ASA y características del Grupo-bloqueo del Cisco IOS y atributos AAA y ejemplo de configuración del WebVPN

Contenido

Introducción

Este artículo describe las características grupo-que bloquean en el dispositivo de seguridad adaptante de Cisco (ASA) y en el ® del Cisco IOS y presenta el comportamiento para diversos atributos del Authentication, Authorization, and Accounting (AAA). Para el Cisco IOS, la diferencia entre el grupo-bloqueo y los usuario-VPN-grupos se explica junto con un ejemplo que utilice ambas características complementarias al mismo tiempo. Hay también un ejemplo del WebVPN del Cisco IOS con los dominios de la autenticación.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del baisc de estos temas:

- Configuración CLI ASA y configuración VPN de Secure Sockets Layer (SSL)

- Configuración del VPN de acceso remoto en el ASA y el Cisco IOS

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software ASA, versión 8.4 y posterior
- Cisco IOS, versión 15.1 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configuraciones

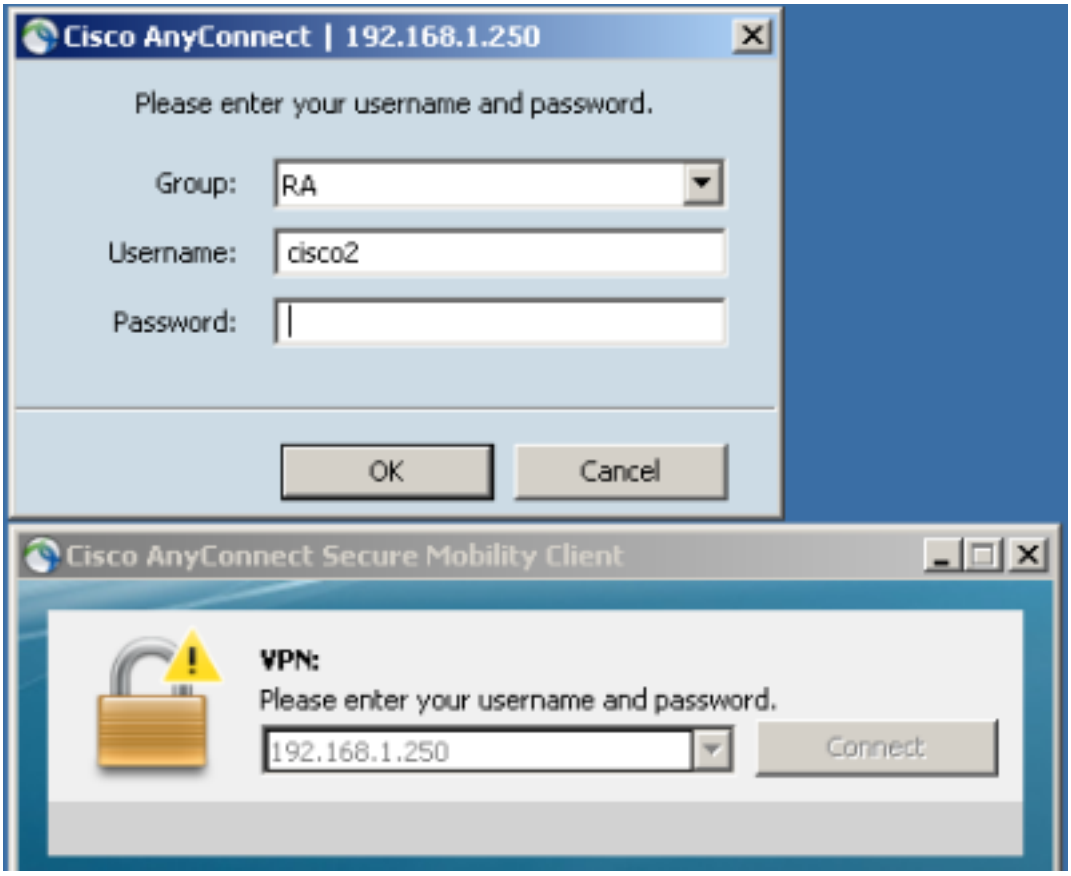
Grupo-bloqueo del Local ASA

Usted puede definir este atributo bajo el usuario o grupo-directiva. Aquí está un ejemplo para el atributo del usuario local.

```
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
```

El usuario de Cisco puede utilizar solamente al grupo de túnel RA, y el usuario cisco2 puede utilizar solamente el grupo de túnel RA2.

Si el usuario cisco2 elige al grupo de túnel RA, después se niega la conexión:

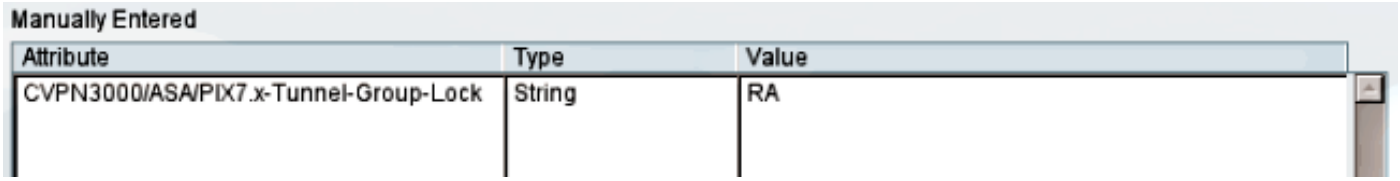



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

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

Atribuya 3076/85 (Túnel-Grupo-bloqueo) que sea vuelto por el servidor de AAA haga exactamente lo mismo. Puede ser pasado junto con el usuario o la autenticación del grupo de políticas (o el atributo 25 de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF)) y bloquea al usuario en un grupo de túnel específico.

Aquí está un perfil de la autorización del ejemplo en el Access Control Server de Cisco (ACS):



Cuando el atributo es vuelto por el AAA, los debugs RADIUS lo indican:

```
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
```

El resultado es lo mismo cuando usted intenta acceder el grupo de túnel RA2 mientras que es grupo-bloqueado dentro del grupo de túnel RA:

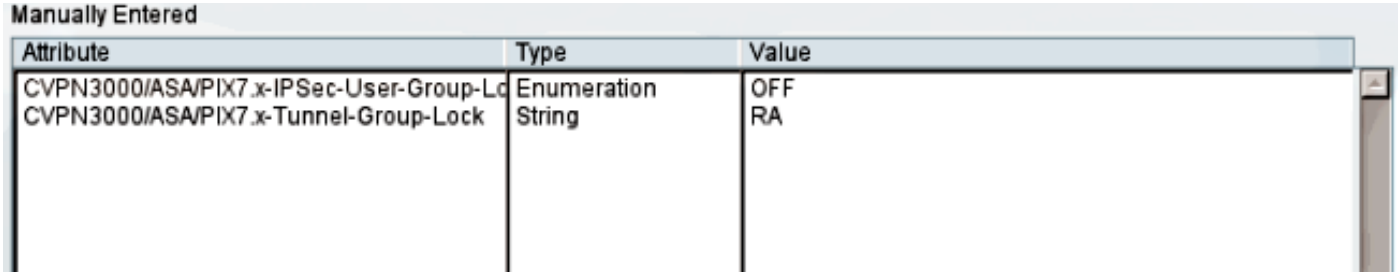
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

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

Este atributo también se toma del directorio VPN3000 heredado por el ASA. Está todavía presente en la guía de configuración 8.4 (aunque se quita en una versión más reciente de la guía de configuración) y descrito como:

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

Aparece que el atributo se podría utilizar para inhabilitar grupo-bloquear, incluso si el atributo del Túnel-Grupo-bloqueo está presente. Si usted intenta volver que atributo fijado a 0 junto con el Túnel-Grupo-bloqueo (ésta sigue siendo apenas autenticación de usuario), aquí es qué sucede. Parece extraño cuando usted intenta inhabilitar grupo-bloquear mientras que vuelve un nombre de grupo de túnel específico:



Demostración de los debugs:

```
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
```

Esto rinde el mismo resultado (se ha aplicado el bloquear del grupo, y el IPSec-Usuario-Grupo-bloqueo no se ha tomado en la consideración).

```
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 <RA>
```

La grupo-directiva externa volvió IPSec-User-Group-Lock=0 y también consiguió Tunnel-Group-Lock=RA para la autenticación de usuario. No obstante, el usuario ha estado bloqueado, así que significa que se ha realizado el bloquear del grupo.

Para la configuración opuesta, la grupo-directiva del externo vuelve un nombre de grupo de túnel específico (Túnel-Grupo-bloqueo) mientras que intenta inhabilitar grupo-bloquear para un usuario específico (IPSec-User-Group-Lock=0), y grupo-bloqueando todavía se ha aplicado para ese usuario.

Esto confirma que el atributo no está utilizado más. Ese atributo fue utilizado en las viejas VPN3000 Series. Se ha abierto el Id. de bug Cisco CSCui34066.

Grupo-bloqueo local del Cisco IOS para el VPN fácil

La opción local del grupo-bloqueo bajo configuración de grupo en los trabajos del Cisco IOS diferentemente que en el ASA. En el ASA, usted especifica el nombre de grupo de túnel al cual el usuario es bloqueado. Los permisos verificación adicional de la opción del grupo-bloqueo del Cisco IOS (no hay argumentos) y comparan al grupo proporcionado el nombre de usuario (formato user@group) con IKEID (nombre del grupo).

Para más información, refiera a la guía de configuración VPN fácil, el Cisco IOS Release 15M&T.

Aquí tiene un ejemplo:

```
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
```

Esto muestra que eso grupo-bloquear la verificación está habilitada para el GROUP1. Para el GROUP1, el único usuario permitido es cisco1@GROUP1. Para el GROUP2 (ningún grupo-bloqueo), ambos usuarios pueden iniciar sesión.

Para la autenticación satisfactoria, utilice cisco1@GROUP1 con el 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
```

Para la autenticación, utilice cisco2@GROUP2 con el GROUP1:

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

IPSec del Cisco IOS AAA: usuario-VPN-grupo para el VPN fácil

El IPSec: el usuario-VPN-grupo es el atributo de RADIUS vuelto por el servidor de AAA, y puede ser solicitado solamente la autenticación de usuario (el grupo-bloqueo fue utilizado para el grupo). Ambas características son complementarias, y son aplicadas en diversas etapas.

Para más información, refiera a la guía de configuración VPN fácil, el Cisco IOS Release 15M&T.

Trabaja diferentemente que el grupo-bloqueo y todavía permite que usted alcance el mismo resultado. La diferencia es que el atributo debe tener un valor específico (como para el ASA) y que el valor específico está comparado con el nombre del grupo del Internet Security Association and Key Management Protocol (ISAKMP) (IKEID); si no hace juego, después la conexión falla. Aquí es qué sucede si usted cambia el ejemplo anterior para tener autenticación AAA del cliente y inhabilitar el grupo-bloqueo por ahora:

```
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
```

Note que el IPSec: el atributo del usuario-VPN-grupo se define para el usuario y el grupo-bloqueo se define para el grupo.

En el ACS, hay dos usuarios, cisco1 y cisco2. Para el usuario cisco1, se vuelve este atributo: **ipsec:user-vpn-group=GROUP1**. Para el usuario cisco2, se vuelve este atributo: **ipsec:user-vpn-group=GROUP2**.

Cuando el usuario cisco2 intenta iniciar sesión con el GROUP1, este error está señalado:

```
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
```

Esto es porque el ACS para el usuario cisco2 vuelve **ipsec:user-vpn-group=GROUP2**, que es comparado por el Cisco IOS al GROUP1.

Esta manera, la misma meta se ha alcanzado en cuanto al grupo-bloqueo. Usted puede ver que ahora, el usuario final no necesita proporcionar user@group como el nombre de usuario, pero puede utilizar al usuario (sin el @group).

Para el grupo-bloqueo, cisco1@GROUP1 debe ser utilizado, porque el Cisco IOS eliminó la parte más reciente (después de @) y la comparó con IKEID (nombre del grupo).

Para el IPSec: usuario-VPN-grupo, es suficiente utilizar solamente cisco1 en el Cliente Cisco VPN, porque definen a ese usuario en el ACS y el IPSec específico: vuelven al usuario-VPN-

grupo (en este caso, es =GROUP1) y ese atributo se compara contra IKEID.

IPSec del Cisco IOS AAA: usuario-VPN-grupo y Grupo-bloqueo para el VPN fácil

¿Por qué no debe usted utilizar ambas características al mismo tiempo?

Usted puede agregar el grupo-bloqueo otra vez:

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

Aquí está el flujo:

1. El usuario del Cisco VPN configura la conexión del GROUP1 y conecta.
2. La fase del modo agresivo es acertada, y el Cisco IOS envía un pedido del Xauth el nombre de usuario y contraseña.
3. El usuario del Cisco VPN recibe un popup, y ingresa el nombre de usuario de cisco1@GROUP1 con la contraseña correcta definida en el ACS.
4. El Cisco IOS realiza una comprobación para el grupo-bloqueo: elimina el nombre del grupo proporcionado en el nombre de usuario y lo compara con IKEID. Es acertado.
5. El Cisco IOS envía una petición AAA al servidor ACS (para el usuario cisco1@GROUP1).

6. El ACS vuelve un RADIUS-validar con **ipsec:user-vpn-group=GROUP1**.

7. El Cisco IOS realiza una segunda verificación; esta vez, compara al grupo proporcionado por el atributo de RADIUS con IKEID.

   Cuando falla en el paso 4 (bloqueo del grupo), se registra el error inmediatamente después que proporciona las credenciales:

   ```
   *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
   ```

   Cuando falla en el paso 7 (IPSec: vuelven al usuario-VPN-grupo), el error después de que reciba el atributo de RADIUS para la autenticación AAA:

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

Bloqueo del grupo IOS Webvpn

En el ASA, el Túnel-Grupo-bloqueo se puede utilizar para todos los servicios del VPN de acceso remoto (IPSec, SSL, WebVPN). Para el grupo-bloqueo del Cisco IOS y el IPSec: usuario-VPN-grupo, trabaja solamente para el IPSec (Easy VPN Server). Para los usuarios específicos del grupo-bloqueo en los contextos específicos del WebVPN (y las grupo-directivas asociadas), los dominios de la autenticación deben ser utilizados.

Aquí tiene un ejemplo:

```
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
```

En el próximo ejemplo, hay dos contextos: C1 y C2. Cada contexto tiene su propia grupo-directiva con las configuraciones específicas. El c1 permite el acceso de AnyConnect. El gataway se configura para escuchar ambos contextos: C1 y C2.

Cuando los accesos del usuario cisco1 el contexto del c1 con https://10.48.67.137/C1, el dominio de la autenticación agregan el **c1** y lo autentican contra (LISTA de la lista) el nombre de usuario localmente definido de cisco1@C1:


```
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"
```

Cuando usted intenta iniciar sesión con cisco2 como nombre de usuario mientras que usted accede el contexto del c1 (https://10.48.67.137/C1), este error está señalado:

```
*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
```

Esto es porque no hay cisco2@C1 definido por el usario. el usuario de Cisco no puede iniciar sesión a ningún contexto.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración VPN fácil, Cisco IOS Release 15M&T
- Guía de configuración CLI de la serie VPN de Cisco ASA, 9.1

- Soporte Técnico y Documentación - Cisco Systems