ميزات تأمين مجموعة ASA و Cisco IOS وسامتو WebVPN نيوكت لاثمو AAA

المحتويات

المقدمة

يصف هذا المقال ميزات تأمين المجموعة على جهاز الأمان القابل للتكيف (ASA) من Cisco وفي برنامج Cisco IOS®، كما يعرض سلوك سمات المصادقة والتفويض والمحاسبة (AAA) المختلفة. ل Cisco IOS، يتم شرح الفرق بين قفل المجموعة ومجموعات المستخدم-VPN مع مثال يستخدم كلا من الميزات التكميلية في نفس الوقت. هناك أيضا مثال Cisco IOS WebVPN مع مجالات المصادقة.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة واسعة من هذا موضوع:

- تكوين ASA CLI وتكوين طبقة مآخذ التوصيل الآمنة (VPN SSL)
- تكوين VPN للوصول عن بعد على ASA و Cisco IOS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج ASA، الإصدار 8.4 والإصدارات الأحدث
- IOS، الإصدار 15.1 والإصدارات الأحدث من Cisco

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوينات

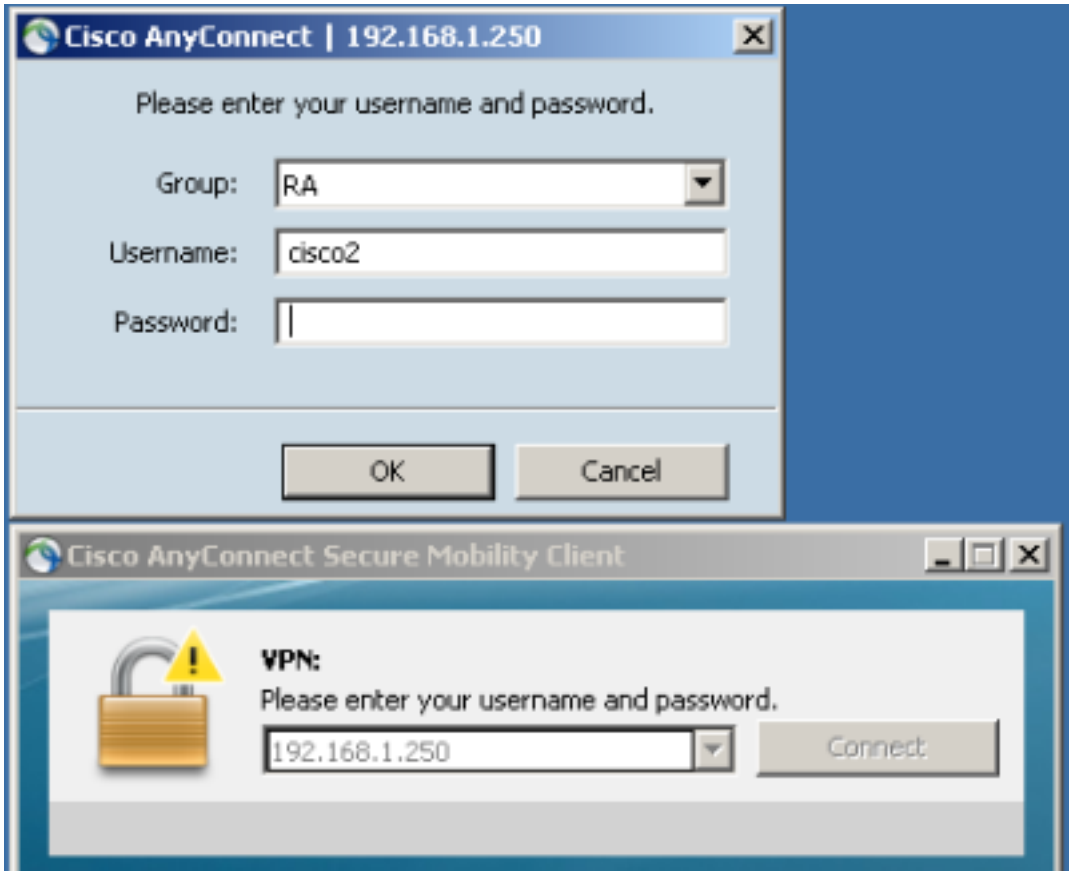
قفل مجموعة ASA المحلي

يمكنك تعريف هذه السمة ضمن المستخدم أو نهج المجموعة. هنا مثال لسمة المستخدم المحلي.

```
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
```

يمكن لمستخدم Cisco إستخدام مجموعة نفق RA فقط، ويمكن لمستخدم Cisco2 إستخدام مجموعة نفق RA2 فقط.

إذا اختار مستخدم Cisco2 مجموعة نفق RA، فسيتم رفض الاتصال:

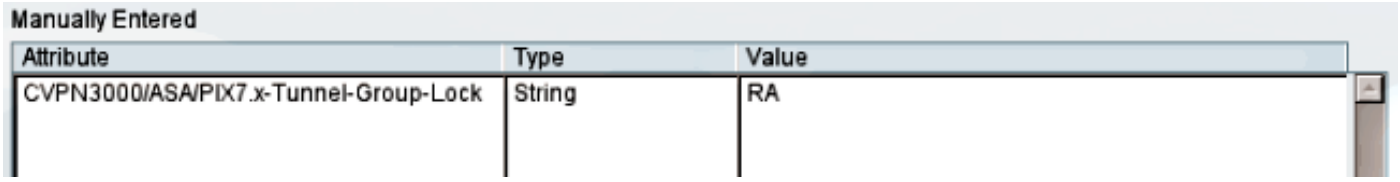



```
<May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88
   Terminating the VPN connection attempt from <RA>. Reason: This connection is
                                                          . group locked to
```

ASA مع سمة AAA VPN3000/ASA/PIX7.x-tunnel-group-lock

السمة 85/3076 (Tunnel-Group-Lock) التي يتم إرجاعها بواسطة خادم AAA تقوم بنفس الإجراء تماما. يمكن تمريره مع مصادقة المستخدم أو مجموعة السياسات (أو مصادقة السمة 25 الخاصة ب "فريق عمل هندسة الإنترنت" (IETF) وقفل المستخدم في مجموعة نفق معينة.

هنا مثال لملف تعريف التفويض على خادم التحكم في الوصول (ACS) من Cisco:



عندما يتم إرجاع السمة بواسطة AAA، تشير تصحيح أخطاء RADIUS إلى ذلك:

```
                                    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
6f                                                 |  cisco 63 73 69 63
                                              Radius: Type = 25 (0x19) Class
                                                  (Radius: Length = 24 (0x18
                                                = (Radius: Value (String
3a 61 63 73 35 34 2f 31 35 38 33 33    |  CACS:acs54/15833 53 43 41 43
2f 33                                              |  4484/3 34 38 34 34
                                      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
RA  |                                                                 41 52
                                                       rad_procpkt: ACCEPT
                                      RADIUS_ACCESS_ACCEPT: normal termination
```

تكون النتيجة هي نفسها عند محاولة الوصول إلى مجموعة نفق RA2 أثناء تأمين المجموعة داخل مجموعة نفق RA:

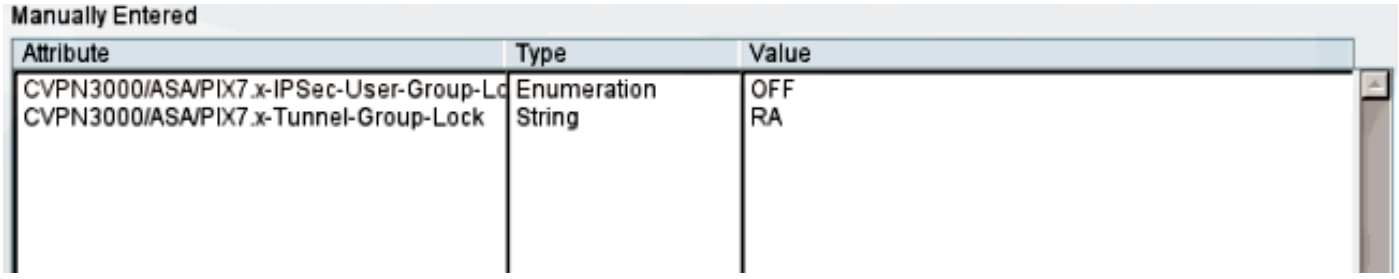
```
<May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
                                                                group locked to
```

ASA مع سمة AAA VPN3000/ASA/PIX7.x-IPSec-user-group-lock

كما يتم أخذ هذه السمة من دليل VPN3000 الموروث بواسطة ASA. ولا يزال موجودا في دليل تكوين 8.4 (على الرغم من أنه تمت إزالته في إصدار أحدث من دليل التكوين) وتم وصفه على النحو التالي:

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

يبدو أنه يمكن إستخدام السمة لتعطيل تأمين المجموعة، حتى إذا كانت السمة Tunnel-Group-Lock موجودة. إذا حاولت إرجاع هذه السمة المعينة على 0 مع Tunnel-Group-Lock (ما زالت هذه هي مصادقة المستخدم)، فيما يلي ما يحدث. يبدو غريبا عند محاولة تعطيل قفل المجموعة أثناء إرجاع اسم مجموعة النفق المحدد:



عرض تصحيح الأخطاء:

```
                                                .....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
6f                                                 |  cisco 63 73 69 63
                                              Radius: Type = 25 (0x19) Class
                                                  (Radius: Length = 24 (0x18
```

```
                                                = (Radius: Value (String
3a 61 63 73 35 34 2f 31 35 38 33 33    |  CACS:acs54/15833 53 43 41 43
          2f 34                                |  4484/4 34 38 34 34
                                    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
                                  RA  |                                 41 52
                                                rad_procpkt: ACCEPT
```

ينتج هذا النتيجة نفسها (تم فرض تأمين المجموعة، ولم يتم أخذ IPSec-User-Group-Lock في الاعتبار).

```
<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
```

قام نهج المجموعة الخارجي بإرجاع IPSec-user-group-lock=0، كما حصل أيضا على Tunnel-Group-Lock=RA لمصادقة المستخدم. مع ذلك، تم تأمين المستخدم، مما يعني أنه تم إجراء "تأمين المجموعة".

بالنسبة للتكوين المعاكس، يرجع نهج المجموعة الخارجي اسم مجموعة نفق محدد (Tunnel-Group-Lock) أثناء محاولة تعطيل تأمين المجموعة لمستخدم محدد (IPSec-user-Group-Lock=0)، ولا يزال يتم فرض تأمين المجموعة لذلك المستخدم.

وهذا يؤكد عدم إستخدام السمة بعد الآن. استعملت أن سمة كان في القديم VPN3000 sery. تم فتح معرف تصحيح الأخطاء من Cisco CSCui34066.

قفل مجموعة IOS المحلي ل VPN سهل من Cisco

يعمل خيار قفل المجموعة المحلي ضمن تكوين المجموعة في Cisco IOS بشكل مختلف عن العمل على ASA. على ال ASA، أنت تعين النفق مجموعة إسم إلى أي المستعمل يكون مقفل. يتيح خيار قفل مجموعة Cisco IOS (لا توجد وسيطات) إمكانية تحقق إضافي ويقارن المجموعة المقدمة باسم المستخدم (تنسيق user@group) باسم IKEID (اسم المجموعة).

لمزيد من المعلومات، ارجع إلى دليل تكوين VPN السهل، Cisco IOS، الإصدار 15M&T.

فيما يلي مثال:

```
                                                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
```

هذا يظهر أن التحقق من تأمين المجموعة ممكن ل GROUP1. بالنسبة للمجموعة 1، المستخدم الوحيد المسموح به هو cisco1@GROUP1. بالنسبة لمجموعة GROUP2 (بدون تأمين مجموعة)، يمكن لكلا المستخدمين تسجيل الدخول.

للمصادقة الناجحة، أستخدم cisco1@GROUP1 مع 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
```

للمصادقة، أستخدم cisco2@GROUP2 مع GROUP1:

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

Cisco IOS AAA IPsec:user-vpn-group for Easy VPN

إن **ips:user-vpn-group** هي سمة RADIUS التي يرجعها خادم AAA، ويمكن تطبيقها فقط لمصادقة المستخدم (تم إستخدام تأمين المجموعة للمجموعة). وكلتا المميزات مكملة، ويتم تطبيقها في مراحل مختلفة.

أحلت ل كثير معلومة، [السهل VPN تشكيل مرشد، cisco ios إطلاق 15M&T](#).

إنه يعمل بشكل مختلف عن قفل المجموعة ومع ذلك يسمح لك بتحقيق نفس النتيجة. الفرق هو أن السمة ينبغي أن يكون لها قيمة محددة (مثل بالنسبة ل ASA) وأن القيمة المحددة يتم مقارنتها مع اسم مجموعة اقتران أمان الإنترنت وإدارة المفاتيح (IKEID) (ISAKMP)؛ وإذا لم تتطابق، يفشل الاتصال. فيما يلي ما يحدث إذا قمت بتغيير المثال السابق للحصول على مصادقة AAA للعميل وتعطيل تأمين المجموعة الآن:

```
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
```

لاحظ أنه تم تعريف السمة ipSec:user-vpn-group للمستخدم وتم تحديد تأمين المجموعة للمجموعة.

في ال ACS، هناك إثنان مستعمل، cisco1 و cisco2. بالنسبة لمستخدم Cisco1، يتم إرجاع هذه السمة: **ips:user-vpn-group=group1**. بالنسبة لمستخدم Cisco2، يتم إرجاع هذه السمة: **ips:user-vpn-group=group2**.

عندما يحاول مستخدم Cisco2 تسجيل الدخول باستخدام GROUP1، يتم الإبلاغ عن هذا الخطأ:

```
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
```

وذلك لأن ACS لمستخدم Cisco2 يرجع **ipSec:user-vpn-group=group2**، أي يقارن ب cisco IOS إلى group1.

وبهذه الطريقة، تم تحقيق الهدف نفسه كما هو الحال بالنسبة للتأمين الجماعي. يمكنك أن ترى أن الآن، المستخدم النهائي لا يحتاج إلى توفير user@group كاسم مستخدم، ولكن يمكنه إستخدام المستخدم (بدون @group).

بالنسبة لقفل المجموعة، يجب إستخدام cisco1@GROUP1، نظرا لأن Cisco IOS قامت بمسح الجزء الأخير (بعد @) وقارنته ب ikeid (اسم المجموعة).

بالنسبة ل ipsEc:user-vpn-group، يكفي إستخدام Cisco1 فقط في عميل Cisco VPN، لأن ذلك المستخدم معرف على ACS ويتم إرجاع ipSec:user-vpn-group المحدد (في هذه الحالة، هي =GROUP1) وتقارن تلك السمة مقابل IKEID.

cisco IOS AAA ipSec:user-vpn-group and Group-lock for Easy VPN

لماذا لا يجب إستخدام كلا السمتين في الوقت نفسه؟

يمكنك إضافة تأمين المجموعة مرة أخرى:

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

هنا هو التدفق:

1. يقوم مستخدم شبكة VPN من Cisco بتكوين اتصال المجموعة 1 وتوصيله.
2. تكون مرحلة الوضع العدواني ناجحة، ويرسل Cisco IOS طلب xAuth لاسم المستخدم وكلمة المرور.
3. ال cisco VPN يستلم مستعمل منبثق، ويدخل ال username cisco1@GROUP1 مع ال يصح كلمة يعين على ال ACS.
4. يقوم Cisco IOS بإجراء تحقق لقفل المجموعة: إنه يجرد اسم المجموعة المتوفر في اسم المستخدم ويقارنه ب ikeid. إنه ناجح.
5. يرسل Cisco IOS طلب AAA إلى خادم ACS (للمستخدم cisco1@GROUP1).
6. يرجع ACS قبول RADIUS مع **ipsEc:user-vpn-group=group1**.
7. يقوم Cisco IOS بإجراء تحقق ثان؛ وهذه المرة، فإنه يقارن المجموعة المقدمة من سمة RADIUS ب ikeid.

عند فشله في الخطوة 4 (قفل المجموعة)، يتم تسجيل الخطأ فورا بعد أن يوفر بيانات الاعتماد:

```
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*
```

عندما يفشل في الخطوة 7 (ipsEc:user-vpn-group)، يرجع الخطأ بعد أن يستلم سمة RADIUS لمصادقة AAA:

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

قفل مجموعة WebVPN ل IOS

على ASA، يمكن إستخدام Tunnel-Group-Lock لجميع خدمات VPN للوصول عن بعد (IPSec، SSL، WebVPN). بالنسبة لقفل مجموعة Cisco IOS و ipSec:user-vpn-group، يعمل فقط ل IPSec (خادم VPN سهل). من أجل تأمين مجموعة مستخدمين محددين في سياقات WebVPN المحددة (وسياسات المجموعة المرفقة)، يجب إستخدام مجالات المصادقة.

فيما يلي مثال:

```
                                                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
 #accessed via https://IP/C1 gateway GW domain 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
 #accessed via https://IP/C2 gateway GW domain C2
 logging enable
 inservice

ip local pool POOL 7.7.7.10 7.7.7.20
```

في المثال التالي، هناك سياقان: C1 و C2. ولكل سياق نهج مجموعة خاص به بإعدادات محددة. يسمح C1 بالوصول إلى AnyConnect. تم تكوين بوابة الوصول للاستماع إلى كلا السياقين: C1 و C2.

عندما ينفذ مستخدم Cisco1 السياق C1 مع https://10.48.67.137/C1، يضيف مجال المصادقة **C1** ويصادق مقابل ال يعرف محليا (قائمة) username 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*
user_name: cisco1, Authentication successful, user logged in 10.61.218.146
"May 20 16:30:07.518: WV-AAA: User "cisco1" has logged in from "10.61.218.146" to gateway "GW*
"context "C1
```

عندما تحاول تسجيل الدخول باستخدام Cisco2 كاسم مستخدم بينما تقوم بالوصول إلى سياق C1 (https://10.48.67.137/C1)، يتم الإبلاغ عن هذا الفشل:

```
: 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
```

وذلك نظرا لعدم وجود مستخدم معرف على cisco2@C1. لا يمكن لمستخدم Cisco تسجيل الدخول إلى أي سياق.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دليل تكوين VPN سهل، Cisco IOS، الإصدار 15M&T

- دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN، الإصدار 9.1
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).