ASA и функции Group-lock Cisco IOS и атрибуты AAA и пример конфигурации WebVPN

Содержание

Введение

Эта статья описывает блокирующие группу функции на устройстве адаптивной защиты Cisco (ASA) и в Cisco IOS® и представляет поведение для других атрибутов Аутентификации, авторизации и учета (AAA). Для Cisco IOS различие между group-lock и пользовательскими группами vpn объяснено наряду с примером, который использует обе дополнительных функции в то же время. Существует также пример Cisco IOS WebVPN с опознавательными доменами.

Предварительные условия

Требования

Cisco рекомендует иметь основное знание этих тем:

- Настройка интерфейса командной строки ASA и конфигурация VPN Уровня

защищенных сокетов (SSL)
- Конфигурация VPN для удаленного доступа на ASA и Cisco IOS

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение ASA, Версия 8.4 и позже
- Cisco IOS, Версия 15.1 и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Конфигурации

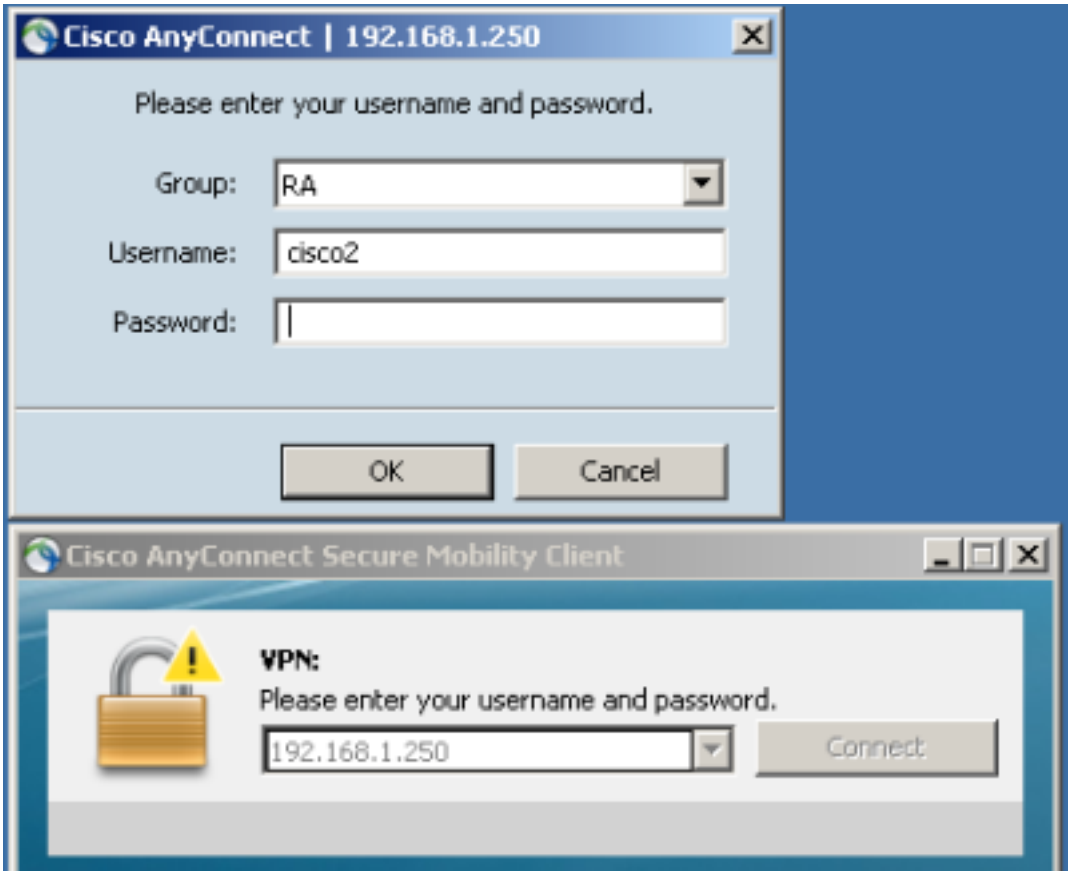
ASA локальный Group-lock

Можно определить этот атрибут при пользователе или групповой политике. Вот пример для атрибута локального пользователя.

```
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
```

Пользователь Cisco в состоянии использовать только туннельную группу RA, и cisco2 пользователь в состоянии использовать только туннельную группу RA2.

Если cisco2 пользователь выбирает туннельную группу RA, то соединение запрещено:

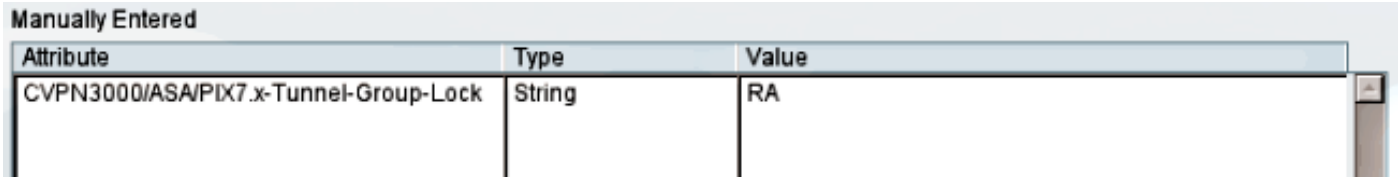



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

ASA с Атрибутом AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

Припишите 3076/85 (Туннельный Group-lock), который возвращен AAA-сервером, делает точно то же. Это можно передать наряду с пользователем или группой политик (или инженерная группа по развитию Интернета (IETF) приписывают 25), аутентификация, и блокирует пользователя в определенной туннельной группе.

Вот профиль авторизации в качестве примера на Access Control Server (ACS) Cisco:



Когда атрибут возвращен AAA, отладки Радиуса указывают на него:

```
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
```

Когда вы пытаетесь обратиться к туннельной группе RA2, в то время как блокировано группой в туннельной группе RA, результатом является то же:

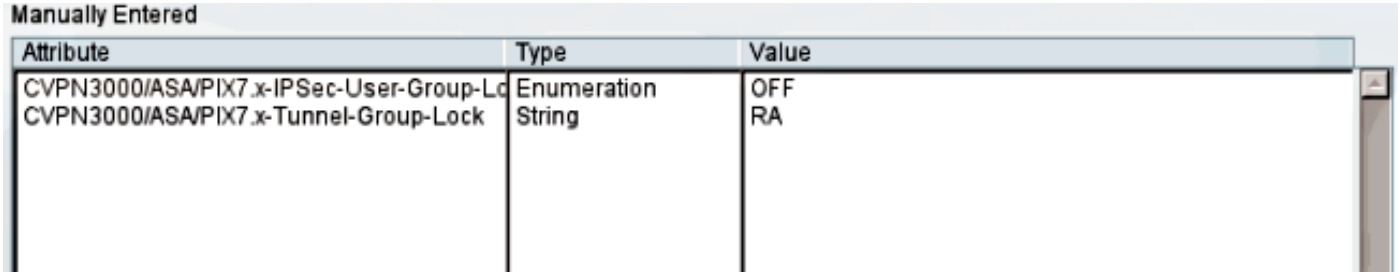
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

ASA с атрибутом AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Этот атрибут также взят из каталога VPN3000, наследованного ASA. Это все еще присутствует в 8.4 руководствах по конфигурации (невзирая на то, что это удалено в более новой версии руководства по конфигурации), и описал как:

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

Кажется, что атрибут мог использоваться для отключения блокировки группы, даже если присутствует атрибут Туннельного Group-lock. При попытке возвратить тот набор атрибута к 0 наряду с Туннельным Group-lock (это - все еще просто проверка подлинности пользователя), вот то, что происходит. Когда вы пытаетесь отключить блокировку группы при возврате определенного имени группы туннелей, выглядит странным:



Отладки показывают:

```
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
```

Это приводит к тому же результату (блокировка группы была принуждена, и IPSec-User-Group-Lock не был учтен).

```
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>
```

Внешняя групповая политика возвратилась IPSec-User-Group-Lock=0 и также добралась Tunnel-Group-Lock=RA для проверки подлинности пользователя. Однако, пользователь был блокирован, что означает, что была выполнена Блокировка Группы.

Для противоположной конфигурации внешняя групповая политика возвращает определенное имя группы туннелей (Туннельный Group-lock), в то время как это пытается отключить блокировку группы для определенного пользователя (IPSec-User-Group-Lock=0), и блокировка группы была все еще принуждена для того пользователя.

Это подтверждает, что атрибут больше не используется. Тот атрибут использовался в старом серии VPN3000. Идентификатор ошибки Cisco CSCui34066 был открыт.

Cisco IOS локальный Group-lock для легкой VPN

Локальная опция group-lock под конфигурацией группы в Cisco IOS работает по-другому, чем на ASA. На ASA вы задаете имя группы туннелей, к которому блокирован пользователь. Опция group-lock Cisco IOS (нет никаких аргументов), включает дополнительную проверку и выдерживает сравнение, группа, которой предоставляют имя пользователя (отформатируйте user@group) с IKEID (имя группы).

Для получения дополнительной информации, передруг Руководству Конфигурации Easy VPN, Cisco IOS Release 15M&T.

Например:

```
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
```

Это показывает, что блокирующая группу проверка включена для GROUP1. Для GROUP1 единственный разрешенный пользователь является cisco1@GROUP1. Для GROUP2 (никакой group-lock), оба пользователя в состоянии войти.

Для успешной аутентификации используйте cisco1@GROUP1 с 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
```

Для аутентификации используйте cisco2@GROUP2 с GROUP1:

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

AAA Cisco IOS ipsec:user-vpn-group для Легкой VPN

Ipsec:user-vpn-group является атрибутом RADIUS, возвращенным AAA-сервером, и это может быть применено только для проверки подлинности пользователя (group-lock использовался для группы). Обе функции дополнительны, и они применены на других этапах.

Для получения дополнительной информации обратитесь к Руководству Конфигурации Easy VPN, Cisco IOS Release 15M&T.

Это работает по-другому, чем group-lock и все еще позволяет вам достигать того же результата. Различие - то, что атрибут должен иметь определенное значение (как для ASA) и что определенное значение по сравнению с именем группы Протокола ISAKMP (IKEID); если это не совпадает, то связь прерывается. Вот то, что происходит, если вы изменяете предыдущий пример, чтобы иметь клиентскую аутентификацию AAA (проверка подлинности, авторизация и учет) и отключить group-lock на данный момент:

```
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
```

Заметьте, что ipsec:user-vpn-group определен для пользователя, и group-lock определен для группы.

На ACS существует два пользователя, cisco1 и cisco2. Для cisco1 пользователя возвращен этот атрибут: **iPSec: user-vpn-group=GROUP1**. Для cisco2 пользователя возвращен этот атрибут : **iPSec: user-vpn-group=GROUP2**.

Когда cisco2 пользователь пытается войти с GROUP1, об этой ошибке сообщают:

```
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
```

Это вызвано тем, что ACS для cisco2 пользователя возвращается **ipsec:user-vpn-group=GROUP2**, который сравнен Cisco IOS с GROUP1.

Таким образом, та же цель была достигнута что касается group-lock. Вы видите, что прямо сейчас, конечный пользователь не должен предоставлять user@group как имя пользователя, но может использовать пользователя (без @group).

Для group-lock должен использоваться cisco1@GROUP1, потому что Cisco IOS разделила последнюю часть (после) и сравнила ее с IKEID (имя группы).

Для ipsec:user-vpn-group достаточно использовать только cisco1 в Cisco VPN Client, потому что тот пользователь определен на ACS, и определенный ipsec:user-vpn-group возвращен (в этом случае, это - =GROUP1), и тот атрибут сравнен с IKEID.

AAA Cisco IOS ipsec:user-vpn-group и Group-lock для Легкой VPN

Почему вы не должны использовать обе функции в то же время?

Можно добавить group-lock снова:

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

Вот поток:

1. Пользователь VPN Cisco настраивает соединение GROUP1 и подключения.
2. Фаза агрессивного режима успешна, и Cisco IOS отправляет xAuth запрос для имени пользователя и пароля.
3. Пользователь VPN Cisco получает всплывающее окно и вводит cisco1@GROUP1 имя пользователя с правильным паролем, определенным на ACS.
4. Cisco IOS выполняет проверку для group-lock: это разделяет имя группы, предоставленное в имени пользователя, и сравнивает его с IKEID. Это успешно.
5. Cisco IOS передает запрос AAA к серверу ACS (для пользователя cisco1@GROUP1).

6. ACS возвращается, RADIUS - Принимают с **ipsec:user-vpn-group=GROUP1**.

7. Cisco IOS выполняет вторую проверку; на этот раз это сравнивает группу, предоставленную атрибутом RADIUS IKEID.

   Когда это отказывает при Шаге 4 (блокировка группы), ошибка сразу зарегистрирована после того, как это предоставляет учетные данные:

   ```
   *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
   ```

   Когда это отказывает при Шаге 7 (ipsec:user-vpn-group), ошибка возвращена после того, как это получает атрибут RADIUS для аутентификации AAA (проверка подлинности, авторизация и учет):

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

Блокировка IOS Webvpn Group

На ASA Туннельный Group-lock может использоваться для всех сервисов VPN для удаленного доступа (IPSec, SSL, WebVPN). Для group-lock Cisco IOS и ipsec:user-vpn-group, это работает только для IPSec (сервер Easy VPN). Чтобы к group-lock определенные пользователи в определенных контекстах WebVPN (и подключенные групповые политики), должны использоваться опознавательные домены.

Например:

```
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
```

В следующем примере существует два контекста: C1 и C2. Каждый контекст имеет свою собственную групповую политику с определенными параметрами настройки. C1 обеспечивает доступ AnyConnect. Отпуск настроен для слушания обоих контекстов: C1 и C2.

Когда cisco1 пользователь обращается к контексту C1 с https://10.48.67.137/C1, опознавательный домен добавляет **C1** и аутентифицирует против локально определенного (СПИСОК списка) cisco1@C1 имя пользователя:


```
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"
```

Когда вы пытаетесь войти с cisco2 как имя пользователя при доступе к контексту C1 (https://10.48.67.137/C1), об этом сбое сообщают:

```
*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
```

Это вызвано тем, что существует определяемый пользователем № cisco2@C1. пользователь Cisco не в состоянии войти к любому контексту.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Руководство конфигурации Easy VPN, Cisco IOS Release 15M&T
- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.1

- Cisco Systems – техническая поддержка и документация