv2-PROTO-3: 6) Verifica individuazione NAT IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_CHG_NAT_T_PORT IKEv2-PROTO-2: 6) NAT: rilevato float sulla porta di entrata 25171, porta di risposta 4500 IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: ID_PROC_EV IKEv2-PROTO-2: 6) Parametri validi ricevuti nell'ID processo IKEv2-PLAT-3: (6) metodo di autenticazione peer impostato su: 0 IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: 6) Recupero dei criteri configurati
IKEv2-PLAT-3: Rilevata nuova connessione del client AnyConnect in base al payload ID
IKEv2-PLAT-3: my_auth_method = 1
IKEv2-PLAT-3: (6) metodo di autenticazione peer impostato su: 256
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) tp_name impostato su: Anu-ikev2
IKEv2-PLAT-3: **trust point impostato su:** Anu-ikev2
IKEv2-PLAT-3: ID P1 = 0
IKEv2-PLAT-3: Conversione di IKE_ID_AUTO in = 9
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_SET_POLICY
IKEv2-PROTO-3: 6) **Impostazione dei criteri configurati**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: 6) Verifica criteri peer
IKEv2-PROTO-3: 6) **Trovato certificato corrispondente**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: MODALITÀ_CONFIG_CHK_EV
IKEv2-PROTO-3: 6) Ricevuti dati validi in modalità di configurazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3: (6) Il nome host DHCP per DNS è impostato su: winxp64template
IKEv2-PROTO-3: 6) Imposta dati modalità di configurazione ricevuti
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_WAIT_AUTH: EV_CHK_EAP
IKEv2-PROTO-3: 6) **Verifica scambio EAP**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento **R_BLD_AUTH**: GEN_GEN_AUTH
IKEv2-PROTO-3: 6) **Genera dati di autenticazione**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_AUTH: V_CHK4_SIGN
IKEv2-PROTO-3: 6) Ottieni metodo di autenticazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_AUTH: SEGNO_EV

IKEv2-PROTO-3: 6) **Firma dati di autenticazione**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_AUTH: EV_OK_AUTH_GEN
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_EAP_AUTH_REQ: EV_AUTHEN_REQ
IKEv2-PROTO-2: 6) **Richiesta all'autenticatore di inviare la richiesta EAP**
Nome elemento creato **valore config-auth**
VPN valore client nome attributo aggiunto all'elemento config-auth
Èstato aggiunto il valore hello del nome attributo all'elemento config-auth
Nome elemento creato valore versione 9.0(2)8
Aggiunto il valore della versione del nome dell'elemento 9.0(2)8 all'elemento config-auth
Aggiunto nome attributo who value sg a versione elemento
Messaggio XML generato di seguito
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="hello**">
<version who="sg">9.0(2)8</version>
</config-auth>

IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_EAP_AUTH_REQ: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: 6) Azione: Azione_Null
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_EAP_AUTH_REQ: V_CHK_REDIRECT
IKEv2-PROTO-3: 6) Verifica reindirizzamento con la piattaforma per il bilanciamento del carico
IKEv2-PLAT-3: Controllo reindirizzamento sulla piattaforma
IKEv2-PLAT-3: ikev2_osal_redirect: Sessione accettata da 10.0.0.1
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 Stato corrente: Evento R_BLD_EAP_AUTH_REQ: EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2: 6) **Invio richiesta EAP**
IKEv2-PROTO-5: Crea payload specifico del fornitore: CISCO-GRANITEIKEv2-PROTO-3: 6) Creazione

L'ASA invia il payload AUTH per richiedere le credenziali utente al client.

IDr. Payload successivo: CERT, riservato: 0x0, lunghezza: 36
Tipo ID: DN DER ASN1, riservato: 0x0 0x0

30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 2d 49 4b 45 56 32

L'ASA invia il metodo AUTH come 'RSA', quindi invia il proprio certificato al client, in modo che possa autenticare il server ASA.

Payload successivo **CERTIFICATO**: CERT, riservato: 0x0, lunghezza: 436
Certificato **codifica X.509** - firma
&Due punti dati certificato; 431 byte

Poiché l'ASA è disposta a utilizzare un metodo di autenticazione estensibile, inserisce un payload EAP nel messaggio 4 e rinvia l'invio di SAr2, TSi e TSr fino al completamento

Payload certificato successivo: AUTH, riservata: 0x0, lunghezza: 436
Codifica certificato X.509 - firma
&Due punti dati certificato; 431 byte
Payload successivo **AUTH**: EAP, riservato: 0x0, lunghezza: 136
Metodo di autenticazione RSA, riservato: 0x0, riservato 0x0
Autentica &due punti; 128 byte
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 154

dell'autenticazione dell'iniziatore in un successivo scambio IKE_AUTH. Pertanto, questi tre payload non sono presenti nei debug.

Il pacchetto EAP contiene:

1. **Codice: richiesta**: questo codice viene inviato dall'autenticatore al peer.
2. **id: 1** - L'ID aiuta a far corrispondere le risposte EAP alle richieste. Qui il valore è 1, che indica che si tratta del primo pacchetto nello scambio EAP. Questa richiesta EAP è di tipo 'config-auth' e viene inviata dall'ASA al client per avviare lo scambio EAP.
3. **Lunghezza: 150** - La lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.
4. **dati EAP**.

Codice: richiesta: **id**: 1, **lunghezza**: 150
Tipo: Sconosciuto - 254
Dati EAP: 145 byte

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x1
IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F**
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, **flag: RISPOSTA MSG RESPONDER**
IKEv2-PROTO-4: ID messaggio: 0x1, lunghezza: 1292
Payload successivo ENCR: VID, riservato: 0x0, lunghezza: 1264
Dati crittografati &due punti; 1260 byte

La frammentazione può verificarsi se i certificati sono di grandi dimensioni o se sono incluse catene di certificati. I payload KE dell'iniziatore e del risponditore possono includere anche chiavi grandi, che possono contribuire alla frammentazione.

IKEv2-PROTO-5: 6) Frammentazione del pacchetto in corso, MTU frammentata: 544, **Numero di frammenti: 3,** ID frammento: 1
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000000

****

Data: 04/23/2013
Ora: 16:25:02
Tipo: Informazioni
Origine: acvpnagent

Descrizione: Funzione: ikev2_verify_X509_SIG_certs

File: .\ikev2_anyconnect_osal.cpp
Riga: 2077
Richiesta di accettazione del certificato all'utente
****
Data: 04/23/2013
Ora: 16:25:02
Tipo: Errore
Origine: acvpnui

Descrizione: Funzione: CCapiCertificate::verifyChainPolicy
File: .\Certificati\CertificatoCapi.cpp
Riga: 2032
Funzione richiamata: VerificaCertCriterioCatenaCertificati
Codice restituito: -2146762487 (0x800B0109)
Descrizione: Catena di certificati elaborata, ma terminata in un certificato radice non considerato attendibile dal provider di attendibilità.
****
Data: 04/23/2013
Ora: 16:25:04
Tipo: Informazioni
Origine: acvpnagent

Descrizione: Funzione: CEAPMgr::RichiestaDatiCB
File: .\EAPMgr.cpp
Riga: 400
Tipo proposto EAP: EAP-ANYCONNECT
****

Il client risponde alla richiesta EAP con una risposta.
Il pacchetto EAP contiene:

1. **Codice: risposta**: questo codice viene inviato dal peer all'autenticatore in risposta alla richiesta EAP.
2. **id: 1 -** L'ID consente di far corrispondere le risposte EAP alle richieste. Il valore è 1, ossia la risposta alla richiesta inviata in precedenza dall'ASA (autenticatore). Il tipo di questa risposta EAP 'config-auth' è 'init'; il client sta inizializzando lo scambio EAP ed è in attesa che l'ASA

IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000002
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x2
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, flag: INIZIATORE
IKEv2-PROTO-4: ID messaggio: 0x2, lunghezza: 332
IKEv2-PROTO-5: 6) La richiesta ha mess_id 2; previsto da 2 a 2
Pacchetto decrittografato REAL:Dati: 256 byte
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 256
Codice: risposta: id: 1, **lunghezza**: 252
Tipo: Sconosciuto - 254
Dati EAP:247 byte
Pacchetto decriptato: Data: 332 byte
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: 6) Interruzione del timer in attesa del messaggio di autenticazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B

generi la richiesta di autenticazione.
3. **Lunghezza: 252** - La lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.
4. **dati EAP**.

L'ASA decrittografa questa risposta e il client indica di aver ricevuto il payload AUTH nel pacchetto precedente (con il certificato) e di aver ricevuto il primo pacchetto di richiesta EAP dall'ASA.

R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_PROC_EAP_RESP: PROC_EV_MSG
IKEv2-PROTO-2: 6) **Elaborazione risposta EAP**
Messaggio XML ricevuto dal client
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="init"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<group-select>ASA-IKEV2</group-select>
<group-access>ASA-IKEV2</group-access>
</config-auth>
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_PROC_EAP_RESP: **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5: 6) Azione: Azione_Null
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_BLD_EAP_REQ: **REV_RECV_EAP_REQ**

Contenuto del pacchetto di risposta EAP 'init'.

Questa è la seconda richiesta inviata dall'ASA al client.

Il pacchetto EAP contiene:

1. **Codice: richiesta**: questo codice viene inviato dall'autenticatore al peer.
2. **id: 2** - L'ID aiuta a far corrispondere le risposte EAP alle richieste. Qui il valore è 2, che indica che si tratta del secondo pacchetto nello scambio. Il tipo 'config-auth' di questa richiesta è 'auth-request'; l'ASA richiede che il client invii le credenziali di autenticazione dell'utente.
3. **Lunghezza: 457** - La lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.

IKEv2-PROTO-2: 6) Invio richiesta EAP
Messaggio XML generato di seguito
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-request"**>
<version who="sg">9.0(2)8</version>
<opaque is-for="sg">
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash>
</opaco>
<csport>443</csport>
<auth id="main">
<modulo>
<input type="text" name="username" label="Username:"></input>
<input type="password" name="password" label="Password:"></input>
</form>
</auth>
</config-auth>
IKEv2-PROTO-3: 6) Creazione pacchetto per crittografia; i contenuti sono:
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 461
Codice: richiesta: id: 2, lunghezza: 457
Tipo: Sconosciuto - 254
Dati EAP: 452 byte

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x2
IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6B94D7F]

****
Data: 04/23/2013
Ora: 16:25:04
Tipo: Informazioni
Origine: acvpnui

Descrizione: Funzione: SDIMgr::DatiRichiestaProcesso
File: .\SDIMgr.cpp
Riga: 281
Il tipo di autenticazione non è SDI.
****
Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnui

Descrizione: Funzione: ConnectMgr::rispostautente
File: .\ConnectMgr.cpp
Riga: 985
Elaborazione della risposta dell'utente.
****

4. **dati EAP**.

Payload **ENCR**:
Il payload viene decrittografato e il relativo contenuto viene analizzato come payload aggiuntivi.

IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, flag: **RISPOSTA MSG RESPONDER**
IKEv2-PROTO-4: ID messaggio: 0x2, lunghezza: 524
Payload successivo **ENCR**: EAP, riservato: 0x0, lunghezza: 496
Dati crittografati &due punti; 492 byte

IKEv2-PLAT-4: **SENT PKT [IKE_AUTH]** [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000002
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_BLD_EAP_REQ: V_INIZIO_TMR
IKEv2-PROTO-3: 6) **Avvio del timer in attesa del messaggio di autenticazione utente** (120 sec)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000002 Stato corrente: Evento R_WAIT_EAP_RESP: EV_NO_EVENT

Il client invia un altro messaggio dell'iniziatore IKE_AUTH con il payload EAP.
Il pacchetto EAP contiene:

1. **Codice: risposta**: questo codice viene inviato dal peer all'autenticatore in risposta alla richiesta EAP.
2. **id: 2** - L'ID aiuta a far corrispondere le risposte EAP alle richieste. Il valore è 2, ossia la risposta alla richiesta inviata in precedenza dall'ASA (autenticatore).
3. **Lunghezza: 420** - La

IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:450 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x3
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: **Tipo di scambio: IKE_AUTH, flag: INIZIATORE**
IKEv2-PROTO-4: ID messaggio: 0x3, lunghezza: 492
IKEv2-PROTO-5: 6) La richiesta ha mess_id 3; previsto da 3 a 3

Pacchetto decrittografato REAL:Dati: 424 byte
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 424
Codice: risposta: id: 2, lunghezza: 420
Tipo: Sconosciuto - 254
Dati EAP: 415 byte

lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.

4. **dati EAP**.

L'ASA elabora questa risposta. Il client ha richiesto l'immissione delle credenziali da parte dell'utente. Il tipo 'config-auth' di questa risposta EAP è 'auth-reply'. Il pacchetto contiene le credenziali immesse dall'utente.

Pacchetto decrittografato:dati: 492 byte
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: 6) Interruzione del timer in attesa del messaggio di autenticazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_PROC_EAP_RESP: PROC_EV_MSG
IKEv2-PROTO-2: 6) **Elaborazione risposta EAP**
Messaggio XML ricevuto dal client
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-reply"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<id-sessione></id-sessione>
<opaque is-for="sg">
<tunnel-group>**ASA-IKEV2**</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<auth>
<password>cisco123</password>
<username>Anu</username></auth>
</config-auth>
IKEv2-PLAT-1: **EAP: autenticazione utente avviata**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_PROC_EAP_RESP: EV_NO_EVENT
IKEv2-PLAT-5: EAP:In callback AAA
Digest certificato server recuperato: DACE1C274785F28BA11D64453096BAE294A3172E
IKEv2-PLAT-5: **EAP:operazione riuscita nel callback AAA**
IKEv2-PROTO-3: Risposta ricevuta dall'autenticatore
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_PROC_EAP_RESP: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: 6) Azione: Azione_Null

L'ASA crea una terza richiesta EAP nello scambio.
Il pacchetto EAP contiene:

1. **Codice: richiesta**: questo codice viene

IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_BLD_EAP_REQ: REV_RECV_EAP_REQ
IKEv2-PROTO-2: 6) Invio richiesta EAP
Messaggio XML generato di seguito
<?xml version="1.0" encoding="UTF-8"?>

inviato dall'autenticatore al peer.

2. **id: 3** - L'ID aiuta a far corrispondere le risposte EAP alle richieste. Qui il valore è 3, che indica che si tratta del terzo pacchetto in scambio. Il tipo 'config-auth' di questo pacchetto è 'complete'; L'appliance ASA ha ricevuto una risposta e lo scambio EAP è completo.
3. **Lunghezza: 4235** - La lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.
4. **dati EAP**.

Payload **ENCR**:
Il payload viene decrittografato e il relativo contenuto viene analizzato come payload aggiuntivi.

<config-auth client="vpn" **type="complete"**>
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag</session-token>
<auth id="success">
<message id="0" param1="" param2=""></message>
</auth>

IKEv2-PROTO-3: 6) Creazione pacchetto per crittografia; i contenuti sono:
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 4239
Codice: richiesta: id: 3, lunghezza: 4235
Tipo: Sconosciuto - 254
Dati EAP: 4230 byte

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x3
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, flag: **RISPOSTA MSG RESPONDER**
IKEv2-PROTO-4: ID messaggio: 0x3, lunghezza: 4300
Payload successivo **ENCR**: EAP, riservato: 0x0, lunghezza: 4272
Dati crittografati &due punti;4268 byte
IKEv2-PROTO-5: 6) Frammentazione del pacchetto in corso, MTU frammentata: 544, **Numero di frammenti: 9**, ID frammento: 2
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000003
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento R_BLD_EAP_REQ: V_INIZIO_TMR
IKEv2-PROTO-3: 6) Avvio timer in attesa del messaggio di autenticazione utente (120 sec)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 Stato corrente: Evento

R_WAIT_EAP_RESP: EV_NO_EVENT
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnagent

Descrizione: **Profilo corrente: Anyconnect-ikev2.xml**
Impostazioni di configurazione sessione VPN ricevuta:
Mantieni installati: attivato
Impostazione proxy: non modificare
Server proxy: nessuna
URL PAC proxy: nessuna
Eccezioni proxy: nessuna
Blocco proxy: attivato
Escludi divisione: la preferenza di accesso LAN locale è disabilitata
Includi divisione: disattivato
Dividi DNS: disattivato
Carattere jolly LAN locale: la preferenza di accesso LAN locale è disabilitata
Regole firewall: nessuna
Indirizzo client: 10.2.2.1
Maschera client: 255.0.0.0
Indirizzo IPv6 client: sconosciuto
Maschera IPv6 client: sconosciuto
MTU: 1406
IKE Keep Alive: 20 secondi
DPD IKE: 30 secondi
Timeout sessione: 0 secondi
Timeout disconnessione: 1800 secondi
Timeout di inattività: 1800 secondi
Server: sconosciuto
Host MUS: sconosciuto
Messaggio utente DAP: nessuna
Stato quarantena: disattivato
VPN sempre attiva: non disabilitato
Durata lease: 0 secondi
Dominio predefinito: sconosciuto
Home page: sconosciuto
Disconnessione rimozione smart card: attivato
Risposta licenza: sconosciuto
****

Il client invia il pacchetto dell'iniziatore con il payload EAP.

Il pacchetto EAP contiene:

1. **Codice: risposta**: questo codice viene inviato dal peer all'autenticatore in risposta alla richiesta EAP.
2. **id: 3** - L'ID aiuta a far

IKEv2-PLAT-4: **RECV PKT** [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:450
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000004
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x4
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: **Tipo di scambio: IKE_AUTH, flag: INIZIATORE**
IKEv2-PROTO-4: ID messaggio: 0x4, lunghezza: 252
IKEv2-PROTO-5: 6) La richiesta ha mess_id 4; previsto da 4 a 4

corrispondere le risposte EAP alle richieste. Il valore è 3, ossia la risposta alla richiesta inviata in precedenza dall'ASA (autenticatore). L'ASA riceve ora il pacchetto di risposta dal client, il cui tipo 'config-auth' è 'ack'; questa risposta riconosce il messaggio EAP "complete" inviato in precedenza dall'ASA.

3. **Lunghezza: 173** - La lunghezza del pacchetto EAP include il codice, l'ID, la lunghezza e i dati EAP.
4. **dati EAP**.

Pacchetto decrittografato REAL:Dati: 177 byte
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 177
Codice: risposta: id: 3, lunghezza: 173
Tipo: Sconosciuto - 254
Dati EAP: 168 byte

L'appliance ASA elabora il pacchetto. OSPF (Open Shortest Path First) Scambio EAP riuscito. L'appliance ASA si prepara a inviare il gruppo di tunnel nel pacchetto successivo, che è stato richiesto in precedenza dal client in il payload IDi. L'appliance ASA riceve la pacchetto di risposta dal client, che ha il tipo 'config-auth' di 'ack'. Questo la risposta riconosce il punto di accesso messaggio 'complete' inviato dal in precedenza, l'appliance ASA.

Pacchetto decrittografato:dati:252 byte
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: 6) Interruzione del timer in attesa del messaggio di autenticazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento R_PROC_EAP_RESP: PROC_EV_MSG
IKEv2-PROTO-2: 6) **Elaborazione risposta EAP**
Messaggio XML ricevuto dal client
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="ack"**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
</config-auth>

IKEv2-PLAT-3: (6) aggrAuthHdl impostato su 0x2000
IKEv2-PLAT-3: (6) **tg_name impostato su: ASA-IKEV2**
IKEv2-PLAT-3: (6) **tunn grp type impostato su: RA**
IKEv2-PLAT-1: **EAP: autenticazione riuscita**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento R_PROC_EAP_RESP: EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2: 6) Invio messaggio di stato EAP

Configurazione pertinente:

```
tunnel-group ASA-IKEV2
type remote-access
tunnel-group ASA-IKEV2
general-attributes
```

```
 address-pool webvpn1
 authorization-server-group
 LOCAL default-group-policy
ASA-IKEV2
tunnel-group ASA-IKEV2
webvpn-attributes
 group-alias ASA-IKEV2
enable
```

Lo scambio EAP è ora riuscito.

Il pacchetto EAP contiene:

1. **Codice**: **success** - Questo codice è inviato dall'autenticatore al peer dopo il completamento di un EAP metodo di autenticazione. Questo indica che il peer ha autenticato correttamente in autenticatore.
2. **id: 3** - L'ID aiuta a corrispondere al Risposte EAP con le richieste. Il valore è 3, che indica che si tratta di una risposta a la richiesta precedentemente inviata ASA (autenticatore). La terza serie di pacchetti nello scambio è stato e lo scambio EAP ha esito positivo.
3. **Lunghezza: 4** - Lunghezza dell'EAP il pacchetto include il codice, l'id, lunghezza e dati EAP.
4. **dati EAP**.

Poiché lo scambio EAP ha esito positivo, il client invia

IKEv2-PROTO-3: 6) Creazione pacchetto per crittografia; i contenuti sono:
Payload successivo **EAP**: NONE, riservato: 0x0, lunghezza: 8
Codice: operazione riuscita: id: 3, lunghezza: 4

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x4
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, flag: RISPOSTA MSG RESPONDER
IKEv2-PROTO-4: ID messaggio: 0x4, lunghezza: 76
Payload successivo ENCR: EAP, riservato: 0x0, lunghezza: 48
Dati crittografati &due punti;44 byte

IKEv2-PLAT-4: **SENT PKT [IKE_AUTH]** [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000004
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento R_PROC_EAP_RESP: V_INIZIO_TMR
IKEv2-PROTO-3: 6) Avvio del timer in attesa del messaggio di autenticazione (30 sec)
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 Stato corrente: Evento **R_WAIT_EAP_AUTH_VERIFY**: EV_NO_EVENT

IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:450
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005

il pacchetto dell'iniziatore IKE_AUTH con il payload AUTH. Il payload AUTH viene generato dalla chiave segreta condivisa.

IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x5
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: Tipo di scambio: IKE_AUTH, **flag: INIZIATORE**
IKEv2-PROTO-4: ID messaggio: 0x5, lunghezza: 92
IKEv2-PROTO-5: 6) La richiesta ha mess_id 5; previsto da 5 a 5

Pacchetto decrittografato REAL:Dati:28 byte
Payload successivo **AUTH**: NONE, riservato: 0x0, lunghezza: 28
PSK metodo di autenticazione, riservato: 0x0, riservato 0x0
Dati autenticazione: 20 byte

Quando è specificata l'autenticazione EAP o implicito dal profilo client e dal
il profilo non contiene <IKEIdentity>, il client invia un payload ID_GROUP di tipo IDi con
la stringa fissa *$AnyConnectClient$*. L'appliance ASA elabora il messaggio.

Pacchetto decrittografato:dati: 92 byte
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH
IKEv2-PROTO-3: 6) Interruzione del timer in attesa del messaggio di autenticazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_GET_EAP_KEY
IKEv2-PROTO-2: 6) Invia AUTH, per verificare il peer dopo lo scambio EAP
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_VERIFICA_AUTH
IKEv2-PROTO-3: 6) **Verifica dati di autenticazione**
IKEv2-PROTO-3: 6) **Usa chiave già condivisa per id *$AnyConnectClient$*, chiave len 20**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: Risposta modalità configurazione in coda
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-3: PSH: client=AnyConnect client-version=3.0.1047 client-os=Windows client-os-version=
IKEv2-PLAT-3: Risposta modalità configurazione completata
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_OK_GET_CONFIG
IKEv2-PROTO-3: 6) Dati modalità di configurazione da inviare
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: V_CHK4_IC
IKEv2-PROTO-3: 6) Elaborazione del contatto iniziale
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: V_CHK_REDIRECT
IKEv2-PROTO-5: 6) Il controllo di reindirizzamento è già stato eseguito per

Configurazione pertinente:

```
crypto dynamic-map dynmap 1000
set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside
```

	questa sessione. Verrà ignorato IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: V_PROC_SA_TS IKEv2-PROTO-2: 6) **Elaborazione del messaggio di autenticazione** IKEv2-PLAT-1: **Mappa crittografica: Mappa dynmap seq 1000. Selettore regolato con IP assegnato** IKEv2-PLAT-3: **Mappa crittografica: corrispondenza su mappa dinamica dynmap seq 1000** IKEv2-PLAT-3: PFS disabilitato per la connessione RA IKEv2-PROTO-3: 6) IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_NO_EVENT IKEv2-PLAT-2: Ricevuto callback PFKEY SPI per SPI 0x30B848A4, errore FALSE IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_VERIFY_AUTH: EV_OK_RECD_IPSEC_RESP IKEv2-PROTO-2: 6) **Elaborazione del messaggio di autenticazione**
L'ASA crea il messaggio di risposta IKE_AUTH con i payload SA, TSi e TSr. Il pacchetto del risponditore IKE_AUTH contiene: 1. **Intestazione ISAKMP** - SPI/versione/flag. 2. **Payload AUTH** - Con il metodo di autenticazione scelto. 3. **CFG** - CFG_REQUEST/ CFG_REPLY consente a un endpoint IKE di richiedere informazioni dal peer. Se un attributo nel payload di configurazione CFG_REQUEST non è di lunghezza zero, viene preso come suggerimento per tale attributo. Il payload di configurazione CFG_REPLY può restituire tale valore o uno nuovo. È inoltre	IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento **R_BLD_AUTH**: METODO_AUTH_EV IKEv2-PROTO-3: 6) **Ottieni metodo di autenticazione** IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_AUTH: EV_GET_PRESHR_KEY IKEv2-PROTO-3: 6) **Ottieni chiave già condivisa del peer per *$AnyConnectClient$*** IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_AUTH: GEN_GEN_AUTH IKEv2-PROTO-3: 6) **Genera dati di autenticazione** IKEv2-PROTO-3: 6) **Usa chiave già condivisa per id nomehost=ASA-IKEV2, chiave len 20** IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_AUTH: V_CHK4_SIGN IKEv2-PROTO-3: 6) Ottieni metodo di autenticazione IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_AUTH: EV_OK_AUTH_GEN IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_EAP_AUTH_VERIFY: GEN_GEN_AUTH IKEv2-PROTO-3: 6) Genera dati di autenticazione IKEv2-PROTO-3: 6) Usa chiave già condivisa per id nomehost=ASA-IKEV2, chiave len 20 IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH IKEv2-PROTO-2: 6) **Invia AUTH, per verificare il peer dopo lo scambio EAP** IKEv2-PROTO-3: Proposta ESP: 1, dimensione SPI: 4 (negoziazione IPSec

possibile che vengano aggiunti nuovi attributi senza includere alcuni di quelli richiesti. I richiedenti ignorano gli attributi restituiti che non riconoscono. L'ASA risponde al client con gli attributi di configurazione del tunnel nel pacchetto CFG_REPLY.

4. **SAr2** - SAr2 avvia l'associazione di protezione, simile allo scambio di set di trasformazioni di fase 2 in IKEv1.
5. **TSi** e **TSr** - I selettori del traffico dell'iniziatore e del risponditore contengono, rispettivamente, l'indirizzo di origine e di destinazione dell'iniziatore e del risponditore per inoltrare e ricevere traffico crittografato. L'intervallo di indirizzi specifica che tutto il traffico da e verso l'intervallo è sottoposto a tunneling. Se la proposta è accettabile per il risponditore, verranno restituiti payload di Servizi terminal identici.

Payload **ENCR**:
Il payload viene decrittografato e il relativo contenuto viene analizzato come payload aggiuntivi.

N. trasformazioni: 3
AES-CBC SHA96
IKEv2-PROTO-5: Payload notifica costruzione:
ESP_TFC_NO_SUPPORTIKEv2-PROTO-5: Payload notifica costruzione:
NON_FIRST_FRAGSIKEv2-PROTO-3: 6) Creazione pacchetto per crittografi
i contenuti sono:
Payload successivo **AUTH**: CFG, riservato: 0x0, lunghezza: 28
PSK metodo di autenticazione, riservato: 0x0, riservato 0x0
Autentica &due punti; 20 byte
Payload successivo **CFG**: SA, riservato: 0x0, lunghezza: 4196
tipo cfg: **CFG_REPLY,** riservato: 0x0, riservato: 0x0

tipo di attributo: indirizzo IPv4 interno, lunghezza: 4

01 01 01 01
tipo di attributo: netmask IP4 interna, lunghezza: 4

00 00 00 00
tipo di attributo: scadenza indirizzo interno, lunghezza: 4

00 00 00 00
tipo di attributo: versione applicazione, lunghezza: 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
tipo di attributo: Sconosciuto - 28704, lunghezza: 4

00 00 00 00
tipo di attributo: Sconosciuto - 28705, lunghezza: 4

00 00 07 08
tipo di attributo: Sconosciuto - 28706, lunghezza: 4

00 00 07 08
tipo di attributo: Sconosciuto - 28707, lunghezza: 1

01
tipo di attributo: Sconosciuto - 28709, lunghezza: 4

00 00 00 1e
tipo di attributo: Sconosciuto - 28710, lunghezza: 4

00 00 00 14
tipo di attributo: Sconosciuto - 28684, lunghezza: 1

01
tipo di attributo: Sconosciuto - 28711, lunghezza: 2

05 7e
tipo di attributo: Sconosciuto - 28679, lunghezza: 1

00
tipo di attributo: Sconosciuto - 28683, lunghezza: 4

80 0b 00 01
tipo di attributo: Sconosciuto - 28725, lunghezza: 1

00
tipo di attributo: Sconosciuto - 28726, lunghezza: 1

00
tipo di attributo: Sconosciuto - 28727, lunghezza: 4056

3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
46 2d 38 22 3f 3e 3c 63 6f 6e 66 69 67 2d 61 75
74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2d
69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<cattura>
72 6f 66 69 6c 65 2d 6d 61 6e 69 66 65 73 74 3e
3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
67 2d 61 75 74 68 3e 00
tipo di attributo: Sconosciuto - 28729, lunghezza: 1

00
Payload successivo **SA**: TSi, riservato: 0x0, lunghezza: 44
IKEv2-PROTO-4: ultima proposta: 0x0, riservato: 0x0, lunghezza: 40
Proposta: 1, ID protocollo: ESP, dimensione SPI: 4, #trans: 3
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 12
tipo: 1, riservato: 0x0, id: AES-CBC
IKEv2-PROTO-4: ultima trasformazione: 0x3, riservato: 0x0: lunghezza: 8
tipo: 3, riservato: 0x0, id: SHA96
IKEv2-PROTO-4: ultima trasformazione: 0x0, riservato: 0x0: lunghezza: 8
tipo: 5, riservato: 0x0, id:

Payload successivo **TSi**: TSr, riservato: 0x0, lunghezza: 24
Numero di TS: 1, riservato 0x0, riservato 0x0
Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
start port: 0, porta finale: 65535
start addr: 10.2.2.1, end addr: 10.2.2.1
Payload successivo **TSr**: NOTIFY, riservato: 0x0, lunghezza: 24
Numero di TS: 1, riservato 0x0, riservato 0x0
Tipo TS: TS_IPV4_ADDR_RANGE, ID porta: 0, lunghezza: 16
start port: 0, porta finale: 65535
start addr: 0.0.0.0, end addr: 255.255.255.255
IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x5
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Payload successivo: ENCR, versione: 2.0
IKEv2-PROTO-4: **Tipo di scambio: IKE_AUTH, flag: RISPOSTA MSG RESPONDER**

L'ASA invia questo messaggio di risposta IKE_AUTH, frammentato in nove pacchetti. Scambio IKE_AUTH completato.	IKEv2-PROTO-4: ID messaggio: 0x5, lunghezza: 4396 Payload successivo **ENCR**: AUTH, riservata: 0x0, lunghezza: 4368 Dati crittografati &due punti; 4364 byte IKEv2-PROTO-5: 6) Frammentazione del pacchetto in corso, MTU frammentata: 544, **Numero di frammenti: 9**, ID frammento: 3 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000005 IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: _OK IKEv2-PROTO-5: 6) Azione: Azione_Null IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento **AUTH_DONE**: EV_PKI_SESH_CLOSE ************************************ Data: 04/23/2013 Ora: 16:25:07 Tipo: Informazioni Origine: acvpnagent Descrizione: Funzione: log_ikev2 File: .\ikev2_anyconnect_osal.cpp Riga: 2730 **Connessione IPsec stabilita.** ************************************ Data: 04/23/2013 Ora: 16:25:07 Tipo: Informazioni Origine: acvpnagent Descrizione: Registrazione sessione IPsec: Crittografia: AES-CBC PRF SHA1 HMAC: SHA96 **Metodo di autenticazione locale: PSK** **Metodo di autenticazione remota: PSK** ID sequenza: 0

Dimensioni chiave: 192
Gruppo DH: 1
Ora reimpostazione chiave: 4294967 secondi
Indirizzo locale: 192.168.1.1
Indirizzo remoto: 10.0.0.1
Porta locale: 4500
Porta remota: 4500
ID sessione: 1
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnui

Descrizione: **Il profilo configurato sul gateway sicuro è: Anyconnect-ikev2.xml**
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnui

Descrizione: Informazioni sul tipo di messaggio inviate all'utente:
Creazione della sessione VPN in corso...
****

—Fine scambio IKE_AUTH—
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpndownloader

Descrizione: Funzione: ProfileMgr::caricaProfili
File: ..\Api\ProfileMgr.cpp
Riga: 148
Profili caricati:
C:\Documents and Settings\All Utenti\Dati applicazioni\Cisco\Cisco AnyConnect Secure Mobility Client\Profilo\anyconnect-ikev2.xml
****
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpndownloader

Descrizione: Impostazioni preferenze correnti:
Disabilitazione servizio: falso
Override archivio certificati: falso
Archivio certificati: Tutto
MostraMessaggioPreconnessione: falso
AutoConnectOnStart: falso
RiduciSuConnessione: vero
Accesso LAN locale: falso
Riconnessione automatica: vero

Comportamento riconnessione automatica: DisconnettiSuSospensione
UsaInizioPrimaAccesso: falso
Aggiornamento automatico: vero
RSASecurIDIntegrazione: Automatico
Imposizione accesso Windows: AccessoLocaleSingolo
WindowsVPNEstablishment: SoloUtentiLocali
Impostazioni proxy: Nativo
ConsentiConnessioniProxyLocali: vero
Esclusione PPPE: Disattiva
IPserverEsclusionePPE:
CriterioVPNautomatico: falso
CriterioReteAttendibile: Disconnetti
CriterioReteNonAttendibile: Connessione
Domini DNS attendibili:
Server DNS attendibili:
AlwaysOn: falso
Criterio ConnectFailure: Chiusa
AllowCaptivePortalRemediation: falso
Timeout di CaptivePortalRemediation: 5
ApplicaUltimeRegoleRisorseLocaliVPNL: falso
AllowVPNDisconnect: vero
Abilita scripting: falso
TerminateScriptOnNextEvent: falso
EnablePostSBLOnConnectScript: vero
SelezioneCertAutomatica: vero
Mantieni VpnOnLogoff: falso
Applicazione utente: SoloStessoUtente
AttivaSelezioneAutomaticaServer: falso
SelezioneAutomaticaServer: 20
TempoSospensioneSelezioneServerAutomatico: 4
Timeout autenticazione: 12
Integrazione SafeWordSofToken: falso
AllowIPsecOverSSL: falso
ClearSmartcardPin: vero
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnui

Descrizione: Informazioni sul tipo di messaggio inviate all'utente: **Definizione VPN - Analisi del sistema in corso...**
****

Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnui

Descrizione: Informazioni sul tipo di messaggio inviate all'utente: **Definizione della VPN - Attivazione della scheda VPN in corso...**
****

Data: 04/23/2013
Ora: 16:25:07

Tipo: Informazioni
Origine: acvpnagent

Descrizione: Funzione: CVirtualAdapter::RipristinoRegistroDiSistema
File: .\WindowsVirtualAdapter.cpp
Riga: 1869
Trovato tasto di controllo VA:
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control
****
Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnagent

Descrizione: **È stata rilevata una nuova interfaccia di rete.**
****
Data: 04/23/2013
Ora: 16:25:07
Tipo: Informazioni
Origine: acvpnagent

Descrizione: Funzione: CRouteMgr::interfacce log
File: .\RouteMgr.cpp
Riga: 2076
Funzione richiamata: logInterfacce
Codice restituito: 0 (0x00000000)
Descrizione: Elenco interfacce indirizzi IP:
10.2.2.1
192.168.1.1
****
Data: 04/23/2013
Ora: 16:25:08
Tipo: Informazioni
Origine: acvpnagent

Descrizione: Configurazione host:
Indirizzo pubblico: 192.168.1.1
Maschera pubblica: 255.255.255.0
Indirizzo privato: 10.2.2.1
Maschera privata: 255.0.0.0
Indirizzo IPv6 privato: N/D
Maschera IPv6 privata: N/D
Peer remoti: 10.0.0.1 (porta TCP 443, porta UDP 500), 10.0.0.1 (porta UDP 4500)
Reti private: nessuna
Reti pubbliche: nessuna
Modalità tunnel: sì
****

La connessione viene immessa nel database dell'associazione di protezione (SA, Security Association) e lo stato è

IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: **EV_INSERISCI_IKE**
IKEv2-PROTO-2: 6) **SA creato; inserimento di un'associazione di sicurezza nel database**

REGISTERED. L'appliance ASA esegue anche alcuni controlli, ad esempio le statistiche CAC (Common Access Card), la presenza di associazioni di protezione duplicate e imposta valori come DPD (Dead Peer Detection) e così via.

IKEv2-PLAT-3:
STATO CONNESSIONE: UP... peer: 192.168.1.1:25171, phase1_id: *$AnyConnect Client$*
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: **EV_REGISTRA_SESSIONE**
IKEv2-PLAT-3: (6) **username impostato su: Anu**
IKEv2-PLAT-3:
STATO CONNESSIONE: peer **REGISTRATO**: 192.168.1.1:25171, **phase1_id**
$AnyConnect Client$
IKEv2-PROTO-3: 6) Inizializzazione DPD, configurata per 10 secondi
IKEv2-PLAT-3: (6) mib_index impostato su: 4501
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: 6) Carica materiale della chiave IPSEC
IKEv2-PLAT-3: Mappa crittografica: corrispondenza su mappa dinamica dynmap seq 1000
IKEv2-PLAT-3: (6) Il **tempo massimo DPD sarà: 30**
IKEv2-PLAT-3: (6) Il **tempo massimo DPD sarà: 30**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: AVVIA
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: EV_CHECK_DUPE
IKEv2-PROTO-3: 6) **Ricerca di associazioni di protezione duplicate**
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento AUTH_DONE: V_CHK4_RUOLO
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento READY: EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: Nuova richiesta sa ikev2 attivata
IKEv2-PLAT-5: Conteggio decrementi per la negoziazione in ingresso
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento READY: _OK
IKEv2-PROTO-3: 6) Avvio del timer per eliminare il contesto di negoziazione
IKEv2-PROTO-5: 6) Traccia SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 Stato corrente: Evento READY: EV_NO_EVENT
IKEv2-PLAT-2: Ricevuto PFKEY add SA per SPI 0x77EE5348, errore FALSE
IKEv2-PLAT-2: È stato ricevuto un aggiornamento PFKEY SA per SPI 0x30B848A4. Errore FALSE
****

Data: 04/23/2013
Ora: 16:25:08
Tipo: Informazioni
Origine: acvpnagent

Descrizione: **La connessione VPN è stata stabilita e può ora passare dati.**
****

Data: 04/23/2013
Ora: 16:25:08
Tipo: Informazioni
Origine: acvpnui

Descrizione: Informazioni sul tipo di messaggio inviate all'utente: **Configurazione della VPN - Configurazione del sistema in corso...**
****
Data: 04/23/2013
Ora: 16:25:08
Tipo: Informazioni
Origine: acvpnui

Descrizione: Informazioni sul tipo di messaggio inviate all'utente: Creazione VPN in corso...
****
Data: 04/23/2013
Ora: 16:25:37
Tipo: Informazioni
Origine: acvpnagent

File: .\IPsecProtocol.cpp
Riga: 945
Tunnel IPsec stabilito
****

Verifica tunnel

AnyConnect

L'output di esempio del comando **show vpn-sessiondb detail anyconnect** è:

```
Session Type: AnyConnect Detailed

Username     : Anu                    Index        : 2
Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 11192
Pkts Tx      : 0                      Pkts Rx      : 171
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
Login Time   : 22:06:24 UTC Mon Apr 22 2013
Duration     : 0h:02m:26s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
```

```
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.1
  Encryption   : none                  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
  Client Type  : AnyConnect
Client Ver   : 3.0.1047
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 25171                 UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES192                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86254 Seconds
  PRF          : SHA1                  D/H Group    : 1
  Filter Name  :
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.2.2.1/255.255.255.255/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 0                     Bytes Rx     : 11192
  Pkts Tx      : 0                     Pkts Rx      : 171
 NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 146 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
Redirect URL :
```

ISAKMP

L'output di esempio del comando **show crypto ikev2 sa** è:

```
ASA-IKEV2#  show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
     Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
   Life/Active Time: 86400/112 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
```

L'output di esempio del comando **show crypto ikev2 sa detail** è:

```
ASA-IKEV2# show crypto ikev2 sa detail

IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
      Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/98 sec
      Session-id: 2
      Status Description: Negotiation done
      Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
      Local id: hostname=ASA-IKEV2
      Remote id: *$AnyConnectClient$*
      Local req mess id: 0              Remote req mess id: 9
      Local next mess id: 0             Remote next mess id: 9
      Local req queued: 0               Remote req queued: 9       Local window:
1                  Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

L'output di esempio del comando **show crypto ipsec sa** è:

```
ASA-IKEV2# show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

   local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 192.168.1.1, username: Anu
      dynamic allocated peer ip: 10.2.2.1

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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: 55

     local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
      path mtu 1488, ipsec overhead 82, media mtu 1500
      current outbound spi: 77EE5348
      current inbound spi : 30B848A4

  inbound esp sas:
     spi: 0x30B848A4 (817383588)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={RA, Tunnel,  NAT-T-Encaps, }
        slot: 0, conn_id: 8192, crypto-map: dynmap
        sa timing: remaining key lifetime (sec): 28685
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
```

```
    0xFFAD6BED 0x7ABFD5BF
outbound esp sas:
  spi: 0x77EE5348 (2012107592)
     transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={RA, Tunnel,  NAT-T-Encaps, }
     slot: 0, conn_id: 8192, crypto-map: dynmap
     sa timing: remaining key lifetime (sec): 28685
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
     0x00000000 0x00000001
```

Informazioni correlate

- RFC 4306, protocollo IKEv2 (Internet Key Exchange)
- RFC 3748, protocollo EAP (Extensible Authentication Protocol)
- RFC 5996, IKEv2 (Internet Key Exchange Protocol versione 2)
- Documentazione e supporto tecnico – Cisco Systems