Esempio di funzioni ASA e Cisco IOS Group-Lock e di attributi AAA e di configurazione WebVPN

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazioni](#)
[ASA Local Group-Lock](#)
[ASA con attributo AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock](#)
[ASA con attributo AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock](#)
[Cisco IOS Local Group-Lock per Easy VPN](#)
[Cisco IOS AAA ipsec:user-vpn-group per Easy VPN](#)
[Cisco IOS AAA ipsec:user-vpn-group e Group-lock per Easy VPN](#)
[IOS Webvpn Group Lock](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo articolo vengono descritte le funzionalità di blocco dei gruppi su Cisco Adaptive Security Appliance (ASA) e su Cisco IOS® e viene descritto il comportamento dei diversi attributi di autenticazione, autorizzazione e accounting (AAA). Per Cisco IOS, viene spiegata la differenza tra i gruppi group-lock e gli utenti-vpn-group e un esempio che usa entrambe le funzionalità complementari contemporaneamente. È inoltre disponibile un esempio di Cisco IOS WebVPN con domini di autenticazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ASA CLI e configurazione VPN SSL (Secure Sockets Layer)

- Configurazione della VPN ad accesso remoto su ASA e Cisco IOS

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software ASA, versione 8.4 e successive
- Cisco IOS versione 15.1 e successive

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.

Configurazioni

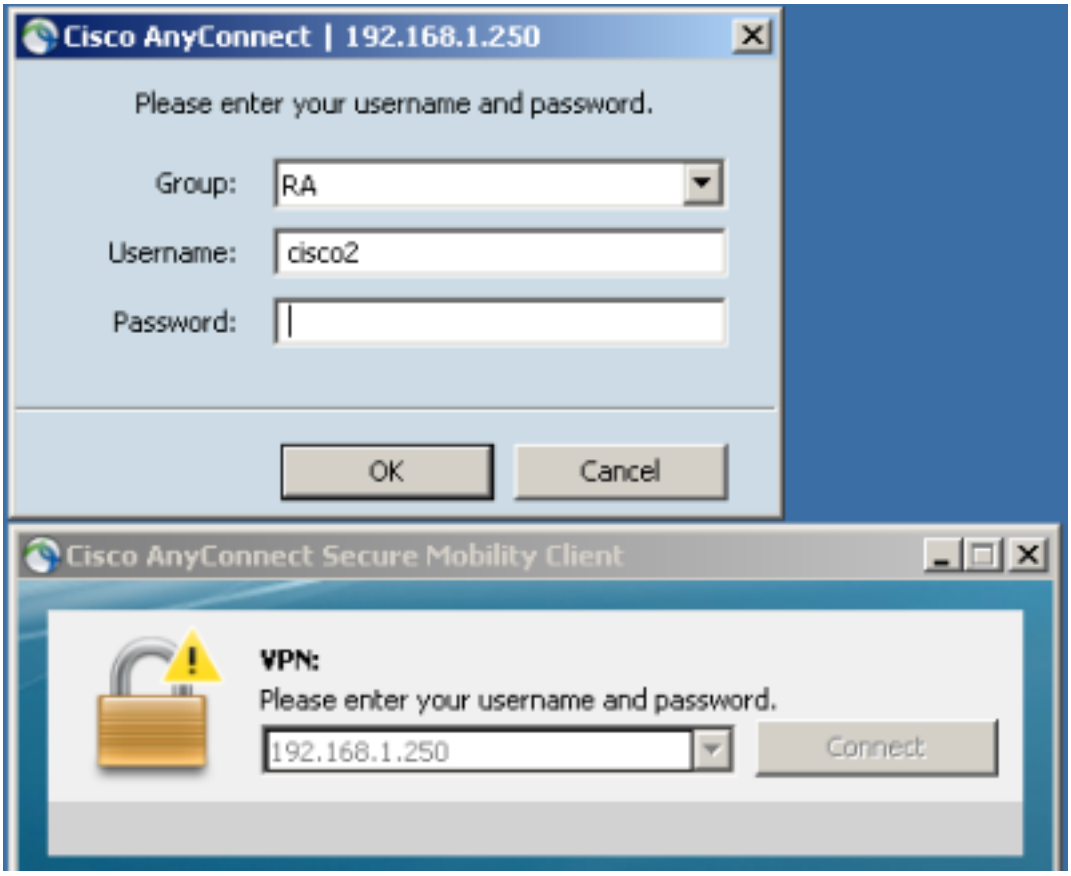
ASA Local Group-Lock

Èpossibile definire questo attributo nell'ambito dell'utente o dei criteri di gruppo. Di seguito è riportato un esempio per l'attributo utente locale.

```
username cisco password 3USUcOPFUiMCO4Jk encrypted
username cisco attributes
 group-lock value RA
username cisco2 password BAtr3u1T7j1eEcYr encrypted
username cisco2 attributes
 group-lock value RA2

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 default-group-policy MY
tunnel-group RA webvpn-attributes
 group-alias RA enable

tunnel-group RA2 type remote-access
tunnel-group RA2 general-attributes
 default-group-policy MY
tunnel-group RA2 webvpn-attributes
 group-alias RA2 enable

group-policy MY attributes
 address-pools value POOL

webvpn
 enable inside
 anyconnect enable
 tunnel-group-list enable
```

L'utente cisco può usare solo il gruppo di tunnel RA e l'utente cisco2 può usare solo il gruppo di tunnel RA2.

Se l'utente cisco2 sceglie il gruppo di tunnel RA, la connessione viene negata:

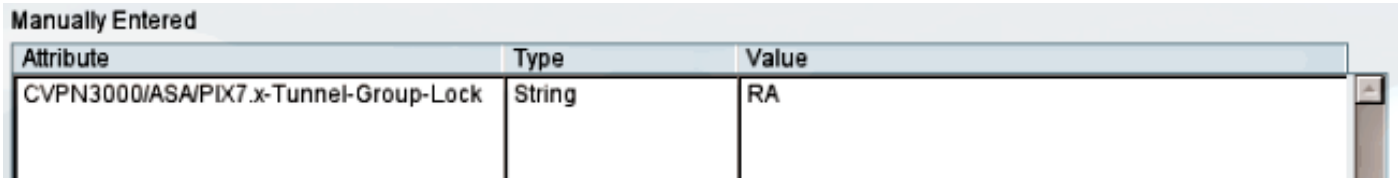



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA con attributo AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

L'attributo 3076/85 (Tunnel-Group-Lock) restituito dal server AAA ha esattamente lo stesso effetto. Può essere passata insieme all'autenticazione dell'utente o del gruppo di criteri (o all'attributo 25 della Internet Engineering Task Force (IETF)) e blocca l'utente in un gruppo di tunnel specifico.

Di seguito è riportato un esempio di profilo di autorizzazione su Cisco Access Control Server (ACS):



Quando l'attributo viene restituito da AAA, i debug RADIUS lo indicano:

```
tunnel-group RA2 general-attributes
 authentication-server-group ACS54

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 2 (0x02)
Radius: Length = 61 (0x003D)
Radius: Vector: E55D5EBF1558CA455DA46F5BF3B67354
Radius: Type = 1 (0x01) User-Name
```

```
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                  |  cisco
Radius: Type = 25 (0x19) Class
Radius: Length = 24 (0x18)
Radius: Value (String) =
43 41 43 53 3a 61 63 73 35 34 2f 31 35 38 33 33  |  CACS:acs54/15833
34 34 38 34 2f 33                                |  4484/3
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 10 (0x0A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 85 (0x55) The tunnel group that tunnel must be associated with
Radius: Length = 4 (0x04)
Radius: Value (String) =
52 41                                           |  RA
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
```

Il risultato è lo stesso quando si tenta di accedere al gruppo di tunnel RA2 mentre il gruppo è bloccato all'interno del gruppo di tunnel RA:

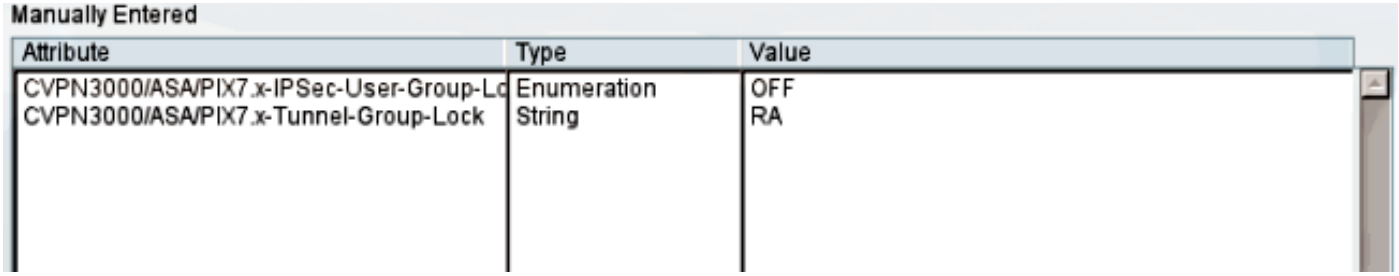
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA con attributo AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Questo attributo viene preso anche dalla directory VPN3000 ereditata dall'ASA. È ancora presente nella guida alla configurazione 8.4 (sebbene venga rimossa in una versione più recente della guida alla configurazione) e descritta come:

```
IPsec-User-Group-Lock
0 = Disabled
1 = Enabled
```

Sembra che l'attributo possa essere usato per disabilitare il blocco di gruppo, anche se è presente l'attributo Tunnel-Group-Lock. Se si tenta di restituire l'attributo impostato su 0 insieme a Tunnel-Group-Lock (si tratta ancora solo dell'autenticazione utente), l'operazione viene eseguita di seguito. Se si tenta di disattivare il blocco di gruppo restituendo il nome di un gruppo di tunnel specifico, si verifica un errore anomalo:



Debug visualizzati:

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 3 (0x03)
Radius: Length = 73 (0x0049)
Radius: Vector: 7C6260DDFC3E523CCC34AD8B828DD014
```

```
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                  |  cisco
Radius: Type = 25 (0x19) Class
Radius: Length = 24 (0x18)
Radius: Value (String) =
43 41 43 53 3a 61 63 73 35 34 2f 31 35 38 33 33  |  CACS:acs54/15833
34 34 38 34 2f 34                                |  4484/4
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 33 (0x21) Group-Lock
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 0 (0x0000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 10 (0x0A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 85 (0x55) The tunnel group that tunnel must be associated with
Radius: Length = 4 (0x04)
Radius: Value (String) =
52 41                                           |  RA
rad_procpkt: ACCEPT
```

In questo modo si ottiene lo stesso risultato (è stato applicato il blocco dei gruppi e IPSec-User-Group-Lock non è stato preso in considerazione).

```
May 17 2013 17:42:34: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

Il criterio di gruppo esterno ha restituito IPSec-User-Group-Lock=0 e ha ottenuto anche Tunnel-Group-Lock=RA per l'autenticazione utente. Tuttavia, l'utente è stato bloccato, ovvero è stato eseguito il blocco gruppo.

Per la configurazione opposta, i criteri di gruppo esterni restituiscono un nome di gruppo di tunnel specifico (Tunnel-Group-Lock) mentre tentano di disabilitare il blocco di gruppo per un utente specifico (IPSec-User-Group-Lock=0) e il blocco di gruppo è ancora applicato per tale utente.

Ciò conferma che l'attributo non è più utilizzato. Questo attributo è stato utilizzato nella vecchia serie VPN3000. L'ID bug Cisco CSCui34066 è stato aperto.

Cisco IOS Local Group-Lock per Easy VPN

L'opzione local group-lock nella configurazione del gruppo in Cisco IOS funziona in modo diverso rispetto all'appliance ASA. Sull'appliance ASA, è possibile specificare il nome del gruppo di tunnel a cui è bloccato l'utente. L'opzione group-lock di Cisco IOS (senza argomenti) consente di eseguire ulteriori verifiche e confronta il gruppo fornito con il nome utente (formato user@group) con IKEID (nome gruppo).

Per ulteriori informazioni, consultare la guida alla configurazione di Easy VPN, Cisco IOS versione 15M&T.

Di seguito è riportato un esempio:

```
aaa new-model
```

```
aaa authentication login LOGIN local
aaa authorization network LOGIN local

username cisco1@GROUP1 password 0 cisco1
username cisco2@GROUP2 password 0 cisco2

crypto isakmp client configuration group GROUP1
 key cisco
 pool POOL
 group-lock
 save-password
!
crypto isakmp client configuration group GROUP2
 key cisco
 pool POOL
 save-password

crypto isakmp profile prof1
   match identity group GROUP1
   client authentication list LOGIN
   isakmp authorization list LOGIN
   client configuration address respond
   client configuration group GROUP1
   virtual-template 1

crypto isakmp profile prof2
   match identity group GROUP2
   client authentication list LOGIN
   isakmp authorization list LOGIN
   client configuration address respond
   client configuration group GROUP2
   virtual-template 2

crypto ipsec transform-set aes esp-aes 256 esp-sha-hmac
 mode tunnel

crypto ipsec profile prof1
 set transform-set aes
 set isakmp-profile prof1

crypto ipsec profile prof2
 set transform-set aes
 set isakmp-profile prof2

interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof1

interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof2

ip local pool POOL 10.10.10.10 10.10.10.15
```

Ciò indica che la verifica del blocco del gruppo è abilitata per GROUP1. Per GROUP1, l'unico utente consentito è cisco1@GROUP1. Per GROUP2 (nessun blocco del gruppo), entrambi gli utenti sono in grado di accedere.

Per un'autenticazione corretta, utilizzare cisco1@GROUP1 con GROUP1:

```
*May 19 18:21:37.983: ISAKMP:(0): Profile prof1 assigned peer the group named GROUP1
*May 19 18:21:40.595: ISAKMP/author: Author request for group GROUP1successfully
sent to AAA
```

Per l'autenticazione, utilizzare cisco2@GROUP2 con GROUP1:

```
*May 19 18:24:10.210: ISAKMP:(1011):User Authentication in this group failed
```

Cisco IOS AAA ipsec:user-vpn-group per Easy VPN

ipsec:user-vpn-group è l'attributo RADIUS restituito dal server AAA e può essere applicato solo per l'autenticazione dell'utente (per il gruppo è stato utilizzato group-lock). Entrambe le feature sono complementari e vengono applicate in fasi diverse.

Per ulteriori informazioni, fare riferimento alla guida alla configurazione di Easy VPN, Cisco IOS release 15M&T.

Funziona in modo diverso rispetto al blocco gruppo e consente comunque di ottenere lo stesso risultato. La differenza è che l'attributo deve avere un valore specifico (come per l'ASA) e tale valore viene confrontato con il nome del gruppo ISAKMP (Internet Security Association and Key Management Protocol) (IKEID); se non corrisponde, la connessione non riesce. Di seguito viene riportato ciò che accade se si modifica l'esempio precedente per avere l'autenticazione AAA del client e disabilitare per il momento il blocco di gruppo:

```
username cisco password 0 cisco        #for testing
aaa authentication login AAA group radius

crypto isakmp client configuration group GROUP1
no group-lock
crypto isakmp client configuration group GROUP2
no group-lock

crypto isakmp profile prof1
client authentication list AAA
crypto isakmp profile prof2
client authentication list AAA
```

Si noti che per l'utente è definito l'attributo ipsec:user-vpn-group e che per il gruppo è definito group-lock.

Su ACS, ci sono due utenti, cisco1 e cisco2. Per l'utente cisco1, viene restituito questo attributo: **ipsec:user-vpn-group=GROUP1**. Per l'utente cisco2, viene restituito questo attributo: **ipsec:user-vpn-group=GROUP2**.

Quando l'utente cisco2 tenta di eseguire l'accesso con GROUP1, viene segnalato questo errore:

```
debug radius verbose
debug crypto isakmp
debug crypto isakmp aaa

*May 19 19:44:10.153: RADIUS:   Cisco AVpair       [1]   29
"ipsec:user-vpn-group=GROUP2"
*May 19 19:44:10.153: RADIUS(00000055): Received from id 1645/23
AAA/AUTHOR/IKE: Processing AV user-vpn-group
*May 19 19:44:10.154:
AAA/AUTHOR/IKE: User group GROUP2 does not match VPN group GROUP1 - access denied
```

Infatti, il valore ACS per l'utente cisco2 restituisce **ipsec:user-vpn-group=GROUP2**, che viene confrontato da Cisco IOS con GROUP1.

In questo modo, è stato raggiunto lo stesso obiettivo di Group-Lock. Come si può notare al momento, l'utente finale non deve specificare user@group come nome utente, ma può utilizzare user (senza @group).

Per group-lock, utilizzare cisco1@GROUP1, perché Cisco IOS ha rimosso l'ultima parte (dopo @) e l'ha confrontata con IKEID (nome del gruppo).

Per il parametro ipsec:user-vpn-group, è sufficiente utilizzare solo cisco1 nel client VPN Cisco, in quanto tale utente è definito nell'ACS e viene restituito il parametro ipsec:user-vpn-group specifico (in questo caso, è =GROUP1) e tale attributo viene confrontato con IKEID.

Cisco IOS AAA ipsec:user-vpn-group e Group-lock per Easy VPN

Perché non è consigliabile utilizzare entrambe le funzionalità contemporaneamente?

Èpossibile aggiungere di nuovo il blocco di gruppo:

```
crypto isakmp client configuration group GROUP1
group-lock
crypto isakmp client configuration group GROUP2
group-lock
```

Ecco il flusso:

1. L'utente VPN Cisco configura la connessione e la connessione a GROUP1.
2. La fase della modalità aggressiva ha esito positivo e Cisco IOS invia una richiesta xAuth per il nome utente e la password.
3. L'utente Cisco VPN riceve un popup e immette il nome utente cisco1@GROUP1 con la password corretta definita sull'ACS.
4. Cisco IOS esegue un controllo per verificare la presenza di group-lock: elimina il nome del gruppo specificato nel nome utente e lo confronta con IKEID. Ha successo.
5. Cisco IOS invia una richiesta AAA al server ACS (per l'utente cisco1@GROUP1).
6. ACS restituisce un valore RADIUS-Accept con **ipsec:user-vpn-group=GROUP1**.
7. Cisco IOS esegue una seconda verifica; in questo caso, confronta il gruppo fornito dall'attributo RADIUS con IKEID.

   Se si verifica un errore al passaggio 4 (blocco gruppo), l'errore viene registrato immediatamente dopo che sono state specificate le credenziali:

```
*May 19 20:14:31.678: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
*May 19 20:14:31.678: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
*May 19 20:14:31.678: ISAKMP:(1041):User Authentication in this group failed
```

Se l'operazione non riesce nel passaggio 7 (ipsec:user-vpn-group), l'errore viene restituito dopo la ricezione dell'attributo RADIUS per l'autenticazione AAA:

```
AAA/AUTHOR/IKE: User group GROUP2 does not match VPN group GROUP1 - access denied
```

IOS Webvpn Group Lock

Sull'appliance ASA, il comando Tunnel-Group-Lock può essere usato per tutti i servizi VPN di accesso remoto (IPSec, SSL, WebVPN). Per il group-lock Cisco IOS e ipsec:user-vpn-group, funziona solo per IPSec (easy VPN server). Per bloccare utenti specifici in contesti WebVPN specifici (e criteri di gruppo associati), è consigliabile utilizzare i domini di autenticazione.

Di seguito è riportato un esempio:

```
aaa new-model
aaa authentication login LIST local

username cisco password 0 cisco
username cisco1@C1 password 0 cisco
username cisco2@C2 password 0 cisco

webvpn gateway GW
 ip address 10.48.67.137 port 443
 http-redirect port 80
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.02040-k9.pkg sequence 1
 !
webvpn context C1
 ssl authenticate verify all
 !
 policy group C1
  functions file-access
  functions file-browse
  functions file-entry
  functions svc-enabled
  svc address-pool "POOL"
  svc default-domain "cisco.com"
  svc keep-client-installed
 default-group-policy C1
 aaa authentication list LIST
 aaa authentication domain @C1
 gateway GW domain C1           #accessed via https://IP/C1
 logging enable
 inservice
!
!
webvpn context C2
 ssl authenticate verify all

 url-list "L2"
  heading "Link2"
  url-text "Display2" url-value "http://2.2.2.2"

 policy group C2
  url-list "L2"
 default-group-policy C2
```

```
 aaa authentication list LIST
 aaa authentication domain @C2
 gateway GW domain C2              #accessed via https://IP/C2
 logging enable
 inservice

ip local pool POOL 7.7.7.10 7.7.7.20
```

Nell'esempio seguente vengono illustrati due contesti: C1 e C2. Ogni contesto dispone di criteri di gruppo specifici con impostazioni specifiche. C1 consente l'accesso ad AnyConnect. Il gateway è configurato per l'ascolto di entrambi i contesti: C1 e C2.

Quando l'utente cisco1 accede al contesto C1 con https://10.48.67.137/C1, il dominio di autenticazione aggiunge **C1** e esegue l'autenticazione in base al nome utente (elenco) cisco1@C1 definito localmente:


```
debug webvpn aaa
debug webvpn

*May 20 16:30:07.518: WV: validated_tp :  cert_username :  matched_ctx :
*May 20 16:30:07.518: WV-AAA: AAA authentication request sent for user: "cisco1"
*May 20 16:30:07.518: WV: ASYNC req sent
*May 20 16:30:07.518: WV-AAA: AAA Authentication Passed!
*May 20 16:30:07.518: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: C1 vw_gw: GW remote_ip:
10.61.218.146 user_name: cisco1, Authentication successful, user logged in
*May 20 16:30:07.518: WV-AAA: User "cisco1" has logged in from "10.61.218.146" to gateway "GW"
            context "C1"
```

Quando si tenta di accedere con cisco2 come nome utente mentre si accede al contesto C1 (https://10.48.67.137/C1), viene segnalato questo errore:

```
*May 20 16:33:56.930: WV: validated_tp :  cert_username :  matched_ctx :
*May 20 16:33:56.930: WV-AAA: AAA authentication request sent for user: "cisco2"
*May 20 16:33:56.930: WV: ASYNC req sent
*May 20 16:33:58.930: WV-AAA: AAA Authentication Failed!
*May 20 16:33:58.930: %SSLVPN-5-LOGIN_AUTH_REJECTED: vw_ctx: C1 vw_gw: GW
remote_ip: 10.61.218.146 user_name: cisco2, Failed to authenticate user credentials
```

Ciò è dovuto al fatto che non è stato definito alcun cisco2@C1 utente. l'utente cisco non è in grado di accedere ad alcun contesto.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione di Easy VPN, Cisco IOS release 15M&T
- Guida alla configurazione di Cisco ASA VPN CLI, 9.1
- Documentazione e supporto tecnico – Cisco Systems