

L'Accès à distance VPN ne fonctionne pas quand l'authentification et l'autorisation de RAYON est configurée

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Autorisation locale contre l'autorisation RADIUS](#)

[Configuration en cours](#)

[Configuration du routeur](#)

[Configuration du serveur RADIUS](#)

[Dépannez](#)

[Debugs de Protocole ISAKMP \(Internet Security Association and Key Management Protocol\)](#)

[L'AAA met au point](#)

Introduction

Ce document décrit le comportement pour l'authentification étendue (XAUTH) pour des utilisateurs VPN quand l'authentification et l'autorisation sont configurées.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification, autorisation et comptabilité (AAA)
- Accès à distance VPN

[Composants utilisés](#)

Les informations dans ce document sont basées sur un routeur de services d'agrégation de Cisco (gamme ASR)1000 qui exécute le logiciel du Cisco IOS® XE.

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.

Problème

Des utilisateurs VPN sont configurés afin de pour être authentifiés et autorisés par un serveur de RAYON. La configuration sur l'ASR est affichée ici :

```
aaa group server radius ACS-Rad
server-private 10.88.171.27 key cisco123
ip vrf forwarding Mgmt-intf
aaa group server tacacs+ ACS-Tac
server-private 10.88.171.27 key cisco123
ip vrf forwarding Mgmt-intf
aaa authentication login VPN_Client group ACS-Rad
aaa authentication login login_local local
aaa authorization network VPN_Client group ACS-Rad
aaa authorization network login_local local
aaa accounting network VPN_Client start-stop group ACS-Rad
aaa accounting network login_local start-stop group ACS-Rad
aaa session-id common
```

Cependant, toutes les fois que vous essayez d'authentifier, vous n'obtenez jamais incité pour vos qualifications. Sur le client, ce message d'erreur est vu dans les messages de log :

```
Unable to establish Phase 1 SA with server "X.X.X.X" because of
"DEL_REASON_PEER_NOT_RESPONDING"
```

Met au point sur l'ASR indiquent que le nom de groupe VPN est utilisé comme **username** pour la tentative d'autorisation.

```
Sep 26 20:01:49.298: RADIUS(000025EA): Sending a IPv4 Radius Packet
Sep 26 20:01:49.298: RADIUS(000025EA): Send Access-Request to X.X.X.X id
1645/88,len 123
Sep 26 20:01:49.298: RADIUS:  authenticator 0B 18 41 30 23 35 91 D5 - C3 DE 78
4E BB AC 30 4C
Sep 26 20:01:49.298: RADIUS:  User-Name          [1]  19  "vpnclient.cisco.com"
Sep 26 20:01:49.298: RADIUS:  User-Password      [2]  18  *
Sep 26 20:01:49.298: RADIUS:  Calling-Station-Id [31] 16  "X.X.X.X"
Sep 26 20:01:49.298: RADIUS:  NAS-Port-Type     [61]  6  Virtual          [5]
Sep 26 20:01:49.298: RADIUS:  NAS-Port       [5]  6  0
Sep 26 20:01:49.299: RADIUS:  NAS-Port-Id    [87] 16  "X.X.X.X"
Sep 26 20:01:49.299: RADIUS:  Service-Type   [6]  6  Outbound        [5]
Sep 26 20:01:49.299: RADIUS:  NAS-IP-Address [4]  6  192.168.0.55
Sep 26 20:01:49.299: RADIUS:  Acct-Session-Id [44] 10  "00002CD6"
Sep 26 20:01:49.299: RADIUS(000025EA): Started 5 sec timeout
Sep 26 20:01:49.326: RADIUS: Received from id 1645/88 X.X.X.X:1812, Access-Accept,
len 26
Sep 26 20:01:49.326: RADIUS:  authenticator D3 9D 20 7E 09 89 68 BD - 1A DF A3
B6 6E 25 8D 77
Sep 26 20:01:49.326: RADIUS:  Service-Type     [6]  6  Framed          [2]
Sep 26 20:01:49.326: RADIUS(000025EA): Received from id 1645/88
Sep 26
iacc02.crt#20:01:49.326: ISAKMP:(0):ISAKMP/tunnel: received callback from AAA
Sep 26 20:01:49.326: ISAKMP/tunnel: received tunnel atts
Sep 26 20:01:49.326: ISAKMP:Error - skey id.
```

Remarque: Cependant, tout fonctionne bien quand l'autorisation locale est configurée.

Solution

Le comportement signalé n'est prévu et pas une bogue. L'Accès à distance VPN a deux processus distincts d'authentification :

1. Authentification de clé pré-partagée pour le tunnel auquel l'utilisateur se connecte.
2. XAUTH qui authentifie l'utilisateur individuel.

Le XAUTH est la phase 1.5 et se produit seulement après que l'authentification de clé pré-partagée réussit au Phase 1. La raison vous ne pouvez pas voir qu'un utilisateur inciter pour un mot de passe est parce que le Phase 1 ne s'est pas encore terminé. Le nom d'utilisateur qui est introduit met au point est réellement pour l'authentification de clé pré-partagée de Phase 1.

Autorisation locale contre l'autorisation RADIUS

Quand l'authoriation local est configuré, le headend VPN prend la valeur principale configurée sous la configuration de groupe afin de finir le Phase 1. Ceci accorde la phase 1 pour se terminer, ainsi le routeur peut poursuivre au XAUTH :

```
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: setting up tunnel vpnclient
pw request
*Dec 26 12:42:13.926: AAA/AUTHOR (0x12): Pick method list 'login_local'
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: Tunnel vpnclient PW Request
successfully sent to AAA
*Dec 26 12:42:13.926: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Dec 26 12:42:13.926: ISAKMP:(0):Old State = IKE_READY New State =
IKE_R_AM_AAA_AWAIT

*Dec 26 12:42:13.927: ISAKMP:(0):ISAKMP/tunnel: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:13.927: ISAKMP/tunnel: received tunnel atts
*Dec 26 12:42:13.927: ISAKMP:(35002): constructed NAT-T vendor-02 ID
*Dec 26 12:42:13.927: ISAKMP:(35002):SA is doing pre-shared key authentication
plus XAUTH using id type ID_IPV4_ADDR
*Dec 26 12:42:13.927: ISAKMP (35002): ID payload
next-payload : 10
type : 1
address : 172.16.161.24
protocol : 0
port : 0
length : 12
*Dec 26 12:42:13.927: ISAKMP:(35002):Total payload length: 12
*Dec 26 12:42:13.927: ISAKMP:(35002): sending packet to X.X.X.X my_port 500
peer_port 65328 (R) AG_INIT_EXCH
*Dec 26 12:42:13.927: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:13.927: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
*Dec 26 12:42:13.927: ISAKMP:(35002):Old State = IKE_R_AM_AAA_AWAIT New State =
IKE_R_AM2
```

*Dec 26 12:42:14.017: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport 59464 Mgmt-intf (R) AG_INIT_EXCH

*Dec 26 12:42:14.017: ISAKMP:(35002): processing HASH payload. message ID = 0

*Dec 26 12:42:14.017: ISAKMP:(35002): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 0x7F7796C1DDC0

*Dec 26 12:42:14.018: ISAKMP:received payload type 20

*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT

*Dec 26 12:42:14.018: ISAKMP:received payload type 20

*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT

*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated

*Dec 26 12:42:14.018: ISAKMP:(35002):SA has been authenticated with X.X.X.X

*Dec 26 12:42:14.018: ISAKMP:(35002):Detected port,floating to port = 59464

*Dec 26 12:42:14.018: ISAKMP: Trying to find existing peer
X.X.X.X/X.X.X.X/59464/Outside

*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated

*Dec 26 12:42:14.018: ISAKMP AAA: Profile vpnclient.cisco.com in use with AAA list VPN_Client for peer X.X.X.X

*Dec 26 12:42:14.018: ISAKMP AAA: No peer record for address X.X.X.X, port 59464.
Create Accounting Record

*Dec 26 12:42:14.018: ISAKMP: Attempting to insert peer index node : 0x2

*Dec 26 12:42:14.018: ISAKMP AAA: Create Accounting Record 0x7F779645B5E0 for peer X.X.X.X/59464 - peer-index 0x2

*Dec 26 12:42:14.018: ISAKMP AAA: NAS Port Id is already set to X.X.X.X

*Dec 26 12:42:14.018: ISAKMP AAA: crypto_ikmp_aaa_acct_rec_create: pki_sd 0

*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH

*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_R_AM2 New State =
IKE_P1_COMPLETE

*Dec 26 12:42:14.018: ISAKMP:(35002):Need XAUTH

*Dec 26 12:42:14.018: ISAKMP: set new node 2793554424 to CONF_XAUTH

*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2

*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2

*Dec 26 12:42:14.018: ISAKMP:(35002): initiating peer config to X.X.X.X.
ID = 2793554424

*Dec 26 12:42:14.018: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH

*Dec 26 12:42:14.018: ISAKMP:(35002):Sending an IKE IPv4 Packet.

*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE

*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_XAUTH_REQ_SENT

*Dec 26 12:42:21.572: ISAKMP (35002): received packet from X.X.X.X dport 4500
sport 59464 Mgmt-intf (R) CONF_XAUTH

*Dec 26 12:42:21.572: ISAKMP:(35002):processing transaction payload from
X.X.X.X. message ID = 2793554424

*Dec 26 12:42:21.572: ISAKMP: Config payload REPLY

*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2

*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2

*Dec 26 12:42:21.572: ISAKMP AAA: NAS Port Id is already set to X.X.X.X

*Dec 26 12:42:21.572: ISAKMP/Authen: unique id = 19

*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: setting up authen_request

*Dec 26 12:42:21.572: AAA/AUTHEN/LOGIN (00000013): Pick method list 'VPN_Client'

*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: Successfully sent authen
info to AAA

*Dec 26 12:42:21.572: ISAKMP:(35002):deleting node 2793554424 error FALSE
reason "Done with xauth request/reply exchange"

*Dec 26 12:42:21.572: ISAKMP:(35002):Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY

*Dec 26 12:42:21.572: ISAKMP:(35002):Old State = IKE_XAUTH_REQ_SENT New

State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

```
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013):Orig. component type = VPN IPSEC
*Dec 26 12:42:21.573: RADIUS: AAA Unsupported Attr: interface [221]
13 32631
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): dropping service type,
"radius-server attribute 6 on-for-login-auth" is off
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IP: 0.0.0.0
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IPv6: ::
*Dec 26 12:42:21.573: Getting session id for EXEC(00000013) : db=7F7792DEEAB8
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): acct_session_id: 8
*Dec 26 12:42:21.573: RADIUS(00000013): sending
*Dec 26 12:42:21.573: RADIUS/ENCODE: Best Local IP-Address X.X.X.X for
Radius-Server X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Sending a IPv4 Radius Packet
*Dec 26 12:42:21.573: RADIUS(00000013): Send Access-Request to 10.88.171.27:1645
id 1645/1,len 95
*Dec 26 12:42:21.573: RADIUS: authenticator B6 8C 79 D9 91 0C 79 50 - CB B0
2A 87 2A 61 03 E8
*Dec 26 12:42:21.573: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.573: RADIUS: User-Password [2] 18 *
*Dec 26 12:42:21.573: RADIUS: Calling-Station-Id [31] 14 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*Dec 26 12:42:21.573: RADIUS: NAS-Port [5] 6 0
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Id [87] 15 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-IP-Address [4] 6 X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Started 5 sec timeout
*Dec 26 12:42:21.671: RADIUS: Received from id 1645/1 X.X.X.X:1645, Access-Accept,
len 56
*Dec 26 12:42:21.671: RADIUS: authenticator E7 C1 B1 3D 04 59 48 22 - 4B 80 9D
1A 5E CA 0A A6
*Dec 26 12:42:21.671: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.671: RADIUS: Class [25] 26
*Dec 26 12:42:21.671: RADIUS: 43 41 43 53 3A 41 43 53 2D 35 78 2F 31 37 33 32
[CACS:ACS-5x/1732]
*Dec 26 12:42:21.671: RADIUS: 37 32 35 30 33 2F 31 34 [ 72503/14]
*Dec 26 12:42:21.671: RADIUS(00000013): Received from id 1645/1
*Dec 26 12:42:21.672: ISAKMP:(35002):ISAKMP/author: Class attribute (len=24)
'CACS:ACS-5x/173272503/14'
*Dec 26 12:42:21.672: ISAKMP:(35002):AAA Authen: No group atts added
*Dec 26 12:42:21.672: ISAKMP: set new node 1771945814 to CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002): initiating peer config to X.X.X.X. ID =
1771945814
*Dec 26 12:42:21.672: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.672: ISAKMP:(35002):Input = IKE_MSG_FROM_AAA,
IKE_AAA_CONT_LOGIN
*Dec 26 12:42:21.672: ISAKMP:(35002):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT

*Dec 26 12:42:21.759: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) CONF_XAUTH
*Dec 26 12:42:21.759: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 1771945814
*Dec 26 12:42:21.759: ISAKMP: Config payload ACK
*Dec 26 12:42:21.759: ISAKMP:(35002): (blank) XAUTH ACK Processed
*Dec 26 12:42:21.759: ISAKMP:(35002):deleting node 1771945814 error FALSE reason
"Transaction mode done"
*Dec 26 12:42:21.759: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_XAUTH_SET_SENT New State =
IKE_P1_COMPLETE
```

*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 26 12:42:21.763: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) QM_IDLE
*Dec 26 12:42:21.763: ISAKMP: set new node 3504137478 to QM_IDLE
*Dec 26 12:42:21.763: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 3504137478
*Dec 26 12:42:21.763: ISAKMP: Config payload REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):checking request:
*Dec 26 12:42:21.763: ISAKMP: IP4_ADDRESS
*Dec 26 12:42:21.763: ISAKMP: IP4_NETMASK
*Dec 26 12:42:21.763: ISAKMP: IP4_DNS
*Dec 26 12:42:21.763: ISAKMP: IP4_NBNS
*Dec 26 12:42:21.763: ISAKMP: ADDRESS_EXPIRY
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BANNER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SAVEPWD
*Dec 26 12:42:21.763: ISAKMP: DEFAULT_DOMAIN
*Dec 26 12:42:21.763: ISAKMP: SPLIT_INCLUDE
*Dec 26 12:42:21.763: ISAKMP: SPLIT_DNS
*Dec 26 12:42:21.763: ISAKMP: PFS
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BROWSER_PROXY
*Dec 26 12:42:21.763: ISAKMP: BACKUP_SERVER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SMARTCARD_REMOVAL_DISCONNECT
*Dec 26 12:42:21.763: ISAKMP: APPLICATION_VERSION
*Dec 26 12:42:21.763: ISAKMP: Client Version is : Cisco Systems VPN Client
5.0.07.0440:WinNTp
*Dec 26 12:42:21.763: ISAKMP: FW_RECORD
*Dec 26 12:42:21.763: ISAKMP: MODECFG_HOSTNAME
*Dec 26 12:42:21.763: ISAKMP:(35002):ISAKMP/author: setting up the authorization
request for vpnclient
*Dec 26 12:42:21.763: AAA/AUTHOR (0x13): Pick method list 'login_local'
***Dec 26 12:42:21.763: ISAKMP/author: Author request for group vpnclientsuccessfully
sent to AAA**
*Dec 26 12:42:21.763: ISAKMP:(35002):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Dec 26 12:42:21.764: ISAKMP:(0):ISAKMP/author: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
*Dec 26 12:42:21.764:
AAA/AUTHOR/IKE: no WINS addresses
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:21.764: ISAKMP:(35002):ISAKMP/author: No Class attributes
*Dec 26 12:42:21.764: ISAKMP:(35002):attributes sent in message:
*Dec 26 12:42:21.764: Address: 0.2.0.0
*Dec 26 12:42:21.766: ISAKMP:(35002):allocating address X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending private address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending subnet mask: 255.255.255.0
*Dec 26 12:42:21.766: ISAKMP: Sending IP4_DNS server address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the
address: 86392
*Dec 26 12:42:21.766: ISAKMP: Sending save password reply value 0
*Dec 26 12:42:21.766: ISAKMP: Sending DEFAULT_DOMAIN default domain name:
vpnclient.cisco.com
*Dec 26 12:42:21.766: ISAKMP: Sending smartcard_removal_disconnect reply

value 0

```
*Dec 26 12:42:21.766: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software,
IOS-XE Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(4)S,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 23-Jul-12 20:02 by mcpre
*Dec 26 12:42:21.766: ISAKMP (35002): Unknown Attr: MODECFG_HOSTNAME (0x700A)
*Dec 26 12:42:21.766: ISAKMP:(35002): responding to peer config from 72.163.84.76.
ID = 3504137478
*Dec 26 12:42:21.766: ISAKMP: Marking node 3504137478 for late deletion
*Dec 26 12:42:21.766: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500 peer_port
59464 (R) CONF_ADDR
*Dec 26 12:42:21.766: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.766: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New
State = IKE_P1_COMPLETE
*Dec 26 12:42:21.766: ISAKMP:FSM error - Message from AAA grp/user.
*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

Quand le routeur est configuré pour autoriser contre le serveur de RAYON, cela ne fonctionne pas parce qu'afin d'obtenir la **clé** (pour l'authentification preshared), il doit faire une requête d'Access-demande au serveur de RAYON. Cependant, la requête d'Access-demande exige d'un **nom d'utilisateur** d'être envoyé à RADIUS et puisque le XAUTH n'est pas fait encore, elle ne peut pas utiliser le **nom d'utilisateur de client**. Dans cette situation, il utilise le **nom de groupe** comme **nom d'utilisateur** à la place. Cependant, puisque le serveur de RAYON n'a pas été installé pour ne vérifier aucun utilisateur par cet ID, il rejette la demande. Pour cette raison, le Phase 1 ne se termine jamais, et l'utilisateur n'est jamais incité pour des qualifications.

Configuration en cours

Configuration du routeur

Voici la configuration pour le routeur.

```
aaa group server radius Radius-Server
server-private X.X.X.X auth-port 1812 acct-port 1813 key 7 <removed>
```

```
aaa authentication login VPN_Client group Radius-Server
aaa authorization network VPN_Client Radius-Server
aaa accounting network VPN_Client start-stop group Radius-Server
```

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp client configuration group vpnclient
key <removed>
dns x.x.x.x
```

```
wins x.x.x.x
domain cisco.com
pool VPN_Pool
acl 101
group-lock
```

```
crypto isakmp profile vpnclient.cisco.com
match identity group vpnclinet
client authentication list VPN_Client
isakmp authorization list VPN_Client
client configuration address respond
accounting VPN_Client
```

```
crypto ipsec transform-set TRANS-DES esp-des esp-md5-hmac
mode tunnel
```

```
crypto dynamic-map DYN-MAP 10
set transform-set TRANS-DES
set isakmp-profile vpnclient.cisco.com
reverse-route
```

```
crypto map VPN local-address TenGigabitEthernet 0/0/0
crypto map VPN 10 ipsec-isakmp dynamic DYN-MAP
```

```
interface TenGigabitEthernet0/0/0
ip address X.X.X.X 255.255.255.0
crypto map VPN
```

[Configuration du serveur RADIUS](#)

Terminez-vous ces étapes afin de configurer le serveur de RAYON.

1. Configurez l'utilisateur de **Groupname** :

General

Name: Status:

Description:

Identity Group:

Password Information

Password must:

- Contain 4 - 32 characters

Password:

Confirm Password:

Change password on next login

Enable Password Information

Enable Password:

Confirm Password:

User Information

ACS-RESERVED-Never-Expired:

= Required fields

2. Configurez un profil d'autorisation afin de donner toutes les paires de la valeur d'attribut (poids du commerce) :

General Common Tasks **RADIUS Attributes**

Name:

Description:

Required fields

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
CVPN3000/ASA/PIX7.x-IPSec-Authentication	Enumeration	Internal
CVPN3000/ASA/PIX7.x-Group-Based-Address	String	VPN_Pool
CVPN3000/ASA/PIX7.x-Access-List-Inbound	String	101
CVPN3000/ASA/PIX7.x-IPSec-Group-Name	String	vpnclient.cisco.com
CVPN3000/ASA/PIX7.x-IPSec-Split-DNS-Nan	String	X.X.X.X

Add Edit Replace Delete

Dictionary Type:

Required fields RADIUS Attribute:

Attribute Type:

Attribute Value:

Required fields

3. Configurez une stratégie d'Access afin de permettre la connexion et l'utilisation qui profilent :

General
 Name: Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

NDG:Location:

Time And Date:

Device IP Address:

Results
 Authorization Profiles:

vpnclient.cisco.com

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Dépannez

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines commandes **show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Ceux-ci met au point sont activés sur le headend VPN :

Debugs de Protocole ISAKMP (Internet Security Association and Key Management Protocol)

```
debug crypto isakmp
```

L'AAA met au point

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug radius authentication
```