

La VPN ad accesso remoto non funziona quando sono configurate l'autenticazione e l'autorizzazione RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

[Autorizzazione locale e autorizzazione RADIUS](#)

[Configurazione di lavoro](#)

[Configurazione router](#)

[Configurazione server RADIUS](#)

[Risoluzione dei problemi](#)

[Debug del protocollo ISAKMP \(Internet Security Association and Key Management Protocol\)](#)

[Debug AAA](#)

Introduzione

In questo documento viene descritto il comportamento di XAUTH (Extended Authentication) per gli utenti VPN quando sono configurate sia l'autenticazione che l'autorizzazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione, autorizzazione e accounting (AAA)
- VPN ad accesso remoto

Componenti usati

Per la stesura del documento, è stato usato un Cisco Aggregation Services Router (ASR)serie 1000 con software Cisco IOS[®] XE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Gli utenti VPN sono configurati in modo da essere autenticati e autorizzati da un server RADIUS. Di seguito è riportata la configurazione dell'ASR:

```
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
```

Tuttavia, ogni volta che si tenta di eseguire l'autenticazione, non viene mai richiesta l'immissione delle credenziali. Nel client, questo messaggio di errore viene visualizzato nei messaggi di log:

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

I debug sull'ASR indicano che il nome del gruppo VPN viene utilizzato come **nome utente** per il tentativo di autorizzazione.

```
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.
```

Nota: Tuttavia, se l'autorizzazione locale è configurata, tutto funziona correttamente.

Soluzione

Il comportamento previsto non è un bug. La VPN ad accesso remoto prevede due processi di autenticazione distinti:

1. Autenticazione con chiave già condivisa per il tunnel a cui si connette l'utente.
2. XAUTH che autentica il singolo utente.

XAUTH è la fase 1.5 e si verifica solo dopo che l'autenticazione con chiave già condivisa ha avuto esito positivo nella fase 1. Non è possibile visualizzare la richiesta di una password all'utente perché la fase 1 non è stata ancora completata. Il nome utente inviato nei debug è in realtà associato alla fase 1 dell'autenticazione con chiave già condivisa.

Autorizzazione locale e autorizzazione RADIUS

Quando viene configurata l'autorizzazione locale, l'headend VPN riceve il valore della chiave configurata nella configurazione del gruppo per completare la fase 1. In questo modo, viene completata la fase 1 e il router può procedere verso 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_MSG_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_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

```

Quando il router è configurato per l'autorizzazione sul server RADIUS, non funziona perché per ottenere la **chiave** (per l'autenticazione precondivisa) deve eseguire una query di richiesta di accesso al server RADIUS. Tuttavia, la query di richiesta di accesso richiede l'invio di un **nome utente** a RADIUS e, poiché XAUTH non è ancora stato eseguito, non può utilizzare il **nome utente** del client. In questo caso, viene utilizzato invece il **nome del gruppo** come **nome utente**. Tuttavia, poiché il server RADIUS non è stato configurato per verificare gli utenti in base a tale ID, rifiuta la richiesta. Per questo motivo, la fase 1 non viene mai completata e all'utente non vengono mai richieste le credenziali.

Configurazione di lavoro

Configurazione router

Ecco la configurazione del router.

```

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 vpnclient
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
```

Configurazione server RADIUS

Completare questa procedura per configurare il server RADIUS.

1. Configurare l'utente **Groupname**:

General

Name: Status:

Description:

Identity Group:

Password Information

Password must:

- Contain 4 - 32 characters

Change password on next login

Enable Password Information

User Information

ACS-RESERVED-Never-Expired:

= Required fields

2. Configurare un profilo di autorizzazione per fornire tutte le coppie di valori attributo (AV):

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	vpncient.cisco.com
CVPN3000/ASA/PIX7.x-IPSec-Split-DNS-Nan	String	X.X.X.X

Dictionary Type:


RADIUS Attribute:


Attribute Type:

Attribute Value:

= Required fields

3. Configurare un criterio di accesso per consentire la connessione e utilizzare il profilo:

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.

Risoluzione dei problemi

Lo [strumento Output Interpreter \(solo utenti registrati\) supporta alcuni comandi show](#). Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug prima di usare i comandi di debug](#).

Questi debug sono abilitati sull'headend VPN:

Debug del protocollo ISAKMP (Internet Security Association and Key Management Protocol)

```
debug crypto isakmp
```

Debug AAA

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