ASA および Cisco IOS グループ ロック機能と AAA 属性および WebVPN の設定例

内容

概要

この記事では、Cisco 適応型セキュリティ アプライアンス（ASA）と Cisco IOS® でのグループ ロック（group-lock）機能について説明しています。また、認証、認可、およびアカウンティング（AAA）の各種属性の動作も示しています。Cisco IOS については、group-lock と user-vpn-group の違いについて、両方の相互に補完する機能を同時に使用する例とともに説明しています。また、認証ドメインを使用した Cisco IOS WebVPN の例も示しています。

前提条件

要件

次の項目に関して基本的な知識があることが推奨されます。

- ASA CLI の設定およびセキュア ソケット レイヤ（SSL）VPN の設定
- ASA と Cisco IOS でのリモート アクセス VPN の設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ASA ソフトウェア バージョン 8.4 以降
- Cisco IOS バージョン 15.1 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

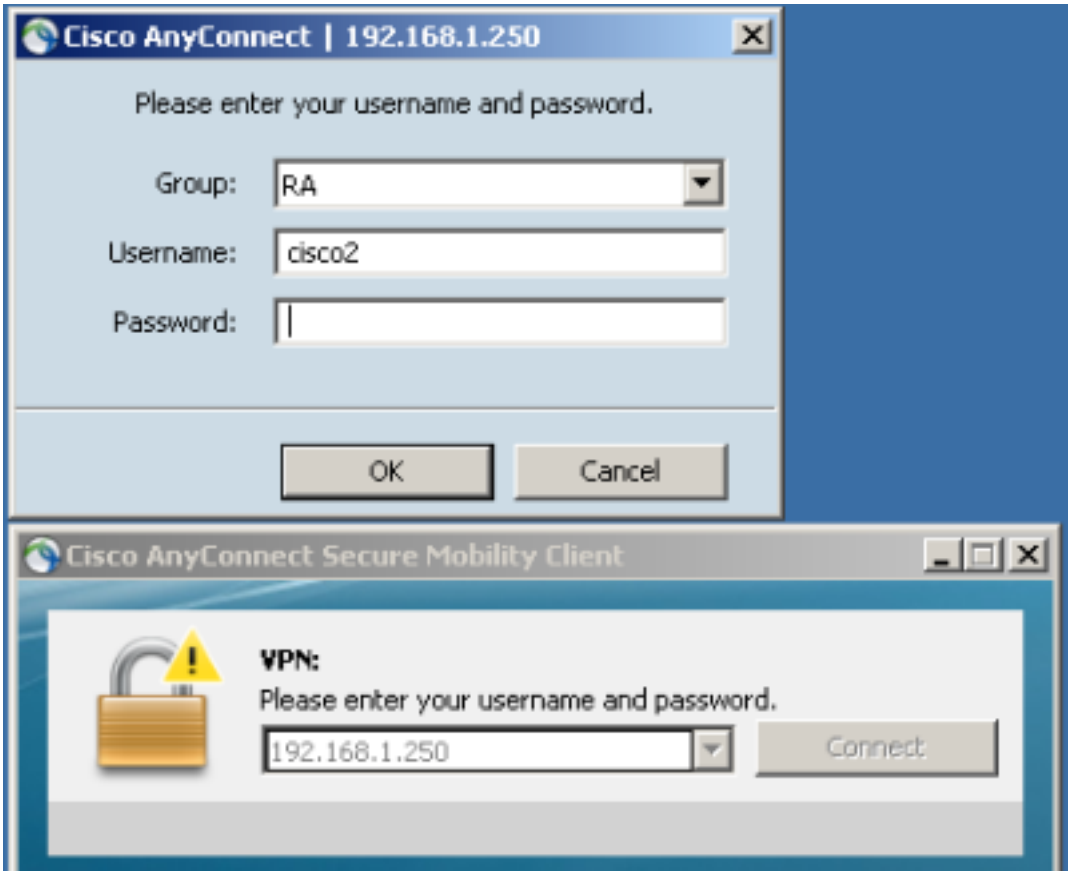
ASA ローカルの group-lock

この属性は、ユーザまたは group-policy で定義できます。次に、ローカル ユーザの属性の例を示します。

```
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
```

ユーザの cisco は RA tunnel-group だけを使用でき、ユーザの cisco2 は RA2 tunnel-group だけを使用できます。

ユーザの cisco2 が RA tunnel-group を選択すると、次に示すように接続が拒否されます。

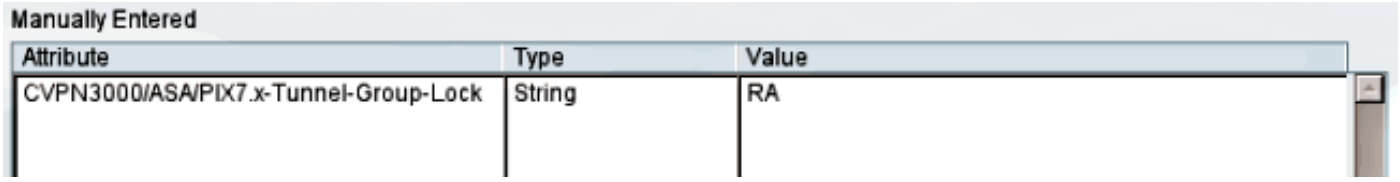



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

AAA 属性の VPN3000/ASA/PIX7.x-Tunnel-Group-Lock を使用した ASA

AAA サーバから返される属性の 3076/85（Tunnel-Group-Lock）では、まったく同じ動作を行います。この属性はユーザまたは policy-group（または Internet Engineering Task Force（IETF）の属性 25）認証とともに渡すことができ、そのユーザを特定の tunnel-group にロックします。

次に Cisco Access Control Server（ACS）の許可プロファイルの例を示します。



属性が AAA から返されると、RADIUS デバッグによってその属性が次のように表示されます。

```
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
```

結果は、RA2 tunnel-group にアクセスを試みるとともに、RA tunnel-group 内で group-lock される場合と同じです。

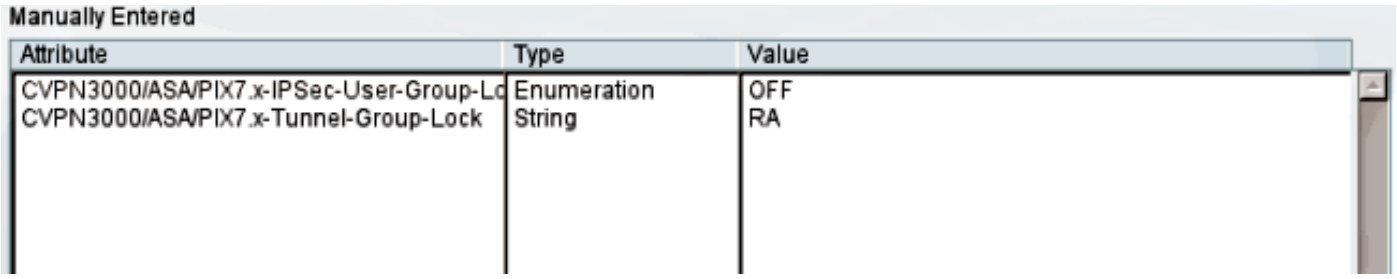
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

AAA 属性の VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock を使用した ASA

この属性も、ASA によって継承された VPN3000 ディレクトリから取得されます。この属性は、8.4 の構成ガイドにまだ存在し（ただし、新しいバージョンの構成ガイドでは削除されました）、次のように説明されています。

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

Tunnel-Group-Lock 属性が存在している場合でも、この属性はグループ ロックを無効にするために使用できるように見えます。Tunnel-Group-Lock とともに 0 に設定したこの属性を返そうとする（これは、まだ単なるユーザ認証です）とどうなるかを下に示します。これは、グループ ロックの無効化を試みるとともに、特定の tunnel-group 名を返す場合に奇妙に思われることでしょう。



デバッグでは、次のように表示されます。

```
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
```

これによって、同じ結果（グループ ロックが適用されたままですが、IPSec-User-Group-Lock は考慮されなくなりました）が得られます。

```
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
```

外部の group-policy では IPSec-User-Group-Lock=0 を返し、ユーザ認証用に Tunnel-Group-Lock=RA も受け取りました。ただし、そのユーザは引き続きロックされたままで、グループ ロックが実行されたままであることを意味します。

反対側の設定では、外部の group-policy が特定の tunnel-group の名前（Tunnel-Group-Lock）を返すとともに、特定のユーザの group-lock の無効化（IPSec-User-Group-Lock=0）を試みますが、そのユーザに対してはグループ ロックが引き続き適用されたままです。

これにより、この属性がこれ以上使用されないことが確認されます。この属性は、古い VPN3000 シリーズで使用されていました。Cisco Bug ID の CSCui34066 が開かれています。

Easy VPN に関する Cisco IOS ローカルの group-lock

Cisco IOS のグループ設定でのローカル group-lock のオプションは、ASA 上とは動作が異なります。ASA では、ユーザがロックされている tunnel-group の名前を指定します。Cisco IOS の group-lock オプション（引数なし）では、追加の検証が可能になり、username（形式：user@group）で提供されたグループが IKEID（グループ名）と比較されます。

詳細については、「Easy VPN 構成ガイド、Cisco IOS リリース 15M&T」を参照してください。

以下が一例です。

```
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
```

これは、GROUP1に対してグループロック検証が有効になっていることを示しています。GROUP1に対して許可されている唯一のユーザはcisco1@GROUP1です。GROUP2（グループロックなし）に対しては、両方のユーザがログインできます。

次に示すように、認証に成功するには、GROUP1 とともに cisco1@GROUP1 を使用します。

```
*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
```

次に示すように、認証のためには、GROUP1 とともに cisco2@GROUP2 を使用します。

```
*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は、AAAサーバから返されるRADIUS属性で、ユーザ認証にのみ適用できます（group-lockがグループに使用されました）。 両方の機能は相互に補完的なもので、さまざまな局面で適用されます。

詳細については、「Easy VPN 構成ガイド、Cisco IOS リリース 15M&T」を参照してください。

この属性は group-lock とは動作が異なりますが、同じ結果が得られます。違いは、この属性には特定の値が必要であること（ASA の場合と同様）、および特定の値が Internet Security Association and Key Management Protocol（ISAKMP）のグループ名（IKEID）と比較されることです。それらが一致しない場合、接続は失敗します。クライアントに AAA 認証を受けさせ、group-lock を現時点では無効にするために前の例を変更した場合、どうなるかを次に示します。

```
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
```

ユーザにipsec:user-vpn-group属性が定義され、グループにgroup-lockが定義されていることに注意してください。

ACSには、cisco1とcisco2の2つのユーザがあります。cisco1ユーザの場合、次の属性が返されます。**ipsec:user-vpn-group=GROUP1**。cisco2ユーザの場合、**ipsec:user-vpn-group=GROUP2という属性が返されます**。

ユーザの cisco2 が GROUP1 でログインしようとすると、次のエラーが報告されます。

```
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
```

これは、ユーザの cisco2 の ACS が、Cisco IOS で GROUP1 と比較する **ipsec:user-vpn-group=GROUP2** を返すためです。

このようにして、group-lock の場合と同様に、同じ目標が達成されました。エンド ユーザがユー

ザ名として user@group を入力する必要はありませんが、user (@group なしで) を使用できることがここで分かるはずです。

group-lock の場合は、cisco1@GROUP1 を使用する必要があります。これは、Cisco IOS で最後の部分 (@ 以降) が除去されて、残りの部分が IKEID (グループ名) と比較されるためです。

ipsec:user-vpn-groupでは、Cisco VPN Clientでcisco1だけを使用すれば十分です。そのユーザはACSで定義され、特定のipsec:user-vpn-groupが返され (この場合は=GROUP1)、その属性はIKEIDと比較されます。

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

両方の機能を同時に使用すべきではない理由を以下に示します。

次のように、group-lock は再度追加できます。

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

ここで、フローを示します。

1. Cisco VPN ユーザが GROUP1 の接続を設定して、接続します。
2. アグレッシブ モードのフェーズが成功し、Cisco IOS によってユーザ名とパスワードを求める xAuth 要求が送信されます。
3. Cisco VPN ユーザがポップアップを受け取って、ACS 上で定義された正しいパスワードとともにユーザ名の cisco1@GROUP1 を入力します。
4. Cisco IOS で、group-lock のチェックが実行されます。つまり、ユーザ名に指定されたグループ名が除去されて、IKEID と比較されます。一致して比較が成功します。
5. Cisco IOS で、ACS サーバに (ユーザーの cisco1@GROUP1 を求めて) AAA 要求が送信されます。

6. ACS によって、**ipsec:user-vpn-group=GROUP1** とともに RADIUS-Accept が返されます。

7. Cisco IOS で、2 番目の確認が実行されます。つまり、今度は RADIUS 属性によって提供されたグループが IKEID と比較されます。

   ステップ 4 (グループ ロック) で比較が失敗した場合、クレデンシャル (資格情報) が提供された直後に次のエラーがログに記録されます。

   ```
   *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
   ```

   ステップ7(ipsec:user-vpn-group)で障害が発生すると、AAA認証のRADIUS属性を受信した後にエラーが返されます。

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

IOS WebVPN のグループ ロック

ASA 上では、Tunnel-Group-Lock をすべてのリモート アクセス VPN サービス（IPsec、SSL、WebVPN）に対して使用できます。 Cisco IOSグループロックおよびipsec:user-vpn-groupの場合、IPSec（easy VPNサーバ）でのみ動作します。 特定の WebVPN コンテキスト（および付加された group-policy）内の特定のユーザに対して group-lock を行うには、認証ドメインを使用する必要があります。

以下が一例です。

```
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
```

この例には、2 つのコンテキストC1とC2。各コンテキストには、固有の設定を持つ独自のグループポリシーがあります。C1 では AnyConnect アクセスが許可されています。両方のコンテキスト C1 と C2 があります。

次に示すように、ユーザの cisco1 が https://10.48.67.137/C1 を使用して C1 のコンテキストにアクセスすると、認証ドメインでは **C1 が追加されて、ローカルで定義された (list LIST) cisco1@C1 ユーザ名と照合して認証されます。**


```
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"
```

C1 コンテキスト (https://10.48.67.137/C1) にアクセス中に、ユーザ名として cisco2 でログインしようとすると、次の障害が報告されます。

```
*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
```

これは、ユーザの cisco2@C1 が定義されていないためです。ユーザの cisco は、どのコンテキストにもログインできません。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Easy VPN 構成ガイド、Cisco IOS リリース 15M&T
- Cisco ASA シリーズ VPN CLI 構成ガイド 9.1
- テクニカル サポートとドキュメント – Cisco Systems