Exemplo de recursos de bloqueio de grupo do ASA e do Cisco IOS e atributos AAA e configuração da WebVPN

Contents

Introduction

Este artigo descreve os recursos de bloqueio de grupo no Cisco Adaptive Security Appliance (ASA) e no Cisco IOS® e apresenta o comportamento para diferentes atributos de Autenticação, Autorização e Contabilidade (AAA). Para o Cisco IOS, a diferença entre o group-lock e os user-vpn-groups é explicada junto com um exemplo que usa ambos os recursos complementares ao mesmo tempo. Há também um exemplo do Cisco IOS WebVPN com domínios de autenticação.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- Configuração do ASA CLI e configuração de VPN SSL (Secure Sockets Layer)
- Configuração de VPN de acesso remoto no ASA e no Cisco IOS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software ASA, versão 8.4 e posterior
- Cisco IOS, versão 15.1 e posterior

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.

Configurações

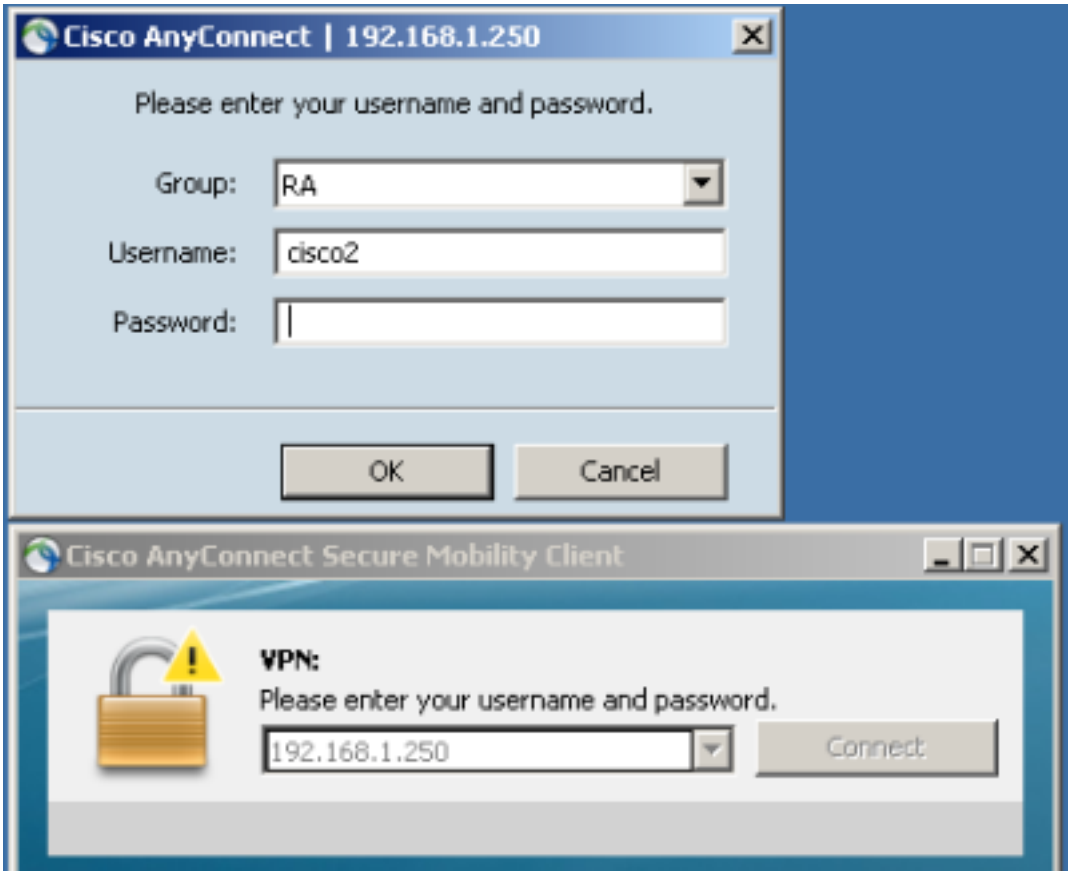
Bloqueio de grupo local do ASA

Você pode definir esse atributo no usuário ou na política de grupo. Aqui está um exemplo do atributo de usuário local.

```
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
```

O usuário cisco pode usar somente o grupo de túnel RA e o usuário cisco2 pode usar somente o grupo de túnel RA2.

Se o usuário cisco2 escolher o grupo de túnel RA, a conexão será negada:

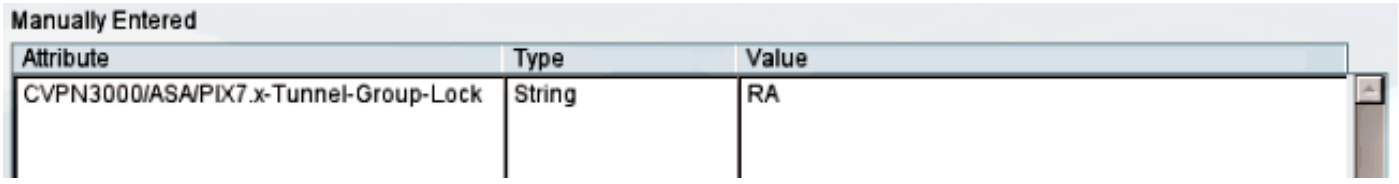



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA com atributo AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

O atributo 3076/85 (Tunnel-Group-Lock) retornado pelo servidor AAA faz exatamente o mesmo. Ele pode ser passado junto com a autenticação do usuário ou do grupo de políticas (ou atributo Internet Engineering Task Force (IETF) 25) e bloqueia o usuário em um grupo de túneis específico.

Aqui está um exemplo de perfil de autorização no Cisco Access Control Server (ACS):



Quando o atributo é retornado por AAA, as depurações de RADIUS indicam:

```
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
```

O resultado é o mesmo quando você tenta acessar o grupo de túneis RA2 enquanto o grupo está bloqueado no grupo de túneis RA:

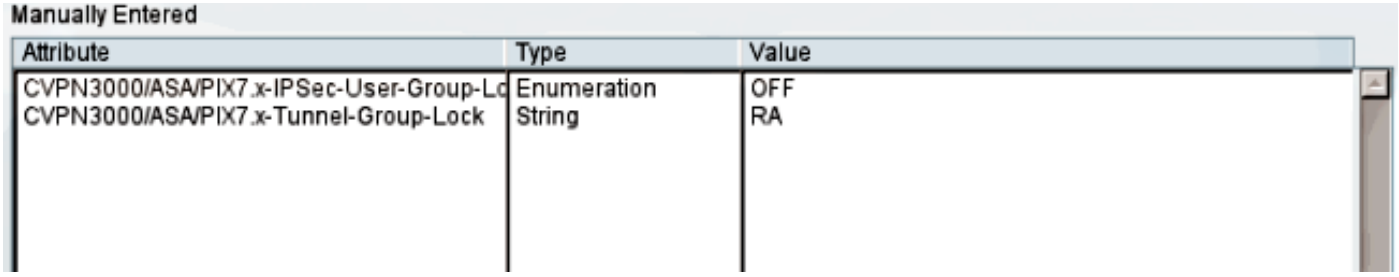
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA com atributo AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Esse atributo também é retirado do diretório VPN3000 herdado pelo ASA. Ele ainda está presente no guia de configuração 8.4 (embora seja removido em uma versão mais recente do guia de configuração) e descrito como:

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

Parece que o atributo pode ser usado para desabilitar o bloqueio de grupo, mesmo que o atributo Tunnel-Group-Lock esteja presente. Se você tentar retornar esse atributo definido como 0 junto com o Tunnel-Group-Lock (ainda é apenas a autenticação do usuário), aqui está o que acontece. Parece estranho quando você tenta desabilitar o bloqueio de grupo ao retornar um nome de grupo de túnel específico:



As depurações mostram:

```
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
```

Isso resulta no mesmo resultado (o bloqueio de grupo foi imposto e o IPSec-User-Group-Lock não foi considerado).

```
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
```

A política de grupo externa retornou IPSec-User-Group-Lock=0 e também obteve Tunnel-Group-Lock=RA para autenticação do usuário. Ainda assim, o usuário foi bloqueado, o que significa que o Bloqueio de Grupo foi realizado.

Para a configuração oposta, a política de grupo externa retorna um nome de grupo de túnel específico (Tunnel-Group-Lock) enquanto tenta desabilitar o bloqueio de grupo para um usuário específico (IPSec-User-Group-Lock=0), e o bloqueio de grupo ainda foi forçado para esse usuário.

Isso confirma que o atributo não é mais usado. Esse atributo foi usado na antiga série VPN3000. O bug da Cisco ID CSCui34066 foi aberto.

Bloqueio de grupo local do Cisco IOS para Easy VPN

A opção local group-lock na configuração do grupo no Cisco IOS funciona de forma diferente da do ASA. No ASA, especifique o nome do grupo de túneis ao qual o usuário está bloqueado. A opção group-lock do Cisco IOS (não há argumentos) permite verificação adicional e compara o grupo fornecido com o nome de usuário (formato user@group) com IKEID (nome do grupo).

Para obter mais informações, refere ao Guia de Configuração de VPN Fácil, Cisco IOS versão 15M&T.

Aqui está um exemplo:

```
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
```

Isso mostra que a verificação de bloqueio de grupo está habilitada para GROUP1. Para GROUP1, o único usuário permitido é cisco1@GROUP1. Para GROUP2 (sem bloqueio de grupo), ambos os usuários podem fazer logon.

Para obter uma autenticação bem-sucedida, use cisco1@GROUP1 com 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
```

Para autenticação, use cisco2@GROUP2 com GROUP1:

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

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

O **ipsec:user-vpn-group** é o atributo RADIUS retornado pelo servidor AAA e pode ser aplicado somente para autenticação de usuário (o group-lock foi usado para o grupo). Ambas as características são complementares e são aplicadas em estágios diferentes.

Para obter mais informações, consulte o Easy VPN Configuration Guide, Cisco IOS versão 15M&T.

Ele funciona de forma diferente do group-lock e ainda permite que você obtenha o mesmo resultado. A diferença é que o atributo deve ter um valor específico (como o ASA) e esse valor específico é comparado com o nome do grupo ISAKMP (Internet Security Association and Key Management Protocol); se não corresponder, a conexão falhará. Aqui está o que acontece se você alterar o exemplo anterior para ter a autenticação de AAA do cliente e desativar o group-lock para o momento:

```
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
```

Observe que o atributo ipsec:user-vpn-group está definido para o usuário e que group-lock está definido para o grupo.

No ACS, há dois usuários, cisco1 e cisco2. Para o usuário cisco1, este atributo é retornado: **ipsec:user-vpn-group=GROUP1**. Para o usuário cisco2, este atributo é retornado: **ipsec:user-vpn-group=GROUP2**.

Quando o usuário cisco2 tenta fazer login com o GROUP1, esse erro é relatado:

```
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
```

Isso ocorre porque o ACS para o usuário cisco2 retorna **ipsec:user-vpn-group=GROUP2**, que é comparado pelo Cisco IOS ao GROUP1.

Desta forma, o mesmo objetivo foi alcançado para o bloqueio de grupo. Você pode ver que, no momento, o usuário final não precisa fornecer user@group como nome de usuário, mas pode usar o usuário (sem o @group).

Para o group-lock, cisco1@GROUP1 deve ser usado, pois o Cisco IOS removeu a última parte (depois de @) e comparou com IKEID (nome do grupo).

Para o ipsec:user-vpn-group, é suficiente usar somente cisco1 no Cisco VPN Client, pois esse usuário é definido no ACS e o ipsec específico:user-vpn-group é retornado (nesse caso, é =GROUP1) e esse atributo é comparado ao IKEID.

Cisco IOS AAA ipsec:user-vpn-group e Group-lock para Easy VPN

Por que você não deve usar os dois recursos ao mesmo tempo?

Você pode adicionar o group-lock novamente:

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

Aqui está o fluxo:

1. O usuário do Cisco VPN configura a conexão GROUP1 e se conecta.
2. A fase de modo agressivo foi bem-sucedida e o Cisco IOS envia uma solicitação xAuth para o nome de usuário e a senha.
3. O usuário do Cisco VPN recebe um pop-up e insere o nome de usuário cisco1@GROUP1 com a senha correta definida no ACS.
4. O Cisco IOS executa uma verificação para o group-lock: retira o nome do grupo fornecido no nome de usuário e o compara com IKEID. É um sucesso.
5. O Cisco IOS envia uma solicitação AAA ao servidor ACS (para o usuário cisco1@GROUP1).
6. O ACS retorna um RADIUS-Accept com **ipsec:user-vpn-group=GROUP1**.
7. O Cisco IOS executa uma segunda verificação; desta vez, ele compara o grupo fornecido pelo atributo RADIUS com IKEID.

   Quando ele falha na Etapa 4 (bloqueio de grupo), o erro é registrado imediatamente após fornecer as credenciais:

```
*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
```

Quando ele falha na Etapa 7 (ipsec:user-vpn-group), o erro é retornado depois de receber o atributo RADIUS para autenticação AAA:

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

Bloqueio de Grupo Webvpn do IOS

No ASA, o Tunnel-Group-Lock pode ser usado para todos os serviços de VPN de acesso remoto (IPSec, SSL, WebVPN). Para o group-lock do Cisco IOS e o ipsec:user-vpn-group, ele funciona somente para IPSec (fácil servidor VPN). Para bloquear em grupo usuários específicos em contextos WebVPN específicos (e políticas de grupo anexadas), os domínios de autenticação devem ser usados.

Aqui está um exemplo:

```
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
```

No próximo exemplo, há dois contextos: C1 e C2. Cada contexto tem sua própria política de grupo com configurações específicas. C1 permite acesso ao AnyConnect. O gateway é configurado para ouvir os dois contextos: C1 e C2.

Quando o usuário cisco1 acessa o contexto C1 com https://10.48.67.137/C1, o domínio de autenticação adiciona **C1** e autentica em relação ao nome de usuário (lista) definido localmente cisco1@C1:


```
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"
```

Quando você tenta fazer login com cisco2 como nome de usuário enquanto acessa o contexto C1 (https://10.48.67.137/C1), essa falha é relatada:

```
*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
```

Isso porque não há um usuário cisco2@C1 definido. o usuário da cisco não consegue fazer login em nenhum contexto.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração Easy VPN, Cisco IOS versão 15M&T
- Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1
- Suporte Técnico e Documentação - Cisco Systems