Debugs ASA IKEv2 pour le dépannage VPN d'Accès à distance

Contenu

Introduction

Ce document décrit comment comprendre met au point sur l'appliance de sécurité adaptable Cisco (ASA) quand la version 2 (IKEv2) d'échange de clés Internet (IKE) est utilisée avec un Client à mobilité sécurisé Cisco AnyConnect. Ce document fournit également des informations sur la façon dont traduire certain mettent au point des lignes dans une configuration ASA.

Ce document ne décrit pas comment passer le trafic après qu'un tunnel VPN ait été établi à l'ASA, ni il inclut des concepts de base d'IPSec ou d'IKE.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de l'échange de paquet pour IKEv2. Le pour en savoir plus, se rapportent à l'[échange du paquet IKEv2 et à l'élimination des imperfections de niveau de Protocol](#).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2 (IKEv2) d'échange de clés Internet (IKE)
- Version 8.4 ou ultérieures de l'appliance de sécurité adaptable Cisco (ASA)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Principale question

Le centre d'assistance technique Cisco (TAC) emploie souvent l'IKE et les commandes de débogage d'IPSec afin de comprendre où il y a un problème avec l'établissement de tunnel VPN d'IPSec, mais les commandes peuvent être cryptiques.

Scénario

Commandes de débogage

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

Configuration ASA

Cette configuration ASA est strictement de base, sans l'utilisation des serveurs externes.

```
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
```

Fichier XML

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

> Remarque: Le nom d'usergroup dans le profil de client XML doit être identique que le nom du groupe de tunnels sur l'ASA. Autrement, entrée de hôte non valide du message d'erreur « . Ressaisissez s'il vous plaît » est vu sur le client d'AnyConnect.

Logs et descriptions de debug

> Remarque: Les logs des diagnostics et de l'outil de génération de rapports (DART) sont généralement logs très bavards, ainsi certains de DART ont été omis dans cet exemple dû à l'insignifiance.

Description de messages	Debugs

serveur

Date : 04/23/2013
Temps : 16:24:55
Type : Les informations
Source : acvpnui

Description : Fonction : ClientIfcBase : : connectez
Fichier : . \ ClientIfcBase.cpp
Ligne : 964
Une connexion VPN à Anu-IKEV2 a été demandée par l'utilisateur.
****
Date : 04/23/2013
Temps : 16:24:55
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur : Contacter Anu-IKEV2.
****
Date : 04/23/2013
Temps : 16:24:55
Type : Les informations
Source : acvpnui

Description : Fonction : ApiCert : : getCertList
Fichier : . \ ApiCert.cpp
Ligne : 259
Nombre de Certificats trouvés : 0
****
Date : 04/23/2013
Temps : 16:25:00
Type : Les informations
Source : acvpnui

Description : **Initier la connexion VPN à la passerelle sécurisée https://10.0.0.1/ASA-IKEV2**
****
Date : 04/23/2013
Temps : 16:25:00
Type : Les informations
Source : acvpnagent

Description : Tunnel initié par le client GUI.
****

Date : 04/23/2013
Temps : 16:25:02
Type : Les informations
Source : acvpnagent

Description : Fonction : CIPsecProtocol : : connectTransport
Fichier : . \ IPsecProtocol.cpp
Ligne : 1629

Socket ouvert d'IKE de 192.168.1.1:25170 à 10.0.0.1:500
****

----------Débuts d'échange IKE_SA_INIT----------

L'ASA reçoit le message IKE_SA_INIT du client.

IKEv2-PLAT-4 : PAQUET RECV [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1]:500 InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000 MID=00000000

IKEv2-PROTO-3 : Rx [L m_id 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0

La première paire de messages est l'échange IKE_SA_INIT. Ces messages négocient des algorithmes de chiffrement, des nonces d'échange, et font un échange de Protocole DH (Diffie-Hellman).

IKEv2-PROTO-3 : **HDR[i:58AFF71141BA436B** - r : 0000000000000000]

IKEv2-PROTO-4 : **Ispi** IKEV2 HDR **: 58AFF71141BA436B - rspi : 0000000000000000**

IKEv2-PROTO-4 : Prochaine charge utile : SA, **version : 2.0**

IKEv2-PROTO-4 : Type d'échange : IKE_SA_INIT, **indicateurs : DEMAND**

IKEv2-PROTO-4 : Id de message : 0x0, longueur : 528

Le message IKE_SA_INIT reçu du client contient ces champs :

1. **En-tête d'ISAKMP** - SPI/version/flags.
2. **SAi1** - Algorithme de chiffrement que le demandeur d'IKE prend en charge.
3. **KEi** - Valeur principale publique CAD du demandeur.
4. **N** - Nonce de demandeur.

Prochaine charge utile **SA** : Le KE, réservé : 0x0, longueur : 168

IKEv2-PROTO-4 : dernière proposition : 0x0, réservé : 0x0, longueur : 16

Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans : 18

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 1
type : 1, réservé : 0x0, id : AES-CBC

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 1
type : 1, réservé : 0x0, id : AES-CBC

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 1
type : 1, réservé : 0x0, id : AES-CBC

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 1, réservé : 0x0, id : 3DES

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 1, réservé : 0x0, id : DES

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA512

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA384

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA256

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : SHA1

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 2, réservé : 0x0, id : MD5

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA512

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA384

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA256

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : MD596

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1536_MODP/Group 5

IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_1024_MODP/Group 2

IKEv2-PROTO-4 : dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 4, réservé : 0x0, id : DH_GROUP_768_MODP/Group 1

Prochaine charge utile du **KE** : N, réservé : 0x0, longueur : 104
Groupe CAD : 1, réservé : 0x0

ed 4a 54 b1 13 7c b8 89 des Cb 2e d1 28 technicien eb 5e 29
f7 62 13 6b DF 95 88 28 Ba b5 97 52 e4 E-F 1d 28
Ca 06 d1 36 b6 67 densité double 4e d8 c7 80 De 20 32 9a C2
36 34 ed 5f c5 b3 3e 1d 83 1a c7 FB 9d b8 c5 f5
Ba 4f b6 b2 e2 43 2d de Ba 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
Prochaine charge utile **N** : VID, réservé : 0x0, longueur : 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 FD a8 77
ce 7c 0b b4
IKEv2-PROTO-5 : Analysez la charge utile spécifique de constructeur :
Prochaine charge utile CISCO-DELETE-REASON VID : VID, réservé : 0x0
longueur : 23
Paquet déchiffré : Données : 528 octets
IKEv2-PLAT-3 : Charges utiles de processus de la coutume VID
IKEv2-PLAT-3 : Cisco Copyright VID reçu du pair
IKEv2-PLAT-3 : EAP VID d'AnyConnect reçu du pair
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement DE VEILLE : **EV_RECV_INIT**
IKEv2-PROTO-3 : (6) : Détection NAT de contrôle
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement DE VEILLE : EV_CHK_REDIRECT
IKEv2-PROTO-5 : (6) : Réorientez le contrôle n'est pas nécessaire, en l'ig
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement DE VEILLE : EV_CHK_CAC
IKEv2-PLAT-5 : **Nouvelle demande d'ikev2 SA admise**
IKEv2-PLAT-5 : Incrémentation du compte de négociation entrant SA par
IKEv2-PLAT-5 : TRAITEMENT NON VALIDE PSH
IKEv2-PLAT-5 : TRAITEMENT NON VALIDE PSH
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement DE VEILLE : EV_CHK_COOKIE
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement DE VEILLE : EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : **EV_VERIFY_MSG**
IKEv2-PROTO-3 : (6) : **Vérifiez le message d'init SA**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : EV_INSERT_SA
IKEv2-PROTO-3 : (6) : Insérez SA
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : EV_GET_IKE_POLICY

L'ASA vérifie et traite Message IKE_INIT. L'ASA :

1. Choisit la crypto suite de ceux offerts par le demandeur.
2. Calcule sa propre clé de secret CAD.
3. Calcule une valeur SKEYID de pour ce que toutes les clés peuvent être dérivées cet IKE_SA. Les en-têtes de tous les messages ultérieurs sont chiffré et authentifié. clés utilisées pour le cryptage et la protection d'intégrité sont dérivées de SKEYID et sont connus en tant que :

   SK_e - Cryptage.**SK_a** - Authentification.**SK_d** - Dérivé et utilisé pour la dérivation d'autre matériel de base pour CHILD_SAs.Un SK_e et un SK_a distincts sont calculé pour chaque direction.

Configuration appropriée :

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

IKEv2-PROTO-3 : (6) : **Obtenir des stratégies configurées**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : **EV_PROC_MSG**
IKEv2-PROTO-2 : (6) : Traitement du message initial
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : EV_DETECT_NAT
IKEv2-PROTO-3 : (6) : La détection NAT de processus annoncent
IKEv2-PROTO-5 : (6) : Le traitement nat détectent le src annoncent
IKEv2-PROTO-5 : (6) : Adresse distante non appariée
IKEv2-PROTO-5 : (6) : Le traitement nat détectent le dst annoncent
IKEv2-PROTO-5 : (6) : Adresse locale appariée
IKEv2-PROTO-5 : (6) : L'hôte se trouve l'extérieur NAT
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : EV_CHK_CONFIG_MODE
IKEv2-PROTO-3 : (6) : Données valides reçues de mode de config
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_INIT : EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3 : (6) : Placez les données reçues de mode de config
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_SET_POLICY
IKEv2-PROTO-3 : (6) : **Établissement des stratégies configurées**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_CHK_AUTH4PKI
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_PKI_SESH_OPEN
IKEv2-PROTO-3 : (6) : Ouvrir une session de PKI
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_GEN_DH_KEY
IKEv2-PROTO-3 : (6) : **Calculer la clé publique CAD**
IKEv2-PROTO-3 : (6) :
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_NO_EVENT
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_GEN_DH_SECRET
IKEv2-PROTO-3 : (6) : **Calculer la clé de secret CAD**
IKEv2-PROTO-3 : (6) :
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_NO_EVENT

IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_GEN_SKEYID
IKEv2-PROTO-3 : (6) : **Générez le skeyid**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : EV_GET_CONFIG_MODE

L'ASA construit le message de réponse pour l'échange IKE_SA_INIT.
Ce paquet contient :

1. **En-tête d'ISAKMP** - SPI/version/flags.
2. **SAr1** - Algorithme de chiffrement que le responder d'IKE choisit.
3. **KEr** - Valeur principale publique CAD du responder.
4. **N** - Nonce de responder.

IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 Cu
: Événement R_BLD_INIT : **EV_BLD_MSG**
IKEv2-PROTO-2 : (6) : **Envoi du message initial**
IKEv2-PROTO-3 : Proposition d'IKE : 1, taille SPI : 0 (négociation initiale
Numérique. transforme : 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2-PROTO-5 : Charge utile spécifique de constructeur d'élaboration :
DELETE-REASONIKEv2-PROTO-5 : Charge utile spécifique de construct
d'élaboration : (CUSTOM)IKEv2-PROTO-5 : Charge utile spécifique de
constructeur d'élaboration : (CUSTOM)IKEv2-PROTO-5 : L'élaboration inf
la charge utile : NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5 : L'élab
informent la charge utile : NAT_DETECTION_DESTINATION_IPIKEv2-PL
Pour récupérer a fait confiance que les émetteurs hache ou aucun dispon
IKEv2-PROTO-5 : Charge utile spécifique de constructeur d'élaboration :
FRAGMENTATIONIKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:500/R
192.168.1.1:25170/VRF i0:f0] : 0x0
IKEv2-PROTO-3 : **HDR[i:58AFF71141BA436B** - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : **Ispi** IKEV2 HDR **: 58AFF71141BA436B - rspi :**
FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : SA, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_SA_INIT, **indicateurs : RESPON**
MSG-RESPONSE
IKEv2-PROTO-4 : Id de message : 0x0, longueur : 386
Prochaine charge utile **SA** : Le KE, réservé : 0x0, longueur : 48
IKEv2-PROTO-4 : dernière proposition : 0x0, réservé : 0x0, longueur : 44
Proposition : 1, id de Protocol : IKE, taille SPI : 0, #trans : 4
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : AES-CBC
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 2, réservé : 0x0, id : SHA1
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 3, réservé : 0x0, id : SHA96
IKEv2-PROTO-4 : dernier transformez : 0x0, réservé : 0x0 : longueur :
type : 4, réservé : 0x0, id : DH_GROUP_768_MODP/Group 1

Prochaine charge utile du **KE** : N, réservé : 0x0, longueur : 104
Groupe CAD : 1, réservé : 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
ce b4 a4 3c F2 8b 74 4e 20 d'E1 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 f7 E-F 1a DF 33 cc
C.C 9c 34 a1 8e fa 45 79 1a 7c 29 05 87 8a courant alternatif 02
98 Cb 41 2e 7d fc c7 76 technicien 51 d6 83 1d 03 b0 d7
Prochaine charge utile **N** : VID, réservé : 0x0, longueur : 24

l'EC 97 b8 67 du fc eb f1 97 C2 28 7f 8c 7d b3 1e 51
d5 e7 C2 f5
Prochaine charge utile VID : VID, réservé : 0x0, longueur : 23

L'ASA envoie le message de réponse pour l'échange IKE_SA_INIT. L'échange IKE_SA_INIT est maintenant complet. L'ASA met en marche le temporisateur pour la procédure d'authentification.

IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_SA_INIT] [10.0.0.1]:500->[192.168.1.1]:25170
InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f
MID=00000000
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 CurState : Événement INIT_DONE : EV_DONE
IKEv2-PROTO-3 : (6) : La fragmentation est activée
IKEv2-PROTO-3 : (6) : Cisco DeleteReason Notify est activé
IKEv2-PROTO-3 : (6) : Échange complet d'init SA
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 CurState : Événement INIT_DONE : EV_CHK4_ROLE
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 CurState : Événement INIT_DONE : EV_START_TMR
IKEv2-PROTO-3 : (6) : Démarrant le temporisateur pour attendre le message authentique (sec 30)
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000000 CurState : Événement R_WAIT_AUTH : EV_NO_EVENT

----------IKE_SA_INIT se terminent----------
---------- IKE_AUTH commence----------
****

Date : 04/23/2013
Temps : 16:25:00
Type : Les informations
Source : acvpnagent

Description : Sécurisez les paramètres de passerelle :

****
Date : 04/23/2013
Temps : 16:25:02
Type : Les informations
Source : acvpnagent

Description : Fonction : CIPsecProtocol : : initiateTu
Fichier : . \ IPsecProtocol.cp
Ligne : 345
Le tunnel d'IPsec initie
****

Adresse IP : 10.0.0.1
Port : 443
URL : "10.0.0.1"
Méthode authentique : **IKE - Eap-AnyConnect**
Identité d'IKE :
****

Date : 04/23/2013
Temps : 16:25:00
Type : Les informations
Source : acvpnagent

Description : **Initier la connexion de Client à mobilité sécurisé Cisco AnyC**
version 3.0.1047
****

Date : 04/23/2013
Temps : 16:25:02
Type : Les informations
Source : acvpnagent

Description : Fonction : ikev2_log
Fichier : .\ikev2_anyconnect_osal.cpp
Ligne : 2730
Demande reçue d'établir un tunnel d'IPsec ; sélecteur du trafic local = plag
d'adresses : 0.0.0.0-255.255.255.255 Protocol : 0 chaînes de port : 0-655
sélecteur distant du trafic = plage d'adresses : 0.0.0.0-255.255.255.255 P
: 0 chaînes de port : 0-65535
****

Date : 04/23/2013
Temps : 16:25:02
Type : Les informations
Source : acvpnagent

Description : Fonction : CIPsecProtocol : : connectTransport
Fichier : . \ IPsecProtocol.cpp
Ligne : 1629
Socket ouvert d'IKE de 192.168.1.1:25171 à 10.0.0.1:4500
****

L'authentification est faite avec l'EAP. Seulement on permet une méthode d'authentification EAP simple dans une conversation d'EAP. L'ASA reçoit le message IKE_AUTH du client.

IKEv2-PLAT-4 : **PAQUET RECV [IKE_AUTH]** [192.168.1.1]:25171->[10.0.
4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000001
IKEv2-PROTO-3 : **Rx** [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
0x1

Quand le client inclut une charge utile IDI mais pas une charge utile AUTHENTIQUE, ceci indique le client a déclaré une identité mais l'a non avéré lui. Dans met au point, l'AUTHENTIQUE la charge utile n'est pas

IKEv2-PROTO-3 : **HDR[i:58AFF71141BA436B** - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : **Ispi** IKEV2 **HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F**
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, **version : 2.0**
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, **indicateurs : DEMANDEU**
IKEv2-PROTO-4 : Id de message : 0x1, longueur : 540
IKEv2-PROTO-5 : (6) : La demande a le mess_id 1 ; 1 prévu à 1
VRAI paquet déchiffré : Données : 465 octets
IKEv2-PROTO-5 : Analysez la charge utile spécifique de constructeur :

présente dans l'IKE_AUTH paquet envoyé par le client. Le client envoie la charge utile AUTHENTIQUE seulement après L'échange d'EAP est réussi. Si l'ASA est disposé à utiliser un extensible méthode d'authentification, il place un EAP la charge utile dans le message 4 et reporte l'envoi SAr2, TSi, et TSr jusqu'au demandeur l'authentification est complète dans a échange ultérieur IKE_AUTH. Le paquet de demandeur IKE_AUTH contient :

1. **En-tête d'ISAKMP** - SPI/version/flags.
2. **IDI** - Le nom de groupe de tunnels cela les souhaits de client à connecter à peut être livré par l'IDI charge utile du type ID_KEY_ID dedans le message initial du Échange IKE_AUTH. Ceci se produit quand le profile* de client est préconfiguré avec un nom de groupe ou, après un réussi précédent l'authentification, le client a a caché le nom de groupe dans le son fichier de préférences. L'ASA tentatives de concurrencer un groupe de tunnels nom avec le contenu de l'IKE

(COUTUME) prochaine charge utile VID : IDI, réservée : 0x0, longueur : 2

58 af f6 11 52 8d b0 2c b8 DA 30 46 soient 91 56 fa

Prochaine charge utile **IDI** : CERTREQ, réservé : 0x0, longueur : 28

Type d'id : Nom de groupe, réservé : 0x0 0x0

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

Prochaine charge utile **CERTREQ** : CFG, réservé : 0x0, longueur : 25

CERT encodant le certificat X.509 - signature Data&colon de CertReq ; 20 octets

Prochaine charge utile **CFG** : SA, réservée : 0x0, longueur : 196

type de cfg : **CFG_REQUEST**, réservé : 0x0, réservé : 0x0

type d'attrib : adresse IP4 interne, longueur : 0

type d'attrib : netmask IP4 interne, longueur : 0

type d'attrib : DN IP4 internes, longueur : 0

type d'attrib : IP4 interne NBNS, longueur : 0

type d'attrib : échéance d'adresse interne, longueur : 0

type d'attrib : version d'application, longueur : 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

type d'attrib : adresse IP6 interne, longueur : 0

type d'attrib : sous-réseau IP4 interne, longueur : 0

type d'attrib : Inconnu - 28682, longueur : 15

77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65

type d'attrib : Inconnu - 28704, longueur : 0

type d'attrib : Inconnu - 28705, longueur : 0

type d'attrib : Inconnu - 28706, longueur : 0

type d'attrib : Inconnu - 28707, longueur : 0

type d'attrib : Inconnu - 28708, longueur : 0

type d'attrib : Inconnu - 28709, longueur : 0

type d'attrib : Inconnu - 28710, longueur : 0

type d'attrib : Inconnu - 28672, longueur : 0

type d'attrib : Inconnu - 28684, longueur : 0

Charge utile IDI. Après le premier
IPSec réussi VPN est établi, le client cache nom de groupe (groupe alias) auquel l'utilisateur authentifié. Ce groupe le nom est fourni dans l'IDI charge utile de la prochaine connexion tentative afin d'indiquer groupe probable désiré par utilisateur. Quand l'authentification EAP est spécifié ou implicite par le client le profil et le profil ne fait pas contenez le <IKEIdentity> l'élément, le client envoie Charge utile IDI de type ID_GROUP avec la chaîne fixe *$AnyConnectClient$*.

3. **CERTREQ** - Le client est demande de l'ASA pour a certificat préféré. Certificat des charges utiles de demande peuvent être incluses dans un échange quand l'expéditeur doit obtenir le certificat du récepteur. La demande de certificat la charge utile est traitée par inspection du « codage de CERT » champ afin de

type d'attrib : Inconnu - 28711, longueur : 2

05 7e
type d'attrib : Inconnu - 28674, longueur : 0

type d'attrib : Inconnu - 28712, longueur : 0

type d'attrib : Inconnu - 28675, longueur : 0

type d'attrib : Inconnu - 28679, longueur : 0

type d'attrib : Inconnu - 28683, longueur : 0

type d'attrib : Inconnu - 28717, longueur : 0

type d'attrib : Inconnu - 28718, longueur : 0

type d'attrib : Inconnu - 28719, longueur : 0

type d'attrib : Inconnu - 28720, longueur : 0

type d'attrib : Inconnu - 28721, longueur : 0

type d'attrib : Inconnu - 28722, longueur : 0

type d'attrib : Inconnu - 28723, longueur : 0

type d'attrib : Inconnu - 28724, longueur : 0

type d'attrib : Inconnu - 28725, longueur : 0

type d'attrib : Inconnu - 28726, longueur : 0

type d'attrib : Inconnu - 28727, longueur : 0

type d'attrib : Inconnu - 28729, longueur : 0

Prochaine charge utile **SA** : TSi, réservé : 0x0, longueur : 124
IKEv2-PROTO-4 : dernière proposition : 0x0, réservé : 0x0, longueur : 12
Proposition : 1, id de Protocol : L'ESP, taille SPI : 4, #trans : 12
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : AES-CBC
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : AES-CBC
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : AES-CBC
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : 3DES
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : DES
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :
type : 1, réservé : 0x0, id : NULL
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur :

déterminer
si le processeur en a
Certificats de ceci type.
Si oui,
Le champ « d'autorité de
certification » est
examiné afin de
déterminer si
le processeur a tous les
Certificats
cela peut être validé
jusqu'à un de
la certification spécifiée
autorités. Ceci peut être
une chaîne de
Certificats.

4. **CFG** - CFG_REQUEST/
CFG_REPLY permet un
IKE
point final pour
demander les
informations
de son pair. Si un attribut
dans
Configuration
CFG_REQUEST
la charge utile n'est pas
zéro-longueur, il est
pris comme suggestion
pour cela
attribut. Le CFG_REPLY
la charge utile de
configuration peut
retourner
cette valeur ou un neuf. Il
peut
ajoutez également les
nouveaux attributs et pas
en incluez a demandé
ceux.
Les demandeurs
ignorent retourné
attributs qu'ils ne font
pas
reconnaissez. Dans ces
derniers met au point,
le client demande le

```
    type : 3, réservé : 0x0, id : SHA512
IKEv2-PROTO-4 :     dernier transformez : 0x3, réservé : 0x0 : longueur : 8
    type : 3, réservé : 0x0, id : SHA384
IKEv2-PROTO-4 :     dernier transformez : 0x3, réservé : 0x0 : longueur : 8
    type : 3, réservé : 0x0, id : SHA256
IKEv2-PROTO-4 :     dernier transformez : 0x3, réservé : 0x0 : longueur : 8
    type : 3, réservé : 0x0, id : SHA96
IKEv2-PROTO-4 :     dernier transformez : 0x3, réservé : 0x0 : longueur : 8
    type : 3, réservé : 0x0, id : MD596
IKEv2-PROTO-4 :     dernier transformez : 0x0, réservé : 0x0 : longueur : 8
    type : 5, réservé : 0x0, id :

 Prochaine charge utile de TSi : TSr, réservé : 0x0, longueur : 24
    Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
    Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, lon
16
    port de début : 0, port de fin : 65535
    adr de début : 0.0.0.0, adr de fin : 255.255.255.255
 Prochaine charge utile de TSr : ANNONCEZ, avez réservé : 0x0, longueu
    Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
    Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, lon
16
    port de début : 0, port de fin : 65535
    adr de début : 0.0.0.0, adr de fin : 255.255.255.255
```

tunnel
configuration dans
CFG_REQUEST. L'ASA
les réponses à ceci et
envoie le tunnel
attributs de configuration
seulement après
l'échange d'EAP est
réussi.

5. SAi2 - SAi2 initie SA,
ce qui est semblable à la
phase 2
échange de jeu de
transformations dans
IKEv1.
6. TSi et TSr - Le
demandeur et
sélecteurs du trafic de
responder
contenez,
respectivement, la
source
et adresse de destination
de
demandeur et responder
expédiez et recevez
chiffré
le trafic. La plage
d'adresses
spécifie que tous
trafiquent à et de
cette plage est percée un
tunnel. Si la
la proposition semble
acceptable au
responder, il envoie les
SOLIDES TOTAUX
identiques
les charges utiles
soutiennent.

Les attributs que le client doit
fournir pour
l'authentification de groupe
sont enregistrées dans
Fichier des profils
d'AnyConnect.

**Configuration *Relevant de
profil :**

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

L'ASA génère une réponse au message IKE_AUTH et prépare pour s'authentifier au client.

Paquet déchiffré : Data&colon ; 540 octets
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_RECV_AUTH
IKEv2-PROTO-3 : (6) : Arrêter le temporisateur pour attendre le message
authentique
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_CHK_NAT_T
IKEv2-PROTO-3 : (6) : Détection NAT de contrôle
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_CHG_NAT_T_PORT
IKEv2-PROTO-2 : (6) : Flotteur détecté NAT au port 25171 d'init, port 450
resp
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_PROC_ID
IKEv2-PROTO-2 : (6) : Parameteres valides reçus dans l'identificateur de
processus
IKEv2-PLAT-3 : (6) méthode authentique de pair réglée à : 0
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH :
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3 : (6) : Obtenir des stratégies configurées
IKEv2-PLAT-3 : Nouvelle connexion client d'AnyConnect détectée basée s
charge utile d'ID
IKEv2-PLAT-3 : my_auth_method = 1
IKEv2-PLAT-3 : (6) méthode authentique de pair réglée à : 256
IKEv2-PLAT-3 : supported_peers_auth_method = 16
IKEv2-PLAT-3 : (6) tp_name réglé à : Anu-ikev2
IKEv2-PLAT-3 : **point de confiance réglé à :** Anu-ikev2
IKEv2-PLAT-3 : ID P1 = 0
IKEv2-PLAT-3 : Traduire IKE_ID_AUTO = à 9
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_SET_POLICY
IKEv2-PROTO-3 : (6) : **Établissement des stratégies configurées**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3 : (6) : Vérifiez la stratégie du pair
IKEv2-PROTO-3 : (6) : **Certificat assorti trouvé**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_CHK_CONFIG_MODE
IKEv2-PROTO-3 : (6) : Données valides reçues de mode de config
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3 : (6) l'adresse Internet DHCP pour DDNS est placée à :
winxp64template
IKEv2-PROTO-3 : (6) : Placez les données reçues de mode de config
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_CHK_AUTH4EAP
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_WAIT_AUTH : EV_CHK_EAP
IKEv2-PROTO-3 : (6) : **Vérifiez l'échange d'EAP**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement **R_BLD_AUTH** : EV_GEN_AUTH
IKEv2-PROTO-3 : (6) : **Générez mes données d'authentification**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_BLD_AUTH : EV_CHK4_SIGN
IKEv2-PROTO-3 : (6) : Obtenez ma méthode d'authentification
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_BLD_AUTH : EV_SIGN
IKEv2-PROTO-3 : (6) : **Données authentiques de signe**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_BLD_AUTH : EV_OK_AUTH_GEN
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu
: Événement R_BLD_EAP_AUTH_REQ : EV_AUTHEN_REQ
IKEv2-PROTO-2 : (6) : **Demander à l'authentificateur pour envoyer la dem**
d'EAP
Valeur créée de **config-auth de** nom de l'élément
Vpn ajouté de valeur de client de nom d'attribut au config-auth d'élément
Valeur de type ajoutée de nom d'attribut bonjour au config-auth d'élément
Valeur créée 9.0(2)8 de version de nom de l'élément
Valeur ajoutée 9.0(2)8 de version de nom de l'élément au config-auth d'él
Nom ajouté d'attribut qui évaluent le SG à la version d'élément
Message généré XML ci-dessous
<? xml version="1.0" encoding="UTF-8"?>
type= " de " vpn de client= » de <config-auth **bonjour** " >
<version who="sg">9.0(2)8</version>
</config-auth>

IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu : Événement R_BLD_EAP_AUTH_REQ : EV_RECV_EAP_AUTH
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu : Événement R_BLD_EAP_AUTH_REQ : EV_CHK_REDIRECT
IKEv2-PROTO-3 : (6) : Réorientez le contrôle avec la plate-forme pour l'Équilibrage de charge
IKEv2-PLAT-3 : Réorientez le contrôle sur la plate-forme
IKEv2-PLAT-3 : ikev2_osal_redirect : Session reçue par 10.0.0.1
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000001 Cu : Événement R_BLD_EAP_AUTH_REQ : EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2 : (6) : **Envoi de la demande d'EAP**
IKEv2-PROTO-5 : Charge utile spécifique de constructeur d'élaboration : G
GRANITEIKEv2-PROTO-3 : (6) : Construction

L'ASA envoie la charge utile AUTHENTIQUE afin de demander des identifiants utilisateurs du client. L'ASA envoie la méthode AUTHENTIQUE en tant que la « RSA, » ainsi elle envoie son propre certificat au client, ainsi le client peut authentifier le serveur ASA.
Puisque l'ASA est disposée à utiliser une méthode d'authentification extensible, elle place une charge utile d'EAP dans le message 4 et reporte envoyer SAr2, TSi, et TSr jusqu'à ce que l'authentification de demandeur soit complète dans un échange ultérieur IKE_AUTH. Ainsi, ces trois charges utiles ne sont pas présentes dans met au point.
Le paquet d'EAP contient :

1. **Code : demande** - Ce code est envoyé par l'authentificateur au pair.
2. **id : 1** - L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 1, qui indique que c'est le premier paquet dans l'échange d'EAP. Cette demande d'EAP a

Prochaine charge utile **différence interdécile** : CERT, réservé : 0x0, longu 36
Type d'id : DN DER ASN1, réservé : 0x0 0x0

30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 49 2d 4b 45 56 32
Prochaine charge utile de **CERT** : CERT, réservé : 0x0, longueur : 436
CERT encodant le certificat **X.509** - signature Data&colon de CERT ; 431 octets
Prochaine charge utile de CERT : AUTHENTIQUE, réservé : 0x0, longue
CERT encodant le certificat X.509 - signature Data&colon de CERT ; 431 octets
Prochaine charge utile **AUTHENTIQUE** : EAP, réservé : 0x0, longueur : 1
Méthode authentique RSA, réservée : 0x0, 0x0 réservé Data&colon authentique ; 128 octets
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 154
Code : demande : **id** : 1, **longueur** : 150
Type : Inconnu - 254
Données d'EAP : 145 octets

IKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f 0x1
IKEv2-PROTO-3 : **HDR[i:58AFF71141BA436B** - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : **Ispi IKEV2 HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F**
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, **indicateurs : RESPONDE MSG-RESPONSE**
IKEv2-PROTO-4 : Id de message : 0x1, longueur : 1292
Prochaine charge utile ENCR : VID, réservé : 0x0, longueur : 1264 Data&colon chiffré ; 1260 octets

le « config-auth » type de « bonjour ; » il est envoyé de l'ASA au client afin d'initier l'échange d'EAP.
3. **Longueur : 150** - La longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.
4. **Données d'EAP**.

La fragmentation peut résulter si les Certificats sont grands ou si des chaînes de certificat sont incluses. Les charges utiles du KE de demandeur et de responder peuvent également inclure les grandes clés, qui peuvent également contribuer à la fragmentation.

```
IKEv2-PROTO-5 : (6) : Fragmenter le paquet, MTU de fragment : 544, nor
de fragments : 3, ID de fragment : 1
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000001
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000001
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000001
******************************************
Date : 04/23/2013
Temps : 16:25:02
Type : Les informations
Source : acvpnagent

Description : Fonction : ikev2_verify_X509_SIG_certs
Fichier : .\ikev2_anyconnect_osal.cpp
Ligne : 2077
Demande de l'acceptation de certificat de l'utilisateur
******************************************
Date : 04/23/2013
Temps : 16:25:02
Type : Erreur
Source : acvpnui

Description : Fonction : CCapiCertificate : : verifyChainPolicy
Fichier : . \ Certificats \ CapiCertificate.cpp
Ligne : 2032
Fonction appelée : CertVerifyCertificateChainPolicy
Code retour : -2146762487 (0x800B0109)
Description : Une chaîne de certificat traitée, mais terminée en certificat ra
qui n'est pas fait confiance par le fournisseur de confiance.
******************************************
Date : 04/23/2013
Temps : 16:25:04
Type : Les informations
Source : acvpnagent

Description : Fonction : CEAPMgr : : dataRequestCB
```

Fichier : . \ EAPMgr.cpp
Ligne : 400
Type proposé par EAP : EAP-ANYCONNECT
****

Le client répond à la demande d'EAP avec une réponse.
Le paquet d'EAP contient :

1. **Code : réponse** - Ce code est envoyé par le pair à l'authentificateur en réponse à la demande d'EAP.
2. **id : 1 -** L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 1, qui indique que c'est une réponse à la demande précédemment envoyée par l'ASA (authentificateur). Cette réponse d'EAP a le type de « config-auth » de « init » ; le client initialise l'échange d'EAP et attend l'ASA pour générer la demande d'authentification.
3. **Longueur : 252** - La longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.
4. **Données d'EAP**.

L'ASA déchiffre cette réponse, et le client dit qu'elle a reçu la charge utile AUTHENTIQUE dans le paquet précédent (avec le certificat) et a reçu le premier paquet de demandes d'EAP de l'ASA. Est ce ce que le paquet de réponse d'EAP de « init » contient.

IKEv2-PLAT-4 : **PAQUET RECV [IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b9 MID=00000002
IKEv2-PROTO-3 : Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0: 0x2
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, indicateurs : DEMANDEU
IKEv2-PROTO-4 : Id de message : 0x2, longueur : 332
IKEv2-PROTO-5 : (6) : La demande a le mess_id 2 ; 2 prévus à 2
VRAI paquet déchiffré : Données : 256 octets
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 256
Code : réponse : **id : 1**, **longueur** : 252
Type : Inconnu - 254
Octets de l'**EAP data:247**
Paquet déchiffré : Data&colon ; 332 octets
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 Cu : Événement R_WAIT_EAP_RESP : EV_RECV_AUTH
IKEv2-PROTO-3 : (6) : Arrêter le temporisateur pour attendre le message authentique
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 Cu : Événement R_WAIT_EAP_RESP : EV_RECV_EAP_RESP
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 Cu : Événement R_PROC_EAP_RESP : EV_PROC_MSG
IKEv2-PROTO-2 : (6) : **Traitement de la réponse d'EAP**
Message reçu XML ci-dessous du client
<? xml version="1.0" encoding="UTF-8"?>
type= " init " de " vpn » de client= de <config-auth >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<group-select>ASA-IKEV2</group-select>
<group-access>ASA-IKEV2</group-access>
</config-auth>
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 Cu : Événement R_PROC_EAP_RESP : **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 Cu : Événement R_BLD_EAP_REQ : **EV_RECV_EAP_REQ**

C'est la deuxième requête envoyée par l'ASA au client.
Le paquet d'EAP contient :

1. **Code : demande** - Ce

IKEv2-PROTO-2 : (6) : Envoi de la demande d'EAP
Message généré XML ci-dessous
<? xml version="1.0" encoding="UTF-8"?>

****
Date : 04/23/2013
Temps : 16:25:04
Type : Les informations

code est envoyé par l'authentificateur au pair.

2. **id : 2** - L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 2, qui indique que c'est le deuxième paquet dans l'échange. Cette demande a le type de « config-auth » de « demande d'autorisation » ; l'ASA demande que le client envoient les qualifications d'authentification de l'utilisateur.
3. **Longueur : 457** - La longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.
4. **Données d'EAP**.

Charge utile **ENCR** :
Cette charge utile est déchiffrée, et son contenu est analysé en tant que charges utiles supplémentaires.

type= " demande d'autorisation " de " vpn »
de client= de <config-auth >
<version who="sg">9.0(2)8</version>
is-for= " SG " de <opaque >
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash>
</opaque>
<csport>443</csport>
id= <authentic " canalisation " >
<form>
nom d'utilisateur de label= " de " nom d'utilisateur de name= » des " textes » de type= de <input : « ></input>
mot de passe de label= " de " mot de passe de name= » de " mot de passe » de type= de <input : « ></input>
</form>
</authentic>
</config-auth>
IKEv2-PROTO-3 : (6) : Paquet de construction pour le cryptage ; le contenu est :
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 461
Code : demande : id : 2, longueur : 457
Type : Inconnu - 254
Données d'EAP : 452 octets

IKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] : 0x2
IKEv2-PROTO-3 : **HDR[i:58AFF71141BA436B** - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, indicateurs : **RESPONDER MSG-RESPONSE**
IKEv2-PROTO-4 : Id de message : 0x2, longueur : 524
Prochaine charge utile **ENCR** : EAP, réservé : 0x0, longueur : 496
Data&colon chiffré ; 492 octets

IKEv2-PLAT-4 : **PAQUET ENVOYÉ [IKE_AUTH]** [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f

Source : acvpnui

Description : Fonction : SDIMgr : : ProcessPromptD
Fichier : . \ SDIMgr.cpp
Ligne : 281
Le type d'authentification n'
SDI.
****
Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnui

Description : Fonction : ConnectMgr : : userRespon
Fichier : . \ ConnectMgr.cpp
Ligne : 985
Traitement de la réponse de l'utilisateur.
****

MID=00000002
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 CurState : Événement R_BLD_EAP_REQ : EV_START_TMR
IKEv2-PROTO-3 : (6) : **Démarrant le temporisateur pour attendre le message authentique d'utilisateur** (sec 120)
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000002 CurState : Événement R_WAIT_EAP_RESP : EV_NO_EVENT

Le client envoie un autre message de demandeur IKE_AUTH avec la charge utile d'EAP.
Le paquet d'EAP contient :

1. **Code : réponse** - Ce code est envoyé par le pair à l'authentificateur en réponse à la demande d'EAP.
2. **id : 2** - L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 2, qui indique que c'est une réponse à la demande précédemment envoyée par l'ASA (authentificateur).
3. **Longueur : 420** - La longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.
4. **Données d'EAP**.

IKEv2-PLAT-4 : PAQUET RECV [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b9 MID=00000003
IKEv2-PROTO-3 : Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0: 0x3
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : **Type d'échange : IKE_AUTH, indicateurs : DEMANDEU**
IKEv2-PROTO-4 : Id de message : 0x3, longueur : 492
IKEv2-PROTO-5 : (6) : La demande a le mess_id 3 ; 3 prévus à 3

VRAI paquet déchiffré : Données : 424 octets
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 424
Code : réponse : id : 2, longueur : 420
Type : Inconnu - 254
Données d'EAP : 415 octets

L'ASA traite cette réponse. Le client avait demandé que l'utilisateur entrent dans des qualifications. Cette réponse d'EAP a le type de « config-auth » de « authentique-réponse. » Ce paquet contient les qualifications entrées par l'utilisateur.

Paquet déchiffré : Données : 492 octets
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu : Événement R_WAIT_EAP_RESP : EV_RECV_AUTH
IKEv2-PROTO-3 : (6) : Arrêter le temporisateur pour attendre le message authentique
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu : Événement R_WAIT_EAP_RESP : EV_RECV_EAP_RESP
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_PROC_EAP_RESP : EV_PROC_MSG
IKEv2-PROTO-2 : (6) : **Traitement de la réponse d'EAP**
Message reçu XML ci-dessous du client
<? xml version="1.0" encoding="UTF-8"?>
type= " authentique-réponse " de " vpn » de client= de <config-auth >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<session-id></session-id>
is-for= " SG " de <opaque >
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<authentic>
<password>cisco123</password>
<username>Anu</username></authentic>
</config-auth>
IKEv2-PLAT-1 : **EAP : Authentification de l'utilisateur initiée**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_PROC_EAP_RESP : EV_NO_EVENT
IKEv2-PLAT-5 : EAP : Dans le rappel d'AAA
Condensé récupéré de CERT de serveur :
DACE1C274785F28BA11D64453096BAE294A3172E
IKEv2-PLAT-5 : **EAP : succès dans le rappel d'AAA**
IKEv2-PROTO-3 : Réponse reçue d'authentificateur
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_PROC_EAP_RESP : EV_RECV_EAP_AUTH
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_BLD_EAP_REQ : EV_RECV_EAP_REQ
IKEv2-PROTO-2 : (6) : Envoi de la demande d'EAP
Message généré XML ci-dessous
<? xml version="1.0" encoding="UTF-8"?>
le type= " de " vpn de client= » de <config-auth **se terminent " >**
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag</session-token>
id= <authentic " succès " >
<message id="0" param1="" param2=""></message>
</authentic>

IKEv2-PROTO-3 : (6) : Paquet de construction pour le cryptage ; le conten
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 4239
Code : demande : id : 3, longueur : 4235
Type : Inconnu - 254
Données d'EAP : 4230 octets

IKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
0x3

L'ASA établit une troisième demande d'EAP dans l'échange.
Le paquet d'EAP contient :

1. **Code : demande** - Ce code est envoyé par l'authentificateur au pair.
2. **id : 3** - L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 3, qui indique que c'est le troisième paquet dans l'échange. Ce paquet fait « se terminer » le type de « config-auth » de ; l'ASA a reçu une réponse, et l'échange d'EAP est complet.
3. **Longueur : 4235** - La

longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.

4. **Données d'EAP**.

Charge utile **ENCR** :
Cette charge utile est déchiffrée, et son contenu est analysé en tant que charges utiles supplémentaires.

```
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi :
FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, indicateurs : RESPONDE
MSG-RESPONSE
IKEv2-PROTO-4 : Id de message : 0x3, longueur : 4300
 Prochaine charge utile ENCR : EAP, réservé : 0x0, longueur : 4272
Octets data&colon;4268 chiffrés
IKEv2-PROTO-5 : (6) : Fragmenter le paquet, MTU de fragment : 544, nor
de fragments : 9, ID de fragment : 2
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000003
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_BLD_EAP_REQ : EV_START_TMR
IKEv2-PROTO-3 : (6) : Démarrant le temporisateur pour attendre le mess
authentique d'utilisateur (sec 120)
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000003 Cu
: Événement R_WAIT_EAP_RESP : EV_NO_EVENT
***************************************

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : Profil en cours : Anyconnect-ikev2.xml
```

Paramètres de configuration reçus de session VPN :
Maintenez installé : activé
Paramètre de proxy : ne modifiez pas
Serveur proxy : aucun
URL PAC de proxy : aucun
Exceptions de proxy : aucun
Lockdown de proxy : activé
Le fractionnement les excluent : la préférence d'accès local au LAN est désactivée
Le fractionnement incluent : handicapé
DN fendus : handicapé
Masque local de RÉSEAU LOCAL : la préférence d'accès local au LAN e désactivée
Règles de Pare-feu : aucun
Adresse du client : 10.2.2.1
Masque de client : 255.0.0.0
Ipv6 addres de client : inconnu
Masque d'IPv6 de client : inconnu
MTU : 1406
Keepalive d'IKE : 20 secondes
IKE DPD : 30 secondes
Session Timeout : secondes 0
Délai d'attente de débranchement : 1800 secondes
Délai d'attente de veille : 1800 secondes
Serveur : inconnu
Hôte MUS : inconnu
Message d'utilisateur DAP : aucun
État de quarantaine : handicapé
Toujours sur le VPN : non handicapé
Durée de bail : secondes 0
Domaine par défaut : inconnu
Page d'accueil : inconnu
Débranchement de suppression de Smart Card : activé
Réponse de permis : inconnu
****

Le client envoie le paquet de demandeur avec la charge utile d'EAP.
Le paquet d'EAP contient :

1. **Code : réponse** - Ce code est envoyé par le pair à l'authentificateur en réponse à la demande d'EAP.
2. **id : 3** - L'id aide la correspondance les réponses d'EAP avec les demandes. Ici la valeur est 3, qui indique que c'est une réponse à la demande précédemment envoyée par l'ASA

IKEv2-PLAT-4 : **PAQUET RECV** [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b9 MID=00000004
IKEv2-PROTO-3 : Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0: 0x4
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi : FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : **Type d'échange : IKE_AUTH, indicateurs : DEMANDEU**
IKEv2-PROTO-4 : Id de message : 0x4, longueur : 252
IKEv2-PROTO-5 : (6) : La demande a le mess_id 4 ; 4 prévus à 4

VRAI paquet déchiffré : Données : 177 octets
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 177
Code : réponse : id : 3, longueur : 173
Type : Inconnu - 254

(authentificateur). L'ASA reçoit maintenant le paquet de réponse du client, qui a le type de « config-auth » de « ACK » ; cette réponse reconnaît message le « complet » d'EAP envoyé précédemment par l'ASA.

3. **Longueur : 173** - La longueur du paquet d'EAP inclut le code, l'id, la longueur, et les données d'EAP.
4. **Données d'EAP**.

Données d'EAP : 168 octets

L'ASA traite ce paquet. L'échange d'EAP est réussi. L'ASA prépare pour envoyer le groupe de tunnels configuration dans le paquet suivant, qui a été précédemment demandé par le client dedans la charge utile IDI. L'ASA reçoit paquet de réponse du client, qui a le type de « config-auth » de « ACK ». Ceci la réponse reconnaît l'EAP « terminez-vous » le message qui a été envoyé par ASA précédemment.

Octets packet:Data:252 déchiffrés
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement R_WAIT_EAP_RESP : EV_RECV_AUTH
IKEv2-PROTO-3 : (6) : Arrêter le temporisateur pour attendre le message authentique
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement R_WAIT_EAP_RESP : EV_RECV_EAP_RESP
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement R_PROC_EAP_RESP : EV_PROC_MSG
IKEv2-PROTO-2 : (6) : **Traitement de la réponse d'EAP**
Message reçu XML ci-dessous du client
<? xml version="1.0" encoding="UTF-8"?>
type= " ACK " de " vpn » de client= de <config-auth >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
</config-auth>

Configuration appropriée :

```
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) aggrAuthHdl réglé à 0x2000
IKEv2-PLAT-3 : (6) **tg_name réglé à : ASA-IKEV2**
IKEv2-PLAT-3 : (6) **type de grp de tunn réglé à : RA**
IKEv2-PLAT-1 : **EAP : Authentification réussie**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement R_PROC_EAP_RESP : EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2 : (6) : Envoi du message d'état d'EAP
IKEv2-PROTO-3 : (6) : Paquet de construction pour le cryptage ; le conter
Prochaine charge utile d'**EAP** : AUCUN, réservé : 0x0, longueur : 8
Code : succès : id : 3, longueur : 4

L'échange d'EAP est maintenant réussi.
Le paquet d'EAP contient :

1. **Code** : **succès** - Ce code est

IKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
0x4
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]

envoyé par
l'authentificateur au
pair à la fin d'un EAP
méthode
d'authentification. Ceci
indique que le pair a
authentifié avec succès
au
authentificateur.

2. **id : 3** - L'id aide la
correspondance
Réponses d'EAP avec
les demandes.
Ici la valeur est 3, qui
indique que c'est une
réponse à
la demande
précédemment envoyée
par
ASA (authentificateur).
Le troisième
positionnement
des paquets dans
l'échange était
réussi, et l'échange
d'EAP
est réussi.
3. **Longueur : 4** - Longueur
de l'EAP
le paquet inclut le code,
id,
longueur, et données
d'EAP.
4. **Données d'EAP**.

IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi :
FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, indicateurs : RESPONDE
MSG-RESPONSE
IKEv2-PROTO-4 : Id de message : 0x4, longueur : 76
Prochaine charge utile ENCR : EAP, réservé : 0x0, longueur : 48
Octets data:44 chiffrés

IKEv2-PLAT-4 : **PAQUET ENVOYÉ [IKE_AUTH]** [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000004
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement R_PROC_EAP_RESP : EV_START_TMR
IKEv2-PROTO-3 : (6) : Démarrant le temporisateur pour attendre le messa
authentique (sec 30)
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000004 Cu
: Événement **R_WAIT_EAP_AUTH_VERIFY** : EV_NO_EVENT

Puisque l'échange d'EAP est réussi, le client envoie le paquet de demandeur IKE_AUTH avec la charge utile AUTHENTIQUE. La charge utile AUTHENTIQUE est générée de la clé secrète partagée.

IKEv2-PLAT-4 : PAQUET RECV [IKE_AUTH] [192.168.1.1]:25171-
>[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b9
MID=00000005
IKEv2-PROTO-3 : Rx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
0x5
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi :
FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : Type d'échange : IKE_AUTH, **indicateurs : DEMANDEU**
IKEv2-PROTO-4 : Id de message : 0x5, longueur : 92
IKEv2-PROTO-5 : (6) : La demande a le mess_id 5 ; 5 prévus à 5

VRAIS octets packet:Data:28 déchiffrés

Quand l'authentification EAP est spécifiée ou implicite par le profil de client et le profil ne contient pas l'élément de <IKEIdentity>, le client envoie une charge utile IDI de type ID_GROUP avec la chaîne fixe *$AnyConnectClient$*. L'ASA traite ce message.

Configuration appropriée :

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

Prochaine charge utile **AUTHENTIQUE** : AUCUN, réservé : 0x0, longueu
Méthode authentique PSK, réservée : 0x0, 0x0 réservé
Données authentiques : 20 octets
Paquet déchiffré : Données : 92 octets
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_WAIT_EAP_AUTH_VERIFY : EV_RECV_AUTH
IKEv2-PROTO-3 : (6) : Arrêter le temporisateur pour attendre le message authentique
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_GET_EAP_KEY
IKEv2-PROTO-2 : (6) : Envoyez AUTHENTIQUE, pour vérifier le pair après qu'échange d'EAP
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_VERIFY_AUTH
IKEv2-PROTO-3 : (6) : **Vérifiez les données d'authentification**
IKEv2-PROTO-3 : (6) : **Utilisez la clé pré-partagée pour l'id *$AnyConnectClient$*, clé len 20**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_GET_CONFIG_MODE
IKEv2-PLAT-3 : Réponse de mode de config alignée
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_NO_EVENT
IKEv2-PLAT-3 : PSH : client-os-version= de client-os=Windows du client=AnyConnect client-version=3.0.1047
IKEv2-PLAT-3 : Réponse de mode de config terminée
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_OK_GET_CONFIG
IKEv2-PROTO-3 : (6) : Ayez les données de mode de config à envoyer
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_CHK4_IC
IKEv2-PROTO-3 : (6) : Traitement du contact initial
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_CHK_REDIRECT
IKEv2-PROTO-5 : (6) : Réorientez le contrôle est déjà fait pour cette sess l'ignorant
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement R_VERIFY_AUTH : EV_PROC_SA_TS
IKEv2-PROTO-2 : (6) : **Traitement du message authentique**
IKEv2-PLAT-1 : **Crypto map : Dynmap 1000 seq de carte. Sélecteur ajust utilisant l'adresse IP attribuée**
IKEv2-PLAT-3 : **Crypto map : correspondance sur le dynmap dynamique seq de carte**
IKEv2-PLAT-3 : PFS désactivé pour la connexion de RA
IKEv2-PROTO-3 : (6) :

L'ASA établit le message de réponse IKE_AUTH avec les charges utiles SA, de TSi, et de TSr.
Le paquet de responder IKE_AUTH contient :

1. **En-tête d'ISAKMP** - SPI/version/flags.
2. **Charge utile AUTHENTIQUE** - Avec la méthode d'authentification choisie.
3. **CFG** - CFG_REQUEST/CFG_REPLY permet à un point final d'IKE pour demander les informations de son pair. Si un attribut dans la charge utile de configuration CFG_REQUEST n'est pas zéro-longueur, il est pris comme suggestion pour cet attribut. La charge utile de configuration CFG_REPLY peut renvoyer cette valeur ou un neuf. Il peut également ajouter de nouveaux attributs et ne pas en inclure a demandé ceux. Les demandeurs ignorent les attributs retournés qu'ils n'identifient pas. L'ASA répond au client avec les atrributes de configuration de tunnel dans le paquet

IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_VERIFY_AUTH : EV_NO_EVENT
IKEv2-PLAT-2 : Rappel reçu PFKEY SPI pour SPI 0x30B848A4, erreur FA
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_VERIFY_AUTH : EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2 : (6) : **Traitement du message authentique**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement **R_BLD_AUTH** : EV_MY_AUTH_METHOD
IKEv2-PROTO-3 : (6) : **Obtenez ma méthode d'authentification**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_AUTH : EV_GET_PRESHR_KEY
IKEv2-PROTO-3 : (6) : **Obtenez la clé pré-partagée du pair pour *$AnyConnectClient$***
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_AUTH : EV_GEN_AUTH
IKEv2-PROTO-3 : (6) : **Générez mes données d'authentification**
IKEv2-PROTO-3 : (6) : **Utilisez la clé pré-partagée pour l'id hostname=AS IKEV2, clé len 20**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_AUTH : EV_CHK4_SIGN
IKEv2-PROTO-3 : (6) : Obtenez ma méthode d'authentification
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_AUTH : EV_OK_AUTH_GEN
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_EAP_AUTH_VERIFY : EV_GEN_AUTH
IKEv2-PROTO-3 : (6) : Générez mes données d'authentification
IKEv2-PROTO-3 : (6) : Utilisez la clé pré-partagée pour l'id hostname=AS IKEV2, clé len 20
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement R_BLD_EAP_AUTH_VERIFY : EV_SEND_AUTH
IKEv2-PROTO-2 : (6) : **Envoyez AUTHENTIQUE, pour vérifier le pair aprè qu'échange d'EAP**
IKEv2-PROTO-3 : Proposition de l'ESP : 1, taille SPI : 4 (négociation IPS Numérique. transforme : 3
AES-CBC SHA96
IKEv2-PROTO-5 : L'élaboration informent la charge utile : ESP_TFC_NO_SUPPORTIKEv2-PROTO-5 : L'élaboration informent la ch utile : NON_FIRST_FRAGSIKEv2-PROTO-3 : (6) : Paquet de construction le cryptage ; le contenu est :
Prochaine charge utile **AUTHENTIQUE** : CFG, réservé : 0x0, longueur : 2
Méthode authentique PSK, réservée : 0x0, 0x0 réservé
Data&colon authentique ; 20 octets
Prochaine charge utile **CFG** : SA, réservée : 0x0, longueur : 4196
type de cfg : **CFG_REPLY,** réservé : 0x0, réservé : 0x0

CFG_REPLY.

4. **SAr2** - SAr2 initie SA, qui est semblable à l'échange de jeu de transformations de la phase 2 dans IKEv1.
5. **TSi** et **TSr** - Les sélecteurs du trafic de demandeur et de responder contiennent, respectivement, l'adresse source et de destination du demandeur et le responder afin d'expédier et recevoir le trafic chiffré. La plage d'adresses spécifie que toute trafique à et de cette plage est percée un tunnel. Si la proposition semble acceptable au responder, elle renvoie les charges utiles identiques de SOLIDES TOTAUX.

Charge utile **ENCR** :
Cette charge utile est déchiffrée, et son contenu est analysé en tant que charges utiles supplémentaires.

type d'attrib : adresse IP4 interne, longueur : 4

01 01 01 01
type d'attrib : netmask IP4 interne, longueur : 4

00 00 00 00
type d'attrib : échéance d'adresse interne, longueur : 4

00 00 00 00
type d'attrib : version d'application, longueur : 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
type d'attrib : Inconnu - 28704, longueur : 4

00 00 00 00
type d'attrib : Inconnu - 28705, longueur : 4

00 00 07 08
type d'attrib : Inconnu - 28706, longueur : 4

00 00 07 08
type d'attrib : Inconnu - 28707, longueur : 1

01
type d'attrib : Inconnu - 28709, longueur : 4

00 00 00 1e
type d'attrib : Inconnu - 28710, longueur : 4

00 00 00 14
type d'attrib : Inconnu - 28684, longueur : 1

01
type d'attrib : Inconnu - 28711, longueur : 2

05 7e
type d'attrib : Inconnu - 28679, longueur : 1

00
type d'attrib : Inconnu - 28683, longueur : 4

80 0b 00 01
type d'attrib : Inconnu - 28725, longueur : 1

00
type d'attrib : Inconnu - 28726, longueur : 1

00
type d'attrib : Inconnu - 28727, longueur : 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 38 2d 22 3f 3e 3c 63 6f 6e 66 69 67 61 2d 75
74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2d
69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<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 61 2d 75 74 68 3e 00
type d'attrib : Inconnu - 28729, longueur : 1

00
Prochaine charge utile **SA** : TSi, réservé : 0x0, longueur : 44
IKEv2-PROTO-4 : dernière proposition : 0x0, réservé : 0x0, longueur : 40
Proposition : 1, id de Protocol : L'ESP, taille SPI : 4, #trans : 3
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 1
type : 1, réservé : 0x0, id : AES-CBC
IKEv2-PROTO-4 : dernier transformez : 0x3, réservé : 0x0 : longueur : 8
type : 3, réservé : 0x0, id : SHA96
IKEv2-PROTO-4 : dernier transformez : 0x0, réservé : 0x0 : longueur : 8
type : 5, réservé : 0x0, id :

Prochaine charge utile de **TSi** : TSr, réservé : 0x0, longueur : 24
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, lon
16
port de début : 0, port de fin : 65535
adr de début : 10.2.2.1, adr de fin : 10.2.2.1
Prochaine charge utile de **TSr** : ANNONCEZ, avez réservé : 0x0, longueu
Numérique des solides solubles totaux : 1, 0x0 réservé, 0x0 réservé
Type de SOLIDES TOTAUX : TS_IPV4_ADDR_RANGE, id proto : 0, lon
16
port de début : 0, port de fin : 65535
adr de début : 0.0.0.0, adr de fin : 255.255.255.255
IKEv2-PROTO-3 : Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
0x5
IKEv2-PROTO-3 : HDR[i:58AFF71141BA436B - r : FC696330E6B94D7F]
IKEv2-PROTO-4 : Ispi IKEV2 HDR : 58AFF71141BA436B - rspi :
FC696330E6B94D7F
IKEv2-PROTO-4 : Prochaine charge utile : ENCR, version : 2.0
IKEv2-PROTO-4 : **Type d'échange : IKE_AUTH, indicateurs : RESPONDE**
MSG-RESPONSE
IKEv2-PROTO-4 : Id de message : 0x5, longueur : 4396
Prochaine charge utile **ENCR** : AUTHENTIQUE, réservé : 0x0, longueur :
Data&colon chiffré ; 4364 octets

L'ASA envoie ce message de réponse IKE_AUTH, qui est fragmenté dans neuf paquets. L'échange IKE_AUTH est complet.

IKEv2-PROTO-5 : (6) : Fragmenter le paquet, MTU de fragment : 544, **nor**
de fragments : 9, ID de fragment : 3
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-

```
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PLAT-4 : PAQUET ENVOYÉ [IKE_AUTH] [10.0.0.1]:4500-
>[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b
RespSPI=0xfc696330e6b94d7f MID=00000005
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_OK
IKEv2-PROTO-5 : (6) : Action : Action_Null
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_PKI_SESH_CLOSE
***************************************
Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : Fonction : ikev2_log
Fichier : .\ikev2_anyconnect_osal.cpp
Ligne : 2730
La connexion d'IPsec a été établie.
***************************************
Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : Enregistrement de session d'IPsec :
 Cryptage : AES-CBC
 PRF : SHA1
 HMAC : SHA96
 Méthode authentique locale : PSK
 Méthode authentique distante : PSK
 Id d'ordre : 0
```

Taille de clé : 192
Groupe CAD : 1
Temps de rekey : 4294967 secondes
Adresse locale : 192.168.1.1
Adresse distante : 10.0.0.1
Port local : 4500
Port distant : 4500
Id de session : 1
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnui

Description : **Le profil configuré sur la passerelle sécurisée est : Anyconne**
ikev2.xml
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur :
Établissant la session VPN…
****

----------Extrémités d'échange IKE_AUTHENTIC----------

****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpndownloader

Description : Fonction : ProfileMgr : : loadProfiles
Fichier : . \ Api \ ProfileMgr.cpp
Ligne : 148
Profils chargés :
Utilisateurs de C:\Documents and Settings\All \ données des applications
\ mobilité sécurisée Client\Profile\anyconnect-ikev2.xml de Cisco AnyConn
****
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpndownloader

Description : Configurations des préférences en cours :
ServiceDisable : faux
CertificateStoreOverride : faux
CertificateStore : Tous
ShowPreConnectMessage : faux
AutoConnectOnStart : faux
MinimizeOnConnect : vrai

LocalLanAccess : faux
AutoReconnect : vrai
AutoReconnectBehavior : DisconnectOnSuspend
UseStartBeforeLogon : faux
AutoUpdate : vrai
RSASecurIDIntegration : Automatique
WindowsLogonEnforcement : SingleLocalLogon
WindowsVPNEstablishment : LocalUsersOnly
ProxySettings : Indigène
AllowLocalProxyConnections : vrai
PPPExclusion : Débronchement
PPPExclusionServerIP :
AutomaticVPNPolicy : faux
TrustedNetworkPolicy : Débranchement
UntrustedNetworkPolicy : Connectez
TrustedDNSDomains :
TrustedDNSServers :
AlwaysOn : faux
ConnectFailurePolicy : Fermé
AllowCaptivePortalRemediation : faux
CaptivePortalRemediationTimeout : 5
ApplyLastVPNLocalResourceRules : faux
AllowVPNDisconnect : vrai
EnableScripting : faux
TerminateScriptOnNextEvent : faux
EnablePostSBLOnConnectScript : vrai
AutomaticCertSelection : vrai
RetainVpnOnLogoff : faux
UserEnforcement : SameUserOnly
EnableAutomaticServerSelection : faux
AutoServerSelectionImprovement : 20
AutoServerSelectionSuspendTime : 4
AuthenticationTimeout : 12
SafeWordSofTokenIntegration : faux
AllowIPsecOverSSL : faux
ClearSmartcardPin : vrai
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur : **Établissant le VPN - Système de examen…**
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur : **Établissant le VPN - Adaptateur de lancement VPN…**
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : Fonction : CVirtualAdapter : : DoRegistryRepair
Fichier : . \ WindowsVirtualAdapter.cpp
Ligne : 1869
Touche Ctrl trouvée VA :
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : **Une nouvelle interface réseau a été détectée.**
****

Date : 04/23/2013
Temps : 16:25:07
Type : Les informations
Source : acvpnagent

Description : Fonction : CRouteMgr : : logInterfaces
Fichier : . \ RouteMgr.cpp
Ligne : 2076
Fonction appelée : logInterfaces
Code retour : 0 (0x00000000)
Description : Liste interface d'adresse IP :
10.2.2.1
192.168.1.1
****

Date : 04/23/2013
Temps : 16:25:08
Type : Les informations
Source : acvpnagent

Description : Configuration d'hôte :
Annonce publique : 192.168.1.1
Masque public : 255.255.255.0
Adresse privée : 10.2.2.1
Masque privé : 255.0.0.0
Ipv6 addres privé : S/O
Masque privé d'IPv6 : S/O
Pairs distants : 10.0.0.1 (port TCP 443, port UDP 500), 10.0.0.1 (port UDI
Réseaux privés : aucun
Réseaux publics : aucun
Tunnel mode : oui
****

La connexion est écrite dans la base de données de l'association de sécurité (SA), et l'état EST ENREGISTRÉ.

IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu : Événement AUTH_DONE : **EV_INSERT_IKE**
IKEv2-PROTO-2 : (6) : **SA créée ; insertion de SA dans la base de donné**

L'ASA exécute également certains contrôles comme des stats communs de la carte d'accès (CAC), la présence du doublon SAS, et des valeurs de positionnements comme la détection morte de pair (DPD) et ainsi de suite.

IKEv2-PLAT-3 :
ÉTAT DE LA CONNEXION : VERS LE HAUT… du pair : 192.168.1.1:251
phase1_id : *$AnyConnectClient$*
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : **EV_REGISTER_SESSION**
IKEv2-PLAT-3 : (6) **nom d'utilisateur réglé à : Anu**
IKEv2-PLAT-3 :
ÉTAT DE LA CONNEXION : … Pair **ENREGISTRÉ** : 192.168.1.1:25171,
phase1_id : *$AnyConnectClient$*
IKEv2-PROTO-3 : (6) : Initialiser DPD, configuré pendant 10 secondes
IKEv2-PLAT-3 : (6) mib_index réglé à : 4501
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3 : (6) : Élément de clé du chargement IPSEC
IKEv2-PLAT-3 : Crypto map : correspondance sur le dynmap dynamique
seq de carte
IKEv2-PLAT-3 : (6) le **temps maximum DPD sera : 30**
IKEv2-PLAT-3 : (6) le **temps maximum DPD sera : 30**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_START_ACCT
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_CHECK_DUPE
IKEv2-PROTO-3 : (6) : **Vérifier SA en double**
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement AUTH_DONE : EV_CHK4_ROLE
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement PRÊT : EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5 : Nouvelle demande d'ikev2 SA lancée
IKEv2-PLAT-5 : Compte de décrément pour la négociation entrante
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement PRÊT : EV_R_OK
IKEv2-PROTO-3 : (6) : Démarrer le temporisateur pour supprimer le conte
négociation
IKEv2-PROTO-5 : (6) : Trace-> SA SM : I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (r) identification de message = 00000005 Cu
: Événement PRÊT : EV_NO_EVENT
IKEv2-PLAT-2 : PFKEY reçus ajoutent SA pour SPI 0x77EE5348, erreur
FAUSSE
IKEv2-PLAT-2 : Mise à jour reçue SA PFKEY pour SPI 0x30B848A4, erre
FAUSSE
****

Date : 04/23/2013
Temps : 16:25:08
Type : Les informations
Source : acvpnagent

Description : **La connexion VPN a été établie et peut maintenant passer d**
données.
****

Date : 04/23/2013
Temps : 16:25:08
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur :
Établissant le VPN - Configurant le système…
****

Date : 04/23/2013
Temps : 16:25:08
Type : Les informations
Source : acvpnui

Description : Type de message les informations envoyées à l'utilisateur :
Établissant le VPN…
****

Date : 04/23/2013
Temps : 16:25:37
Type : Les informations
Source : acvpnagent

Fichier : . \ IPsecProtocol.cpp
Ligne : 945
Le tunnel d'IPsec est établi
****

Vérification de tunnel

AnyConnect

La sortie témoin de la commande d'**anyconnect de détail de VPN-sessiondb d'exposition** est :

```
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

La sortie témoin de la **crypto** commande d'**ikev2 SA d'exposition** est :

```
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
```

La sortie témoin de la **crypto** commande de **détail d'ikev2 SA d'exposition** est :

```
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

La sortie témoin de la commande de **show crypto ipsec sa** est :

```
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
```

Informations connexes

- RFC 4306, échange de clés Internet (IKE) (IKEv2) Protocol
- RFC 3748, Protocole EAP (Extensible Authentication Protocol)
- RFC 5996, version 2 (IKEv2) de Protocol d'échange de clés Internet (IKE)
- Support et documentation techniques - Cisco Systems