ASA en Cisco IOS groepsblokkeringsfuncties en AAA-kenmerken en Configuratievoorbeeld van WebVPN

Inhoud

Inleiding

Dit artikel beschrijft de groepsvergrendelingsfuncties op de Cisco adaptieve security applicatie (ASA) en in Cisco IOS® en presenteert het gedrag voor verschillende verificatie-, autorisatie- en accounting (AAA) eigenschappen. Voor Cisco IOS wordt het verschil tussen het groepsslot en de gebruikersVPN-groepen uitgelegd in combinatie met een voorbeeld dat beide complementaire functies tegelijkertijd gebruikt. Er is ook een Cisco IOS WebVPN-voorbeeld met verificatiedomeinen.

Voorwaarden

Vereisten

Cisco raadt u aan om basiskennis van deze onderwerpen te hebben:

- ASA CLI-configuratie en Secure Socket Layer (SSL) VPN-configuratie

- VPN-configuratie voor externe toegang op ASA en Cisco IOS

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- ASA-software, versie 8.4 en hoger
- Cisco IOS, versie 15.1 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configuraties

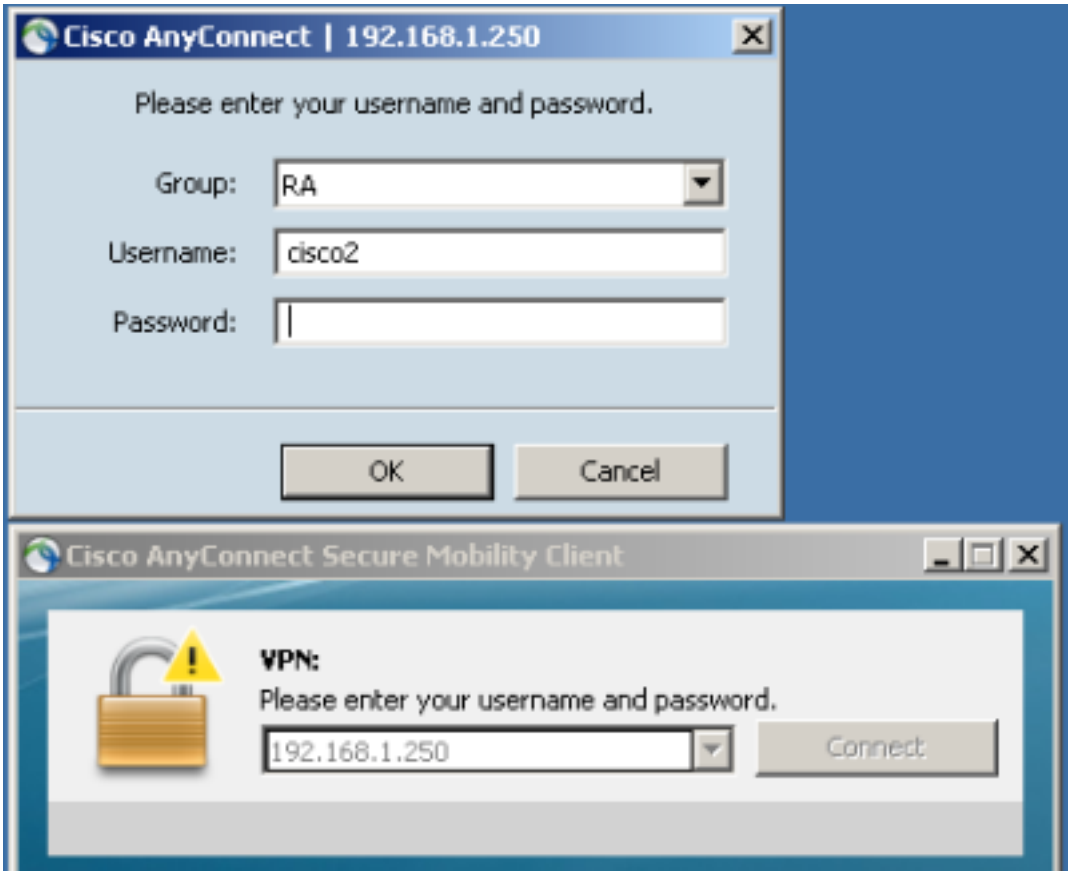
ASA lokaal groepsslot

U kunt deze eigenschap definiëren onder de gebruiker of het groepsbeleid. Hier is een voorbeeld voor de lokale gebruikerseigenschap.

```
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
```

De cisco-gebruiker kan alleen de RA tunnelgroep gebruiken en de cisco2-gebruiker kan alleen de RA2 tunnelgroep gebruiken.

Als de cisco2-gebruiker de RA tunnelgroep kiest, wordt de verbinding ontkend:

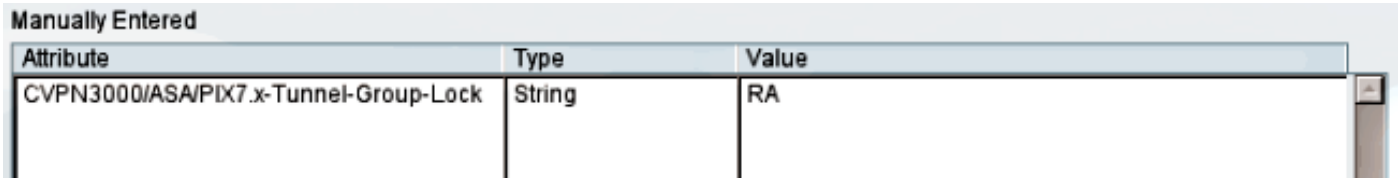



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA met AAA-kenmerk VPN3000/ASA/PIX7.x-Tunnel-groep-slot

Kenmerk 3076/85 (Tunnel-Group-Lock) dat door de AAA-server wordt teruggegeven, doet precies hetzelfde. Het kan samen met de gebruiker of de beleidsgroep (of de Internet Engineering Task Force (IETF) attributie 25) authenticatie worden doorgegeven en de gebruiker wordt vastgezet in een specifieke tunnelgroep.

Hier is een voorbeeldvergunningprofiel op de Cisco Access Control Server (ACS):



Wanneer de eigenschap door AAA wordt teruggegeven, wijzen de RADIUS-kenmerken op:

```
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
```

Het resultaat is hetzelfde wanneer u probeert toegang te krijgen tot de RA2-tunnelgroep terwijl de groep gesloten is binnen de RA-tunnelgroep:

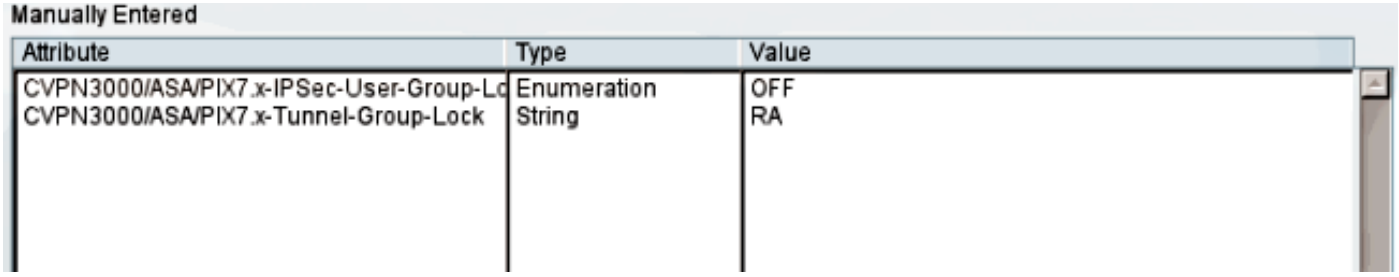
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA met AAA eigenschap VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Deze eigenschap wordt ook afgeleid uit de VPN3000 folder die door de ASA werd geërfd. Het is nog steeds aanwezig in de 8.4 configuratiehandleiding (hoewel het in een nieuwere versie van de configuratiehandleiding is verwijderd) en wordt beschreven als:

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

Het lijkt erop dat de eigenschap kan worden gebruikt om groepsblokkering uit te schakelen, zelfs als de eigenschap Tunnel-Groep-Lock aanwezig is. Als u probeert om die eigenschap terug te geven die op 0 is ingesteld samen met het Tunnel-Groeeks-Slot (dit is nog steeds slechts gebruikersauthenticatie), is dit wat er gebeurt. Het ziet vreemd uit als u groepsblokkering probeert uit te schakelen terwijl u een specifieke tunnelgroepnaam teruggeeft:



Debugs toont:

```
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
```

Dit levert hetzelfde resultaat op (er is sprake van groepsvergrendeling en het IPSec-User-Group-Lock is niet in overweging genomen).

```
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
```

Het externe groepsbeleid gaf IPSec-User-Group-Lock=0 terug en kreeg ook Tunnel-Group-Lock=RA voor gebruikersverificatie. Maar toch is de gebruiker vergrendeld, wat betekent dat het groepsvergrendelen is uitgevoerd.

Voor de tegenovergestelde configuratie, keert het externe groepsbeleid een specifieke tunnel-groepsnaam (Tunnel-Groep-Lock) terug terwijl het probeert om groepssluitingen voor een specifieke gebruiker uit te schakelen (IPSec-User-Group-Lock=0), en de groepsblokkering is voor die gebruiker nog steeds afgedwongen.

Dit bevestigt dat de eigenschap niet meer wordt gebruikt. Die eigenschap werd gebruikt in de oude VPN3000-serie. Cisco bug-ID CSCui34066 is geopend.

Cisco IOS lokale groepsvergrendeling voor Makkelijk VPN

De lokale optie van het groepsslot onder de groepsconfiguratie in Cisco IOS werkt anders dan op de ASA. In de ASA, specificeert u de tunnel-groepsnaam waaraan de gebruiker is vergrendeld. De Cisco IOS-groepsvergrendelingsoptie (er zijn geen argumenten) maakt extra verificatie mogelijk en vergelijkt de groep met de gebruikersnaam (formaat user@group) met IKEID (groepsnaam).

Raadpleeg de Makkelijk VPN-configuratiegids, Cisco IOS release 15M&T voor meer informatie.

Hierna volgt een voorbeeld:

```
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
```

Dit toont aan dat de groepsvergrendelende verificatie voor GROUP1 is ingeschakeld. Voor GROUP1 is de enige toegestane gebruiker cisco1@GROUP1. Voor GROUP2 (geen groepsslot) kunnen beide gebruikers inloggen.

Voor succesvolle authenticatie, gebruik cisco1@GROUP1 met 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
```

Gebruik cisco2@GROUP2 voor authenticatie met GROUP1:

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

Cisco IOS AAA-sec:gebruiker-VPN-groep voor Easy VPN

De **ipsec:user-vpn-group** is de RADIUS-eigenschap die wordt teruggegeven door de AAA-server en kan alleen worden toegepast op gebruikersverificatie (group-lock werd gebruikt voor de groep). Beide functies zijn complementair en worden in verschillende fasen toegepast.

Raadpleeg de Makkelijk VPN-configuratiegids, Cisco IOS release 15M&T voor meer informatie.

Het werkt anders dan het groepsslot en laat je nog steeds hetzelfde resultaat bereiken. Het verschil is dat de eigenschap een specifieke waarde moet hebben (zoals voor de ASA) en dat de specifieke waarde wordt vergeleken met de groepsnaam van de ISAKMP (Internet Security Association and Key Management Protocol); Als de verbinding niet overeenkomt, mislukt de verbinding. Dit is wat er gebeurt als u het vorige voorbeeld wijzigt om client-AAA verificatie te hebben en groepsblokkering voor nu uit te schakelen:

```
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
```

Merk op dat de ipsec:user-vpn-group eigenschap is gedefinieerd voor de gebruiker en het groepsslot is gedefinieerd voor de groep.

Op ACS zijn er twee gebruikers, cisco1 en cisco2. Voor de cisco1 gebruiker, wordt deze eigenschap teruggegeven: **ipsec:user-vpn-group=GROUP1**. Voor de cisco2 gebruiker wordt deze eigenschap teruggegeven: **ipsec:user-vpn-group=GROUP2**.

Wanneer de cisco2-gebruiker probeert in te loggen met GROUP1, wordt deze fout gemeld:

```
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
```

Dit komt doordat ACS voor de cisco2 gebruiker **ipsec:user-vpn-group=GROUP2** teruggeeft, wat

door Cisco IOS wordt vergeleken met GROUP1.

Op deze manier is hetzelfde doel bereikt als voor het groepsslot. U kunt zien dat de eindgebruiker op dit moment user@group niet hoeft op te geven als de gebruikersnaam, maar de gebruiker kan gebruiken (zonder de @group).

Voor groepsvergrendeling moet cisco1@GROUP1 worden gebruikt, omdat Cisco IOS het laatste onderdeel (na @) heeft verwijderd en het heeft vergeleken met IKEID (groepsnaam).

Voor de ipsec:user-vpn-group is het voldoende om alleen cisco1 in de Cisco VPN-client te gebruiken, omdat die gebruiker op de ACS is gedefinieerd en de specifieke ipsec:user-vpn-group wordt teruggegeven (in dit geval is het =GROUP1) en die eigenschap wordt vergeleken met IKEID.

Cisco IOS AAA-sec:gebruiker-VPN-groep en groepsvergrendeling voor Makkelijk VPN

Waarom zou u beide functies niet tegelijkertijd gebruiken?

U kunt groepsvergrendeling opnieuw toevoegen:

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

Hier is de stroom:

1. De gebruiker van Cisco VPN vormt de verbinding GROUP1 en verbindt.
2. De agressieve mode fase is succesvol, en Cisco IOS verstuurt een xAuth verzoek om de gebruikersnaam en het wachtwoord.
3. De gebruiker van Cisco VPN ontvangt een pop-up, en gaat de gebruikersnaam van cisco1@GROUP1 in met het juiste wachtwoord dat op ACS wordt bepaald.
4. Cisco IOS voert een controle uit voor de groepsvergrendeling: het schrapt de in de gebruikersnaam opgegeven groepsnaam en vergelijkt het met IKEID. Het is een succes.
5. Cisco IOS stuurt een AAA-verzoek naar de ACS-server (voor gebruiker cisco1@GROUP1).

6. ACS retourneert een RADIUS-Accept met **ipsec:user-VPN-group=GROUP1**.

7. Cisco IOS voert een tweede verificatie uit; deze keer wordt de door de RADIUS-eigenschap geleverde groep vergeleken met IKEID.

   Wanneer het bij Stap 4 (groepsvergrendeling) faalt, wordt de fout direct na het bieden van aanmeldingsgegevens vastgelegd:

```
*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
```

Wanneer het in Stap 7 (ipsec:user-vpn-group) faalt, wordt de fout teruggegeven nadat het de RADIUS-eigenschap voor AAA-verificatie ontvangt:

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

IOS WebVPN-groepsslot

Op de ASA, kan het Tunnel-Groep-Lock voor alle verre toegang de diensten van VPN (IPSec, SSL, WebVPN) worden gebruikt. Voor het Cisco IOS groepsslot en de ipsec:user-VPN-group werkt het alleen voor IPSec (makkelijke VPN-server). Om specifieke gebruikers in specifieke WebVPN-contexten (en op groep aangesloten groepsbeleid) te groeperen-slot moeten de authentificatiedomeinen worden gebruikt.

Hierna volgt een voorbeeld:

```
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
```

In het volgende voorbeeld zijn er twee contexten: C1 en C2. Elke context heeft zijn eigen groepsbeleid met specifieke instellingen. C1 maakt toegang tot AnyConnect mogelijk. De afvoerslang is zo geconfigureerd dat hij naar beide contexten luistert: C1 en C2.

Wanneer de cisco1-gebruiker de C1-context met https://10.48.67.137/C1 benadert, voegt het authenticatiedomein **C1** toe en authenticeert het lokaal gedefinieerde (lijst LIST) cisco1@C1 gebruikersnaam:


```
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"
```

Wanneer u probeert in te loggen met cisco2 als gebruikersnaam terwijl u tot de C1 context (https://10.48.67.137/C1) toegang hebt, wordt deze mislukking gemeld:

```
*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
```

Dit komt doordat er geen cisco2@C1 gebruiker is gedefinieerd. de cisco-gebruiker kan niet in om het even welke context inloggen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Makkelijk VPN-configuratiegids, Cisco IOS-softwarerelease 15M&T
- Cisco ASA Series 5000 Series VPN CLI-configuratiegids, 9.1
- Technische ondersteuning en documentatie – Cisco Systems