ASA 및 Cisco IOS Group-lock 기능, AAA 특성 및 WebVPN 컨피그레이션 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 및 Cisco IOS®의 그룹 잠금 기능에 대해 설명하고 다양한 AAA(Authentication, Authorization, and Accounting) 특성에 대한 동작을 소개합니다. Cisco IOS의 경우 그룹 잠금과 사용자-vpn-그룹 간의 차이점에 대해 두 보완 기능을 동시에 사용하는 예와 함께 설명합니다. 인증 도메인과 함께 Cisco IOS WebVPN 예도 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- ASA CLI 컨피그레이션 및 SSL(Secure Sockets Layer) VPN 컨피그레이션
- ASA 및 Cisco IOS의 원격 액세스 VPN 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- ASA 소프트웨어, 버전 8.4 이상
- Cisco IOS, 버전 15.1 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

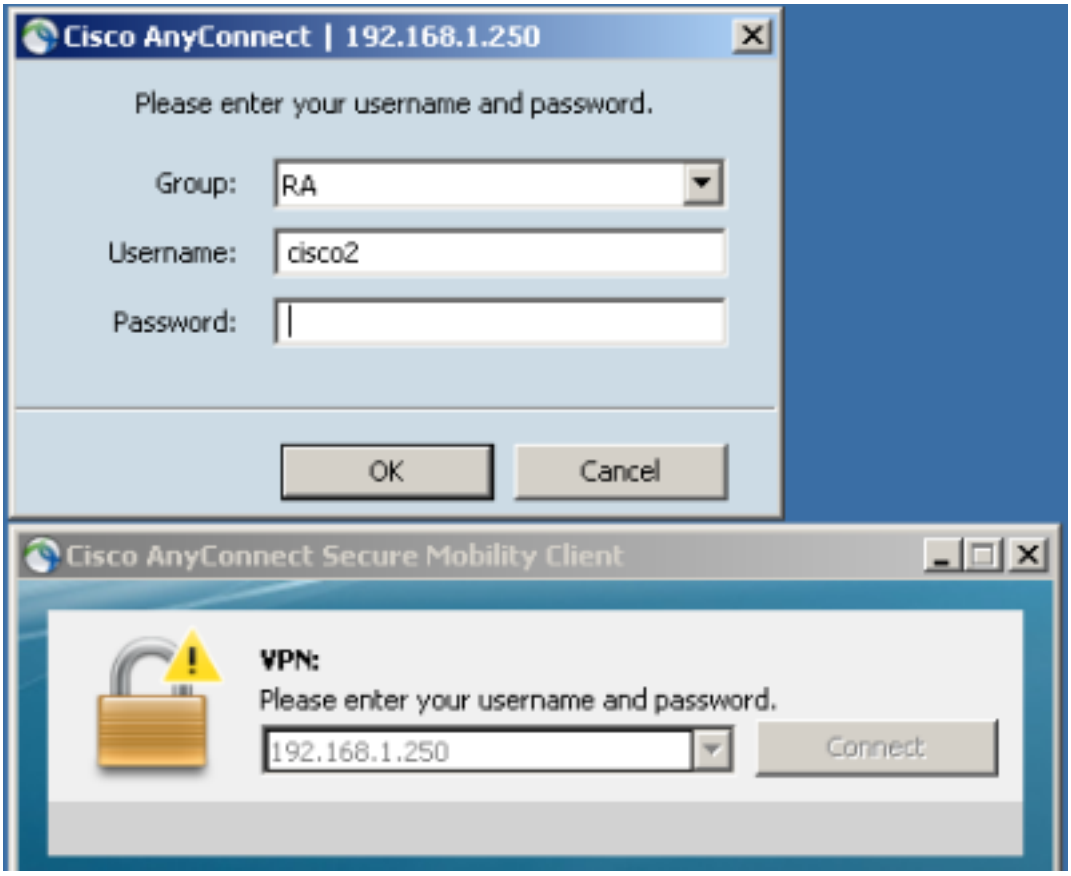
ASA 로컬 그룹 잠금

사용자 또는 그룹 정책에서 이 특성을 정의할 수 있습니다. 다음은 로컬 사용자 특성의 예입니다.

```
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
```

cisco 사용자는 RA 터널 그룹만 사용할 수 있으며, cisco2 사용자는 RA2 터널 그룹만 사용할 수 있습니다.

cisco2 사용자가 RA 터널 그룹을 선택하면 연결이 거부됩니다.

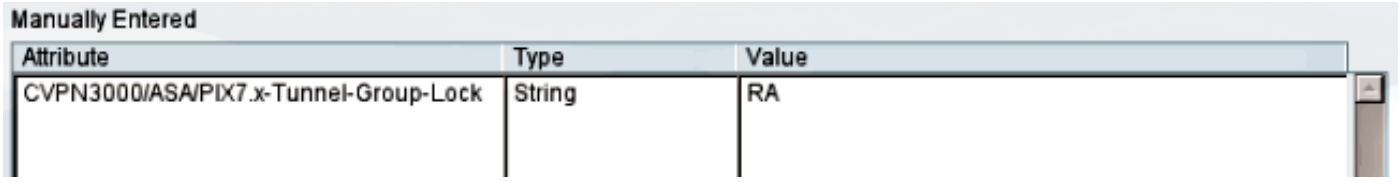



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA with AAA Attribute VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

AAA 서버에서 반환되는 특성 3076/85(Tunnel-Group-Lock)는 정확히 동일합니다. 사용자 또는 정책 그룹(또는 IETF(Internet Engineering Task Force) 특성 25) 인증과 함께 전달되고 특정 터널 그룹에서 사용자를 잠글 수 있습니다.

다음은 Cisco ACS(Access Control Server)의 인증 프로파일의 예입니다.



AAA에서 특성을 반환하면 RADIUS 디버그가 이를 나타냅니다.

```
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
```

RA 터널 그룹 내에서 그룹을 잠그는 동안 RA2 터널 그룹에 액세스하려고 할 때 결과는 동일합니다.

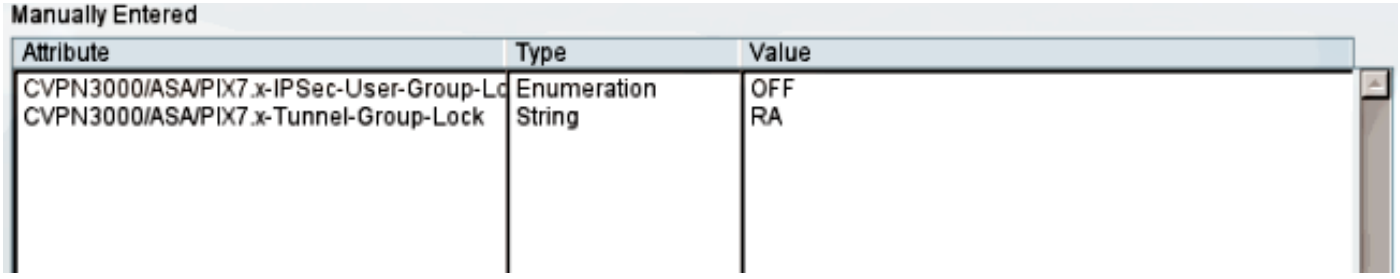
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA with AAA attribute VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

이 특성은 ASA에서 상속된 VPN3000 디렉토리에서도 가져옵니다. 8.4 컨피그레이션 가이드(최신 컨피그레이션 가이드에서 제거되지만) 및 다음과 같이 설명됩니다.

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

Tunnel-Group-Lock 특성이 있는 경우에도 그룹 잠금을 비활성화하기 위해 특성을 사용할 수 있습니다. Tunnel-Group-Lock(Tunnel-Group-Lock)과 함께 0으로 설정된 특성을 반환하려고 하면(여전히 사용자 인증에만 해당) 다음과 같은 결과가 발생합니다. 특정 터널 그룹 이름을 반환하는 동안 그룹 잠금을 비활성화하려고 하면 이상하게 보입니다.



디버깅 표시:

```
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
```

이렇게 하면 동일한 결과가 발생합니다(그룹 잠금이 적용되었으며 IPSec-User-Group-Lock이 고려되지 않음).

```
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
```

외부 그룹 정책에서 IPSec-User-Group-Lock=0을 반환하고 사용자 인증을 위해 Tunnel-Group-Lock=RA를 가져왔습니다. 여전히 사용자가 잠겼으므로 그룹 잠금이 수행되었음을 의미합니다.

반대 컨피그레이션의 경우 외부 그룹 정책은 특정 사용자에 대해 그룹 잠금을 비활성화하는 동안 특정 터널 그룹 이름(Tunnel-Group-Lock)을 반환하며(IPSec-User-Group-Lock=0), 그룹 잠금은 해당 사용자에 대해 계속 시행되고 있습니다.

그러면 해당 속성이 더 이상 사용되지 않음을 확인합니다. 이 특성은 이전 VPN3000 시리즈에 사용되었습니다. Cisco 버그 ID CSCui34066이 열렸습니다.

Cisco IOS Local Group-lock for Easy VPN

Cisco IOS의 그룹 컨피그레이션 아래의 로컬 그룹 잠금 옵션은 ASA와 다르게 작동합니다. ASA에서 사용자가 잠길 터널 그룹 이름을 지정합니다. Cisco IOS group-lock 옵션(인수 없음)을 사용하면 추가 확인을 수행할 수 있으며 사용자 이름(형식 user@group)과 IKEID(그룹 이름)를 사용하여 제공된 그룹을 비교합니다.

자세한 내용은 Easy VPN Configuration Guide, Cisco IOS Release 15M&T를 참조하십시오.

예를 들면 다음과 같습니다.

```
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
```

이것은 그룹 잠금 확인이 GROUP1에 대해 활성화되었음을 보여줍니다. GROUP1의 경우, 허용된 사용자는 cisco1@GROUP1뿐입니다. GROUP2(그룹 잠금 없음)의 경우 두 사용자 모두 로그인할 수 있습니다.

인증에 성공하려면 cisco1@GROUP1을 GROUP1과 함께 사용하십시오.

```
*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
```

인증을 위해 GROUP1과 함께 cisco2@GROUP2을 사용합니다.

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

Cisco IOS AAA ipsec: Easy VPN용 user-vpn-group

ipsec:**user-vpn-group**은 AAA 서버에서 반환한 RADIUS 특성이며 사용자 인증에만 적용할 수 있습니다(그룹에 그룹 잠금이 사용됨). 두 기능 모두 상호 보완적이며 서로 다른 단계에 적용됩니다.

자세한 내용은 Easy VPN Configuration Guide, Cisco IOS Release 15M&T를 참조하십시오.

그룹 잠금과 다르게 작동하며 동일한 결과를 얻을 수 있습니다. 차이점은 특성에 특정 값(예: ASA의 경우)이 있어야 하며 해당 특정 값을 ISAKMP(Internet Security Association and Key Management Protocol) IKEID(Group Name)와 비교한다는 것입니다. 일치하지 않으면 연결이 실패합니다. 다음은 클라이언트 AAA 인증을 위해 이전 예를 변경하고 지금은 그룹 잠금을 비활성화하는 경우 발생하는 작업입니다.

```
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
```

사용자에 대해 ipsec:user-vpn-group 특성이 정의되고 그룹에 대해 group-lock이 정의됩니다.

ACS에는 cisco1과 cisco2라는 두 명의 사용자가 있습니다. cisco1 사용자의 경우 이 속성이 반환됩니다. **ipsec:user-vpn-group=GROUP1**. cisco2 사용자의 경우 이 속성이 반환됩니다. **ipsec:user-vpn-group=GROUP2**.

cisco2 사용자가 GROUP1을 사용하여 로그인을 시도하면 다음 오류가 보고됩니다.

```
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
```

이는 cisco2 사용자의 ACS가 ipsec:**user-vpn-group=GROUP2**를 반환하기 때문입니다. 이는 Cisco IOS와 GROUP1의 비교 결과입니다.

이렇게 하면 그룹 잠금에 대한 동일한 목표가 달성됩니다. 이제 최종 사용자가 user@group을 사용자 이름으로 제공할 필요는 없지만 @group 없이 사용자를 사용할 수 있습니다.

Cisco IOS가 마지막 부품(@ 이후)을 제거하고 IKEID(그룹 이름)와 비교했으므로 그룹 잠금에는 cisco1@GROUP1을 사용해야 합니다.

ipsec:user-vpn-group의 경우 해당 사용자가 ACS에 정의되어 있고 특정 ipsec:user-vpn-group이 반환되고(이 경우 사용자-vpn-group = GROUP1) 해당 특성이 IKEID와 비교되므로 Cisco VPN 클라이

언트에서 cisco1만 사용할 수 있습니다.

Cisco IOS AAA ipsec: user-vpn-group 및 Group-lock for Easy VPN

두 기능을 동시에 사용하지 않는 이유는 무엇입니까?

그룹 잠금을 다시 추가할 수 있습니다.

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

플로우는 다음과 같습니다.

1. Cisco VPN 사용자는 GROUP1 연결을 구성하고 연결합니다.
2. 적극적인 모드 단계가 성공했으며 Cisco IOS는 사용자 이름 및 비밀번호에 대해 xAuth 요청을 전송합니다.
3. Cisco VPN 사용자는 팝업을 수신하고 ACS에 정의된 올바른 비밀번호로 cisco1@GROUP1 사용자 이름을 입력합니다.
4. Cisco IOS는 그룹 잠금을 확인합니다. 사용자 이름에 제공된 그룹 이름을 제거하고 IKEID와 비교합니다. 성공적이다.
5. Cisco IOS는 ACS 서버에 AAA 요청을 보냅니다(사용자 cisco1@GROUP1).

6. ACS는 ipsec**:user-vpn-group=GROUP1을** 사용하여 RADIUS**-Accept를 반환합니다**.

7. Cisco IOS는 두 번째 확인을 수행합니다. 이번에는 RADIUS 특성에서 제공한 그룹을 IKEID와 비교합니다.

   4단계(그룹 잠금)에서 오류가 발생하면 자격 증명을 제공한 후 즉시 오류가 기록됩니다.

   ```
   *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
   ```

   7단계(ipsec:user-vpn-group)에서 장애가 발생하면 AAA 인증을 위한 RADIUS 특성을 수신한 후 오류가 반환됩니다.

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

IOS Webvpn 그룹 잠금

ASA에서 Tunnel-Group-Lock을 모든 원격 액세스 VPN 서비스(IPSec, SSL, WebVPN)에 사용할 수 있습니다. Cisco IOS 그룹 잠금 및 ipsec:user-vpn-group의 경우 IPSec(easy VPN 서버)에서만 작동합니다. 특정 WebVPN 컨텍스트(및 연결된 그룹 정책)에서 특정 사용자를 그룹 잠그려면 인증 도메인을 사용해야 합니다.

예를 들면 다음과 같습니다.

```
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
```

다음 예에서는 두 개의 컨텍스트가 있습니다. C1 및 C2. 각 컨텍스트에는 특정 설정을 가진 고유한 그룹 정책이 있습니다. C1에서는 AnyConnect 액세스를 허용합니다. 게이트웨이는 두 컨텍스트를 모두 수신하도록 구성됩니다. C1 및 C2.

cisco1 사용자가 https://10.48.67.137/C1을 사용하여 C1 컨텍스트에 액세스하면 인증 도메인은 **C1**을 추가하고 로컬로 정의된(목록 LIST) cisco1@C1 사용자 이름에 대해 인증합니다.


```
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"
```

C1 컨텍스트(https://10.48.67.137/C1)에 액세스하는 동안 사용자 이름으로 cisco2를 사용하여 로그인하려고 하면 이 오류가 보고됩니다.

```
*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
```

이는 정의된 cisco2@C1 사용자가 없기 때문입니다. cisco 사용자는 어떤 컨텍스트에도 로그인할 수 없습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Easy VPN 컨피그레이션 가이드, Cisco IOS 릴리스 15M&T
- Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1
- 기술 지원 및 문서 – Cisco Systems