ASA- und Cisco IOS-Gruppensperrfunktionen, AAA-Attribute und WebVPN-Konfigurationsbeispiel

Inhalt

Einführung

Dieser Artikel beschreibt die Gruppensperrungsfunktionen der Cisco Adaptive Security Appliance (ASA) und von Cisco IOS® und zeigt das Verhalten für verschiedene AAA-Attribute (Authentication, Authorization, and Accounting). Für Cisco IOS wird der Unterschied zwischen der Gruppensperre und den Benutzer-VPN-Gruppen zusammen mit einem Beispiel erläutert, das beide ergänzenden Funktionen gleichzeitig verwendet. Es gibt auch ein Cisco IOS WebVPN-Beispiel mit Authentifizierungsdomänen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- ASA CLI-Konfiguration und SSL-VPN-Konfiguration (Secure Sockets Layer)

- VPN-Konfiguration für Remote-Zugriff auf ASA und Cisco IOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- ASA Software, Version 8.4 und höher
- Cisco IOS, Version 15.1 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurationen

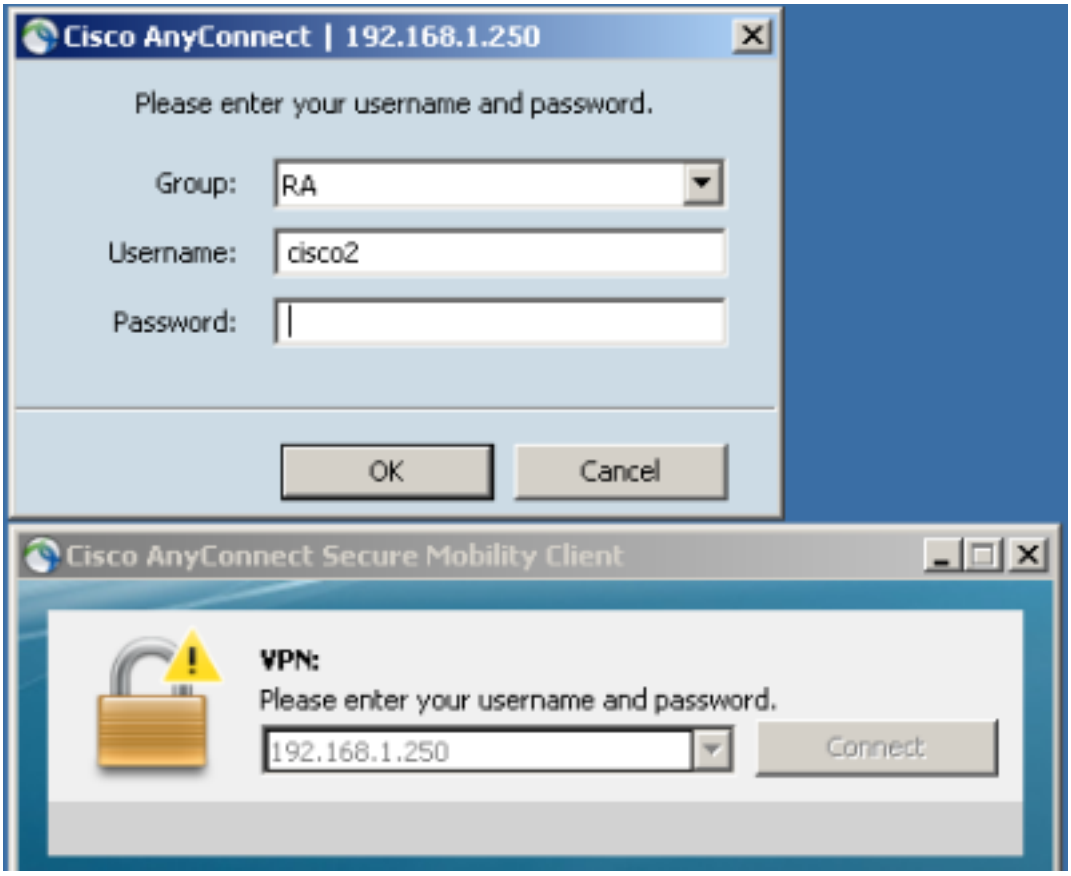
ASA Lokale Gruppensperre

Sie können dieses Attribut unter dem Benutzer oder der Gruppenrichtlinie definieren. Hier ein Beispiel für das lokale Benutzerattribut.

```
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
```

Der Benutzer von cisco kann nur die RA-Tunnelgruppe verwenden, und der Benutzer von cisco2 kann nur die RA2-Tunnelgruppe verwenden.

Wenn der cisco2-Benutzer die RA-Tunnelgruppe auswählt, wird die Verbindung verweigert:

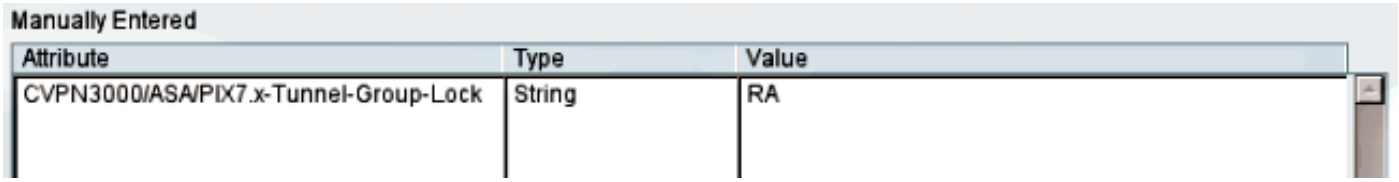



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA mit AAA-Attribut VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

Das Attribut 3076/85 (Tunnel-Group-Lock), das vom AAA-Server zurückgegeben wird, erfüllt genau das gleiche. Sie kann zusammen mit dem Benutzer oder der Richtliniengruppe (oder IETF-Attribut 25) übergeben werden und sperrt den Benutzer in einer bestimmten Tunnelgruppe.

Im Folgenden finden Sie ein Beispiel für ein Autorisierungsprofil auf dem Cisco Access Control Server (ACS):



Wenn das Attribut von AAA zurückgegeben wird, wird es vom RADIUS-Debugger folgendermaßen angezeigt:

```
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
```

Das Ergebnis ist dasselbe, wenn Sie versuchen, auf die RA2-Tunnelgruppe zuzugreifen, während Sie die Gruppe innerhalb der RA-Tunnelgruppe sperren:

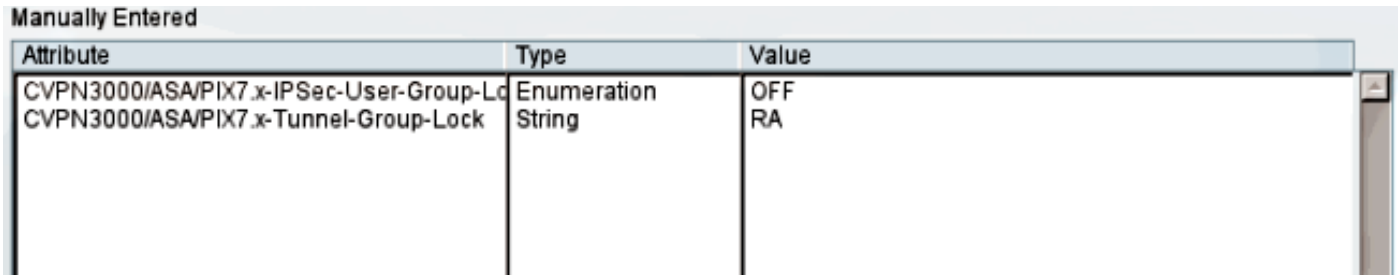
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA mit AAA-Attribut VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Dieses Attribut stammt auch aus dem von der ASA geerbten VPN3000-Verzeichnis. Sie ist weiterhin im 8.4-Konfigurationsleitfaden enthalten (wird jedoch in einer neueren Version des Konfigurationsleitfadens entfernt) und wird wie folgt beschrieben:

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

Es scheint, dass das Attribut verwendet werden könnte, um die Gruppensperrung zu deaktivieren, selbst wenn das Attribut "Tunnel-Group-Lock" vorhanden ist. Wenn Sie versuchen, dieses Attribut zusammen mit der Tunnel-Group-Lock auf 0 zurücksetzen (dies ist immer noch nur Benutzerauthentifizierung), dann geschieht Folgendes: Es sieht seltsam aus, wenn Sie versuchen, die Gruppensperrung zu deaktivieren, während Sie einen bestimmten Tunnelgruppennamen zurückgeben:



Debuggen werden angezeigt:

```
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
```

Dies führt zu demselben Ergebnis (Gruppensperrung wurde erzwungen, IPSec-User-Group-Lock wurde nicht berücksichtigt).

```
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
```

Die externe Gruppenrichtlinie gab IPSec-User-Group-Lock=0 zurück und erhielt außerdem die Tunnel-Group-Lock=RA für die Benutzerauthentifizierung. Der Benutzer wurde jedoch gesperrt, d. h. die Gruppensperrung wurde durchgeführt.

Für die andere Konfiguration gibt die externe Gruppenrichtlinie einen bestimmten Tunnelgruppennamen zurück (Tunnel-Group-Lock), während versucht wird, die Gruppensperrung für einen bestimmten Benutzer zu deaktivieren (IPSec-User-Group-Lock=0), und die Gruppensperrung für diesen Benutzer wurde noch erzwungen.

Damit wird bestätigt, dass das Attribut nicht mehr verwendet wird. Dieses Attribut wurde in der alten VPN300-Serie verwendet. Cisco Bug ID CSCui34066 wurde geöffnet.

Cisco IOS Local Group Lock für Easy VPN

Die lokale Gruppensperroption unter der Gruppenkonfiguration in Cisco IOS funktioniert anders als bei der ASA. Auf der ASA geben Sie den Namen der Tunnelgruppe an, an die der Benutzer gesperrt ist. Die Cisco IOS-Gruppensperroption (es sind keine Argumente vorhanden) ermöglicht eine zusätzliche Überprüfung und vergleicht die Gruppe mit dem Benutzernamen (Format user@group) und IKEID (Gruppenname).

Weitere Informationen finden Sie im Easy VPN-Konfigurationshandbuch, Cisco IOS Release 15M&T.

Hier ein Beispiel:

```
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
```

Dies zeigt, dass die Gruppensperrungsüberprüfung für GROUP1 aktiviert ist. Für GROUP1 ist der einzige zugelassene Benutzer cisco1@GROUP1. Für GROUP2 (ohne Gruppensperre) können sich beide Benutzer anmelden.

Verwenden Sie für eine erfolgreiche Authentifizierung cisco1@GROUP1 mit 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
```

Zur Authentifizierung verwenden Sie cisco2@GROUP2 mit GROUP1:

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

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

Die **ipsec:user-vpn-group** ist das vom AAA-Server zurückgegebene RADIUS-Attribut, das nur für die Benutzerauthentifizierung angewendet werden kann (für die Gruppe wurde Gruppensperre verwendet). Beide Funktionen sind komplementär und werden in verschiedenen Phasen angewendet.

Weitere Informationen finden Sie im Easy VPN-Konfigurationshandbuch, Cisco IOS Release 15M&T.

Sie funktioniert anders als die Gruppensperre und ermöglicht es Ihnen weiterhin, dasselbe Ergebnis zu erzielen. Der Unterschied besteht darin, dass das Attribut einen bestimmten Wert haben muss (wie für die ASA) und dass der spezifische Wert mit dem ISAKMP-Gruppennamen (Internet Security Association and Key Management Protocol) (IKEID) verglichen wird. Wenn sie nicht übereinstimmt, schlägt die Verbindung fehl. Das folgende Beispiel wird verwendet, wenn Sie das vorherige Beispiel ändern, um die AAA-Clientauthentifizierung zu aktivieren und die Gruppensperrung für den Moment zu deaktivieren:

```
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
```

Beachten Sie, dass das ipsec:user-vpn-group-Attribut für den Benutzer definiert ist und die Gruppensperrung für die Gruppe definiert ist.

Auf dem ACS gibt es zwei Benutzer: cisco1 und cisco2. Für den Benutzer cisco1 wird dieses Attribut zurückgegeben: **ipsec:user-vpn-group=GROUP1**. Für den cisco2-Benutzer wird dieses Attribut zurückgegeben: **ipsec:user-vpn-group=GROUP2**.

Wenn der cisco2-Benutzer versucht, sich bei GROUP1 anzumelden, wird dieser Fehler gemeldet:

```
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
```

Dies liegt daran, dass der ACS für den Cisco2-Benutzer ipsec:user-vpn-group=GROUP2 zurückgibt, was von Cisco IOS mit GROUP1 verglichen wird.

Auf diese Weise wurde dasselbe Ziel wie bei der Gruppensperre erreicht. Sie sehen, dass der Endbenutzer derzeit nicht user@group als Benutzernamen bereitstellen muss, sondern Benutzer (ohne die @gruppe) verwenden kann.

Für Gruppensperre sollte cisco1@GROUP1 verwendet werden, da Cisco IOS den letzten Teil (nach @) entfernt und mit IKEID (Gruppenname) verglichen hat.

Für die ipsec:user-vpn-Gruppe reicht es aus, im Cisco VPN-Client nur cisco1 zu verwenden, da dieser Benutzer im ACS definiert ist und die spezifische ipsec:user-vpn-Gruppe zurückgegeben wird (in diesem Fall ist dies =GROUP1) und dieses Attribut mit IKEID verglichen wird.

Cisco IOS AAA ipsec:benutzer-vpn-group und Gruppensperre für Easy VPN

Warum sollten Sie nicht beide Funktionen gleichzeitig verwenden?

Sie können die Gruppensperrung erneut hinzufügen:

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

Hier ist der Ablauf:

1. Der Cisco VPN-Benutzer konfiguriert die GROUP1-Verbindung und stellt eine Verbindung her.
2. Die Phase des aggressiven Modus ist erfolgreich, und Cisco IOS sendet eine xAuth-Anfrage für Benutzername und Kennwort.
3. Der Cisco VPN-Benutzer erhält ein Popup-Fenster und gibt den cisco1@GROUP1-Benutzernamen mit dem im ACS definierten Kennwort ein.
4. Cisco IOS führt eine Überprüfung der Gruppensperrung durch: Sie entfernt den im Benutzernamen angegebenen Gruppennamen und vergleicht ihn mit IKEID. Es ist erfolgreich.
5. Cisco IOS sendet eine AAA-Anfrage an den ACS-Server (für Benutzer cisco1@GROUP1).
6. ACS gibt ein RADIUS-Accept mit ipsec:user-vpn-group=GROUP1 zurück.
7. Cisco IOS führt eine zweite Überprüfung durch. Dieses Mal vergleicht er die vom RADIUS-Attribut bereitgestellte Gruppe mit IKEID.

   Wenn der Fehler bei Schritt 4 (Gruppensperre) fehlschlägt, wird er sofort protokolliert, nachdem er Anmeldeinformationen bereitgestellt hat:

```
*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
```

Wenn der Fehler bei Schritt 7 (ipsec:user-vpn-group) auftritt, wird der Fehler zurückgegeben, nachdem das RADIUS-Attribut für die AAA-Authentifizierung empfangen wurde:

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

IOS WebVPN-Gruppensperre

Auf der ASA kann die Tunnel-Group-Lock für alle VPN-Services für den Remote-Zugriff (IPSec, SSL, WebVPN) verwendet werden. Für die Cisco IOS-Gruppensperre und die ipsec:user-vpn-Gruppe funktioniert sie nur für IPSec (Easy VPN-Server). Um bestimmte Benutzer in bestimmten WebVPN-Kontexten (und angehängten Gruppenrichtlinien) zu sperren, sollten Authentifizierungsdomänen verwendet werden.

Hier ein Beispiel:

```
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
```

Im nächsten Beispiel gibt es zwei Kontexte: C1 und C2. Jeder Kontext verfügt über eine eigene Gruppenrichtlinie mit spezifischen Einstellungen. C1 ermöglicht den AnyConnect-Zugriff. Das Gateway wird so konfiguriert, dass beide Kontexte überwacht werden: C1 und C2.

Wenn der cisco1-Benutzer mit https://10.48.67.137/C1 auf den C1-Kontext zugreift, fügt die Authentifizierungsdomäne **C1 hinzu** und authentifiziert sich anhand des lokal definierten (Liste LIST) cisco1@C1-Benutzernamens:


```
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"
```

Wenn Sie versuchen, sich bei cisco2 als Benutzername anzumelden, während Sie auf den C1-Kontext zugreifen (https://10.48.67.137/C1), wird dieser Fehler gemeldet:

```
*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
```

Der Grund hierfür ist, dass kein cisco2@C1 benutzerdefiniert ist. der Cisco Benutzer kann sich in keinem Kontext anmelden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Easy VPN-Konfigurationsleitfaden, Cisco IOS Release 15M&T
- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.1
- Technischer Support und Dokumentation - Cisco Systems