ASA and Cisco IOS Group−lock Features and AAA Attributes and WebVPN Configuration Example

Document ID: 117634

Contributed by Michal Garcarz, Cisco TAC Engineer.
Apr 25, 2014

Contents

Introduction

This article describes the group−locking features on the Cisco Adaptive Security Appliance (ASA) and in Cisco IOS® and presents the behavior for different Authentication, Authorization, and Accounting (AAA) attributes. For Cisco IOS, the difference between the group−lock and the user−vpn−groups is explained along with an example that uses both complementary features at the same time. There is also a Cisco IOS WebVPN example with authentication domains.

Prerequisites

Requirements

Cisco recommends that you have baisc knowledge of these topics:

- ASA CLI configuration and Secure Sockets Layer (SSL) VPN configuration
- Remote access VPN configuration on the ASA and Cisco IOS

Components Used

The information in this document is based on these software versions:

- ASA software, Version 8.4 and later
- Cisco IOS, Version 15.1 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurations

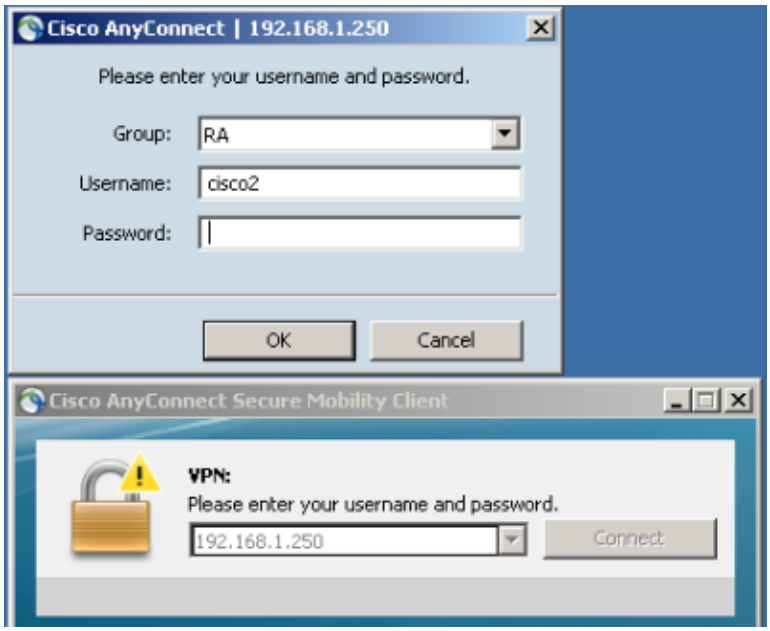
ASA Local Group−lock

You can define this attribute under the user or the group−policy. Here is an example for the local user attribute.

```
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
```

The cisco user is able to use only the RA tunnel−group, and the cisco2 user is able to use only the RA2 tunnel−group.

If the cisco2 user chooses the RA tunnel−group, then the connection is denied:

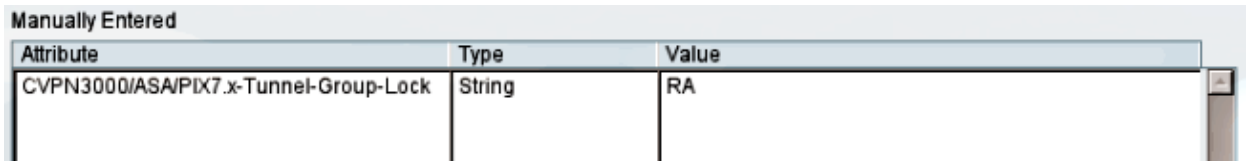



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

ASA with AAA Attribute VPN3000/ASA/PIX7.x−Tunnel−Group−Lock

Attribute 3076/85 (Tunnel−Group−Lock) that is returned by the AAA server does exactly the same. It can be passed along with the user or the policy−group (or Internet Engineering Task Force (IETF) attribute 25) authentication and locks the user in a specific tunnel−group.

Here is an example authorization profile on the Cisco Access Control Server (ACS):



When the attribute is returned by AAA, the RADIUS debugs indicate it:

```
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
```

The result is the same when you try to access the RA2 tunnel−group while group−locked within the RA tunnel−group:

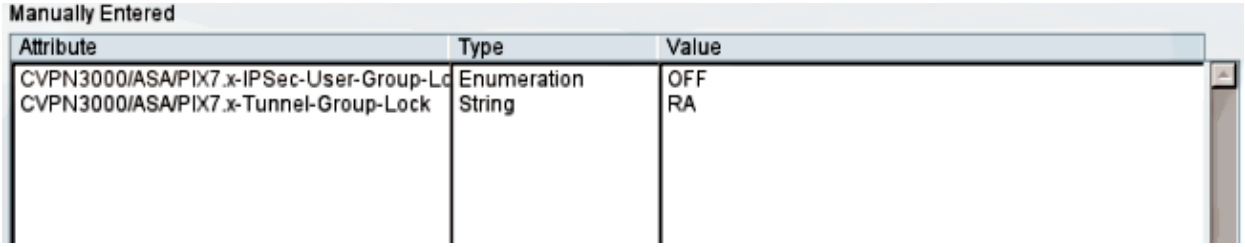
```
May 17 2013 17:41:33: %ASA−4−113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

ASA with AAA attribute VPN3000/ASA/PIX7.x−IPSec−User−Group−Lock

This attribute is also taken from the VPN3000 directory inherited by the ASA. It is still present in the 8.4 configuration guide (although it is removed in a newer version of configuration guide) and described as:

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

It appears that the attribute could be used in order to disable group−locking, even if the Tunnel−Group−Lock attribute is present. If you try to return that attribute set to 0 along with the Tunnel−Group−Lock (this is still just user authentication), here is what happens. It looks strange when you try to disable group−locking while returning a specific tunnel−group name:



Debugs show:

```
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
```

This yields the same result (group locking has been enforced, and the IPSec−User−Group−Lock has not been taken into consideration).

```
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>
```

The external group−policy returned IPSec−User−Group−Lock=0 and also got Tunnel−Group−Lock=RA for user authentication. Still, the user has been locked, which means that Group Locking has been performed.

For the opposite configuration, the external group−policy returns a specific tunnel−group name (Tunnel−Group−Lock) while it tries to disable group−locking for a specific user (IPSec−User−Group−Lock=0), and group−locking has still been enforced for that user.

This confirms that the attribute is not used anymore. That attribute was used in the old VPN3000 series. Cisco bug ID CSCui34066 has been opened.

Cisco IOS Local Group−lock for Easy VPN

The local group−lock option under the group configuration in Cisco IOS works differently than on the ASA. On the ASA, you specify the tunnel−group name to which the user is locked. The Cisco IOS group−lock option (there are no arguments) enables additional verification and compares the group provided with the username (format user@group) with IKEID (group name).

For more information, refere to the Easy VPN Configuration Guide, Cisco IOS Release 15M&T.

Here is an example:

```
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
```

This shows that group−locking verification is enabled for GROUP1. For GROUP1, the only allowed user is cisco1@GROUP1. For GROUP2 (no group−lock), both users are able to log in.

For successful authentication, use cisco1@GROUP1 with 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
```

For authentication, use cisco2@GROUP2 with 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

The ***ipsec:user−vpn−group*** is the RADIUS attribute returned by the AAA server, and it can be applied only for user authentication (group−lock was used for the group). Both features are complementary, and they are applied at different stages.

For more information, refer to the Easy VPN Configuration Guide, Cisco IOS Release 15M&T.

It works differently than the group−lock and still allows you to achieve the same result. The difference is that the attribute must have a specific value (like for the ASA) and that specific value is compared with the Internet Security Association and Key Management Protocol (ISAKMP) group name (IKEID); if it does not match, then the connection fails. Here is what happens if you change the previous example in order to have client AAA authentication and disable group−lock for now:

```
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
```

Notice that the ipsec:user−vpn−group attribute is defined for the user and group−lock is defined for the group.

On the ACS, there are two users, cisco1 and cisco2. For the cisco1 user, this attribute is returned: ***ipsec:user−vpn−group=GROUP1***. For the cisco2 user, this attribute is returned: ***ipsec:user−vpn−group=GROUP2***.

When the cisco2 user tries to log in with GROUP1, this error is reported:

```
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
```

This is because the ACS for the cisco2 user returns ***ipsec:user−vpn−group=GROUP2***, which is compared by Cisco IOS to GROUP1.

This way, the same goal has been achieved as for the group−lock. You can see that right now, the end user does not need to provide user@group as the username, but can use user (without the @group).

For group−lock, cisco1@GROUP1 should be used, because Cisco IOS stripped the last part (after @) and compared it with IKEID (group name).

For the ipsec:user−vpn−group, it is sufficient to use only cisco1 in the Cisco VPN Client, because that user is defined on the ACS and the specific ipsec:user−vpn−group is returned (in this case, it is =GROUP1) and that attribute is compared against IKEID.

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

Why should you not use both features at the same time?

You can add group−lock again:

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

Here is the flow:

1. The Cisco VPN user configures the GROUP1 connection and connects.

2. The aggressive mode phase is successful, and Cisco IOS sends an xAuth request for the username and password.
3. The Cisco VPN user receives a popup, and enters the cisco1@GROUP1 username with the correct password defined on the ACS.
4. Cisco IOS performs a check for the group−lock: it strips the group name provided in the username and compares it with IKEID. It is successful.
5. Cisco IOS sends an AAA request to the ACS server (for user cisco1@GROUP1).
6. ACS returns a RADIUS−Accept with ***ipsec:user−vpn−group=GROUP1***.
7. Cisco IOS performs a second verification; this time, it compares the group provided by the RADIUS attribute with IKEID.

   When it fails at Step 4 (group lock), the error is logged immediately after it provides credentials:

```
*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
```

   When it fails at Step 7 (ipsec:user−vpn−group), the error is returned after it receives the RADIUS attribute for AAA authentication:

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

IOS Webvpn Group Lock

On the ASA, the Tunnel−Group−Lock can be used for all remote access VPN services (IPSec, SSL, WebVPN). For the Cisco IOS group−lock and the ipsec:user−vpn−group, it works only for IPSec (easy VPN server). In order to group−lock specific users in specific WebVPN contexts (and attached group−policies), authentication domains should be used.

Here is an example:

```
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
```

In the next example, there are two contexts: C1 and C2. Each context has its own group−policy with specific settings. C1 allows for AnyConnect access. The gataway is configured in order to listen to both contexts: C1 and C2.

When the cisco1 user accesses the C1 context with https://10.48.67.137/C1, the authentication domain adds ***C1*** and authenticates against the locally defined (list LIST) cisco1@C1 username:


```
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"
```

When you try to log in with cisco2 as a username while you access the C1 context (https://10.48.67.137/C1), this failure is reported:

```
*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
```

This is because there is no cisco2@C1 user defined. the cisco user is not able to log in to any context.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- ***Easy VPN Configuration Guide, Cisco IOS Release 15M&T***
- ***Cisco ASA Series VPN CLI Configuration Guide, 9.1***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Apr 25, 2014 Document ID: 117634