Le VPN d'accès à distance ne fonctionne pas lorsque l'authentification et l'autorisation RADIUS sont configurées

Contenu

Introduction

Ce document décrit le comportement de l'authentification étendue (XAUTH) pour les utilisateurs VPN lorsque 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)
- VPN d’accès à distance

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problème

Les utilisateurs VPN sont configurés pour être authentifiés et autorisés par un serveur RADIUS. La configuration de l'ASR est présentée 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, lorsque vous essayez de vous authentifier, vous ne serez jamais invité à fournir vos informations d'identification. Sur le client, ce message d'erreur apparaît dans les messages du journal :

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

Les débogages sur l'ASR indiquent que le nom du groupe VPN est utilisé comme **nom d'utilisateur** 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.
```

Note: Cependant, tout fonctionne correctement lorsque l'autorisation locale est configurée.

Solution

Le comportement signalé est attendu et non un bogue. Le VPN d'accès à distance comporte deux processus d'authentification distincts :

1. Authentification par clé prépartagée pour le tunnel auquel l'utilisateur se connecte.
2. XAUTH qui authentifie l'utilisateur individuel.

XAUTH est la phase 1.5 et se produit uniquement après la réussite de l'authentification de clé pré-partagée dans la phase 1. La raison pour laquelle vous ne pouvez pas voir une invite utilisateur pour un mot de passe est que la phase 1 n'est pas encore terminée. Le nom d'utilisateur qui est envoyé dans les débogages est en fait pour l'authentification de clé pré-partagée de phase 1.

Autorisation locale et autorisation RADIUS

Lorsque l'authentification locale est configurée, la tête de réseau VPN sélectionne la valeur de clé configurée dans la configuration du groupe afin de terminer la phase 1. Cela permet de terminer la phase 1, de sorte que le routeur puisse passer à 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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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_MESG_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
```

Lorsque le routeur est configuré pour autoriser le serveur RADIUS, il ne fonctionne pas car pour obtenir la **clé** (pour l'authentification prépartagée), il doit effectuer une requête de demande d'accès au serveur RADIUS. Cependant, la requête de demande d'accès nécessite un **nom d'utilisateur** à envoyer à RADIUSA et comme XAUTH n'est pas encore fait, il ne peut pas utiliser le **nom d'utilisateur** du client. Dans cette situation, il utilise le **nom de groupe** comme **nom d'utilisateur** à la place. Cependant, comme le serveur RADIUS n'a pas été configuré pour vérifier un utilisateur par cet ID, il rejette la demande. Pour cette raison, la phase 1 ne se termine jamais et l'utilisateur n'est jamais invité à fournir des informations d'identification.

Configuration de travail

Configuration du routeur

Voici la configuration du routeur.

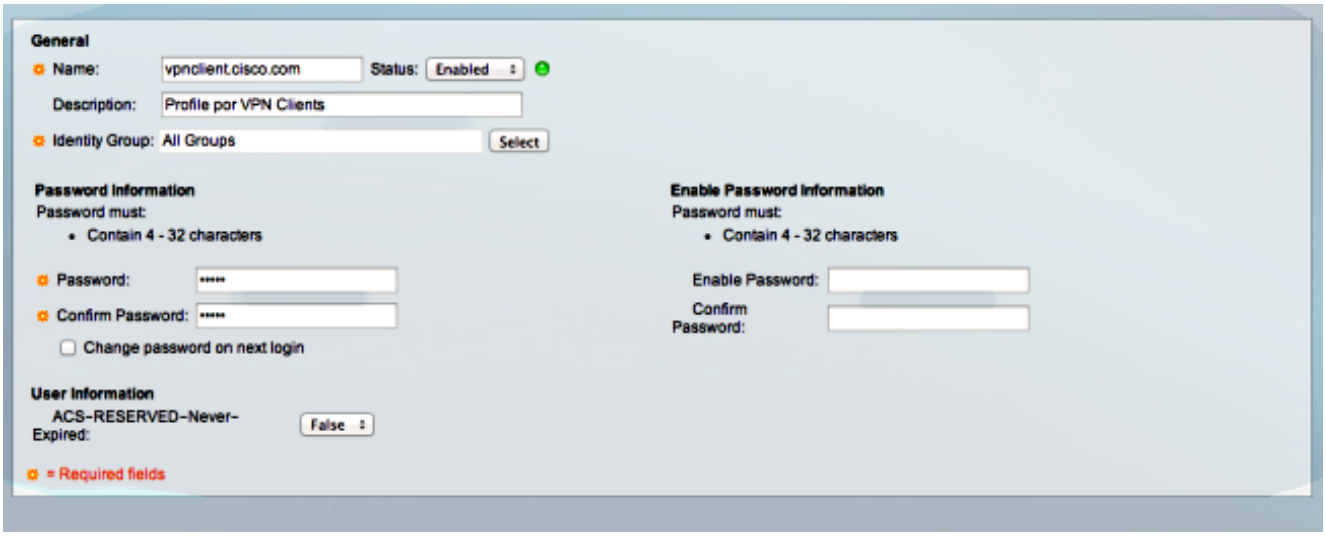
```
aaa group server radius Radius-Server
server-private X.X.X.X auth-port 1812 acct-port 1813 key 7 <removed>


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
```

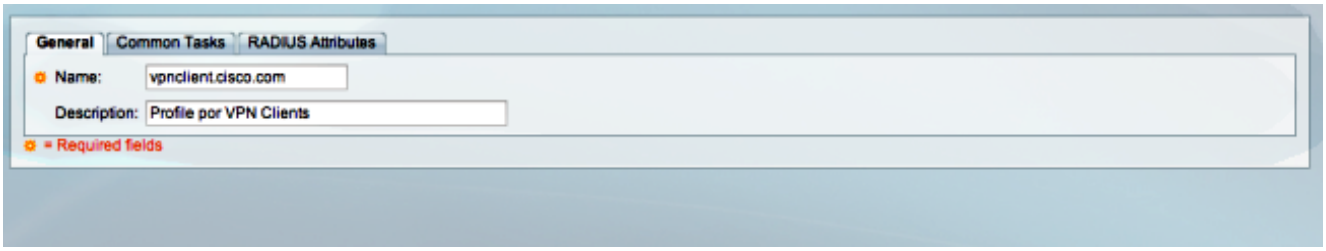
Configuration du serveur RADIUS

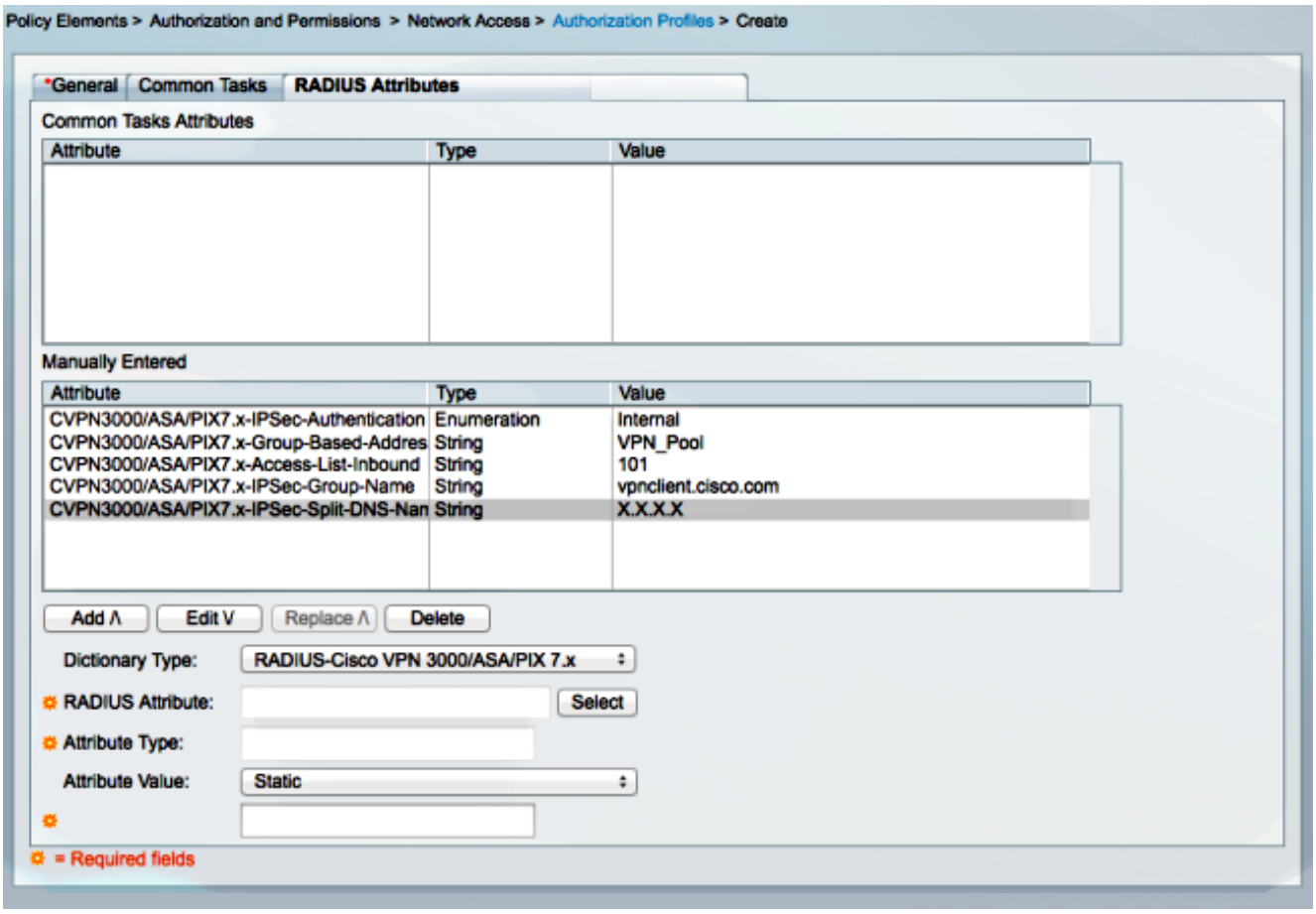
Complétez ces étapes afin de configurer le serveur RADIUS.

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

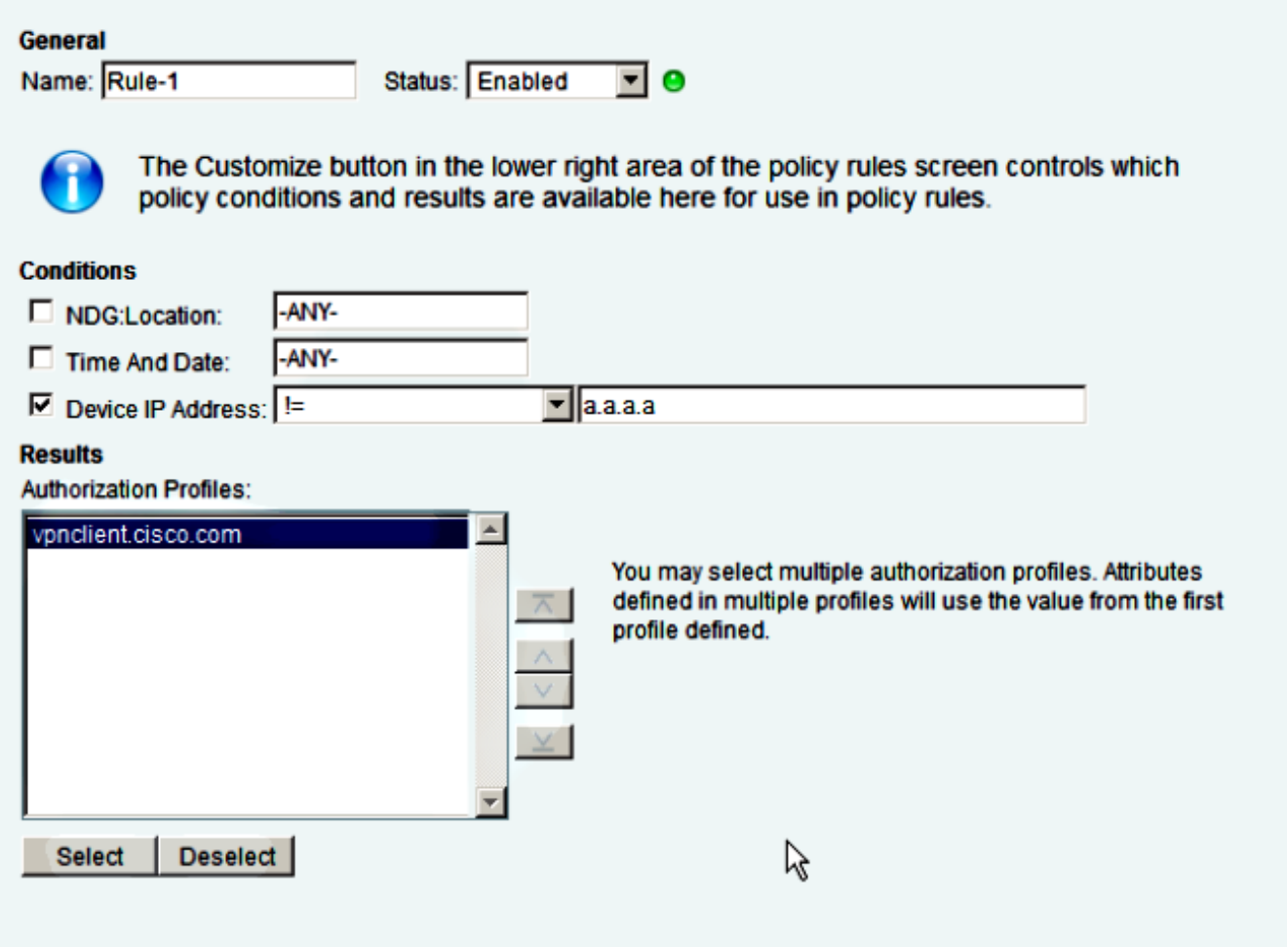


2. Configurez un profil d'autorisation afin de donner toutes les paires Valeur d'attribut (AV) :





3. Configurez une stratégie Access afin d'autoriser la connexion et d'utiliser ce profil :



Dépannage

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Ces débogages sont activés sur la tête de réseau VPN :

Débogues ISAKMP (Internet Security Association and Key Management Protocol)

```
debug crypto isakmp
```

Débogues AAA

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