ASA和Cisco IOS組鎖定功能以及AAA屬性和WebVPN配置示例

目錄

簡介

本文介紹Cisco Adaptive Security Appliance(ASA)和Cisco IOS®中的組鎖定功能，並顯示不同身份驗證、授權和記帳(AAA)屬性的行為。對於Cisco IOS，group-lock和user-vpn-groups之間的區別將隨同時使用兩個互補功能的示例一起解釋。還有一個帶有身份驗證域的Cisco IOS WebVPN示例。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- ASA CLI配置和安全套接字層(SSL)VPN配置
- ASA和Cisco IOS上的遠端訪問VPN配置

採用元件

本檔案中的資訊是根據以下軟體版本：

- ASA軟體8.4版及更高版本
- Cisco IOS 15.1版及更新版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

組態

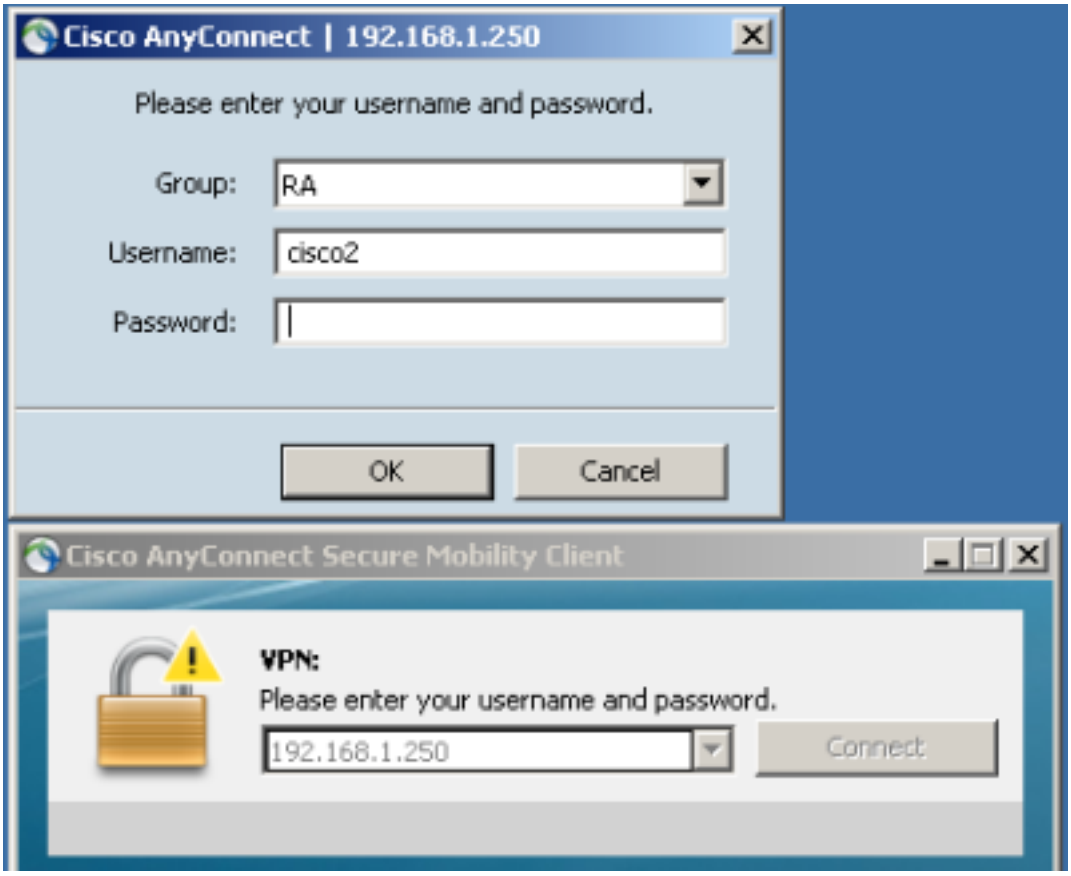
ASA本地組鎖定

您可以在使用者或組策略下定義此屬性。以下是本地使用者屬性的示例。

```
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
```

思科使用者只能使用RA隧道組，思科2使用者只能使用RA2隧道組。

如果cisco2使用者選擇RA通道群組，則連線會遭到拒絕：

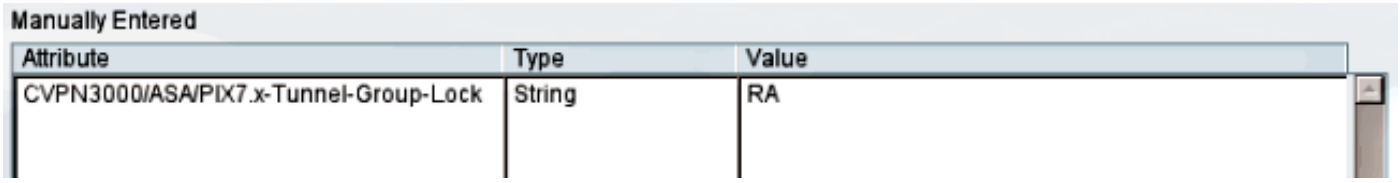



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

具有AAA屬性VPN3000/ASA/PIX7.x-Tunnel-Group-Lock的ASA

AAA伺服器傳回的屬性3076/85(Tunnel-Group-Lock)的作用完全相同。它可以隨使用者或策略組(或Internet工程任務組(IETF)屬性25)身份驗證一起傳遞，並將使用者鎖定在特定隧道組中。

以下是思科存取控制伺服器(ACS)上的授權設定檔範例：



當AAA傳回屬性時，RADIUS偵錯會指出它：

```
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
```

當您嘗試在RA tunnel-group中鎖定組時訪問RA2 tunnel-group時，結果相同：

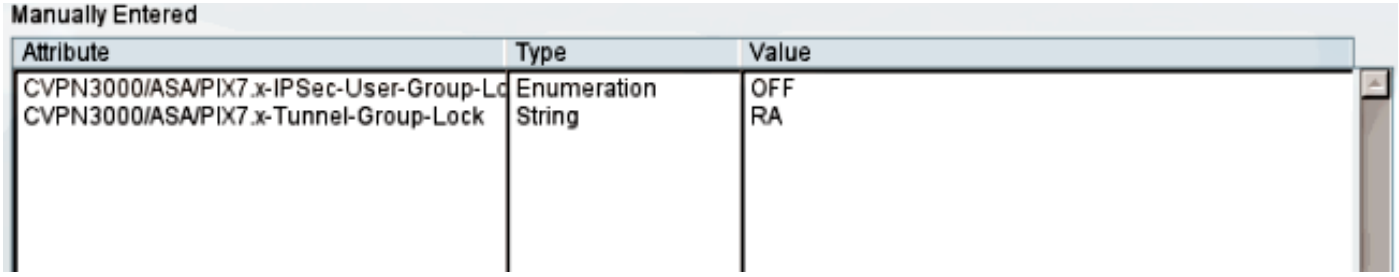
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

具有AAA屬性VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock的ASA

此屬性還取自ASA繼承的VPN3000目錄。它仍存在於8.4 配置指南中（儘管在配置指南的更新版本中將其刪除），說明如下：

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

即使存在Tunnel-Group-Lock屬性，該屬性似乎也可用於禁用組鎖定。如果您嘗試將屬性集與Tunnel-Group-Lock一起返回0（這仍只是使用者身份驗證），則會發生以下情況。當您嘗試在返回特定隧道組名稱時禁用組鎖定時，看起來很奇怪：



調試顯示：

```
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
```

這會產生相同的結果（已實施組鎖定，但未考慮IPSec-User-Group-Lock）。

```
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
```

外部組策略返回IPSec-User-Group-Lock=0，並且獲取了用於使用者身份驗證的Tunnel-Group-Lock=RA。使用者仍然被鎖定，這意味著已執行組鎖定。

對於相反的配置，當外部組策略嘗試為特定使用者禁用組鎖定(IPSec-User-Group-Lock=0)時，它返回特定隧道組名稱(Tunnel-Group-Lock)，並且仍對該使用者強制執行組鎖定。

這確認不再使用該屬性。該屬性用於舊的VPN3000系列。思科錯誤ID CSCui34066已開啟。

適用於Easy VPN的Cisco IOS本機群組鎖定

Cisco IOS中組配置下的本地group-lock選項的工作方式與ASA上的不同。在ASA上，指定使用者被鎖定的隧道組名稱。Cisco IOS group-lock選項（無引數）啟用其他驗證並將使用者名稱(格式user@group)提供的組與IKEID（組名）進行比較。

有關詳細資訊，請參閱Easy VPN配置指南Cisco IOS版本15M&T。

以下是範例：

```
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
```

這顯示為GROUP1啟用了組鎖定驗證。對於GROUP1，只允許使用者cisco1@GROUP1。對於GROUP2（無組鎖定），兩個使用者均能夠登入。

要成功進行身份驗證，請使用cisco1@GROUP1和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
```

要進行身份驗證，請將cisco2@GROUP2與GROUP1一起使用：

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

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

ipsec:user-vpn-group是AAA伺服器返回的RADIUS屬性，它只能應用於使用者身份驗證（組鎖定用於該組）。 這兩個功能是互補的，並且它們在不同階段應用。

有關詳細資訊，請參閱Easy VPN配置指南，Cisco IOS版本15M&T。

它的工作方式與組鎖定不同，並且仍然允許您獲得相同的結果。不同之處在於，屬性必須具有特定值（如ASA），並且將該特定值與網際網路安全關聯和金鑰管理協定(ISAKMP)組名稱(IKEID)進行比較；如果不匹配，則連線失敗。如果要更改上一個示例，以便立即進行客戶端AAA身份驗證並禁用group-lock，將會發生以下情況：

```
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
```

請注意，為使用者定義了ipsec:user-vpn-group屬性，為組定義了組鎖定。

ACS上有兩個使用者：cisco1和cisco2。對於cisco1使用者，此屬性返回：**ipsec:user-vpn-group=GROUP1**。對於cisco2使用者，此屬性返回：**ipsec:user-vpn-group=GROUP2**。

當cisco2使用者嘗試使用GROUP1登入時，報告以下錯誤：

```
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
```

這是因為cisco2使用者的ACS傳回**ipsec:user-vpn-group=GROUP2**，而Cisco IOS會將其與GROUP1進行比較。

這樣，就實現了與群鎖相同的目標。您可以看到，目前，終端使用者無需提供user@group作為使用者名稱，但可以使用user(不帶@group)。

對於group-lock，應使用cisco1@GROUP1，因為Cisco IOS刪除了最後部分（@之後），並將其與IKEID（組名）進行比較。

對於ipsec:user-vpn-group，在Cisco VPN客戶端中僅使用cisco1就足夠了，因為該使用者是在ACS上定義的，並且返回了特定的ipsec:user-vpn-group（在本例中為=GROUP1），並且將該屬性與IKEID進行比較。

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

為什麼不能同時使用這兩個功能？

您可以再次新增組鎖定：

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

以下是流程：

1. Cisco VPN使用者配置GROUP1連線並進行連線。
2. 主動模式階段成功，Cisco IOS會傳送使用者名稱和密碼的xAuth要求。
3. Cisco VPN使用者收到一個彈出視窗，然後輸入cisco1@GROUP1使用者名稱，並使用ACS上定義的正確密碼。
4. Cisco IOS會執行群組鎖定檢查：刪除使用者名稱中提供的組名稱，並將其與IKEID進行比較。它是成功的。
5. Cisco IOS向ACS伺服器傳送AAA請求(針對使用者cisco1@GROUP1)。
6. ACS返回RADIUS-Accept with **ipsec:user-vpn-group=GROUP1**。
7. Cisco IOS執行第二次驗證；這一次，它將RADIUS屬性提供的組與IKEID進行比較。

   如果在第4步失敗（組鎖定），則會在提供憑證後立即記錄錯誤：

```
*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
```

   當其在步驟7失敗(ipsec:user-vpn-group)時，在收到AAA驗證的RADIUS屬性後會返回錯誤：

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

IOS Webvpn群組鎖定

在ASA上，Tunnel-Group-Lock可用於所有遠端訪問VPN服務(IPSec、SSL、WebVPN)。 對於Cisco IOS group-lock和ipsec:user-vpn-group，它僅適用於IPSec（easy VPN伺服器）。 為了對特定WebVPN環境（和附加的組策略）中的特定使用者進行組鎖定，應使用身份驗證域。

以下是範例：

```
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
```

在下一個示例中，有兩個上下文：C1和C2。每個情景都有自己的組策略，並帶有特定設定。C1允許AnyConnect訪問。網關配置為偵聽兩個情景：C1和C2。

當cisco1使用者使用https://10.48.67.137/C1訪問C1情景時，身份驗證域會新增**C1**，並根據本地定義的（清單LIST）cisco1@C1使用者名稱：

```
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"
```

當您在訪問C1情景(https://10.48.67.137/C1)時嘗試使用cisco2作為使用者名稱登入時，會報告以下故障：

```
*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
```

這是因為沒有cisco2@C1使用者定義。思科使用者無法登入任何上下文。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Easy VPN配置指南，Cisco IOS版本15M&T
- Cisco ASA系列VPN CLI配置指南9.1
- 技術支援與文件 - Cisco Systems