ASA和Cisco IOS组锁定功能和AAA属性和WebVPN配置示例

目录

简介

此条款描述组锁定的功能在思科可适应安全工具(ASA)和在Cisco IOS并且提交不同的验证、授权和统计(AAA)属性的行为。对于Cisco IOS，在组锁定和用户VPN组之间的区别与同时使用两个补充功能的示例一起解释。也有与验证域的一Cisco IOS WebVPN示例。

先决条件

要求

思科建议您有这些主题baisc知识：

- ASA CLI配置和安全套接字协议层(SSL) VPN配置
- 在ASA和Cisco IOS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，版本8.4和以上
- Cisco IOS，版本15.1和以上

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

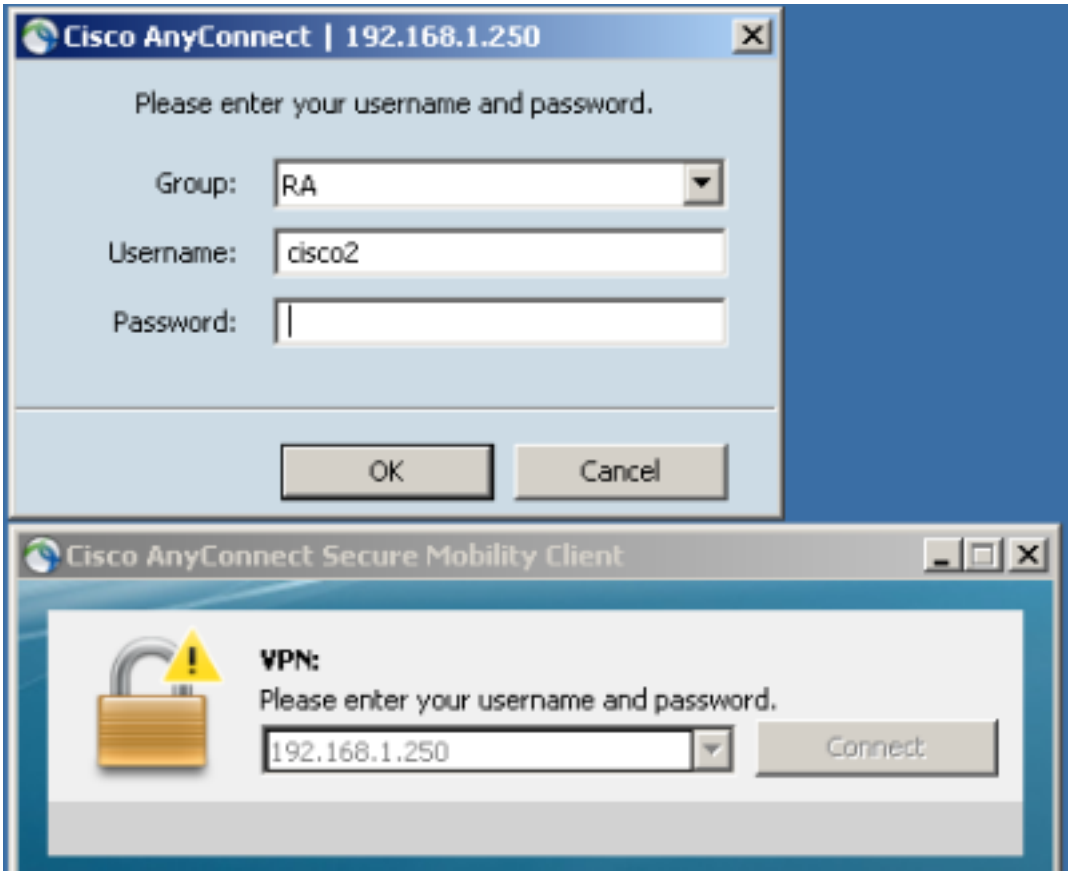
ASA本地组锁定

您能根据用户或组政策定义此属性。这是本地用户属性的一示例。

```
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
```

cisco用户能使用仅RA隧道群，并且cisco2用户能使用仅RA2隧道群。

如果cisco2用户选择RA隧道群，则连接拒绝：

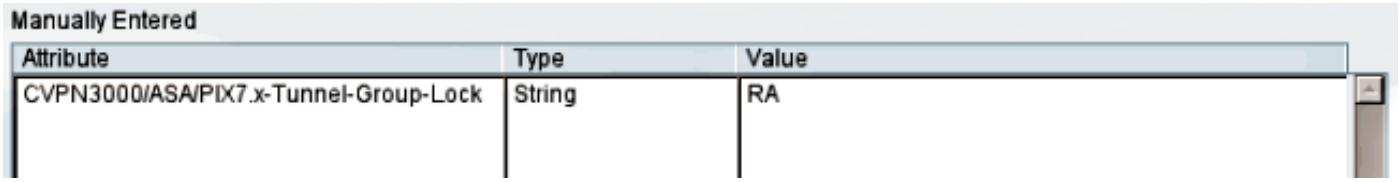



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

与AAA属性VPN3000/ASA/PIX7.x-Tunnel-Group-Lock的ASA

属性3076/85 (通道组LOCK)由AAA服务器返回执行同一。它在一特定隧道群中可以与用户或策略组(或互联网工程任务组(IETF)属性25)验证一起通过并且锁定用户。

这是在思科访问控制服务器(ACS)的一示例授权配置文件：



当属性由AAA时返回， RADIUS调试指示它：

```
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
```

结果是相同的，当您设法访问RA2隧道群时，当组锁定在RA隧道群内时：

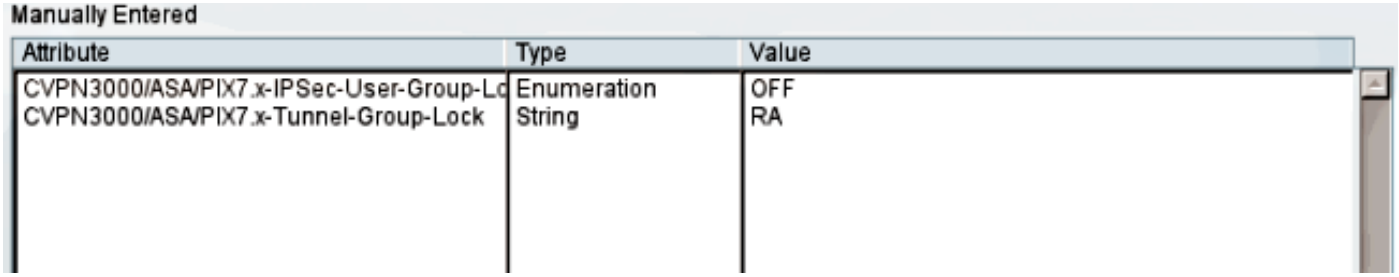
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

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

此属性从ASA继承的VPN3000目录也被采取。它是存在8.4配置指南(虽然在配置指南一个新版本删除)和描述如下：

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

看来属性可能用于为了禁用组锁定，即使通道组LOCK属性存在。如果设法返回该属性设置到0与通道组LOCK一起(这仍然是用户认证)，这是发生了什么。它看起来奇怪，当您设法禁用组锁定时，当返回一个特定组名时：



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
```

这产生同一种结果(组锁定被强制了执行，并且IPSec用户组LOCK未被考虑到)。

```
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 <RA>
```

外部组政策返回IPSec-User-Group-Lock=0并且获得了用户认证的Tunnel-Group-Lock=RA。但是，用户锁定，因此意味着组锁定执行。

对于相反的配置，外部组政策返回一个特定组名(通道组LOCK)，当设法禁用组锁定一个特定用户的(IPSec-User-Group-Lock=0)时，并且组锁定为该用户仍然被强制了执行。

这确认不再使用属性。该属性用于旧有VPN3000系列。打开Cisco Bug ID CSCui34066。

Easy VPN的Cisco IOS本地组锁定

在组配置下的本地锁定选择在Cisco IOS工作不同地跟在ASA。在ASA，您指定用户锁定的组名。Cisco IOS锁定选择(没有参数) enable (event)另外的验证和组带有用户名(格式user@group)与IKEID (组名)比较。

欲知更多信息，参考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
```

这显示组锁定验证的那为GROUP1启用。对于GROUP1，唯一的允许用户是cisco1@GROUP1。对于第2组(没有组锁定)，两个用户能登录。

对于成功认证，请以GROUP1使用cisco1@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
```

对于验证，请以GROUP1使用cisco2@GROUP2 ：

```
*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 ：用户VPN组是AAA服务器返回的RADIUS属性，并且可以为用户认证仅应用(组锁定使用了组)。两个功能是补充的，并且他们应用在不同的阶段。

欲知更多信息，参考Easy VPN配置指南， Cisco IOS版本15M&T。

它跟组锁定不同地运作和仍然允许您取得同一种结果。差异是属性必须有一个特定值(类似ASA)，并且特定值与互联网安全协会和密钥管理协议(ISAKMP)组名(IKEID)比较;如果它不配比，则连接发生故障。这是发生了什么，如果更改前一个示例为了有客户端AAA认证和暂时禁用组锁定：

```
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
```
注意ipsec ：用户VPN组属性为用户定义，并且组锁定为组定义。

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

当cisco2用户设法登录与GROUP1时，此错误报告：

```
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比较。

这样，同一个目标为组锁定达到至于。您看到现在，最终用户不需要提供user@group作为用户名，但是能使用用户(没有@group)。

对于组锁定，应该使用cisco1@GROUP1，因为Cisco IOS剥离最后一部分(以后@)并且它与IKEID (组名)比较。

ipsec ：因为该用户在ACS和特定ipsec，定义用户VPN组，使用仅cisco1在Cisco VPN Client是满足的：用户VPN组在这种情况下返回(它是=GROUP1)，并且该属性对IKEID比较。

Cisco IOS AAA ipsec ：用户VPN组和组锁定Easy VPN的

为什么不应该同时使用两个功能？

您能再添加组锁定：

```
crypto isakmp client configuration group GROUP1
group-lock
crypto isakmp client configuration group GROUP2
group-lock
```
这是流：

1. 思科VPN用户配置GROUP1连接并且连接。
2. 积极模式相位是成功的，并且Cisco IOS发送一个Xauth要求用户名和密码。
3. 思科VPN用户接收弹出式，并且输入cisco1@GROUP1用户名用在ACS定义的正确密码。
4. Cisco IOS执行检查组锁定：它剥离在用户名提供的组名并且它与IKEID比较。它是成功的。
5. Cisco IOS发送AAA请求到ACS服务器(为用户cisco1@GROUP1)。
6. ACS返回与**ipsec:user-vpn-group=GROUP1的**－RADIUS接受。

7. Cisco IOS进行第二个验证;这次，它RADIUS属性提供的组与IKEID比较。

当它失效在步骤4 (组锁定)，错误被记录，在提供凭证之后：

```
*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
```

当它失效在步骤7 (ipsec ：在接收AAA认证的后， RADIUS属性用户VPN组)，错误返回：

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

IOS WebVPN组洛克

在ASA，通道组LOCK可以用于所有远程访问虚拟专用网服务(IPSec， SSL， WebVPN)。Cisco IOS组锁定和ipsec ：用户VPN组，它为IPSec (Easy VPN Server)仅工作。为了应该使用特定WebVPN上下文(和附加的组政策的)组锁定特定用户，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，有两上下文：C1和C2。每上下文有其与特定设置的自己的组政策。C1允许AnyConnect访问。gataway配置为了听两上下文：C1和C2。

当cisco1用户访问有https://10.48.67.137/C1的C1上下文，验证域添加**C1**并且验证本地定义的(列表列表) cisco1@C1用户名：


```
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"
```

当您设法登陆与cisco2作为用户名时，当您访问C1上下文(时https://10.48.67.137/C1)，此失败报告：

```
*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的cisco2@C1。cisco用户不能登录到任何上下文。

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， 9.1
- 技术支持和文档 - Cisco Systems