ASA IKEv2-knooppunten voor VPN-probleemoplossing met externe toegang

Inhoud

Inleiding

Dit document beschrijft hoe u problemen op de Cisco adaptieve security applicatie (ASA) kunt begrijpen wanneer Internet Key Exchange versie 2 (IKEv2) wordt gebruikt met een Cisco AnyConnect Secure Mobility Client. Dit document bevat ook informatie over de manier waarop u bepaalde debug-lijnen in een ASA-configuratie kunt vertalen.

Dit document beschrijft niet hoe u verkeer door kunt geven nadat een VPN-tunnel aan de ASA is geïnstalleerd en bevat ook geen basisconcepten van IPSec of IKE.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van de pakketuitwisseling voor IKEv2. Raadpleeg voor meer informatie IKEv2 Packet Exchange en Protocol Level Debugging.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Internet Key Exchange versie 2 (IKEv2)
- Cisco adaptieve security applicatie (ASA) versie 8.4 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

kernvraagstuk

Het Cisco Technical Assistance Center (TAC) gebruikt vaak IKE en IPSec debug-opdrachten om te begrijpen waar er een probleem is met de IPSec VPN-tunnelvestiging, maar de opdrachten kunnen cryptisch zijn.

Scenario

Opdrachten debug

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

ASA-configuratie

Deze ASA-configuratie is strikt basis, zonder gebruik van externe servers.

```
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
```

XML-bestand

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

Opmerking: De naam van de GebruikerGroup in het XML clientprofiel moet dezelfde zijn als de naam van de tunnelgroep op de ASA. Anders geeft u het foutbericht 'Ongeldige hostvermelding. Voer het programma 'opnieuw in' is gezien op de AnyConnect-client.

Logs en beschrijvingen reinigen

Opmerking: Logs van het Diagnostics and Reporting Tool (DART) zijn over het algemeen erg handig, zodat bepaalde DART-logbestanden in dit voorbeeld zijn weggelaten omdat ze niet van belang zijn.

Beschrijving van serverbericht **Debugs**

Datum: 04/23/2013
Tijd: 16:24:55
Type: Informatie
Bron: acvpnuis

Beschrijving: Functie: ClientIfcBase::connect
Bestand: .\ClientIfcBase.cpp
Lijn: 964
De gebruiker heeft een VPN-verbinding met Anu-IKEV2 gevraagd.
****
Datum: 04/23/2013
Tijd: 16:24:55
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
Contact met Anu-IKEV2.
****
Datum: 04/23/2013
Tijd: 16:24:55
Type: Informatie
Bron: acvpnuis

Beschrijving: Functie: ApiCert:getCertList
Bestand: .\ApiCert.cpp
Lijn: 259
Aantal gevonden certificaten: 0
****
Datum: 04/23/2013
Tijd: 16:25:00
Type: Informatie
Bron: acvpnuis

Beschrijving: **VPN-verbinding initiëren naar de beveiligde gateway https://**
IKEV2
****
Datum: 04/23/2013
Tijd: 16:25:00
Type: Informatie
Bron: hulpstof

Beschrijving: Tunnel geopend door GUI-client.
****

Datum: 04/23/2013
Tijd: 16:25:02
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: CIPsec-protocol::connecttransport
Bestand: 2.2\IPsecProtocol.cpp

Lijn: 1629
Geopende IKE-ingang van 192.168.1.1:25170 tot 10.0.1:500
****

—IKE_SA_INIT Exchange start—

ASA ontvangt het IKE_SA_INIT bericht van de cliënt.
Het eerste paar berichten is de IKE_SA_INIT uitwisseling. Deze berichten onderhandelen over cryptografische algoritmen, uitwisselen nonces en doen een Diffie-Hellman (DH) uitwisseling.
Het IKE_SA_INIT bericht dat van de client wordt ontvangen bevat deze velden:

1. **ISAKMP-header** - SPI/versie/vlaggen.
2. **SAi1** - Cryptografisch algoritme dat IKE-initiator ondersteunt.
3. **KEi** - DH openbare sleutelwaarde van de initiator.
4. **N** - Initiator één keer.

IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1
InitSPI=0x58aff71141ba436b RespSPI=x 0000000000000000 MID=00000
IKEv2-PROTO-3: RX [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_i
IKEv2-PROTO-3: **HDR.**[i:58AFF71141B436B - r: 0000000000000000]
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - RSPI:** 000000
IKEv2-PROTO-4: Volgende lading: SA, **versie:** 2.0
IKEv2-PROTO-4: Wisseltype: IKE_SA_INIT, **vlaggen: INITIATOR**
IKEv2-PROTO-4: Bericht: 0x0, lengte: 528

SA volgende lading: KE, gereserveerd: 0x0, lengte: 168
IKEv2-PROTO-4: laatste voorstel : 0x0, gereserveerd: 0x0, lengte: 164
Voorstel: 1, Protocol-id: IKE, SPI-grootte: 0, #trans: 18
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: 3DES
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: DES
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: SHA512
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: SHA384
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: SHA256
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: SHA1
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: MD5
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA512
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA384
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA256
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA96
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: MD596
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 4, voorbehouden: 0x0, id: DH_GROUP_1536_MODP/Groep 5
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 4, voorbehouden: 0x0, id: DH_GROUP_1024_MODP/groep 2
IKEv2-PROTO-4: laatste transformatie: 0x0, gereserveerd: 0x0: lengte:
type: 4, voorbehouden: 0x0, id: DH_GROUP_768_MODP/Groep 1

KE Volgende lading: N, gereserveerd: 0x0, lengte: 104
DH-groep: 1, voorbehouden: 0x0

b 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 ed 5f
ba ba 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
21 c3 4d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
N volgende lading: VID, gereserveerd: 0x0, lengte: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
7c 0b
IKEv2-PROTO-5: Glasvezelspecifieke payload: CISCO-VERWIJDERING-
volgende lading: VID, gereserveerd: 0x0, lengte: 23

ASA verifieert en verwerkt de IKE_INIT bericht. De ASA:

1. Keuze van de crypto suite
   de voorstellen van de initiatiefnemer.
2. berekent zijn eigen DH geheime sleutel.
3. Berekent een SKEYID-waarde van
   die alle toetsen kunnen worden afgeleid van Deze IKE_SA. De kopregels van alle volgende berichten zijn : versleuteld en geauthentiseerd. Het gebruikte toetsen voor encryptie en bescherming van de integriteit wordt afgeleid van SKEYID en zijn bekend als:

   SK_e - Encryptie.**SK_a** - Verificatie.**SK_d** - Afgeleid en gebruikt voor afleiding van kuilmateriaal voor KIND_SA's.Een afzonderlijke SK_e en SK_a zijn
   berekend voor elke richting.

Versleuteld pakket:Gegevens: 528 bytes
IKEv2-PLAT-3: Aangepaste VID-lading verwerken
IKEv2-PLAT-3: Cisco Copyright VID ontvangen van peer
IKEv2-PLAT-3: AnyConnect EAP-VID ontvangen van peer
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: ONTBEELDI
EV_RECV_INIT
IKEv2-PROTO-3: (6): Controleer NAT-ontdekking
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: ONTBEELDI
EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): Controle omleiden is niet nodig, overslaan
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: ONTBEELDI
EV_CHK_CAC
IKEv2-PLAT-5: **New ikev2 als verzoek toegelaten**
IKEv2-PLAT-5: Toenemende onderhandeling als tellen met één
IKEv2-PLAT-5: ONGELDIG PSH-HANDJE
IKEv2-PLAT-5: ONGELDIG PSH-HANDJE
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: ONTBEELDI
EV_CHK_COOKIE
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: ONTBEELDI
EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_VERIFY_MSG
IKEv2-PROTO-3: (6): **Controleer SA in bericht**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_INSERT_SA
IKEv2-PROTO-3: (6): SA invoegen
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_GET_IKE_POLITION
IKEv2-PROTO-3: (6): **Regeringsbeleid verkrijgen**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B

Relevante configuratie:

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

R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_PROC_MSG
IKEv2-PROTO-2: (6): Eerste bericht verwerken
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_DETECT_NAT
IKEv2-PROTO-3: (6): NAT-ontdekking verwerken
IKEv2-PROTO-5: (6): Verwerking nat detectie src bericht
IKEv2-PROTO-5: (6): Remote-adres niet afgesloten
IKEv2-PROTO-5: (6): Datum van verwerking niet detecteren
IKEv2-PROTO-5: (6): Lokaal gekozen adres
IKEv2-PROTO-5: (6): Host is gevestigd in NAT buiten
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Ontvangen geldige configuratiemodemgegevens
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: (6): Instellen van ontvangen configuratiemodemgegeven
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_SET_POLITION
IKEv2-PROTO-3: (6): Instellen van ingesteld beleid
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_PKI_SESH_OPEN
IKEv2-PROTO-3: (6): Een PKI-sessie openen
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_GEN_DH_KEY
IKEv2-PROTO-3: (6): DH-toets berekenen
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_NO_EVENT
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: (6): Actie: Action_Null
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_GEN_DH_SECRET
IKEv2-PROTO-3: (6): DH-geheime toets berekenen
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_NO_EVENT
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R

EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: (6): Actie: Action_Null
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_GEN_SKEYID
IKEv2-PROTO-3: (6): **Skeyid genereren**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_GET_CONFIG_MODE
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R
EV_BLD_MSG
IKEv2-PROTO-2: (6): **eerste bericht verzenden**
IKEv2-PROTO-3: IKE-voorstel: 1, SPI-grootte: 0 (eerste onderhandeling)
Nee. transformeert: 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Groep 1
IKEv2-PROTO-5: Fabrikant specifieke payload: VERWIJDEREN-REASON
PROTO-5: Fabrikant specifieke payload: (DOUANE)IKEv2-PROTO-5: Fab
specifieke payload: (DOUANE)IKEv2-PROTO-5: Aanmelden bij payload:
NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Aanmelden bij payload
NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2: Ophalen vertrouwde
mislukt
IKEv2-PROTO-5: Fabrikant specifieke payload: FRAGMENTATIONIKEv2
[L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0
IKEv2-PROTO-3: **HDR.**[i:58AFF71141B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - RSPI: FC6963**
IKEv2-PROTO-4: Volgende lading: SA, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_SA_INIT, **vlaggen: RESPONDER MSG**
IKEv2-PROTO-4: Bericht: 0x0, lengte: 386
SA volgende lading: KE, gereserveerd: 0x0, lengte: 48
IKEv2-PROTO-4: laatste voorstel : 0x0, gereserveerd: 0x0, lengte: 44
Voorstel: 1, Protocol-id: IKE, SPI-grootte: 0, #trans: 4
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 2, voorbehouden: 0x0, id: SHA1
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA96
IKEv2-PROTO-4: laatste transformatie: 0x0, gereserveerd: 0x0: lengte:
type: 4, voorbehouden: 0x0, id: DH_GROUP_768_MODP/Groep 1

KE Volgende lading: N, gereserveerd: 0x0, lengte: 104
DH-groep: 1, voorbehouden: 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 FC7 76 83 1d 03 b0 d7
Geen volgende lading: VID, gereserveerd: 0x0, lengte: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 eg 97 b8 67

ASA bouwt het antwoordbericht voor IKE_SA_INIT uitwisseling. Dit pakket bevat:

1. **ISAKMP-header** - SPI/versie/vlaggen.
2. **SAr1** - Cryptografisch algoritme dat IKE-responder kiest.
3. **KEr** - DH openbare sleutelwaarde van de responder.
4. **N** - Responder één keer.

	d5 e7 c2 f5 VID volgende lading: VID, gereserveerd: 0x0, lengte: 23
De ASA stuurt het antwoordbericht voor IKE_SA_INIT uitwisseling. De IKE_SA_INIT uitwisseling is nu voltooid. De ASA start de timer voor het verificatieproces.	IKEv2-PLAT-4: VERZENDEN PKT [IKE_SA_INIT] [10.0.1]:500->[192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=FC69630e6b94d7f MID=00000000 IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event INIT_DONE: EV_DONE IKEv2-PROTO-3: (6): Fragmentation is ingeschakeld IKEv2-PROTO-3: (6): Cisco Delete Reason Notify is ingeschakeld IKEv2-PROTO-3: (6): Volledige SA-inruil IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event INIT_DONE: EV_CHK4_ROLE IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event INIT_DONE: EV_START_TMR IKEv2-PROTO-3: (6): Begintimer om te wachten op automatisch bericht (30 seconden) IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_WAIT_AUTH: EV_NO_EVENT **—IKE_SA_INIT compleet—** **— IKE_AUTH begint—** ********** Datum: 04/23/2013 Tijd: 16:25:00 Type: Informatie Bron: hulpstof Beschrijving: Beveiligde gatewayparameters: IP-adres: 10.0.0.1 Port: 443 URL: "10.0.0.1" Auteur: **IKE - EAP-AnyConnect** **IKE-identiteit:** ********** Datum: 04/23/2013 Tijd: 16:25:00	********** Datum: 04/23/2013 Tijd: 16:25:02 Type: Informatie Bron: hulpstof Beschrijving: Functie: CIPsec-p initiaalTunnel Bestand: 2.2\IPsecProtocol.cpp Lijn: 345 IPsec-tunnel start **********

	Type: Informatie Bron: hulpstof Beschrijving: **Cisco AnyConnect Secure Mobility Client-verbinding, versie** ********** Datum: 04/23/2013 Tijd: 16:25:02 Type: Informatie Bron: hulpstof Beschrijving: Functie: ikev2_log Bestand: .\ikev2_anyconnect_osal.cpp Lijn: 2730 **Ontvangen verzoek om een IPsec-tunnel op te zetten; lokale verkeerskiez** **adresbereik: 0.0.0.0-255.255.255.255 Protocol: 0 poortbereik: 0-65535; S** **afstandsverkeer = adresbereik: 0.0.0.0-255.255.255.255 Protocol: 0 poort** **65535** ********** Datum: 04/23/2013 Tijd: 16:25:02 Type: Informatie Bron: hulpstof Beschrijving: Functie: CIPsec-protocol::connecttransport Bestand: 2.2\IPsecProtocol.cpp Lijn: 1629 **Geopende IKE-ingang van 192.168.1.1:25171 tot 10.0.1:4500** **********
Verificatie vindt plaats met EAP. Binnen een MAP-gesprek is slechts één MAP-verificatiemethode toegestaan. ASA ontvangt het IKE_AUTH bericht van de client.	IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:**4** InitSPI=0x58aff7141ba436Resultaat pSPI=0xfc696330e6b94d7f MID=000 IKEv2-PROTO-3: **RX** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
Wanneer de client een IDi-lading bevat maar geen AUTH-lading. de cliënt heeft zijn identiteit verklaard , maar niet bewezen. In de uiteinden is AUTH lading is niet aanwezig in IKE_AUTH pakket verzonden door de client. De cliënt de AUTH-lading pas na de De MAP-uitwisseling is succesvol. Als de ASA bereid is een verlengbaar middel te gebruiken authenticatiemethode : er wordt een MAP	IKEv2-PROTO-3: **HDR.**[i:58AFF71141B436B - r: FC69630E6B94D7F] IKEv2-PROTO-4: IKEV2 **HDR ispi: 58AFF71141BA436B - RSPI: FC6963** IKEv2-PROTO-4: Volgende lading: ENCR, **versie:** 2.0 IKEv2-PROTO-4: Wisseltype: IKE_AUTH, **vlaggen: INITIATOR** IKEv2-PROTO-4: Bericht: 0x1, lengte: 540 IKEv2-PROTO-5: (6): Aanvraag heeft zootje_id 1; Verwacht 1 tot en met 1 REAL gedecrypteerd pakket:Gegevens: 465 bytes IKEv2-PROTO-5: Glasvezelspecifieke payload: (AANGEPAST) VID Volge IDi, gereserveerd: 0x0, lengte: 20 58 af f6 11 52 8d b0 2c b8 da 30 46 be 91 56 fa **IDi** volgende lading: CERTREQ, voorbehouden: 0x0, lengte: 28 **Type identificatie: Groepsnaam**, voorbehouden: 0x0 0x0 2 bis 24 41 6e 79 43 6f 6e 65 63 74 43 6c 69 65 6 sexies 74 24 2 bis **CERTREQ** volgende lading: CFG, gereserveerd: 0x0, lengte: 25 Cert encodering X.509 Certificaat - handtekening

payload in bericht 4 en het verzenden van
SAr2, TSi, en TSr tot de initiatiefnemer
Verificatie is voltooid in een daaropvolgende IKE_AUTH-uitwisseling.
Het initiatorpakket IKE_AUTH bevat:

1. **ISAKMP-header** - SPI/versie/vlaggen.
2. **IDi** - De naam van de tunnelgroep die de cliënt wenst verbinding te maken met kan door de IDi worden geleverd lading van type ID_KEY_ID in de eerste boodschap van de IKE_AUTH-uitwisseling. Dit gebeurt wanneer het clientprofiel* is vooraf ingesteld met een groepsnaam of, na een vorige succesvol authenticatie de cliënt de naam van de groep in zijn voorkeuren-bestand. De ASA pogingen om een tunnel-groep aan te passen naam met de inhoud van het IKE IDi lading. Na de eerste succesvol IPSec VPN is de cliënt neemt de groepsnaam (alias groep) waaraan de gebruiker is echt bevonden. Deze groep de naam wordt in het IDi geleverd lading van de volgende verbinding

CertReq data: 20 bytes
CFG volgende lading: SA, gereserveerd: 0x0, lengte: 196
cfg-type: **CFG_REQUEST**, alleen: 0x0, gereserveerd: 0x0

type attrib: intern IP4-adres, lengte: 0

type attrib: interne IP4-netmasker, lengte: 0

type attrib: interne IP4 DNS, lengte: 0

type attrib: interne IP4 NBS, lengte: 0

type attrib: interne adresaanduiding, lengte: 0

type attrib: toepassingsversie, lengte: 27

41 6e 79 43 6f 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
type attrib: intern IP6-adres, lengte: 0

type attrib: interne IP4-SUBNET, lengte: 0

type attrib: Onbekend - 28682, lengte: 15

77 69 6e 78 70 36 34 74 65 60 d 70 6c 61 74 65
type attrib: Onbekend - 28704, lengte: 0

type attrib: Onbekend - 28705, lengte: 0

type attrib: Onbekend - 28706, lengte: 0

type attrib: Onbekend - 28707, lengte: 0

type attrib: Onbekend - 28708, lengte: 0

type attrib: Onbekend - 28709, lengte: 0

type attrib: Onbekend - 28710, lengte: 0

type attrib: Onbekend - 28672, lengte: 0

type attrib: Onbekend - 28684, lengte: 0

type attrib: Onbekend - 28711, lengte: 2

05 7e
type attrib: Onbekend - 28674, lengte: 0

type attrib: Onbekend - 28712, lengte: 0

type attrib: Onbekend - 28675, lengte: 0

type attrib: Onbekend - 28679, lengte: 0

probeert de waarschijnlijke groep gewenst door de gebruiker. Wanneer MAP-authenticatie door de cliënt gespecificeerd of geïmpliceerd profiel en het profiel niet de <IKEIdentity> de cliënt stuurt een ID_GROUP type IDi lading met de vaste string *$AnyConnectClient$*.

3. **CERTREQ** - De cliënt is de ASA om een geprefereerd certificaat. Certificaat aanvraag-betaling kan worden opgenomen in een ruil wanneer de verzender moet het certificaat van ontvanger. Het certificaatverzoek lading wordt verwerkt door inspectie van de "Cert-codering" te bepalen of de verwerker certificaten van dit type. Zo ja, dan Het veld van de certificeringsinstantie is: geïnspecteerd om te bepalen of de verwerker over elk certificaat beschikt die kunnen worden gevalideerd tot een van de gespecificeerde certificering autoriteiten. Dit kan een ketting zijn certificaten.

type attrib: Onbekend - 28683, lengte: 0

type attrib: Onbekend - 28717, lengte: 0

type attrib: Onbekend - 28718, lengte: 0

type attrib: Onbekend - 28719, lengte: 0

type attrib: Onbekend - 28720, lengte: 0

type attrib: Onbekend - 28721, lengte: 0

type attrib: Onbekend - 28722, lengte: 0

type attrib: Onbekend - 28723, lengte: 0

type attrib: Onbekend - 28724, lengte: 0

type attrib: Onbekend - 28725, lengte: 0

type attrib: Onbekend - 28726, lengte: 0

type attrib: Onbekend - 28727, lengte: 0

type attrib: Onbekend - 28729, lengte: 0

SA volgende lading: TSi, voorbehouden: 0x0, lengte: 124
IKEv2-PROTO-4: laatste voorstel : 0x0, gereserveerd: 0x0, lengte: 120
Voorstel: 1, Protocol-id: ESP, SPI-grootte: 4, #trans: 12
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: 3DES
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: DES
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: NULL
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA512
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA384
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA256
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA96
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: MD596
IKEv2-PROTO-4: laatste transformatie: 0x0, gereserveerd: 0x0: lengte:

4. **CFG** - CFG_REQUEST/ Met CFG_REPLY kan een IKE worden gemaakt eindpunt om informatie te vragen van zijn peer. Als een eigenschap in het Configuratie CFG_REQUEST lading is geen lengte nul, het is als suggestie attribuut.The CFG_REPLY configuratielading kan terugvloeien die waarde of een nieuwe. Het kan voegt ook nieuwe eigenschappen toe en niet enkele aanvragen omvatten . Verscheidene aanvragen negeren teruggestuurd eigenschappen die zij niet herkennen. In deze uitwerpselen, cliënt vraagt om de tunnel configuratie in de CFG_REQUEST. De ASA antwoorden hierop en sturen de tunnel alleen nadat de MAP-uitwisseling is succesvol.
5. **SAi2** - SAi2 initieert de SA, die vergelijkbaar is met fase 2 zet de set exchange in IKEv1 om.
6. **TSi** en **TSr** - de initiator en

type: 5, voorbehouden: 0x0, id:

TSi volgende lading: TSr, gereserveerd: 0x0, lengte: 24
Aantal TS: 1, gereserveerd 0x0, gereserveerd 0x0
TS-type: TS_IPV4_ADDR_RANGE, proxy-id: 0, lengte: 16
startpoort: 0, eindpoort: 65535
startpunt: 0.0.0.0, laatste regel: 255.255.255.255
TSr volgende lading: KENNISGEVING, voorbehouden: 0x0, lengte: 24
Aantal TS: 1, gereserveerd 0x0, gereserveerd 0x0
TS-type: TS_IPV4_ADDR_RANGE, proxy-id: 0, lengte: 16
startpoort: 0, eindpoort: 65535
startpunt: 0.0.0.0, laatste regel: 255.255.255.255

selectieschakelaars voor het luchtverkeer bevat respectievelijk de bron en het adres van de bestemming initiator en responder om versleuteld verkeer. Het adresbereik specificeert alle verkeer van en naar dat bereik wordt gekanaliseerd . Als de het voorstel is aanvaardbaar voor antwoordapparaat: het stuurt identieke TS terugbetaling .

De eigenschappen die de cliënt moet leveren groepsidentificatie opgeslagen in een AnyConnect-profielbestand.

***Relevante profielconfiguratie:**

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
```

```
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

ASA genereert een reactie op het IKE_AUTH-bericht en bereidt zich voor om zichzelf op de client te authentiseren.

Versleuteld pakket: Data: 540 bytes
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van R_WAIT_AUTH: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Time-out stilzetten om automatisch bericht te wacht
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van R_WAIT_AUTH: EV_CHK_NAT_T
IKEv2-PROTO-3: (6): Controleer NAT-ontdekking
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van R_WAIT_AUTH: EV_CHG_NAT_T_POORT

IKEv2-PROTO-2: (6): NAT gedetecteerde float naar initpoort 25171, resp.
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_PROC_ID
IKEv2-PROTO-2: (6): Ontvangen geldige parameters in procesid
IKEv2-PLAT-3: 6 . " peer auth " - methode ingesteld op : 0
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHK_FOR_PROF_SEL
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Regeringsbeleid verkrijgen
IKEv2-PLAT-3: Nieuwe AnyConnect-clientverbinding gedetecteerd op bas
lading
IKEv2-PLAT-3: my_auth_methods = 1
IKEv2-PLAT-3: 6 . " peer auth " - methode ingesteld op : 256
IKEv2-PLAT-3: Ondersteund_peers_auth_methods = 16
IKEv2-PLAT-3: (6) tp_name ingesteld op: Anu-ikev2
IKEv2-PLAT-3: **trust point ingesteld op :** Anu-ikev2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Vertaling van IKE_ID_AUTO naar = 9
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_SET_POLITION
IKEv2-PROTO-3: (6): **Instellen van ingesteld beleid**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Controleer het beleid van peer
IKEv2-PROTO-3: (6): **Overeenkomend certificaat gevonden**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Ontvangen geldige configuratiemodemgegevens
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3: (6) DHCP-hostname voor DDNS is ingesteld op: winxp64F
IKEv2-PROTO-3: (6): Instellen van ontvangen configuratiemodemgegeven
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_WAIT_AUTH: EV_CHK_EAP
IKEv2-PROTO-3: (6): **Controleer op EAP-ruil**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event **van E**
EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Mijn verificatiegegevens genereren**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van F
EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Verkrijg mijn authenticatiemethode
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van F
EV_SIGN
IKEv2-PROTO-3: (6): **Auditgegevens tekenen**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van F
EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_BLD_EAP_AUTH_REQ: EV_AUTHEN_REQ
IKEv2-PROTO-2: (6): **De authenticator verzoeken om een MAP-aanvraag**
Naam **van** een element **configuratie-auth maken**
Toegevoegde eigenschap name client waarde vpn aan element configura
Toegevoegde eigenschap naam type waarde hallo aan element configura
Naam van het samengestelde element, versie 9.0(2)8
Optie waarde 9.0(2)8 van de naam van een toegevoegd element in een co
auth
Toegevoegde eigenschap naam die waarde sg aan element versie waard
Gegenereerd XML bericht hieronder
<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="hallo**">
<versie die="sg">9.0(2)8</versie>
</mede-auth>

IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_BLD_EAP_AUTH_REQ: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Actie: Action_Null
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_BLD_EAP_AUTH_REQ: EV_CHK_REDIRECT
IKEv2-PROTO-3: (6): Controleer omleiden met platform voor taakverdelin
IKEv2-PLAT-3: Controleer op platform omleiden
IKEv2-PLAT-3: ikev2_osal_redirect: Door 10.0.0.1 geaccepteerde sessie
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 0000001 CurState: Event van
R_BLD_EAP_AUTH_REQ: EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2: (6): **Toezending van een MAP-aanvraag**
IKEv2-PROTO-5: Fabrikant specifieke payload: CISCO-GRANITEIKEv2-F
gebouwd

De ASA stuurt de AUTH-lading naar de klant om gebruikersreferenties. ASA stuurt de AUTH-methode als 'RSA', zodat het zijn eigen certificaat naar de client stuurt, zodat de client de ASA-server kan authenticeren. Aangezien de ASA bereid is een extensibele

IDr. Volgende lading: CERT, voorbehouden: 0x0, lengte: 36
Type identificatie: DER ASN1 DN, voorbehouden: 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
CERT volgende lading: CERT, voorbehouden: 0x0, lengte: 436
Cert encodering X.509 Certificaat - handtekening
gegevens en kolommen doen oplichten; 431 bytes
CERT volgende lading: AUTH, gereserveerd: 0x0, lengte: 436
Cert encodering X.509 Certificaat - handtekening

authenticatiemethode te gebruiken, plaatst het een MAP nuttige lading in bericht 4 en verbiedt het verzenden van SAr2, TSi en TSr tot de initiator authenticatie voltooid is in een volgende IKE_AUTH uitwisseling. Deze drie nuttige ladingen zijn dus niet aanwezig in de debugs.
Het EAP-pakket bevat:

1. **Code: verzoek** - Deze code wordt door de authenticator naar de peer verzonden.
2. **id: 1** - De steun helpt de MAP-reacties te koppelen aan de verzoeken. Hier is de waarde 1, wat aangeeft dat het het eerste pakket in de EAP-ruil is. Dit MAP-verzoek heeft het type "configuratie-auth" van "hallo"; het wordt van de ASA naar de klant gestuurd om de MAP-uitwisseling te starten.
3. **Length: 150** - De lengte van het EAP-pakket omvat de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

gegevens en kolommen doen oplichten; 431 bytes
AUTH-volgende lading: EAP, gereserveerd: 0x0, lengte: 136
Auth-methode RSA, voorbehouden: 0x0, gereserveerd, 0x0
Auth data: 128 bytes
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 154
Code: verzoek: **id**: 1, **lengte**: 150
Type: Onbekend - 254
EAP-gegevens: 145 bytes

IKEv2-PROTO-3: TX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: **HDR.**[i:58AFF71141B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963**
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_AUTH, **vlaggen: RESPONDER MSG-R**
IKEv2-PROTO-4: Bericht: 0x1, lengte: 1292
ENCR volgende lading: VID, gereserveerd: 0x0, lengte: 1264
Versleuteld gegevens en kolommen; 1260 bytes

Fragmentatie kan resulteren als de certificaten groot zijn of als de certificatenketens zijn opgenomen. Zowel initiator- als responder KE-nuttige ladingen kunnen ook grote sleutels bevatten, die ook kunnen bijdragen tot fragmentatie.

IKEv2-PROTO-5: (6): Fragmentatiepakket, Fragmentatie MTU: 544, **Aanta**
3. Fragment-ID: 1
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000

****

Datum: 04/23/2013
Tijd: 16:25:02
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: ikev2_verify_X509_SIG_certs
Bestand: .\ikev2_anyconnect_osal.cpp

Lijn: 2077
Certificaatacceptatie door gebruiker aanvragen
****

Datum: 04/23/2013
Tijd: 16:25:02
Type: Fout
Bron: acvpnuis

Beschrijving: Functie: ApiCertificate::verifykettingbeleid
Bestand: \Certificates\CapiCertificate.cpp
Lijn: 2032
Vervroegde functie: Controleercertificaatbeleid
Retourencode: -2146762487 (0x800b0109)
Beschrijving: Een certificeringsketen verwerkt, maar beëindigd in een basi
niet door de trust provider wordt vertrouwd.
****

Datum: 04/23/2013
Tijd: 16:25:04
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: CEAPMgr: DataApplicationCB
Bestand: .\EAPMgr.cpp
Lijn: 400
Door MAP voorgesteld type: EAP-ANYCONNECT
****

De klant reageert met een antwoord op het MAP-verzoek.
Het EAP-pakket bevat:

1. **Code: respons** - Deze code wordt door de peer naar de authenticator gestuurd in antwoord op het MAP verzoek.
2. **id: 1 -** De steun helpt de MAP-reacties te koppelen aan de verzoeken. Hier is de waarde 1, wat aangeeft dat dit een antwoord is op het eerder door de ASA verzonden verzoek (authenticator). Dit MAP-antwoord heeft het type "configuratie-auth" van "init"; de cliënt initialiseert de MAP-beurs en wacht op de ASA om een verificatieaanvraag te

IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:4
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
IKEv2-PROTO-3: RX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_AUTH, vlaggen: INITIATOR
IKEv2-PROTO-4: Bericht: 0x2, lengte: 332
IKEv2-PROTO-5: (6): Aanvraag heeft zootje_id 2. verwacht 2 tot 2
REAL gedecrypteerd pakket:Gegevens: 256 bytes
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 256
Code: antwoord : **id: 1**, **lengte**: 252
Type: Onbekend - 254
EAP-gegevens:247 bytes
Versleuteld pakket: Data: 332 bytes
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van
R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Time-out stilzetten om automatisch bericht te wacht
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van
R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van
R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Verwerking van de MAP-respons**
Ontvangen XML bericht hieronder van de cliënt

doen.

3. **Length: 252** - De lengte van het EAP-pakket bestaat uit de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

ASA decrypteert deze reactie, en de client zegt dat hij de AUTH payload in het vorige pakket heeft ontvangen (met het certificaat) en het eerste EAP-aanvraagpakket van de ASA heeft ontvangen. Dit is wat het pakket met antwoorden op de vragen "in" EAP bevat.

<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="init"**>
<apparaat-id>win</apparaat-id>
<versie die="vpn">3.0.1047</versie>
<groep-selectie>ASA-IKEV2</groep-selectie>
<groepstoegang>ASA-IKEV2</groepstoegang>
</mede-auth>
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van R_PROC_EAP_RESP: **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5: (6): Actie: Action_Null
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van R_BLD_EAP_REQ: **EV_RECV_EAP_REQ**

Dit is het tweede verzoek dat de ASA aan de cliënt heeft gestuurd.
Het EAP-pakket bevat:

1. **Code: verzoek** - Deze code wordt door de authenticator naar de peer verzonden.
2. **id: 2** - De steun helpt de MAP-reacties af te stemmen op de verzoeken. Hier is de waarde 2, wat aangeeft dat het het tweede pakket in de uitwisseling is. Dit verzoek heeft het "configuratie-auth"-type van het "auth-request"; de ASA verzoekt de klant de gebruikersverificatiegegevens te verzenden.
3. **Length: 457** - De lengte van het EAP-pakket omvat de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

IKEv2-PROTO-2: (6): Toezending van een MAP-aanvraag
Gegenereerd XML bericht hieronder
<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="auth-request"**>
<versie die="sg">9.0(2)8</versie>
<opaque is-for="sg">
<tunnelgroep>ASA-IKEV2</tunnelgroep>
<span-hash>1367268141499</fig-hash>
</ondoorzichtig>
<transport>443</transport>
<auth id="main">
<formulier>
<input type="text" name="gebruikersnaam" label="Gebruikersnaam:"></input>
<type invoer="wachtwoord" name="wachtwoord" label="Wachtwoord:"></invoer>
</formulier>
</u>
</mede-auth>
IKEv2-PROTO-3: (6): het bouwpakket voor encryptie; de inhoud is :
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 461
Code: verzoek: id: 2, lengte: 457
Type: Onbekend - 254
EAP-gegevens: 452 bytes

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:58AFF71141B436B - r:

ENCR-lading:
Deze lading wordt gedecrypteerd, en de inhoud ervan wordt geparseerd als extra lading.

****
Datum: 04/23/2013
Tijd: 16:25:04
Type: Informatie
Bron: acvpnuis

Beschrijving: Functie: SDIMgr: ProcentPromptData
Bestand: .\SDIMgr.cpp
Lijn: 281
Verificatietype is geen SDI.
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: acvpnuis

Beschrijving: Functie: ConnectM
gebruikersrespons
Bestand: .\ConnectMgr.cpp
Lijn: 985
Reactie van gebruiker verwerke
****

FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC69630E6B94D7F
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_AUTH, vlaggen: **RESPONDER MSG-REACTIE**
IKEv2-PROTO-4: Bericht: 0x2, lengte: 524
ENCR-volgende lading: EAP, gereserveerd: 0x0, lengte: 496
Versleuteld gegevens en kolommen; 492 bytes

IKEv2-PLAT-4: **SENT PKT [IKE_AUTH]** [10.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6): **Begintimer om op gebruikersaanpassingsbericht te wachten** (120 seconden)
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000002 CurState: Event van R_WAIT_EAP_RESP: EV_NO_EVENT

Cliënt stuurt een ander IKE_AUTH initiator-bericht met de MAP-lading.
Het EAP-pakket bevat:

1. **Code: respons** - Deze code wordt door de peer naar de authenticator gestuurd in antwoord op het MAP verzoek.
2. **id: 2** - De steun helpt de MAP-reacties af te stemmen op de verzoeken. Hier is de waarde 2, wat aangeeft dat dit een antwoord is op het eerder door de ASA verzonden verzoek (authenticator).

IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PROTO-3: RX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: **Wisseltype: IKE_AUTH, vlaggen: INITIATOR**
IKEv2-PROTO-4: Bericht: 0x3, lengte: 492
IKEv2-PROTO-5: (6): Aanvraag heeft zootje_id 1; verwacht 3 tot 3

REAL gedecrypteerd pakket:Gegevens: 424 bytes
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 424
Code: antwoord : id: 2, lengte: 420
Type: Onbekend - 254
EAP-gegevens: 415 bytes

3. **Length: 420** - De lengte van het EAP-pakket omvat de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

De ASA verwerkt dit antwoord. De cliënt had gevraagd om de gebruiker in te schrijven. Deze MAP-reactie heeft het 'configuratie-auth'-type van 'auth-antwoording'. Dit pakket bevat de door de gebruiker ingevoerde referenties.

Versleuteld pakket:Gegevens: 492 bytes
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Time-out stilzetten om automatisch bericht te wacht
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Verwerking van de MAP-respons**
Ontvangen XML bericht hieronder van de cliënt
<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="auth-antwoordt"**>
<apparaat-id>win</apparaat-id>
<versie die="vpn">3.0.1047</versie>
<Sessietoken></Sessie-token>
<sessie-id></sessie-id>
<opaque is-for="sg">
<tunnelgroep>**ASA-IKEV2**</tunnelgroep>
<span-hash>1367268141499</fig-hash></opaque>
<auth>
<wachtwoord>cisco123</wachtwoord>
<gebruikersnaam>Anu</gebruikersnaam></auth>
</mede-auth>
IKEv2-PLAT-1: **EAP:geïnitieerde gebruikersverificatie**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_PROC_EAP_RESP: EV_NO_EVENT
IKEv2-PLAT-5: EAP:In AAA terugbellen
Recentste serverfout: DACE1C274785F28B-B11D6453096BAE294A3172
IKEv2-PLAT-5: **EAP:succes in AAA terugbellen**
IKEv2-PROTO-3: Ontvangen respons van de authenticator
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_PROC_EAP_RESP: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Actie: Action_Null

De ASA bouwt een derde MAP verzoek in de ruil. Het EAP-pakket bevat:

1. **Code: verzoek** - Deze code wordt door de authenticator naar de peer verzonden.
2. **id: 3** - De steun helpt de MAP-reacties af te

IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van R_BLD_EAP_REQ: EV_RECV_EAP_REQ
IKEv2-PROTO-2: (6): Toezending van een MAP-aanvraag
Gegenereerd XML bericht hieronder
<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="complete"**>
<versie die="sg">9.0(2)8</versie>
<sessie-id>32768</sessie-id>

stemmen op de verzoeken. Hier is de waarde 3, wat aangeeft dat het het derde pakket in de uitwisseling is. Dit pakje heeft het "configuratie-auth"-type van "complete"; de ASA heeft een antwoord ontvangen en de EAP-uitwisseling is voltooid.
3. **Length: 4235** - De lengte van het EAP-pakket omvat de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

ENCR-lading:
Deze lading wordt gedecrypteerd, en de inhoud ervan wordt geparseerd als extra lading.

<Sessietoken>18wA0TTGmDxPKQCywC7fB7EWLCEgz-ZtjYpAyXX2yJH0H3G3H8t5xpBOx3Ixag</sessie-token>
<auth id="Success">
<bericht id="0" param1="" param2=""></bericht>
</u>

IKEv2-PROTO-3: (6): het bouwpakket voor encryptie; de inhoud is :
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 4239
Code: verzoek: id: 3, lengte: 4235
Type: Onbekend - 254
EAP-gegevens: 4230 bytes

IKEv2-PROTO-3: TX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963(
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_AUTH, vlaggen: **RESPONDER MSG-R**
IKEv2-PROTO-4: Bericht: 0x3, lengte: 4300
ENCR volgende lading: EAP, gereserveerd: 0x0, lengte: 4272
Versleuteld gegevens en kolommen;4268 bytes
IKEv2-PROTO-5: (6): Fragmentatiepakket, Fragmentatie MTU: 544, **Aanta**
9, Fragment-ID: 2
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=FC696330e6b94d7f MID=000000
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van
R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6): Begintimer om te wachten op gebruikersaanpassing
seconden)
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000003 CurState: Event van
R_WAIT_EAP_RESP: EV_NO_EVENT
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: **Huidige profiel:** Anyconnect-ikev2.xml
Instellingen voor VPN-sessie ontvangen:
Installeren: ingeschakeld
Proxyinstelling: wijzigen
Proxyserver: none
Proxy PAC-URL: none
Uitzonderingen voor proxy: none
Proxy-vergrendeling: ingeschakeld
Uitsluiten splitter: voorkeur voor lokale LAN-toegang is uitgeschakeld
Splitsen omvatten: gehandicapt
DNS splitsen: gehandicapt
Local LAN Wildcard: voorkeur voor lokale LAN-toegang is uitgeschakeld
Firewallregels: none
Clientadres: 10.2.2.1
Clientmasker: 255.0.0.0
Clientadres: IPv6: onbekend
Clientmasker voor IPv6: onbekend
MTU: 1406
IKE bewaar het programma: 20 seconden
IKE DPD: 30 seconden
Time-out sessie: 0 seconden
Time-out verbroken: 1800 seconden
Time-out bij inactiviteitstimer: 1800 seconden
Server: onbekend
MUS-host: onbekend
DAP-gebruikersbericht: none
Quarantine State: gehandicapt
Altijd op VPN: niet gehandicapt
Duur lease: 0 seconden
Standaarddomein: onbekend
startpagina: onbekend
Smart Card Verwijdering-verbinding: ingeschakeld
Reactie op licentie: onbekend
****

De klant stuurt het startpakket met de MAP-lading.
Het EAP-pakket bevat:

1. **Code: respons** - Deze code wordt door de peer naar de authenticator gestuurd in antwoord op het MAP verzoek.
2. **id: 3** - De steun helpt de MAP-reacties af te stemmen op de verzoeken. Hier is de waarde 3, wat aangeeft dat dit een antwoord is op het eerder door de ASA verzonden verzoek (authenticator). De ASA

IKEv2-PLAT-4: **RECV PKT** [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4
InitSPI=0x58aff71141ba436b Resp I=0xfc696330e6b94d7f=00000004
IKEv2-PROTO-3: RX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: **Wisseltype: IKE_AUTH, vlaggen: INITIATOR**
IKEv2-PROTO-4: Bericht: 0x4, lengte: 252
IKEv2-PROTO-5: (6): Aanvraag heeft zootje_id 4; verwacht 4 tot 4

REAL gedecrypteerd pakket:Gegevens: 177 bytes
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 177
Code: antwoord : id: 3, lengte: 173
Type: Onbekend - 254
EAP-gegevens: 168 bytes

ontvangt nu het responspakket van de klant, dat het "configuratie-auth" type van "ack" heeft; in dit antwoord wordt de reeds door de ASA verstuurde "complete" boodschap van het MAP erkend .

3. **Length: 173** - De lengte van het EAP-pakket omvat de code, id, lengte en EAP-gegevens.
4. **EAP-gegevens**.

De ASA verwerkt dit pakket. Het De MAP-uitwisseling is succesvol. De ASA bereidt zich voor op het sturen van de tunnelgroep configuratie in het volgende pakket, dat eerder door de cliënt in de lading van de IDi. De ASA ontvangt de reactiepakket van de client, dat heeft het "configuratie-auth"-type van "ack". Dit antwoord erkent dat het MAP "complete" boodschap die door de ASA al eerder.

Versleuteld pakket:Data:252 bytes
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Time-out stilzetten om automatisch bericht te wacht
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Verwerking van de MAP-respons**
Ontvangen XML bericht hieronder van de cliënt
<?xml versie="1.0" codering="UTF-8">
<span-auth client="vpn" **type="ack"**>
<apparaat-id>win</apparaat-id>
<versie die="vpn">3.0.1047</versie>
</mede-auth>

Relevante configuratie:

```
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
```

IKEv2-PLAT-3: (6) AutoHD ingesteld op 0x2000
IKEv2-PLAT-3: (6) **tg_name ingesteld op: ASA-IKEV2**
IKEv2-PLAT-3: (6) **tunneltype ingesteld op: RA**
IKEv2-PLAT-1: **EAP:Verificatie geslaagd**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_PROC_EAP_RESP: EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2: (6): Toezending van een EAP-statusbericht
IKEv2-PROTO-3: (6): het bouwpakket voor encryptie; de inhoud is :
EAP volgende lading: NIET, voorbehouden: 0x0, lengte: 8
Code: succes : id: 3, lengte: 4

De MAP-beurs is nu succesvol.
Het EAP-pakket bevat:

1. **Code**: **succes** - Deze code is door de

IKEv2-PROTO-3: TX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: Wisseltype: IKE_AUTH, vlaggen: RESPONDER MSG-R
IKEv2-PROTO-4: Bericht: 0x4, lengte: 76

echtheidscontrole aan de peer na voltooiing van een MAP authenticatiemethode. Dit geeft aan dat het peer geauthentiseerd naar de authenticator. 2. **id: 3** - De hulp komt overeen met het EAP-antwoorden met de verzoeken. Hier is de waarde 3, die geeft aan dat dit een antwoord is op het eerder door de ASA (authenticator). De derde set van pakketten in de ruil succesvol, en de EAP-uitwisseling is succesvol. 3. **Length: 4** - lengte van het MAP het pakket de code bevat, lengte en MAP gegevens. 4. **EAP-gegevens**.	ENCR volgende lading: EAP, gereserveerd: 0x0, lengte: 48 Versleuteld gegevens en kolommen;44 bytes IKEv2-PLAT-4: **SENT PKT [IKE_AUTH]** [10.0.1]:4500->[192.168.1.1]:2517 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000 IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event van R_PROC_EAP_RESP: EV_START_TMR IKEv2-PROTO-3: (6): Begintimer om te wachten op automatisch bericht (3 IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000000 CurState: Event **van** **R_WAIT_EAP_AUTH_VERIFY**: EV_NO_EVENT
Aangezien de EAP-uitwisseling succesvol is, verstuurt de klant het pakket IKE_AUTH-initiator met de AUTH-lading. De AUTH-lading is gegenereerd vanuit de gedeelde geheime sleutel.	IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4 InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000 IKEv2-PROTO-3: RX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_ IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F] IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963 IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0 IKEv2-PROTO-4: Wisseltype: IKE_AUTH, **vlaggen: INITIATOR** IKEv2-PROTO-4: Bericht: 0x5, lengte: 92 IKEv2-PROTO-5: (6): Aanvraag heeft zootje_id 5. verwacht 5 tot 5
Wanneer MAP-verificatie wordt gespecificeerd of het klantprofiel en het het profiel bevat niet <IKEIdentity>-element, de client verstuurt	REAL gedecrypteerd pakket:Gegevens:28 bytes **AUTH**-volgende lading: NIET, voorbehouden: 0x0, lengte: 28 **Auth-methode PSK**, voorbehouden: 0x0, gereserveerd, 0x0 **Auth data**: 20 bytes Versleuteld pakket:Gegevens: 92 bytes IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH IKEv2-PROTO-3: (6): Time-out stilzetten om automatisch bericht te wacht IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B

een ID_GROUP type IDi lading met
de vaste string *$AnyConnectClient$*.
De ASA verwerkt dit bericht.

Relevante configuratie:

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

R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_GET_EAP_KEY
IKEv2-PROTO-2: (6): Stuur AUTH, om peer na EAP-uitwisseling te contro
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_VERIFY_AUTH
IKEv2-PROTO-3: (6): **Controleer de verificatiegegevens**
IKEv2-PROTO-3: (6): **Gebruik vooraf gedeelde sleutel voor id *$AnyConn**
sleutel 20
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: Wachtwoord voor configuratie-modus
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-3: PSH: client=AnyConnect client-versie=3.0.1047 client-os=
client-os-versie=
IKEv2-PLAT-3: Antwoord op de configuratie voltooid
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_OK_GET_CONFIG
IKEv2-PROTO-3: (6): Bezig met verzenden van wijsgegevens
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_CHK4_IC
IKEv2-PROTO-3: (6): Eerste contactgegevens verwerken
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): Controle omleiden is al gedaan voor deze sessie, h
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_PROC_SA_TS
IKEv2-PROTO-2: (6): **Auditbericht verwerken**
IKEv2-PLAT-1: **Crypto Map: Kaart dynmap seq 1000. Aangepaste selectie**
toegewezen IP
IKEv2-PLAT-3: **Crypto Map: matchen op dynamische kaart - dynmap seq**
IKEv2-PLAT-3: PFS uitgeschakeld voor RA-aansluiting
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-2: Ontvangen PFKEY SPI-callback voor SPI 0x30B848A4, fo
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_VERIFY_AUTH: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (6): **Auditbericht verwerken**

De ASA bouwt het IKE_AUTH antwoordbericht met de SA, TSi en TSr payload.
Het pakket IKE_AUTH bevat:

1. **ISAKMP-header** -

IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event **van R**
EV_MY_AUTH_METHODE
IKEv2-PROTO-3: (6): **Verkrijg mijn authenticatiemethode**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B

SPI/versie/vlaggen.

2. **AUTH - lading** - met de gekozen authenticatiemethode.
3. **CFG** - CFG_REQUEST/CFG_REPLY stelt een IKE-eindpunt in om informatie bij zijn peer te vragen. Indien een eigenschap in de CFG_REQUEST configuratie payload niet lengte nul is, wordt deze als suggestie voor die eigenschap genomen. De CFG_REPLY configuratie lading kan die waarde of een nieuwe teruggeven. Het kan ook nieuwe eigenschappen toevoegen en geen enkele gevraagde eigenschappen bevatten. Verblijvers negeren geretourneerde eigenschappen die zij niet herkennen. De ASA antwoordt op de client met de tunnelconfiguratie delen in het CFG_REPLY-pakket.
4. **SAr2** - SAr2 initieert de SA, wat vergelijkbaar is met de fase 2 transformatie set exchange in IKEv1.
5. **TSi** en **TSr** - De initiator- en responder-verkeersselectors bevatten respectievelijk het bron- en doeladres van de initiator en de responder om versleuteld verkeer door te sturen en te ontvangen. Het

R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van R_
EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (6): **Ontvang de vooraf gedeelde sleutel van peer voor *$AnyConnectClient$***
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van R_
EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Mijn verificatiegegevens genereren**
IKEv2-PROTO-3: (6): **Gebruik vooraf gedeelde toets voor id-hostname=AS reekscode 20**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van R_
EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Verkrijg mijn authenticatiemethode
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van R_
EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_BLD_EAP_AUTH_VERIFY: EV_GEN_AUTH
IKEv2-PROTO-3: (6): Mijn verificatiegegevens genereren
IKEv2-PROTO-3: (6): Gebruik vooraf gedeelde toets voor id-hostname=AS
reekscode 20
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van
R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH
IKEv2-PROTO-2: (6): **Stuur AUTH, om peer na EAP-uitwisseling te contro**
IKEv2-PROTO-3: ESP-voorstel: 1, SPI-grootte: 4 (IPsec-onderhandeling
Nee. transformeert: 3
 AES-CBC SHA96
IKEv2-PROTO-5: Aanmelden bij payload: ESP_TFC_NO_SUPPORTIKEv
Aanmelden bij payload: NON_FIRST_FRAGSIKEv2-PROTO-3: (6): het bo
voor encryptie; de inhoud is :
AUTH-volgende lading: CFG, gereserveerd: 0x0, lengte: 28
 Auth-methode PSK, voorbehouden: 0x0, gereserveerd, 0x0
Auth data: 20 bytes
CFG volgende lading: SA, gereserveerd: 0x0, lengte: 4196
 cfg-type: **CFG_REPLY,** gereserveerd: 0x0, gereserveerd: 0x0

 type attrib: intern IP4-adres, lengte: 4

  01 01 01 01
 type attrib: interne IP4-netmasker, lengte: 4

  00 00 00 00
 type attrib: interne adresaanduiding, lengte: 4

  00 00 00 00
 type attrib: toepassingsversie, lengte: 16

  41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
 type attrib: Onbekend - 28704, lengte: 4

adresbereik specificeert dat al het verkeer naar en van dat bereik getunneld is. Als het voorstel aanvaardbaar is voor de respondent, stuurt het identieke TS-terugbetalingen.

ENCR-lading:
Deze lading wordt gedecrypteerd, en de inhoud ervan wordt geparseerd als extra lading.

00 00 00 00
type attrib: Onbekend - 28705, lengte: 4

00 00 07 08
type attrib: Onbekend - 28706, lengte: 4

00 00 07 08
type attrib: Onbekend - 28707, lengte: 1

01
type attrib: Onbekend - 28709, lengte: 4

00 00 00 1e
type attrib: Onbekend - 28710, lengte: 4

00 00 00 14
type attrib: Onbekend - 28684, lengte: 1

01
type attrib: Onbekend - 28711, lengte: 2

05 7e
type attrib: Onbekend - 28679, lengte: 1

00
type attrib: Onbekend - 28683, lengte: 4

80 0b 00 01
type attrib: Onbekend - 28725, lengte: 1

00
type attrib: Onbekend - 28726, lengte: 1

00
type attrib: Onbekend - 28727, lengte: 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 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 6 d 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 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
<snip>
72 6f 66 69 6c 65 2d 61 6e 69 66 65 73 74 3e
3c 2f 63 6f 6e 69 69 67 3e 3c 2f 63 6f 66 69
67 2d 61 75 74 68 3e 00
type attrib: Onbekend - 28729, lengte: 1

00
SA volgende lading: TSi, voorbehouden: 0x0, lengte: 44

IKEv2-PROTO-4: laatste voorstel : 0x0, gereserveerd: 0x0, lengte: 40
Voorstel: 1, Protocol-id: ESP, SPI-grootte: 4, #trans: 3
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 1, voorbehouden: 0x0, id: AES-CBC
IKEv2-PROTO-4: laatste transformatie: 0x3, gereserveerd: 0x0: lengte:
type: 3, voorbehouden: 0x0, id: SHA96
IKEv2-PROTO-4: laatste transformatie: 0x0, gereserveerd: 0x0: lengte:
type: 5, voorbehouden: 0x0, id:

TSi volgende lading: TSr, gereserveerd: 0x0, lengte: 24
Aantal TS: 1, gereserveerd 0x0, gereserveerd 0x0
TS-type: TS_IPV4_ADDR_RANGE, proxy-id: 0, lengte: 16
startpoort: 0, eindpoort: 65535
startpunt: 10.2.2.1, laatste regel: 10.2.2.1
TSr volgende lading: KENNISGEVING, voorbehouden: 0x0, lengte: 24
Aantal TS: 1, gereserveerd 0x0, gereserveerd 0x0
TS-type: TS_IPV4_ADDR_RANGE, proxy-id: 0, lengte: 16
startpoort: 0, eindpoort: 65535
startpunt: 0.0.0.0, laatste regel: 255.255.255.255
IKEv2-PROTO-3: TX [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_
IKEv2-PROTO-3: HDR[i:58AFF71141B B436B - r: FC69630E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - RSPI: FC6963
IKEv2-PROTO-4: Volgende lading: ENCR, versie: 2.0
IKEv2-PROTO-4: **Wisseltype: IKE_AUTH, vlaggen: RESPONDER MSG-R**
IKEv2-PROTO-4: Bericht: 0x5, lengte: 4396
ENCR-volgende lading: AUTH, gereserveerd: 0x0, lengte: 4368
Versleuteld gegevens en kolommen; 4364 bytes

ASA stuurt dit IKE_AUTH-antwoordbericht uit, dat gefragmenteerd is in negen pakketten. De IKE_AUTH uitwisseling is voltooid.

IKEv2-PROTO-5: (6): Fragmentatiepakket, Fragmentatie MTU: 544, **Aanta**
9, Fragment-ID: 3
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PLAT-4: VERZENDEN PKT [IKE_AUTH] [10.0.1]:4500->[192.168.1
InitSPI=0x58aff71141ba436b RespSPI=fc696330e6b94d7f MID=0000000
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_OK
IKEv2-PROTO-5: (6): Actie: Action_Null
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: **AUTH_DON**

EV_PKI_SESH_CLOSE
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: ikev2_log
Bestand: .\ikev2_anyconnect_osal.cpp
Lijn: 2730
De IPsec-verbinding is ingesteld.
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: Registratie van IPsec-sessies:
Encryptie: AES-CBC
PRF: SHA1
HMAC: SHA96
Plaatselijke gebruikersmethode: PSK
Afstandsbediening: PSK
Volgnummer: 0
Sleutelgrootte: 192
DH-groep: 1
Rekey-tijd: 4294967 seconden
Lokaal adres: 192.168.1.1
Remote-adres: 10.0.0.1
Lokale poort: 4500
Remote-poort: 4500
Sessieid: 1
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: acvpnuis

Beschrijving: **Het profiel dat op de beveiligde poort is ingesteld:** Anyconne
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
VPN-sessie instellen....
****
—IKE_AUTH-uitwisselingen—
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie

Bron: downloader

Beschrijving: Functie: ProfileMgr::loadProfiles
Bestand: ..\Api\ProfileMgr.cpp
Lijn: 148
Laadprofielen:
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyCo
Mobility Client\Profile\anyconnect-ikev2.xml
****
****
Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: downloader

Beschrijving: Huidige referentie-instellingen:
ServiceOff: onjuist
CertificateStoreOverride: onjuist
certificaatwinkel: Alle
PreConnectMessage weergeven: onjuist
AutoConnectOnStart: onjuist
minimaliserenOnConnect: reëel
LocalLANAccess: onjuist
AutoOpnieuw aansluiten: reëel
AutoReconnectBehavior: AfsluitenOp opschorten
StartVoorAanmelden: onjuist
AutoUpdate: reëel
RSASecurIDIntegratie: Automatisch
Handhaving van WindowsLogon SingleLocalLogon
WindowsVPN-instelling: Alleen lokale gebruikers
Proxy-instellingen: Native
LaatLocalProxyconnecties toe: reëel
Samenvatting: Uitschakelen
PPPoXclusionServerIP:
Automatisch VPN-beleid: onjuist
Trusted NetworkPolicy: afsluiten
Onvertrouwd netwerkbeleid: Connect
Trusted DNSD blijft behouden:
Trusted DNS-servers:
AltijdAan: onjuist
ConnectFOUTPolicy: gesloten
AccessoirePortalRemediation: onjuist
Time-out voor copyrightwetgeving van CaptivePortalRemediation: 5
ToepassenLastVPNLocalResourceRules: onjuist
Laat VPN los: reëel
Schrijven inschakelen: onjuist
TerminateScriptOnNextEvent: onjuist
EnablePostSBLOnConnectScript: reëel
Automatisch selecteren: reëel
VpnOnLogoff behouden: onjuist
Handhaving van gebruiker: Alleen dezelfde gebruiker
AutomatischeServerSelectie inschakelen: onjuist
Verbetering in automatische serverselectie: 20

AutoServerSelectionSuspendTime: 4
Time-out verificatie: 12
SafeWordSofTokenIntegratie: onjuist
Sta IPsec overSSL toe: onjuist
ClearSmartcardPin: reëel
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
Instellen van VPN - Onderzoekingssysteem...
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
VPN instellen - VPN-adapter activeren...
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: CVVirtualAdapter:DoRegistrarRepair
Bestand: .\WindowsVirtualAdapter.cpp
Lijn: 1869
Vond VA Control-toets: SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: **Een nieuwe netwerkinterface is gedetecteerd.**
****

Datum: 04/23/2013
Tijd: 16:25:07
Type: Informatie
Bron: hulpstof

Beschrijving: Functie: CRouteMgr::logInterfaces
Bestand: .\RouteMgr.cpp
Lijn: 2076
Vervroegde functie: logInterfaces
Retourencode: 0 (0x00000000)
Beschrijving: IP-interfacelijst:
10.2.2.1
192.168.1.1
****

Datum: 04/23/2013
Tijd: 16:25:08
Type: Informatie
Bron: hulpstof

Beschrijving: Host Configuration:
Openbaar adres: 192.168.1.1
Openbaar masker: 255.255.255.0
Private adres: 10.2.2.1
Private masker: 255.0.0.0
Private IPv6-adres: N.v.t.
Private IPv6-masker: N.v.t.
Afstandspeers: 10.0.0.1 (TCP-poort 443, UDP-poort 500), 10.0.0.1 (UDP-
Private netwerken: none
Openbare netwerken: none
Tunnelmodus: ja
****

De verbinding wordt ingevoerd in de database van de Security Association (SA) en de status wordt geregistreerd. ASA voert ook enkele controles uit zoals de status Common Access Card (CAC), de aanwezigheid van duplicaat SA's, en stelt waarden in zoals dood peer detectie (DPD) enzovoort.

IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_INSERT_IKE
IKEv2-PROTO-2: (6): **SA opgericht; SA in database opnemen**
IKEv2-PLAT-3: VERBINDINGSTATUS: Peer: 192.168.1.1:25171, fase 1_id: *$AnyConne
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_REGISTER_SESSIE
IKEv2-PLAT-3: (6) **gebruikersnaam ingesteld op: Anu**
IKEv2-PLAT-3: **VERBINDINGSTATUS: GEREGISTREERD**... peer: 192.168.1.1:25171, **fa**
$AnyConnect-client$
IKEv2-PROTO-3: (6): DPD initialiseren, ingesteld voor 10 seconden
IKEv2-PLAT-3: (6) mib_index ingesteld op: 4501
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (6): Materiaal van IPSEC-toets laden
IKEv2-PLAT-3: Crypto Map: matchen op dynamische kaart - dynmap seq
IKEv2-PLAT-3: (6) **DPD Max Time is:** 30
IKEv2-PLAT-3: (6) **DPD Max Time is:** 30
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_START_ACCT
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_CHECK_DUPE
IKEv2-PROTO-3: (6): **Op duplicaat SA controleren**
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: Event van A
EV_CHK4_ROLE
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: READY Eve
EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: New ikev2 sa request geactiveerd

IKEv2-PLAT-5: Decrement voor inkomende onderhandelingen
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: READY Eve
IKEv2-PROTO-3: (6): Begintimer voor het verwijderen van onderhandelin
IKEv2-PROTO-5: (6): SM-spoor -> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 000005 CurState: READY Eve
EV_NO_EVENT
IKEv2-PLAT-2: Ontvangen PFKEY add SA voor SPI 0x77E5348, foutmelc
IKEv2-PLAT-2: Ontvangen PFKEY update SA voor SPI 0x30B848A4, fout
****

Datum: 04/23/2013
Tijd: 16:25:08
Type: Informatie
Bron: hulpstof

Beschrijving: **De VPN-verbinding is gemaakt en kan nu gegevens doorgev**
****

Datum: 04/23/2013
Tijd: 16:25:08
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
VPN instellen - Systeem configureren...
****

Datum: 04/23/2013
Tijd: 16:25:08
Type: Informatie
Bron: acvpnuis

Beschrijving: Informatie over het berichttype die naar de gebruiker wordt v
VPN instellen...
****

Datum: 04/23/2013
Tijd: 16:25:37
Type: Informatie
Bron: hulpstof

Bestand: 2.2\IPsecProtocol.cpp
Lijn: 945
IPsec-tunnel wordt ingesteld
****

Tunnelverificatie

AnyConnect

Steekproef uitvoer van het **show vpn-sessiondb detail anyconnect-**opdracht is:

```
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

De voorbeelduitvoer van de **show crypto ikev2 sa** opdracht is:

```
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
```

De voorbeelduitvoer van de **show crypto ikev2 als detail** opdracht is:

```
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

De voorbeelduitvoer van de **show crypto ipsec sa** opdracht is:

```
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
```

Gerelateerde informatie

- RFC 4306, Internet Key Exchange (IKEv2)-protocol
- RFC 3748, Uitbreidbaar verificatieprotocol (EAP)
- RFC 5996, Internet Key Exchange Protocol, versie 2 (IKEv2)
- Technische ondersteuning en documentatie – Cisco Systems