ASA和Cisco IOS组锁功能和AAA属性和WebVPN配置示例

目录

简介
先决条件
要求
使用的组件
配置
ASA本地组锁
具有AAA属性的ASA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock
具有AAA属性VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock的ASA
适用于Easy VPN的Cisco IOS本地组锁
Cisco IOS AAA ipsec:Easy VPN的用户VPN组
Cisco IOS AAA ipsec:Easy VPN的用户VPN组和组锁
IOS Webvpn组锁
验证
故障排除
相关信息

简介

本文介绍Cisco自适应安全设备(ASA)和Cisco IOS®中的组锁定功能，并介绍不同身份验证、授权和记帐(AAA)属性的行为。对于Cisco IOS，解释了group-lock和user-vpn-groups之间的区别，同时使用两个互补功能的示例也说明了这一点。还有一个包含身份验证域的Cisco IOS WebVPN示例。

先决条件

要求

思科建议您基本了解以下主题：

- ASA CLI配置和安全套接字层(SSL)VPN配置
- ASA和Cisco IOS上的远程访问VPN配置

使用的组件

本文档中的信息基于以下软件版本：

- ASA软件8.4版及更高版本
- Cisco IOS 15.1版及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

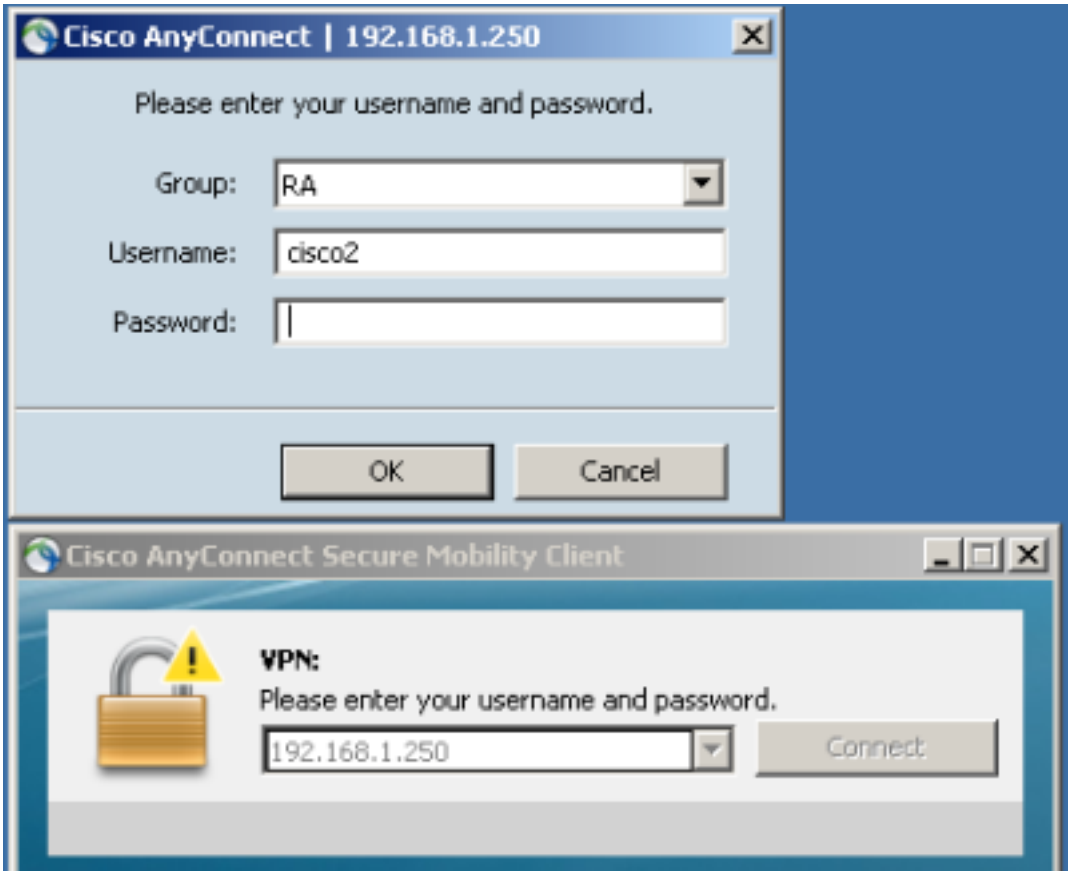
ASA本地组锁

您可以在用户或组策略下定义此属性。以下是本地用户属性的示例。

```
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
```

思科用户只能使用RA隧道组，而cisco2用户只能使用RA2隧道组。

如果cisco2用户选择RA隧道组，则连接被拒绝：

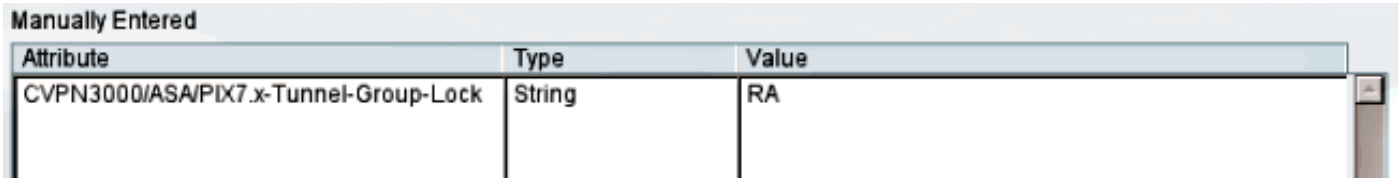



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

具有AAA属性的ASA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

AAA服务器返回的属性3076/85（隧道组锁定）执行完全相同的操作。它可以与用户或策略组(或互联网工程任务组(IETF)属性25)身份验证一起传递，并锁定特定隧道组中的用户。

以下是思科访问控制服务器(ACS)上的授权配置文件示例：



当AAA返回属性时，RADIUS调试会指示它：

```
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
```

当您尝试访问RA2隧道组时，在RA隧道组内锁定组时，结果相同：

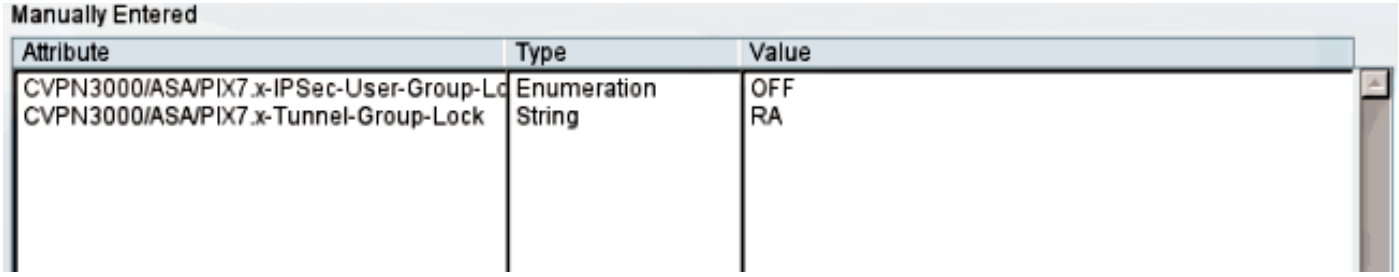
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

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

此属性也取自ASA继承的VPN3000目录。它仍在8.4配置指南中（虽然在较新版本的配置指南中删除），并描述如下：

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

即使存在Tunnel-Group-Lock属性，该属性似乎也可用于禁用组锁定。如果尝试将该属性与Tunnel-Group-Lock一起返回为0（这仍只是用户身份验证），将发生以下情况。当您在返回特定隧道组名称时尝试禁用组锁定时，这看起来很奇怪：



调试显示：

```
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
```

这将产生相同的结果（已实施组锁定，且未考虑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
```

外部组策略返回IPSec-User-Group-Lock=0，并且获取了Tunnel-Group-Lock=RA以进行用户身份验证。但是，用户已被锁定，这意味着已执行组锁定。

对于相反的配置，外部组策略在尝试为特定用户禁用组锁定(IPSec-User-Group-Lock=0)时返回特定隧道组名称(Tunnel-Group-Lock)，并且仍对该用户实施组锁定。

这确认该属性不再使用。该属性在旧VPN3000系列中使用。已打开思科漏洞ID CSCui34066。

适用于Easy VPN的Cisco IOS本地组锁

Cisco IOS中组配置下的本地组锁定选项与ASA上的工作方式不同。在ASA上，指定用户锁定到的隧道组名称。Cisco IOS组锁定选项（无参数）启用其他验证，并将用户名(格式为user@group)提供的组与IKEID（组名）进行比较。

有关详细信息，请参阅《Easy VPN配置指南》（Cisco IOS版本15M&T）。

示例如下：

```
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
```

这显示已为GROUP1启用组锁定验证。对于GROUP1，唯一允许的用户是cisco1@GROUP1。对于GROUP2（无组锁定），两个用户都可以登录。

要成功进行身份验证，请将cisco1@GROUP1与GROUP1配合使用：

```
*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
```

对于身份验证，将cisco2@GROUP2与GROUP1一起使用：

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

Cisco IOS AAA ipsec:Easy VPN的用户VPN组

ipsec:user-vpn-group是AAA服务器返回的RADIUS属性，它只能应用于用户身份验证（组锁用于组）。 这两种功能都是互补的，并且应用于不同的阶段。

有关详细信息，请参[阅《Easy VPN配置指南，Cisco IOS版本15M&T》](#)。

它的工作方式与组锁不同，仍允许您实现相同的结果。区别在于，属性必须具有特定值（如ASA），并且该特定值与互联网安全关联和密钥管理协议(ISAKMP)组名(IKEID)进行比较；如果不匹配，则连接失败。如果更改上一个示例以使客户端AAA身份验证并禁用组锁定，现在会发生以下情况：

```
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
```

请注意，ipsec:user-vpn-group属性已为用户定义，而group-lock已为组定义。

在ACS上，有两个用户，cisco1和cisco2。对于cisco1用户，返回此属性：**ipsec:user-vpn-group=GROUP1**。对于cisco2用户，返回此属性:**ipsec:user-vpn-group=GROUP2**。

当cisco2用户尝试使用GROUP1登录时，会报告以下错误：

```
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
```

这是因为cisco2用户的ACS返回**ipsec:user-vpn-group=GROUP2**，由Cisco IOS与GROUP1进行比较。

这样，就实现了小组锁定的相同目标。您可以看到，目前，最终用户不需要提供user@group作为用户名，但可以使用用户(不含@group)。

对于组锁，应使用cisco1@GROUP1，因为Cisco IOS删除了最后一部分（@之后），并将其与IKEID（组名）进行比较。

对于ipsec:user-vpn-group，在Cisco VPN客户端中仅使用cisco1就足够了，因为该用户在ACS上定义，并返回特定的ipsec:user-vpn-group（在本例中为=GROUP1），该属性与IKEID进行比较。

Cisco IOS AAA ipsec:Easy VPN的用户VPN组和组锁

为什么不同时使用这两个功能？

您可以再次添加组锁：

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

流程如下：

1. Cisco VPN用户配置GROUP1连接并连接。
2. 主动模式阶段成功，Cisco IOS会发送xAuth请求以获取用户名和密码。
3. Cisco VPN用户收到弹出窗口，并输入cisco1@GROUP1用户名和在ACS上定义的正确密码。
4. Cisco IOS对组锁执行检查：它删除用户名中提供的组名，并将其与IKEID进行比较。成功了。
5. Cisco IOS向ACS服务器(对于用户cisco1@GROUP1)发送AAA请求。
6. ACS返回RADIUS-Accept，**其中包含ipsec:user-vpn-group=GROUP1**。
7. Cisco IOS执行第二次验证；此时，它将RADIUS属性提供的组与IKEID进行比较。

   当它在步骤4（组锁定）失败时，错误在提供凭证后立即记录：

   ```
   *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
   ```

   当它在步骤7(ipsec:user-vpn-group)失败时，在收到AAA身份验证的RADIUS属性后返回错误：

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

IOS Webvpn组锁

在ASA上，Tunnel-Group-Lock可用于所有远程访问VPN服务(IPSec、SSL、WebVPN)。 对于Cisco IOS组锁和ipsec:user-vpn-group，它仅适用于IPSec（easy VPN服务器）。 为了在特定WebVPN环境（和附加的组策略）中对特定用户进行组锁定，应使用身份验证域。

示例如下：

```
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
```

在下一个示例中，有两个情景：C1和C2。每个情景都有其自己的组策略和特定设置。C1允许AnyConnect访问。配置网关以侦听两个情景：C1和C2。

当cisco1用户使用https://10.48.67.137/C1访问C1上下文时，身份验证域将添加**C1**，并根据本地定义的（列表LIST）cisco1@C1用户名进行身份验证：


```
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"
```

当您在访问C1情景(https://10.48.67.137/C1)时尝试以cisco2作为用户名登录时，会报告此故障：

```
*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
```

这是因为没有用户定义cisco2@C1。思科用户无法登录任何情景。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Easy VPN配置指南，Cisco IOS版本15M&T
- 思科 ASA 系列 VPN CLI 配置指南，版本 9.1
- 技术支持和文档 - Cisco Systems