ASA IKEv2 Debugs für die Remote Access VPN-Fehlerbehebung

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Kernproblem](#)
[Szenario](#)
[Debugbefehle](#)
[ASA-Konfiguration](#)
[XML-Datei](#)
[Debugprotokolle und Beschreibungen](#)
[Tunnelüberprüfung](#)
[AnyConnect](#)
[ISAKMP](#)
[IPSec](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie die Debugging auf der Cisco Adaptive Security Appliance (ASA) verstehen, wenn Internet Key Exchange Version 2 (IKEv2) mit einem Cisco AnyConnect Secure Mobility Client verwendet wird. Dieses Dokument enthält auch Informationen zum Übersetzen bestimmter Debug-Zeilen in einer ASA-Konfiguration.

In diesem Dokument wird weder beschrieben, wie Datenverkehr nach der Einrichtung eines VPN-Tunnels an die ASA weitergeleitet wird, noch werden grundlegende Konzepte von IPSec oder IKE behandelt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse des Paketaustauschs für IKEv2 zu verfügen. Weitere Informationen finden Sie unter IKEv2-Paketaustausch und Debuggen auf Protokollebene.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Internet Key Exchange Version 2 (IKEv2)
- Cisco Adaptive Security Appliance (ASA) Version 8.4 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Kernproblem

Das Cisco Technical Assistance Center (TAC) verwendet häufig IKE- und IPSec-Debugbefehle, um zu ermitteln, wo ein Problem mit der Einrichtung eines IPSec-VPN-Tunnels besteht. Die Befehle können jedoch kryptisch sein.

Szenario

Debugbefehle

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

ASA-Konfiguration

Diese ASA-Konfiguration ist absolut grundlegend und ohne Verwendung externer Server.

```
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-Datei

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

Hinweis: Der Name der UserGroup im XML-Clientprofil muss mit dem Namen der Tunnelgruppe auf der ASA übereinstimmen. Andernfalls wird die Fehlermeldung 'Invalid Host Entry (Ungültiger Hosteintrag) angezeigt. Bitte geben Sie ' erneut ein. Dies wird auf dem AnyConnect-Client angezeigt.

Debugprotokolle und Beschreibungen

Hinweis: Protokolle des Diagnose- und Reporting-Tools (DART) sind im Allgemeinen sehr

chatty, sodass bestimmte DART-Protokolle in diesem Beispiel aufgrund der Bedeutungslosigkeit ausgelassen wurden.

Beschreibung der Servernachricht

Debugger
Datum: 23.04.2013
Uhrzeit: 16:24:55 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: Funktion: ClientIfcBase::verbinden
Datei: .\ClientIfcBase.cpp
Leitung: 964
Der Benutzer hat eine VPN-Verbindung mit Anu-IKEV2 angefor
****
Datum: 23.04.2013
Uhrzeit: 16:24:55 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum M
Anu-IKEV2 kontaktieren.
****
Datum: 23.04.2013
Uhrzeit: 16:24:55 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: Funktion: ApiCert::getCertList
Datei: .\ApiCert.cpp
Leitung: 259
Anzahl der gefundenen Zertifikate: 0
****
Datum: 23.04.2013
Uhrzeit: 16:25:00 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: **Initiieren der VPN-Verbindung zum sicheren Gat**
https://10.0.0.1/ASA-IKEV2
****
Datum: 23.04.2013
Uhrzeit: 16:25:00 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Vom GUI-Client initiierter Tunnel.
****

Datum: 23.04.2013
Uhrzeit: 16:25:02 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: CIPsecProtocol::connectTransport
Datei: .\IPsecProtocol.cpp
Leitung: 1629
IKE-Socket von 192.168.1.1:25170 bis 10.0.0.1:500 geöffnet
****

—IKE_SA_INIT Exchange beginnt—

Die ASA erhält die Meldung IKE_SA_INIT vom Client.

IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.1.1]:25170-
InitSPI=0x58aff71141ba436b RespSPI=0x0 0000000000000000
IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF

Das erste Nachrichtenpaar ist der IKE_SA_INIT-Austausch. Diese Nachrichten handeln Kryptografiealgorithmen aus, tauschen Nonces aus und tauschen einen Diffie-Hellman (DH)-Austausch aus.
Die vom Client erhaltene Meldung IKE_SA_INIT enthält folgende Felder:

1. **ISAKMP-Header** - SPI/Version/Flags.
2. **SAi1** - Verschlüsselungsalgorithmus, der vom IKE-Initiator unterstützt wird.
3. **KEi** - Der öffentliche DH-Schlüsselwert des Initiators.
4. **N** - Initiator Nonce

IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: 00000000000
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - rspi:**
IKEv2-PROTO-4: Nächste Nutzlast: SA, **Version: 2,0**
IKEv2-PROTO-4: Exchange-Typ: IKE_SA_INIT, **Flaggen: INITIA**
IKEv2-PROTO-4: Nachrichten-ID: 0x0, Länge: 528

SA Next-Payload: KE, reserviert: 0x0, Länge: 168
IKEv2-PROTO-4: letzter Vorschlag: 0x0, reserviert: 0x0, Länge:
Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 18
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: 3DES
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: DES
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: SHA512
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: SHA384
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: SHA256
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: SHA1
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: MD5
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA512
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA384
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA256
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA96
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: MD596
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 4, reserviert: 0x0, ID: DH_GROUP_1536_MODP/Gruppe
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 4, reserviert: 0x0, ID: DH_GROUP_1024_MODP/Gruppe
IKEv2-PROTO-4: letzte Umwandlung: 0x0, reserviert: 0x0: Läng

Typ: 4, reserviert: 0x0, ID: DH_GROUP_768_MODP/Gruppe 1

KE Nächste Payload: N, reserviert: 0x0, Länge: 104
DH-Gruppe: 1, Reserviert: 0 x 0

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
ba ba 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
N Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b4
IKEv2-PROTO-5: Herstellerspezifische Payload analysieren: CI
GRÜNDE VID Nächste Payload: VID, reserviert: 0x0, Länge: 23
Entschlüsseltes Paket:Daten: 528 Byte
IKEv2-PLAT-3: Benutzerdefinierte VID-Payloads verarbeiten
IKEv2-PLAT-3: Cisco Copyright-VID von Peer erhalten
IKEv2-PLAT-3: Von Peer erhaltene AnyConnect EAP-VID
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_RECV_INIT
IKEv2-PROTO-3: 6. NAT-Erkennung prüfen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_CHK_REDIRECT
IKEv2-PROTO-5: 6. Redirect Check ist nicht erforderlich, übersp
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_CHK_CAC
IKEv2-PLAT-5: **New ikev2 als Anforderung zugelassen**
IKEv2-PLAT-5: Erhöhung der Anzahl der eingehenden Verhand
IKEv2-PLAT-5: UNGÜLTIGER PSH-HANDLE
IKEv2-PLAT-5: UNGÜLTIGER PSH-HANDLE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_CHK_COOKIE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_VERIFY_MSG
IKEv2-PROTO-3: 6. **SA-Initnachricht überprüfen**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_INSERT_SA
IKEv2-PROTO-3: 6. SA einfügen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_GET_IKE_RICHTLINIE

Die ASA überprüft und verarbeitet die IKE_INIT-Nachricht. Die ASA:

1. Wählt die Verschlüsselungs-Suite aus
   die vom Initiator angeboten werden.
2. Berechnet seinen eigenen geheimen DH-Schlüssel.
3. Berechnet einen SKEYID-Wert von
   für die alle Schlüssel abgeleitet werden können
   diese IKE_SA. Die Header aller nachfolgende Nachrichten verschlüsselt und authentifiziert. Die
   für die Verschlüsselung und Integritätsschutz wird abgeleitet von SKEYID und bekannt als:

   SK_e - Verschlüsselung.**SK_a** - Authentifizierung.**SK_d** - Abgeleitet und verwendet
   für die Ableitung weiterer Keying-Material für CHILD_SAs.Ein separates SK_e und SK_a sind
   für jede Richtung berechnet.

Relevante Konfiguration:

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

IKEv2-PROTO-3: 6. **Konfigurieren von Richtlinien**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_PROC_MSG
IKEv2-PROTO-2: 6. Verarbeiten der ersten Nachricht
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_DETECT_NAT
IKEv2-PROTO-3: 6. Prozess-NAT-Erkennungsbenachrichtigung
IKEv2-PROTO-5: 6. Verarbeitung von nat detect src notify
IKEv2-PROTO-5: 6. Remote-Adresse nicht zugeordnet
IKEv2-PROTO-5: 6. Verarbeitung von nat detect dnotify
IKEv2-PROTO-5: 6. Lokale Adresse zugeordnet
IKEv2-PROTO-5: 6. Der Host befindet sich außerhalb von NAT.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: 6. Gültige Konfigurationsmodusdaten empfang
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: 6. Daten zum empfangenen Konfigurationsmo
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_SET_POLICY
IKEv2-PROTO-3: 6. **Festlegen konfigurierter Richtlinien**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_PKI_SESH_OPEN
IKEv2-PROTO-3: 6. Öffnen einer PKI-Sitzung
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_GEN_DH_KEY
IKEv2-PROTO-3: 6. **Öffentlicher DH-Schlüssel für Computing**
IKEv2-PROTO-3: 6.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_NO_EVENT
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_GEN_DH_SECRET
IKEv2-PROTO-3: 6. **geheimer DH-Schlüssel für Computing**
IKEv2-PROTO-3: 6.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_NO_EVENT

Die ASA erstellt die Antwortmeldung für den IKE_SA_INIT-Austausch.
Dieses Paket enthält:

1. **ISAKMP-Header** - SPI/Version/Flags.
2. **SAr1** - Verschlüsselungsalgorithmus, den der IKE-Responder auswählt.
3. **KEr** - Der öffentliche DH-Schlüsselwert des Responders.
4. **N** - Responder Nonce.

IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_GEN_SKEYID
IKEv2-PROTO-3: 6. **skeyid generieren**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: EV_GET_CONFIG_MODE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Veranstaltung: **EV_BLD_MSG**
IKEv2-PROTO-2: 6. **Erste Nachricht senden**
IKEv2-PROTO-3: IKE-Angebot: 1, SPI-Größe: 0 (erste Aushand
Anzahl Veränderungen: 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Gruppe 1
IKEv2-PROTO-5: anbieterspezifische Payload erstellen: LÖSCH
PROTO-5: anbieterspezifische Payload erstellen: (BENUTZERD
PROTO-5: anbieterspezifische Payload erstellen: (BENUTZERD
PROTO-5: Benachrichtigungs-Payload erstellen:
NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: Benachrichtig
erstellen: NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2:
vertrauenswürdiger Emittenten fehlgeschlagen oder keine verfüg
IKEv2-PROTO-5: anbieterspezifische Payload erstellen: FRAGM
PROTO-3: Tx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m
IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR **ispi: 58AFF71141BA436B - rspi:**
IKEv2-PROTO-4: Nächste Nutzlast: SA, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_SA_INIT, **Flaggen: ANTW**
REAKTION
IKEv2-PROTO-4: Nachrichten-ID: 0x0, Länge: 386
SA Next-Payload: KE, reserviert: 0x0, Länge: 48
IKEv2-PROTO-4: letzter Vorschlag: 0x0, reserviert: 0x0, Länge:
Angebot: 1, Protokoll-ID: IKE, SPI-Größe: 0, #trans: 4
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 2, vorbehalten: 0x0, ID: SHA1
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA96
IKEv2-PROTO-4: letzte Umwandlung: 0x0, reserviert: 0x0: Läng
Typ: 4, reserviert: 0x0, ID: DH_GROUP_768_MODP/Gruppe 1

KE Nächste Payload: N, reserviert: 0x0, Länge: 104
DH-Gruppe: 1, Reserviert: 0 x 0

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 cc4 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 Nächste Nutzlast: VID, reserviert: 0x0, Länge: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 ec 97 b8 67
d5 e7 c2 f5
VID Nächste Nutzlast: VID, reserviert: 0x0, Länge: 23

Die ASA sendet die Antwortmeldung für den IKE_SA_INIT-Austausch aus. Der Austausch IKE_SA_INIT ist nun abgeschlossen. Die ASA startet den Timer für den Authentifizierungsprozess.

IKEv2-PLAT-4: GESENDETE PKT [IKE_SA_INIT] [10.0.0.1]:500->[192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=0000000
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: INIT_DONE-Veranstaltung: EV_DONE
IKEv2-PROTO-3: 6. Fragmentierung ist aktiviert
IKEv2-PROTO-3: 6. Cisco DeleteReason Notification ist aktiviert
IKEv2-PROTO-3: 6. Vollständiger SA-Initaustausch
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: INIT_DONE-Veranstaltung: EV_CHK4_ROLE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: INIT_DONE-Veranstaltung: EV_START_TMR
IKEv2-PROTO-3: 6. Starter Timer zum Warten auf die Authentifizierungsmeldung (30 Sek.)
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: R_WAIT_AUTH-Ereignis: EV_NO_EVENT
—IKE_SA_INIT abgeschlossen—
— IKE_AUTH beginnt—
****
Datum: 23.04.2013
Uhrzeit: 16:25:00 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Parameter für sichere Gateways:
IP-Adresse: 10.0.0.1
Port: 443
URL: "10.0.0.1"
Auth-Methode: **IKE - EAP-AnyConnect**

****
Datum: 23.04.201
Uhrzeit: 16:25:02
Typ: Informatione
Quelle: Acvpnant

Beschreibung: Fu
CIPsecProtocol::i
Datei: .\IPsecProt
Leitung: 345
IPsec-Tunnel initi
****

IKE-Identität:
****

Datum: 23.04.2013
Uhrzeit: 16:25:00 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: **Initiierung der Cisco AnyConnect Secure Mobility**
Version 3.0.1047
****

Datum: 23.04.2013
Uhrzeit: 16:25:02 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: ikev2_log
Datei: .\ikev2_anyconnect_osal.cpp
Leitung: 2730
Empfangene Anfrage zum Einrichten eines IPsec-Tunnels; Loka
Datenverkehrswähler = Adressbereich: 0.0.0.0-255.255.255.255
Bereich: 0-65535 ; Remote-Datenverkehrswähler = Adressbereich
255.255.255.255 Protokoll: 0-Port-Bereich: 0-65535
****

Datum: 23.04.2013
Uhrzeit: 16:25:02 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: CIPsecProtocol::connectTransport
Datei: .\IPsecProtocol.cpp
Leitung: 1629
IKE-Socket von 192.168.1.1:25171 bis 10.0.0.1:4500 geöffnet
****

Die Authentifizierung erfolgt über EAP. Im Rahmen einer EAP-Konversation ist nur eine einzige EAP-Authentifizierungsmethode zulässig. Die ASA erhält die Meldung IKE_AUTH vom Client.

IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[1
InitSPI=0x58aff71141ba436b Resp SPI=0xfc696330e6b94d7f M
IKEv2-PROTO-3: **Rx** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRI

Wenn der Client eine IDi-Payload enthält
aber keine AUTH-Payload, das heißt, Der Kunde hat eine Identität deklariert, aber
nicht bewiesen. Im Debugger wird AUTH
Die Nutzlast ist in IKE_AUTH nicht vorhanden.
vom Client gesendetes Paket. Der Client sendet die AUTH-Nutzlast nur nach dem EAP-Austausch ist erfolgreich. Wenn die ASA
ist bereit, eine erweiterbare

IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 **HDR-ISPI: 58AFF71141BA436B - rspi:**
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, **Version: 2,0**
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, **Flaggen: INITIAT**
IKEv2-PROTO-4: Nachrichten-ID: 0x1, Länge: 540
IKEv2-PROTO-5: 6. Die Anforderung hat mess_id 1. Erwartete 1
ECHTES entschlüsseltes Paket:Daten: 465 Byte
IKEv2-PROTO-5: Herstellerspezifische Payload analysieren: (BI
VID Nächste Payload: IDi, reserviert: 0x0, Länge: 20

58 af f6 11 52 8d b0 2c b8 da 30 46 BE 91 56 fa
IDi Nächste Payload: CERTREQ, vorbehalten: 0x0, Länge: 28
ID-Typ: Gruppenname, Reserviert: 0x0 0x0

Authentifizierungsmethode, platziert einen EAP
Payload in Nachricht 4 und Zurückstellung des Sendens SAr2, TSi und TSr bis zum Initiator Authentifizierung abgeschlossen in nachfolgender IKE_AUTH-Austausch. Das Initiatorpaket IKE_AUTH enthält:

1. ISAKMP-Header - SPI/Version/Flags.
2. IDi - Der Tunnelgruppenname, der Der Kunde möchte eine Verbindung mit kann mit der IDi Nutzlast vom Typ ID_KEY_ID in die erste Meldung der IKE_AUTH-Austausch. Diese tritt auf, wenn das Clientprofil* vorkonfiguriert mit einem Gruppennamen oder nach einem früheren erfolgreichen Authentifizierung, hat der Client Gruppennamen in der Zwischenablage Voreinstellungsdatei. Die ASA versucht, eine Tunnelgruppe zuzuordnen. Name mit dem Inhalt der IKE IDi-Nutzlast. Nach dem ersten erfolgreiches IPSec VPN ist etabliert, speichert der Client die Gruppenname (Gruppen-Alias), an den Der Benutzer wurde authentifiziert. Diese Gruppe Name wird in IDi geliefert Nutzlast der nächsten Verbindung den Versuch, die von der Benutzer. Wenn die EAP-Authentifizierung angegeben oder implizit vom Client Profil und das Profil nicht enthalten die <IKEIdentity> -Element, sendet der Client eine ID_GROUP Typ-IDi-Nutzlast mit der festen Zeichenfolge *$AnyConnectClient$*.

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65 6e 74 24 2a

CERTREQ Nächste Payload: CFG, reserviert: 0x0, Länge: 25
Zertifikatcodierung X.509 - Signatur
CertReq-Daten und -Doppelpunkte; 20 Byte
CFG Nächste Payload: SA, reserviert: 0x0, Länge: 196
cfg-Typ: CFG_REQUEST, reserviert: 0x0, reserviert: 0 x 0

Attributtyp: interne IP4-Adresse, Länge: 0

Attributtyp: interne IP4-Netzmaske, Länge: 0

Attributtyp: Interner IP4-DNS, Länge: 0

Attributtyp: internes IP4-NBNS, Länge: 0

Attributtyp: interne Adresse, Gültigkeitsdauer: 0

Attributtyp: Anwendungsversion, Länge: 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

Attributtyp: interne IP6-Adresse, Länge: 0

Attributtyp: internes IP4-Subnetz, Länge: 0

Attributtyp: Unbekannt - 28682, Länge: 15

77 69 6e 78 70 36 34 74 65 65 60 61 74 65

Attributtyp: Unbekannt - 28704, Länge: 0

Attributtyp: Unbekannt - 28705, Länge: 0

Attributtyp: Unbekannt - 28706, Länge: 0

Attributtyp: Unbekannt - 28707, Länge: 0

Attributtyp: Unbekannt - 28708, Länge: 0

Attributtyp: Unbekannt - 28709, Länge: 0

Attributtyp: Unbekannt - 28710, Länge: 0

Attributtyp: Unbekannt - 28672, Länge: 0

Attributtyp: Unbekannt - 28684, Länge: 0

Attributtyp: Unbekannt - 28711, Länge: 2

05 7e

Attributtyp: Unbekannt - 28674, Länge: 0

Attributtyp: Unbekannt - 28712, Länge: 0

3. **CERTREQ** - Der Kunde ist Anfordern der ASA für eine bevorzugtes Zertifikat. Zertifikat Anforderungs-Payloads können enthalten sein im Austausch, wenn der Absender benötigt das Zertifikat der Empfänger. Zertifikatsanforderung Nutzlast wird verarbeitet von Überprüfung der "Cert-Codierung" um ob der Prozessor Zertifikate dieser Art. Wenn ja, Das Feld "Zertifizierungsstelle" ist überprüft, um festzustellen, ob Der Prozessor verfügt über Zertifikate. die bis zu die angegebene Zertifizierung Behörden. Dies kann eine Kette von Zertifikate.
4. **CFG** - CFG_REQUEST/ CFG_REPLY ermöglicht IKE Endpunkt zum Anfordern von Informationen von seinem Peer. Wenn ein Attribut im CFG_REQUEST-Konfiguration Nutzlast ist nicht Null-Länge, sondern als Vorschlag dazu Attribut.The CFG_REPLY Konfigurationsnutzungsladung kann zurückgegeben werden diesen oder einen neuen Wert. Sie können Hinzufügen neuer Attribute und nicht einige angeforderte hinzufügen. Rückgabe wird von den Antragstellern ignoriert Attribute, die erkennen. In diesen Debuggen Der Client fordert den Tunnel an Konfiguration im CFG_REQUEST. Die ASA

Attributtyp: Unbekannt - 28675, Länge: 0

Attributtyp: Unbekannt - 28679, Länge: 0

Attributtyp: Unbekannt - 28683, Länge: 0

Attributtyp: Unbekannt - 28717, Länge: 0

Attributtyp: Unbekannt - 28718, Länge: 0

Attributtyp: Unbekannt - 28719, Länge: 0

Attributtyp: Unbekannt - 28720, Länge: 0

Attributtyp: Unbekannt - 28721, Länge: 0

Attributtyp: Unbekannt - 28722, Länge: 0

Attributtyp: Unbekannt - 28723, Länge: 0

Attributtyp: Unbekannt - 28724, Länge: 0

Attributtyp: Unbekannt - 28725, Länge: 0

Attributtyp: Unbekannt - 28726, Länge: 0

Attributtyp: Unbekannt - 28727, Länge: 0

Attributtyp: Unbekannt - 28729, Länge: 0

SA Next-Payload: TSi, reserviert: 0x0, Länge: 124
IKEv2-PROTO-4: letzter Vorschlag: 0x0, reserviert: 0x0, Länge:
Angebot: 1, Protokoll-ID: ESP, SPI-Größe: 4, #trans: 12
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: 3DES
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: DES
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: NULL
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA512
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA384
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA256
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng

antwortet darauf und sendet den Tunnel
Konfigurationsattribute nur nach der EAP-Austausch erfolgreich war.

5. **SAi2** - SAi2 initiiert die SA, die der Phase 2 ähnelt Transformations-Set-Austausch in IKEv1.
6. **TSi** und **TSr** - Der Initiator und Responder-Traffic-Selektoren enthalten bzw. die Quelle und Zieladresse des Initiator und Responder, um verschlüsselt weiterleiten und empfangen
Datenverkehr. Der Adressbereich gibt an, dass der gesamte Datenverkehr von und an dieser Bereich ist getunnelt. Wenn Vorschlag ist für
antwortet, sendet er identischen TS
Nutzlasten zurück.

Attribute, die der Client bereitstellen muss
Gruppenauthentifizierung wird in einer AnyConnect-Profildatei

*** Relevante Profilkonfiguration:**

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

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

Die ASA generiert eine Antwort auf die Meldung IKE_AUTH und bereitet sich auf die Authentifizierung für den Client vor.

Typ: 3, reserviert: 0x0, ID: SHA96
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: MD596
IKEv2-PROTO-4: letzte Umwandlung: 0x0, reserviert: 0x0: Läng
Typ: 5, reserviert: 0x0, ID:

TSi Nächste Payload: TSr, reserviert: 0x0, Länge: 24
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Startport: 0, Endport: 65535
Startanschrift: 0.0.0.0, Endadresse: 255 255 255 255 255
TSr Nächste Payload: BENACHRICHTIGUNG, reserviert: 0x0,
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Startport: 0, Endport: 65535
Startanschrift: 0.0.0.0, Endadresse: 255 255 255 255 255

Entschlüsseltes Paket: Data: 540 Byte
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_RECV_AUTH
IKEv2-PROTO-3: 6. Stoppen des Timers zum Warten auf die Authentifizierungsmeldung

IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK_NAT_T
IKEv2-PROTO-3: 6. NAT-Erkennung prüfen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHG_NAT_T_PORT
IKEv2-PROTO-2: 6. NAT erkannte float to init port 25171 bzw. p
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_PROC_ID
IKEv2-PROTO-2: 6. Gültige Parameter in Prozess-ID erhalten
IKEv2-PLAT-3: (6) Peer-Authentifizierungsmethode festgelegt a
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: 6. Konfigurieren von Richtlinien
IKEv2-PLAT-3: Neue AnyConnect Client-Verbindung basierend
IKEv2-PLAT-3: my_auth_method = 1
IKEv2-PLAT-3: (6) Peer-Authentifizierungsmethode festgelegt a
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) tp_name auf: Anu-IKV2
IKEv2-PLAT-3: **Vertrauenspunkt auf:** Anu-IKV2
IKEv2-PLAT-3: P1 ID = 0
IKEv2-PLAT-3: Übersetzen von IKE_ID_AUTO in = 9
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_SET_POLICY
IKEv2-PROTO-3: 6. **Festlegen konfigurierter Richtlinien**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: 6. Überprüfen der Peer-Richtlinie
IKEv2-PROTO-3: 6. **Übereinstimmendes Zertifikat gefunden**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: 6. Gültige Konfigurationsmodusdaten empfan
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3: (6) Der DHCP-Hostname für DDNS ist wie folgt
winxp64template
IKEv2-PROTO-3: 6. Daten zum empfangenen Konfigurationsmo
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK_EAP

IKEv2-PROTO-3: 6. **Überprüfen Sie den EAP-Austausch.**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_GEN_AUTH
IKEv2-PROTO-3: 6. **Generieren meiner Authentifizierungsdaten**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_CHK4_SIGN
IKEv2-PROTO-3: 6. Authentifizierungsverfahren abrufen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_SIGN
IKEv2-PROTO-3: 6. **Authentifizierungsdaten signieren**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
Ereignis: EV_OK_AUTH_GEN
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
R_BLD_EAP_AUTH_REQ-Ereignis: EV_AUTHEN_REQ
IKEv2-PROTO-2: 6. **Bitten Sie den Authentifizierer, EAP-Anfrag**
Erstellter Elementname **config-auth-Wert**
Dem Element config-auth den Attributnamen-Clientwert vpn hinz
Hinzufügen eines Attributnamentypwerts hello zu element config
Erstellter Elementname, Version-Wert 9.0(2)8
Elementname-Version 9.0(2)8 zu element config-auth hinzugefü
Attributname hinzugefügt, der der Elementversion sg wert
Generierte XML-Nachricht unten
<?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. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
R_BLD_EAP_AUTH_REQ-Ereignis: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
R_BLD_EAP_AUTH_REQ-Ereignis: EV_CHK_REDIRECT
IKEv2-PROTO-3: 6. Redirect Check mit Plattform für Lastenaus
IKEv2-PLAT-3: Redirect Check on Plattform
IKEv2-PLAT-3: ikev2_osal_redirect: Sitzung angenommen von 1
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState:
R_BLD_EAP_AUTH_REQ-Ereignis: EV_SEND_EAP_AUTH_RE
IKEv2-PROTO-2: 6. **EAP-Anforderung senden**
IKEv2-PROTO-5: anbieterspezifische Payload erstellen: CISCO
PROTO-3: 6. Erstellen

Die ASA sendet die AUTH-Payload, um Benutzeranmeldeinformationen vom Client anzufordern. Die ASA sendet die AUTH-Methode als 'RSA', sodass sie ein eigenes Zertifikat an den Client

IDr. Nächste Nutzlast: CERT, reserviert: 0x0, Länge: 36
ID-Typ: DER ASN1 DN, reserviert: 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

sendet, sodass der Client den ASA-Server authentifizieren kann.
Da die ASA bereit ist, eine erweiterbare Authentifizierungsmethode zu verwenden, platziert sie eine EAP-Payload in Nachricht 4 und verzögert das Senden von SAr2, TSi und TSr, bis die Initiatorauthentifizierung in einem nachfolgenden IKE_AUTH-Austausch abgeschlossen ist. Daher sind diese drei Payloads nicht im Debugger vorhanden.
Das EAP-Paket enthält:

1. **Code: request** - Dieser Code wird vom Authentifizierer an den Peer gesendet.
2. **ID: 1** - Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 1, der angibt, dass es sich um das erste Paket im EAP-Austausch handelt. Diese EAP-Anforderung hat den 'config-auth'-Typ "hello"; sie wird von der ASA an den Client gesendet, um den EAP-Austausch zu initiieren.
3. **Länge: 150** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten.
4. **EAP-Daten**.

Eine Fragmentierung kann auftreten, wenn die Zertifikate groß sind oder Zertifikatsketten enthalten sind. Sowohl Initiator- als auch Responder-KE-Payloads können auch große Schlüssel enthalten, was zu Fragmentierung beitragen kann.

CERT Next-Payload: CERT, reserviert: 0x0, Länge: 436
Zertifikatcodierung X.509-Zertifikat - Signatur
Cert data: 431 Byte
CERT Next-Payload: AUTH, reserviert: 0x0, Länge: 436
Zertifikatcodierung X.509 - Signatur
Cert data: 431 Byte
AUTH Next Payload: EAP, reserviert: 0x0, Länge: 136
Auth-Methode RSA, reserviert: 0x0, reserviert 0x0
Auth data: 128 Byte
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 154
Code: Anforderung: **ID**: 1, **Länge**: 150
Typ: Unbekannt - 254
EAP-Daten: 145 Byte

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VR
IKEv2-PROTO-3: **HDR**[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: **IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:**
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, **Flaggen: ANTWO**
REAKTION
IKEv2-PROTO-4: Nachrichten-ID: 0x1, Länge: 1292
ENCR Next-Payload: VID, reserviert: 0x0, Länge: 1264
Verschlüsselte Daten und Doppelpunkte; 1260 Byte

IKEv2-PROTO-5: 6. Fragmentiertes Paket, Fragment-MTU: 544
Fragmente: 3, Fragment-ID: 1
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
****

Datum: 23.04.2013
Uhrzeit: 16:25:02 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: ikev2_verify_X509_SIG_certs
Datei: .\ikev2_anyconnect_osal.cpp
Leitung: 2077
Zertifikat vom Benutzer anfordern
****

Datum: 23.04.2013
Uhrzeit: 16:25:02 Uhr
Typ: Fehler
Quelle: Acvpnui

Beschreibung: Funktion: CAPICertificate::verifyChainPolicy
Datei: \Certificates\CapiCertificate.cpp
Leitung: 2032
Aufgerufene Funktion: CertVerifyCertificateChainPolicy
Rücksendecode: -2146762487 (0 x 800 B0109)
Beschreibung: Eine Zertifikatkette wird verarbeitet, aber in einer
terminiert, das vom Vertrauensanbieter nicht als vertrauenswürd
****

Datum: 23.04.2013
Uhrzeit: 16:25:04 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: CEAPMgr::dataRequestCB
Datei: .\EAPMgr.cpp
Leitung: 400
Von EAP vorgeschlagener Typ: EAP-ANYCONNECT
****

Der Client antwortet auf die EAP-Anfrage mit einer Antwort.
Das EAP-Paket enthält:

1. **Code: response** - Dieser Code wird vom Peer als Antwort auf die EAP-Anforderung an den Authentifizierer gesendet.
2. **ID: 1 -** Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 1, der angibt, dass es sich um eine Antwort auf die Anfrage handelt, die zuvor von der ASA (Authentifizierer) gesendet wurde. Diese EAP-Antwort hat den 'config-auth'-Typ 'init'. Der Client initialisiert den EAP-Austausch und wartet darauf, dass die ASA die Authentifizierungsanfrage generiert.
3. **Länge: 252** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten.
4. **EAP-Daten**.

Die ASA entschlüsselt diese Antwort, und der Client gibt an, dass er die AUTH-Payload im vorherigen Paket (mit dem Zertifikat) erhalten und das erste EAP-Anforderungspaket von der ASA erhalten hat. Das ist das, was das "init"-EAP-Antwortpaket enthält.

IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[1
InitSPI=0x58aff71141ba436b RespSPI=0b xfc696330e6b94d7f
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRI
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, Flaggen: INITIAT
IKEv2-PROTO-4: Nachrichten-ID: 0x2, Länge: 332
IKEv2-PROTO-5: 6. Die Anforderung hat mess_id 2. Erwartete 2
ECHTES entschlüsseltes Paket:Daten: 256 Byte
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 256
Code: Antwort: **ID: 1**, **Länge**: 252
Typ: Unbekannt - 254
EAP-Daten:247 Byte
Entschlüsseltes Paket: Data: 332 Byte
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState:
Ereignis: EV_RECV_AUTH
IKEv2-PROTO-3: 6. Stoppen des Timers zum Warten auf die Authentifizierungsmeldung
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState:
Ereignis: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState:
Ereignis: EV_PROC_MSG
IKEv2-PROTO-2: 6. **Verarbeitung der EAP-Antwort**
Unten vom Client erhaltene XML-Nachricht

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="init">
<Geräte-ID>win</Geräte-ID>
<version Who="vpn">3.0.1047</version>
<Gruppenauswahl>ASA-IKEV2</group select>
<Gruppenzugriff>ASA-IKEV2</group access>
```

</config-auth>
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState:
Ereignis: **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState:
Ereignis: **EV_RECV_EAP_REQ**

Dies ist die zweite Anfrage, die von der ASA an den Client gesendet wird.
Das EAP-Paket enthält:

1. **Code: request** - Dieser Code wird vom Authentifizierer an den Peer gesendet.
2. **ID: 2** - Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 2, der angibt, dass es sich um das zweite Paket im Austausch handelt. Diese Anforderung hat den Typ 'config-auth' von 'auth-request'. die ASA fordert an, dass der Client die Anmeldeinformationen für die Benutzerauthentifizierung sendet.
3. **Länge: 457** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten.
4. **EAP-Daten**.

ENCR-Payload:
Diese Nutzlast wird entschlüsselt, und ihr Inhalt wird als zusätzliche Nutzlasten analysiert.

IKEv2-PROTO-2: 6. EAP-Anforderung senden
Generierte XML-Nachricht unten
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-request"**>
<version Who="sg">9.0(2)8</version>
<Opak is-for="sg">
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash>
</opak>
<csport>443</sport>
<auth id="main">
<Formular>
<input type="text" name="username" label="Benutzername:"></input>
<input type="password" name="password" label="Kennwort:"></input>
</form>
</auth>
</config-auth>
IKEv2-PROTO-3: 6. Erstellung von Paketen für die Verschlüsselung; Inhalt:
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 461
Code: Anforderung: ID: 2, Länge: 457
Typ: Unbekannt - 254
EAP-Daten: 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]
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi: FC69630E6B94D7F
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, Flaggen: **ANTWORT DER MSG-REAKTION**
IKEv2-PROTO-4: Nachrichten-ID: 0x2, Länge: 524
ENCR Next Payload: EAP, reserviert: 0x0, Länge: 496

****
Datum: 23.04.201
Uhrzeit: 16:25:04
Typ: Informationel
Quelle: Acvpnui

Beschreibung: Fu
SDIMgr::ProcessI
Datei: .\SDIMgr.cp
Leitung: 281
Der Authentifizier
****
Datum: 23.04.201
Uhrzeit: 16:25:07
Typ: Informationel
Quelle: Acvpnui

Beschreibung: Fu
ConnectManager
Datei: .\ConnectM
Leitung: 985
Verarbeitung der
****

Verschlüsselte Daten und Doppelpunkte; 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. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_BLD_EAP_REQ-Ereignis: EV_START_TMR
IKEv2-PROTO-3: 6. **Starter Timer zum Warten auf die Benutzerauthentifizierungsmeldung** (120 Sek.)
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: R_WAIT_EAP_RESP-Ereignis: EV_NO_EVENT

Der Client sendet eine weitere IKE_AUTH-Initiatormeldung mit der EAP-Nutzlast.
Das EAP-Paket enthält:

1. **Code: response** - Dieser Code wird vom Peer als Antwort auf die EAP-Anforderung an den Authentifizierer gesendet.
2. **ID: 2** - Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 2, der angibt, dass es sich um eine Antwort auf die Anfrage handelt, die zuvor von der ASA (Authentifizierer) gesendet wurde.
3. **Länge: 420** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten.
4. **EAP-Daten**.

IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRI
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: **Exchange-Typ: IKE_AUTH, Flaggen: INITIAT**
IKEv2-PROTO-4: Nachrichten-ID: 0x3, Länge: 492
IKEv2-PROTO-5: 6. Die Anforderung hat mess_id 1. Erwartete 3

ECHTES entschlüsseltes Paket:Daten: 424 Byte
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 424
Code: Antwort: ID: 2, Länge: 420
Typ: Unbekannt - 254
EAP-Daten: 415 Byte

Die ASA verarbeitet diese Antwort. Der Client hatte angefordert, dass der Benutzer Anmeldeinformationen eingibt. Diese EAP-Antwort hat den 'config-auth'-Typ 'auth-reply'. Dieses Paket enthält die Anmeldeinformationen, die der Benutzer eingegeben hat.

Entschlüsseltes Paket:Daten: 492 Byte
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_RECV_AUTH
IKEv2-PROTO-3: 6. Stoppen des Timers zum Warten auf die Authentifizierungsmeldung
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:

Ereignis: EV_PROC_MSG
IKEv2-PROTO-2: 6. **Verarbeitung der EAP-Antwort**
Unten vom Client erhaltene XML-Nachricht
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="auth-reply"**>
<Geräte-ID>win</Geräte-ID>
<version Who="vpn">3.0.1047</version>
<Session-Token></session-token>
<Session-ID></Session-ID>
<Opak is-for="sg">
<tunnel-group>**ASA-IKEV2**</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<auth>
<Kennwort>cisco123</password>
<Benutzername>Anu</Benutzername></auth>
</config-auth>
IKEv2-PLAT-1: **EAP:Initiated User Authentication**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_NO_EVENT
IKEv2-PLAT-5: EAP:In AAA-Rückruf
Server Cert Digest abrufen: DACE1C274785F28BA11D644530
IKEv2-PLAT-5: **EAP:Erfolg bei der AAA-Rückruffunktion**
IKEv2-PROTO-3: Antwort vom Authentifizierer erhalten
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_RECV_EAP_REQ
IKEv2-PROTO-2: 6. EAP-Anforderung senden
Generierte XML-Nachricht unten
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="complete"**>
<version Who="sg">9.0(2)8</version>
<Session-ID>32768</Session-ID>
<Session-Token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-ZtjYpAyXx2yJH0H3H8t5xpBOx3Ixag</session-Token>
<auth id="Success">
<message id="0" param1="" param2=""></message>
</auth>

IKEv2-PROTO-3: 6. Erstellung von Paketen für die Verschlüsse
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 4239
Code: Anforderung: ID: 3, Länge: 4235
Typ: Unbekannt - 254
EAP-Daten: 4230 Byte

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VR
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0

Die ASA erstellt im Austausch eine dritte EAP-Anforderung.
Das EAP-Paket enthält:

1. **Code: request** - Dieser Code wird vom Authentifizierer an den Peer gesendet.
2. **ID: 3** - Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 3, was anzeigt, dass es sich um das dritte Paket im Austausch handelt. Dieses Paket hat den 'config-auth'-Typ 'complete'. die ASA eine Antwort erhalten hat und der EAP-Austausch abgeschlossen ist.
3. **Länge: 4235** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten.
4. **EAP-Daten**.

ENCR-Payload:
Diese Nutzlast wird entschlüsselt, und ihr Inhalt wird als zusätzliche Nutzlasten analysiert.

IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, Flaggen: **ANTWO**
REAKTION
IKEv2-PROTO-4: Nachrichten-ID: 0x3, Länge: 4300
ENCR Nächste Payload: EAP, reserviert: 0x0, Länge: 4272
Verschlüsselte Daten und Kolon;4.268 Byte
IKEv2-PROTO-5: 6. Fragmentiertes Paket, Fragment-MTU: 544
Fragmente: 9, Fragment-ID: 2
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_START_TMR
IKEv2-PROTO-3: 6. Starter Timer zum Warten auf die Benutzer
Sek.)
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState:
Ereignis: EV_NO_EVENT
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: **Aktuelles Profil: Anyconnect-IKEv2.xml**
Einstellungen für die Konfiguration der empfangenen VPN-Sitzu
Installieren Sie weiter: aktiviert
Proxy-Einstellung: nicht ändern
Proxyserver: Keine
Proxy-PAC-URL: Keine
Proxyausnahmen: Keine
Proxy-Sperrung: aktiviert
Aufteilen ausschließen: Die lokale LAN-Zugriffspräferenz ist de
Aufteilen: deaktiviert
DNS aufteilen: deaktiviert
LAN-Platzhalter: Die lokale LAN-Zugriffspräferenz ist deaktivier
Firewall-Regeln: Keine
Client-Adresse: 10.2.2.1

	Client-Maske: 255.0.0.0 Client-IPv6-Adresse: unbekannt Client-IPv6-Maske: unbekannt MTU: 1406 IKE-Verbindung aufrecht erhalten: 20 Sekunden IKE-DPD: 30 Sekunden Sitzungs-Timeout: 0 Sekunden Trennungs-Timeout: 1800 Sekunden Leerlaufzeitüberschreitung: 1800 Sekunden Server: unbekannt MUS-Host: unbekannt DAP-Benutzermeldung: Keine Quarantänestatus: deaktiviert Stets verfügbares VPN: Nicht deaktiviert Leasingdauer: 0 Sekunden Standarddomäne: unbekannt Startseite: unbekannt Entfernen der Smartcard: aktiviert Lizenzantwort: unbekannt **********
Der Client sendet das Initiator-Paket mit der EAP-Nutzlast. Das EAP-Paket enthält: 1. **Code: response** - Dieser Code wird vom Peer als Antwort auf die EAP-Anforderung an den Authentifizierer gesendet. 2. **ID: 3** - Die ID passt die EAP-Antworten den Anforderungen an. Hier ist der Wert 3, der angibt, dass es sich um eine Antwort auf die Anfrage handelt, die zuvor von der ASA (Authentifizierer) gesendet wurde. Die ASA empfängt jetzt das Antwortpaket vom Client, der den Typ 'config-auth' von 'ack' aufweist. Diese Antwort bestätigt die zuvor von der ASA gesendete "vollständige" EAP-Nachricht. 3. **Länge: 173** - Die Länge des EAP-Pakets umfasst Code-, ID-, Längen- und EAP-Daten. 4. **EAP-Daten**.	IKEv2-PLAT-4: **RECV PKT** [IKE_AUTH] [192.168.1.1]:25171->[InitSPI=0x58aff71141ba436b RespSPI=1 0xfc696330e6b94d7f IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRI IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6 IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi: IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0 IKEv2-PROTO-4: **Exchange-Typ: IKE_AUTH, Flaggen: INITIAT** IKEv2-PROTO-4: Nachrichten-ID: 0x4, Länge: 252 IKEv2-PROTO-5: 6. Die Anforderung hat mess_id 4. Erwartete 4 ECHTES entschlüsseltes Paket:Daten: 177 Byte **EAP** Next Payload: KEINE, reserviert: 0x0, Länge: 177 **Code: Antwort: ID: 3,** Länge: 173 Typ: Unbekannt - 254 **EAP-Daten**: 168 Byte
Die ASA verarbeitet dieses Paket. Die EAP-Austausch ist erfolgreich. Die ASA bereitet das Senden der Tunnelgruppe vor Konfiguration im nächsten Paket, das wurde zuvor vom Client in angefordert IDi-Nutzlast. Die ASA erhält die	Entschlüsseltes Paket:Daten:252 Byte IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436 R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Ereignis: EV_RECV_AUTH IKEv2-PROTO-3: 6. Stoppen des Timers zum Warten auf die Authentifizierungsmeldung IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436

Antwortpaket vom Client, welches hat den 'config-auth'-Typ von 'ack'. Diese
Antwort bestätigt den EAP 'vollständige' Nachricht, die vom ASA.

Relevante Konfiguration:

```
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
```

Der EAP-Austausch ist nun erfolgreich. Das EAP-Paket enthält:

1. **Code**: **Success** - Dieser Code ist vom Authentifizierer an den Peer nach Abschluss eines EAP Authentifizierungsmethode. Diese gibt an, dass der Peer erfolgreich beim Authentifizierer.
2. **ID: 3** - Die ID stimmt mit der EAP-Antworten mit den Anforderungen.
   Hier ist der Wert 3, der zeigt an, dass dies eine Antwort auf
   die zuvor von der ASA (Authentifizierer) Die dritte Gruppe
   der im Austausch befindlichen Pakete
   erfolgreich und der EAP Exchange ist erfolgreich.
3. **Länge: 4** - Länge des EAP Paket enthält Code, ID, Länge und EAP-Daten.
4. **EAP-Daten**.

Da der EAP-Austausch erfolgreich war, sendet der Client das IKE_AUTH-Initiatorpaket mit der AUTH-Nutzlast. Die AUTH-Nutzlast wird aus dem gemeinsamen geheimen Schlüssel generiert.

R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Ereignis: EV_RECV_EAP_RESP
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Ereignis: EV_PROC_MSG
IKEv2-PROTO-2: 6. **Verarbeitung der EAP-Antwort**
Unten vom Client erhaltene XML-Nachricht

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="ack">
<Geräte-ID>win</Geräte-ID>
<version Who="vpn">3.0.1047</version>
</config-auth>
```

IKEv2-PLAT-3: (6) aggrAuthHdl auf 0x2000 eingestellt
IKEv2-PLAT-3: (6) **tg_name auf: ASA-IKEV2**
IKEv2-PLAT-3: (6) **Einstellung des Tuning-Grp-Typs auf: RA**
IKEv2-PLAT-1: **EAP:Authentifizierung erfolgreich**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Ereignis: EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2: 6. Senden der EAP-Statusmeldung
IKEv2-PROTO-3: 6. Erstellung von Paketen für die Verschlüsse
EAP Next Payload: KEINE, reserviert: 0x0, Länge: 8
Code: Erfolg: ID: 3, Länge: 4

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, Flaggen: ANTWO
REAKTION
IKEv2-PROTO-4: Nachrichten-ID: 0x4, Länge: 76
ENCR Next-Payload: EAP, reserviert: 0x0, Länge: 48
Verschlüsselte Daten und Doppelpunkte; 44 Byte

IKEv2-PLAT-4: **SENT PKT [IKE_AUTH]** [10.0.0.1]:4500->[192.1
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f M
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
Ereignis: EV_START_TMR
IKEv2-PROTO-3: 6. Starter Timer zum Warten auf die Authentif
Sek.)
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState:
R_WAIT_EAP_AUTH_VERIFY: EV_NO_EVENT

IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.1.1]:25171->[
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: Exchange-Typ: IKE_AUTH, **Flaggen: INITIAT**

IKEv2-PROTO-4: Nachrichten-ID: 0x5, Länge: 92
IKEv2-PROTO-5: 6. Die Anforderung hat chess_id 5. Erwartete

ECHTES entschlüsseltes Paket:Daten:28 Byte
AUTH Next Payload: KEINE, reserviert: 0x0, Länge: 28
Auth-Methode PSK, reserviert: 0x0, reserviert 0x0
Auth-Daten: 20 Byte
Entschlüsseltes Paket:Daten: 92 Byte
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH
IKEv2-PROTO-3: 6. Stoppen des Timers zum Warten auf die
Authentifizierungsmeldung
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_GET_EAP_KEY
IKEv2-PROTO-2: 6. Senden Sie AUTH, um Peer nach dem EAP
überprüfen.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_VERIFY_AUTH
IKEv2-PROTO-3: 6. **Authentifizierungsdaten überprüfen**
IKEv2-PROTO-3: 6. **Vorinstallierten Schlüssel für ID *$AnyConn**
len 20 verwenden
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: Antwortwarteschlange für Konfigurationsmodus
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_NO_EVENT
IKEv2-PLAT-3: PSH: client=AnyConnect client-version=3.0.104
client-os-version=
IKEv2-PLAT-3: Konfigurationsmodus-Antwort abgeschlossen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_OK_GET_CONFIG
IKEv2-PROTO-3: 6. Konfigurationsmodusdaten zum Senden ha
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_CHK4_IC
IKEv2-PROTO-3: 6. Erstkontakt für die Bearbeitung
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_CHK_REDIRECT
IKEv2-PROTO-5: 6. Die Umleitungsüberprüfung ist für diese Sit
abgeschlossen und übersprungen.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_PROC_SA_TS
IKEv2-PROTO-2: 6. **Verarbeitungsauthentifizierungsmeldung**
IKEv2-PLAT-1: **Crypto Map: Map dynmap seq 1000. Angepasst**

Bei Angabe der EAP-Authentifizierung oder
impliziert durch das Clientprofil und -Profil enthält nicht das <IKEIdentity>-Element, sendet der Client
ID_GROUP-Typ-IDi-Payload mit die feste Zeichenfolge *$AnyConnectClient$*.
Die ASA verarbeitet diese Nachricht.

Relevante Konfiguration:

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

zugewiesener IP
IKEv2-PLAT-3: **Crypto Map: Match auf dynamische Karte dynma**
IKEv2-PLAT-3: PFS deaktiviert für RA-Verbindung
IKEv2-PROTO-3: 6.
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_NO_EVENT
IKEv2-PLAT-2: PFKEY SPI-Rückruf für SPI 0x30B848A4 erhalte
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: 6. **Verarbeitungsauthentifizierungsmeldung**

Die ASA erstellt die IKE_AUTH-Antwortnachricht mit den SA-, TSi- und TSr-Payloads.
Das IKE_AUTH-Responder-Paket enthält:

1. **ISAKMP-Header** - SPI/Version/Flags.
2. **AUTH-Payload** - Mit der gewählten Authentifizierungsmethode.
3. **CFG** - CFG_REQUEST/CFG_REPLY ermöglicht es einem IKE-Endpunkt, Informationen von seinem Peer anzufordern. Wenn ein Attribut in der CFG_REQUEST-Konfigurationsausgabe nicht 0-Length ist, wird es als Vorschlag für dieses Attribut verwendet. Der CFG_REPLY-Konfigurationssatz gibt diesen oder einen neuen Wert zurück. Sie kann auch neue Attribute hinzufügen und nicht einige angeforderte. Anforderer ignorieren zurückgegebene Attribute, die sie nicht erkennen. Die ASA antwortet dem Client mit den Tunnelkonfigurationsattributen im CFG_REPLY-Paket.
4. **SAr2** - SAr2 initiiert die SA, die dem Phase-2-Transformationssatzaustausch in IKEv1 ähnelt.
5. **TSi** und **TSr** - Die Datenverkehrsauswahl für Initiator und Responder enthält jeweils die Quell- und Zieladresse des Initiators und des Responders, um verschlüsselten Datenverkehr

IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_MY_AUTH_METHODE
IKEv2-PROTO-3: 6. **Authentifizierungsverfahren abrufen**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: 6. **Sichern Sie sich den vorinstallierten Schlüs**
$AnyConnectClient$
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_GEN_AUTH
IKEv2-PROTO-3: 6. **Generieren meiner Authentifizierungsdaten**
IKEv2-PROTO-3: 6. **Vorinstallierten Schlüssel für id hostname=A**
len 20 verwenden
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_CHK4_SIGN
IKEv2-PROTO-3: 6. Authentifizierungsverfahren abrufen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Ereignis: EV_OK_AUTH_GEN
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
R_BLD_EAP_AUTH_VERIFY: EV_GEN_AUTH
IKEv2-PROTO-3: 6. Generieren meiner Authentifizierungsdaten
IKEv2-PROTO-3: 6. Vorinstallierten Schlüssel für id hostname=A
len 20 verwenden
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH
IKEv2-PROTO-2: 6. **Senden Sie AUTH, um Peer nach dem EAP**
überprüfen.
IKEv2-PROTO-3: ESP-Angebot: 1, SPI-Größe: 4 (IPSec-Aushan
Anzahl Veränderungen: 1
AES-CBC SHA96
IKEv2-PROTO-5: Benachrichtigungs-Payload erstellen:
ESP_TFC_NO_SUPPORTIKEv2-PROTO-5: Benachrichtigungs-
NON_FIRST_FRAGSIKEv2-PROTO-3: 6. Erstellung von Pakete
Verschlüsselung; Inhalt:
AUTH Next Payload: CFG, reserviert: 0x0, Länge: 28

weiterzuleiten und zu empfangen. Der Adressbereich gibt an, dass der gesamte Datenverkehr zu und von diesem Bereich getunnelt wird. Wenn das Angebot für den Befragten akzeptabel ist, sendet es identische TS-Payloads zurück.

ENCR-Payload:
Diese Nutzlast wird entschlüsselt, und ihr Inhalt wird als zusätzliche Nutzlasten analysiert.

Auth-Methode PSK, reserviert: 0x0, reserviert 0x0
Auth data: 20 Byte
CFG Next Payload: SA, reserviert: 0x0, Länge: 4196
cfg-Typ: **CFG_REPLY,** reserviert: 0x0, reserviert: 0 x 0

Attributtyp: interne IP4-Adresse, Länge: 4

01 01 01 01
Attributtyp: interne IP4-Netzmaske, Länge: 4

00 00 00 00
Attributtyp: interne Adresse, Gültigkeitsdauer: 4

00 00 00 00
Attributtyp: Anwendungsversion, Länge: 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
Attributtyp: Unbekannt - 28704, Länge: 4

00 00 00 00
Attributtyp: Unbekannt - 28705, Länge: 4

00 00 07 08
Attributtyp: Unbekannt - 28706, Länge: 4

00 00 07 08
Attributtyp: Unbekannt - 28707, Länge: 1

01
Attributtyp: Unbekannt - 28709, Länge: 4

00 00 00 1e
Attributtyp: Unbekannt - 28710, Länge: 4

00 00 00 14
Attributtyp: Unbekannt - 28684, Länge: 1

01
Attributtyp: Unbekannt - 28711, Länge: 2

05 7e
Attributtyp: Unbekannt - 28679, Länge: 1

00
Attributtyp: Unbekannt - 28683, Länge: 4

80 0b 00 01
Attributtyp: Unbekannt - 28725, Länge: 1

00
Attributtyp: Unbekannt - 28726, Länge: 1

00

Attributtyp: Unbekannt - 28727, Länge: 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 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
<Snip>
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
Attributtyp: Unbekannt - 28729, Länge: 1

00
SA Next-Payload: TSi, reserviert: 0x0, Länge: 44
IKEv2-PROTO-4: letzter Vorschlag: 0x0, reserviert: 0x0, Länge:
Angebot: 1, Protokoll-ID: ESP, SPI-Größe: 4, #trans: 1
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 1, vorbehalten: 0x0, ID: AES-CBC
IKEv2-PROTO-4: letzte Umwandlung: 0x3, reserviert: 0x0: Läng
Typ: 3, reserviert: 0x0, ID: SHA96
IKEv2-PROTO-4: letzte Umwandlung: 0x0, reserviert: 0x0: Läng
Typ: 5, reserviert: 0x0, ID:

TSi Nächste Payload: TSr, reserviert: 0x0, Länge: 24
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Startport: 0, Endport: 65535
Startanschrift: 10.2.2.1, Endadresse: 10.2.2.1
TSr Nächste Payload: BENACHRICHTIGUNG, reserviert: 0x0,
Anzahl der TSs: 1, reserviert 0x0, reserviert 0x0
TS-Typ: TS_IPV4_ADDR_RANGE, Proto-ID: 0, Länge: 16
Startport: 0, Endport: 65535
Startanschrift: 0.0.0.0, Endadresse: 255 255 255 255 255
IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6
IKEv2-PROTO-4: IKEV2 HDR ISPI: 58AFF71141BA436B - rspi:
IKEv2-PROTO-4: Nächste Nutzlast: ENCR, Version: 2,0
IKEv2-PROTO-4: **Exchange-Typ: IKE_AUTH, Flaggen: ANTWO**
REAKTION
IKEv2-PROTO-4: Nachrichten-ID: 0x5, Länge: 4396
ENCR Next Payload: AUTH, reserviert: 0x0, Länge: 4368
Verschlüsselte Daten und Doppelpunkte; 4364 Byte
IKEv2-PROTO-5: 6. Fragmentiertes Paket, Fragment-MTU: 544
Fragmente: 9, Fragment-ID: 1
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M

Die ASA sendet diese IKE_AUTH-Antwortmeldung, die in neun Pakete aufgeteilt ist. Der Austausch IKE_AUTH ist abgeschlossen.

IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PLAT-4: GESENDETE PKT [IKE_AUTH] [10.0.0.1]:4500-
InitSPI=0x58aff71141ba436b RespSPI=0xfc 696330e6b94d7f M
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Veranstaltung: EV_OK
IKEv2-PROTO-5: 6. Aktion: Aktion_Null
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
EV_PKI_SESH_CLOSE
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: ikev2_log
Datei: .\ikev2_anyconnect_osal.cpp
Leitung: 2730
Die IPsec-Verbindung wurde hergestellt.
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: IPsec-Sitzungsregistrierung:
Verschlüsselung: AES-CBC
PRF: SHA1
HMAC: SHA96
Lokale Authentifizierungsmethode: PSK
Remote-Authentifizierungsmethode: PSK
Sequence-ID: 0
Schlüsselgröße: 192
DH-Gruppe: 1
Uhrzeit neu eingeben: 4294967 Sekunden
Lokale Adresse: 192.168.1.1
Remote-Adresse: 10.0.0.1
Lokaler Port: 4500
Remote-Port: 4500
Sitzungs-ID: 1
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: **Das Profil, das auf dem sicheren Gateway konfig**
Anyconnect-IKEv2.xml
****
Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum M
VPN-Sitzung wird eingerichtet..
****
—IKE_AUTH Exchange ends—
****
Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpndownloader

Beschreibung: Funktion: ProfileManager::loadProfiles
Datei: \Api\ProfileMgr.cpp
Leitung: 148
Geladene Profile:
C:\Documents and Settings\All Users\Application Data\Cisco\Cis
Secure Mobility Client\Profile\anyconnect-ikev2.xml
****
****
Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpndownloader

Beschreibung: Aktuelle Voreinstellungen:
ServiceDisable: falsch
CertificateStoreOverride: falsch
CertificateStore: Alle
ShowPreConnectMessage: falsch
AutoConnectOnStart: falsch
MinimizeOnConnect: wahr
LocalLanAccess: falsch
AutoReconnect: wahr
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: falsch
AutoUpdate: wahr
RSASecurIDI-Integration: Automatisch
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPN-Einrichtung: Nur lokaleBenutzer
ProxySettings: Nativ
AllowLocalProxyConnections: wahr

PPPExklusion: Deaktivieren
PPPExclusionServerIP:
Automatische VPNP-Richtlinie: falsch
TrustedNetworkPolicy: Trennen
UntrustedNetworkPolicy: Verbinden
TrustedDNSDomains:
TrustedDNSServer:
Stets verfügbar: falsch
ConnectFailurePolicy: Geschlossen
AllowCaptivePortalProblembehebung: falsch
CaptivePortalProblembehebungTimeout: 5
ApplyLastVPNocalResourceRules: falsch
AllowVPNDisconnect: wahr
EnableScripting: falsch
TerminateScriptOnNextEvent: falsch
EnablePostSBLOnConnectScript: wahr
AutomaticCertSelection: wahr
RetainVPNOnLogoff: falsch
UserEnforcement: Nur Benutzer identisch
EnableAutomaticServerSelection: falsch
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: falsch
AllowIPsecOverSSL: falsch
ClearSmartcardPin: wahr
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum N
Einrichtung eines VPN-Prüfungssystems..
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum N
VPN einrichten - VPN-Adapter aktivieren...
****

Datum: 23.04.2013
Uhrzeit: 16:25:07 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: Funktion: CVirtualAdapter::DoRegistryRepair
Datei: .\WindowsVirtualAdapter.cpp
Leitung: 1869
VA-Steuerungstaste gefunden:
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control

	********** Datum: 23.04.2013 Uhrzeit: 16:25:07 Uhr Typ: Informationen Quelle: Acvpnant Beschreibung: **Eine neue Netzwerkschnittstelle wurde erkannt.** ********** Datum: 23.04.2013 Uhrzeit: 16:25:07 Uhr Typ: Informationen Quelle: Acvpnant Beschreibung: Funktion: CRouteMgr::logSchnittstellen Datei: .\RouteMgr.cpp Leitung: 2076 Aufgerufene Funktion: LogInterfaces Rücksendecode: 0 (0 x 00000000) **Beschreibung: Liste der IP-Adressen-Schnittstellen: 10.2.2.1 192.168.1.1** ********** Datum: 23.04.2013 Uhrzeit: 16:25:08 Uhr Typ: Informationen Quelle: Acvpnant Beschreibung: Hostkonfiguration: **Öffentliche Adresse: 192.168.1.1** **Öffentliche Maske: 255.255.255,0** **Private Adresse: 10.2.2.1** **Private Maske: 255.0.0.0** Private IPv6-Adresse: K/A Private IPv6-Maske: K/A **Remote-Peers: 10.0.0.1 (TCP-Port 443, UDP-Port 500), 10.0.0.** Private Netzwerke: Keine Öffentliche Netzwerke: Keine Tunnelmodus: Ja **********
Die Verbindung wird in die Datenbank der Security Association (SA) eingegeben, und der Status ist REGISTRIERT. Die ASA führt außerdem Prüfungen wie CAC-Statistiken (Common Access Card), Vorhandensein doppelter SAs durch und legt Werte wie Dead Peer Detection (DPD) usw. fest.	IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436 R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Veranstaltung: **EV_INSERT_IKE** IKEv2-PROTO-2: 6. **SA erstellt; SA in Datenbank einfügen** IKEv2-PLAT-3: VERBINDUNGSSTATUS: UP... Peer: 192.168.1.1:25171, Phas *$AnyConnectClient$* IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436 R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Veranstaltung: **EV_REGISTER_SESSION** IKEv2-PLAT-3: (6) **Der Benutzername ist auf Folgendes festgele** IKEv2-PLAT-3: **VERBINDUNGSSTATUS: REGISTRIERT**.. Peer: 192.168.1.1:2 ***$AnyConnectClient$***

IKEv2-PROTO-3: 6. DPD initialisieren, für 10 Sekunden konfigu
IKEv2-PLAT-3: (6) mib_index auf: 4501
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Veranstaltung: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: 6. IPSEC-Schlüsselmaterial laden
IKEv2-PLAT-3: Crypto Map: Match auf dynamische Karte dynma
IKEv2-PLAT-3: (6) **DPD-Max. Zeit: 30**
IKEv2-PLAT-3: (6) **DPD-Max. Zeit: 30**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Veranstaltung: EV_START_ACCT
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Veranstaltung: EV_CHECK_DUPE
IKEv2-PROTO-3: 6. **Suche nach doppeltem SA**
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
Veranstaltung: EV_CHK4_ROLE
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: Neuer IKV2 als Anforderung aktiviert
IKEv2-PLAT-5: Dezimalzahl für eingehende Verhandlungen
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
EV_R_OK
IKEv2-PROTO-3: 6. Starten des Timers zum Löschen des Verha
IKEv2-PROTO-5: 6. SM Trace-> SA: I_SPI=58AFF71141BA436
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState:
EV_NO_EVENT
IKEv2-PLAT-2: PFKEY Add SA für SPI 0x77EE5348 erhalten, F
IKEv2-PLAT-2: PFKEY-Update-SA für SPI 0x30B848A4 erhalte
****

Datum: 23.04.2013
Uhrzeit: 16:25:08 Uhr
Typ: Informationen
Quelle: Acvpnant

Beschreibung: **Die VPN-Verbindung wurde eingerichtet und kan**
weiterleiten.
****

Datum: 23.04.2013
Uhrzeit: 16:25:08 Uhr
Typ: Informationen
Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum M
VPN einrichten - System wird konfiguriert..
****

Datum: 23.04.2013
Uhrzeit: 16:25:08 Uhr
Typ: Informationen

Quelle: Acvpnui

Beschreibung: An den Benutzer gesendete Informationen zum M
VPN einrichten...
****
Datum: 23.04.2013
Uhrzeit: 16:25:37 Uhr
Typ: Informationen
Quelle: Acvpnant

Datei: .\IPsecProtocol.cpp
Leitung: 945
IPsec-Tunnel ist eingerichtet
****

Tunnelüberprüfung

AnyConnect

Beispielausgabe des Befehls **show vpn-sessiondb detail anyconnect** lautet:

```
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

Beispielausgabe des Befehls **show crypto ikev2 sa** lautet:

```
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
```

Beispielausgabe des Befehls **show crypto ikev2 sa detail** lautet:

```
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

Beispielausgabe des Befehls **show crypto ipsec sa** lautet:

```
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
```

Zugehörige Informationen

- RFC 4306, Internet Key Exchange (IKEv2)-Protokoll
- RFC 3748, Extensible Authentication Protocol (EAP)
- RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2)
- Technischer Support und Dokumentation - Cisco Systems