Características do Grupo-fechamento ASA e de Cisco IOS e atributos AAA e exemplo de configuração WebVPN

Índice

Introdução

Este artigo descreve as características detravamento na ferramenta de segurança adaptável de Cisco (ASA) e no ® do Cisco IOS e apresenta o comportamento para atributos diferentes do Authentication, Authorization, and Accounting (AAA). Para o Cisco IOS, a diferença entre o grupo-fechamento e os USER-VPN-grupos é explicada junto com um exemplo que use ambas as características complementares ao mesmo tempo. Há igualmente um exemplo do Cisco IOS WebVPN com domínios da autenticação.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do baisc destes assuntos:

- Configuração de CLI ASA e configuração de VPN do secure sockets layer (SSL)

- Configuração do acesso remoto VPN no ASA e no Cisco IOS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software ASA, versão 8.4 e mais recente
- Cisco IOS, versão 15.1 e mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurações

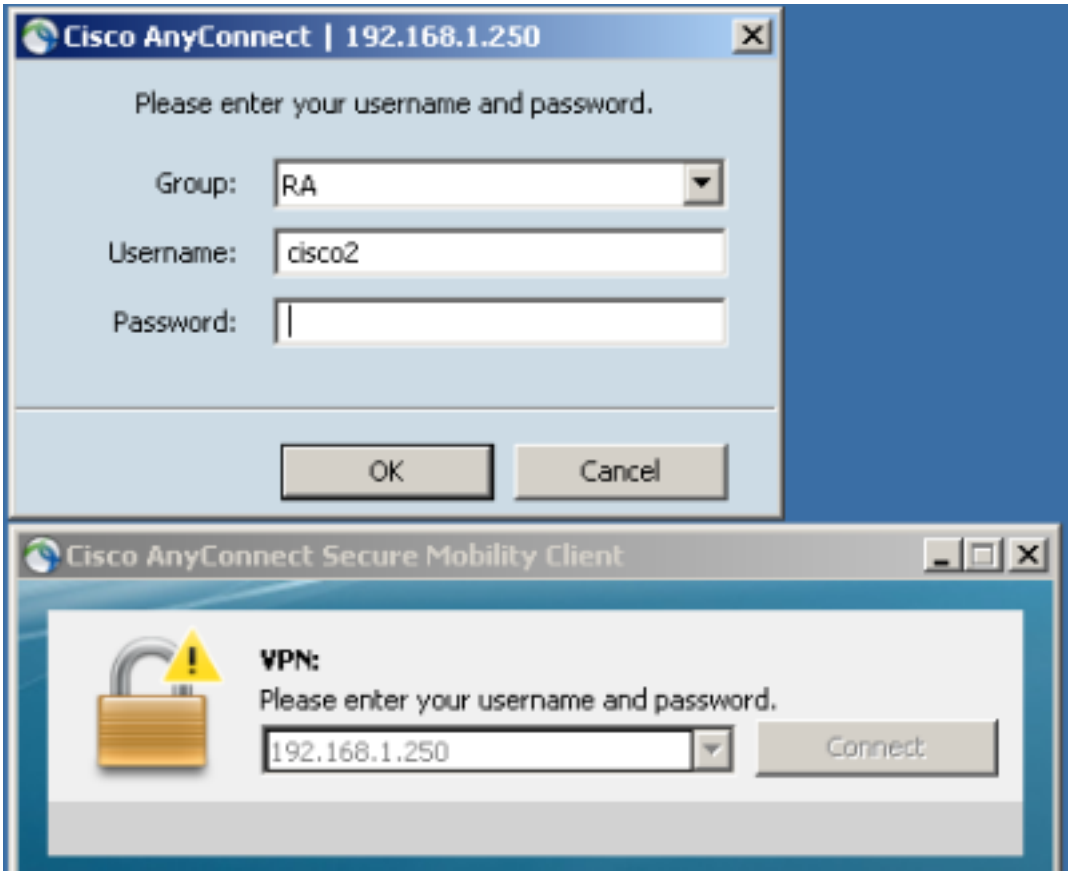
Grupo-fechamento do Local ASA

Você pode definir este atributo sob o usuário ou a grupo-política. Está aqui um exemplo para o atributo do 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 de Cisco pode usar somente o grupo de túneis RA, e o usuário cisco2 pode usar somente o grupo de túneis RA2.

Se o usuário cisco2 escolhe o grupo de túneis RA, a seguir a conexão está negada:

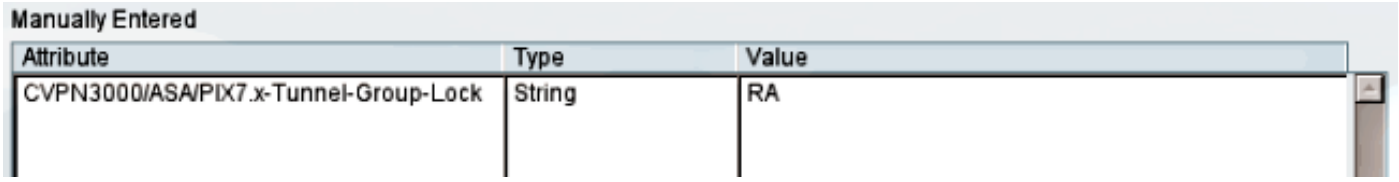



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

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

Atribua 3076/85 (Túnel-Grupo-fechamento) que é retornado pelo servidor AAA faz exatamente o mesmos. Pode ser passado junto com o usuário ou a autenticação do grupo de política (ou o atributo 25 do Internet Engineering Task Force (IETF)) e trava o usuário em um grupo de túneis específico.

Está aqui um perfil da autorização do exemplo no Access Control Server de Cisco (ACS):



Quando o atributo é retornado pelo AAA, o RAIO debuga indica-o:

```
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 alcançar o grupo de túneis RA2 quando grupo-fechado dentro do grupo de túneis RA:

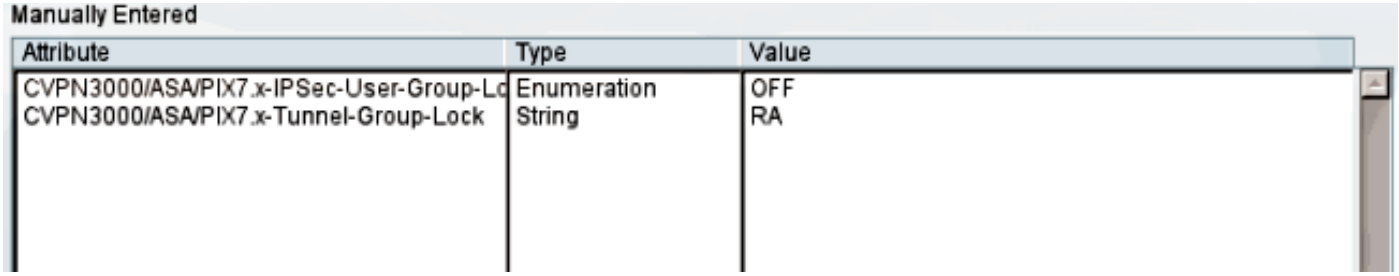
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

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

Este atributo é tomado igualmente do diretório VPN3000 herdado pelo ASA. Está ainda atual no manual de configuração 8.4 (embora é removido em uma versão mais nova do manual de configuração) e descrito como:

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

Parece que o atributo poderia ser usado a fim desabilitar o grupo-travamento, mesmo se o atributo do Túnel-Grupo-fechamento esta presente. Se você tenta retornar que atributo ajustado a 0 junto com o Túnel-Grupo-fechamento (esta é ainda apenas autenticação de usuário), é aqui o que acontece. Olha estranho quando você tenta desabilitar o grupo-travamento ao retornar um nome de grupo de túneis específico:



Debuga a mostra:

```
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
```

Isto rende o mesmo resultado (o travamento do grupo foi reforçado, e o IPsec-USER-Grupo-fechamento não foi tomado na consideração).

```
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>
```

A grupo-política externo retornou IPSec-User-Group-Lock=0 e igualmente obteve Tunnel-Group-Lock=RA para a autenticação de usuário. Ainda, o usuário foi travado, assim que significa que o travamento do grupo esteve executado.

Para a configuração oposta, a grupo-política externo retorna um nome de grupo de túneis específico (Túnel-Grupo-fechamento) quando tentar desabilitar o grupo-travamento para um usuário específico (IPSec-User-Group-Lock=0), e grupo-travando tem sido reforçado ainda para esse usuário.

Isto confirma que o atributo não está usado anymore. Esse atributo foi usado no VPN3000 Series velho. A identificação de bug Cisco CSCui34066 foi aberta.

Grupo-fechamento local do Cisco IOS para o VPN fácil

A opção local do grupo-fechamento sob a configuração de grupo em trabalhos do Cisco IOS diferentemente do que no ASA. No ASA, você especifica o nome de grupo de túneis a que o usuário é travado. A opção do grupo-fechamento do Cisco IOS (não há nenhum argumento) permite a verificação adicional e compara o grupo fornecido com o username (formato user@group) com o IKEID (nome do grupo).

Para mais informação, refira o guia de configuração de VPN fácil, o Cisco IOS Release 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
```

Isto mostra que isso grupo-travar a verificação está permitido para o GRUPO1. Para o GRUPO1, o único usuário permitido é cisco1@GROUP1. Para o GRUPO2 (nenhum grupo-fechamento), ambos os usuários podem entrar.

Para a autenticação bem sucedida, use cisco1@GROUP1 com GRUPO1:

```
*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 a autenticação, use cisco2@GROUP2 com GRUPO1:

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

IPsec do Cisco IOS AAA: USER-VPN-grupo para o VPN fácil

O IPsec: o USER-VPN-grupo é o atributo RADIUS retornado pelo servidor AAA, e pode ser aplicado somente para a autenticação de usuário (o grupo-fechamento foi usado para o grupo). Ambas as características são complementares, e são aplicadas em fases diferentes.

Para mais informação, refira o guia de configuração de VPN fácil, o Cisco IOS Release 15M&T.

Trabalha diferentemente do que o grupo-fechamento e ainda permite que você consiga o mesmo resultado. A diferença é que o atributo deve ter um valor específico (como para o ASA) e que o valor específico está comparado com o nome do grupo do Internet Security Association and Key Management Protocol (ISAKMP) (IKEID); se não combina, a seguir a conexão falha. É aqui o que acontece se você muda o exemplo anterior a fim ter a autenticação de AAA do cliente e desabilitar por agora o grupo-fechamento:

```
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 IPsec: o atributo do USER-VPN-grupo é definido para o usuário e o grupo-fechamento é 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 entrar com GRUPO1, este erro está 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
```

Isto é porque o ACS para o usuário cisco2 retorna **ipsec:user-vpn-group=GROUP2**, que é comparado pelo Cisco IOS ao GRUPO1.

Esta maneira, o mesmo objetivo foi conseguida quanto para ao grupo-fechamento. Você pode ver que agora, o utilizador final não precisa de fornecer user@group como o username, mas pode usar o usuário (sem o @group).

Para o grupo-fechamento, cisco1@GROUP1 deve ser usado, porque o Cisco IOS descascou a última parte (após @) e a comparou com o IKEID (nome do grupo).

Para o IPsec: USER-VPN-grupo, é suficiente usar somente cisco1 no Cisco VPN Client, porque esse usuário é definido no ACS e no IPsec específico: o USER-VPN-grupo é retornado (neste

caso, é =GROUP1) e esse atributo é comparado contra IKEID.

IPsec do Cisco IOS AAA: USER-VPN-grupo e Grupo-fechamento para o VPN fácil

Por que não deve você usar ambas as características ao mesmo tempo?

Você pode adicionar o grupo-fechamento outra vez:

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

Está aqui o fluxo:

1. O usuário de Cisco VPN configura a conexão do GRUPO1 e conecta-a.
2. A fase do modo assertivo é bem sucedida, e o Cisco IOS envia um pedido do Xauth para o nome de usuário e senha.
3. O usuário de Cisco VPN recebe um pop-up, e incorpora o username de cisco1@GROUP1 com a senha correta definida no ACS.
4. O Cisco IOS verifica o grupo-fechamento: descasca o nome do grupo fornecido no username e compara-o com o IKEID. É bem sucedido.
5. O Cisco IOS envia um pedido AAA ao servidor ACS (para o usuário cisco1@GROUP1).

6. O ACS retorna uma Raio-aceitação com **ipsec:user-vpn-group=GROUP1**.

7. O Cisco IOS executa uma segunda verificação; esta vez, compara o grupo fornecido pelo atributo RADIUS com o IKEID.

   Quando falhar em etapa 4 (fechamento do grupo), o erro está registrado imediatamente depois que fornece 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 falhar na etapa 7 (IPsec: o USER-VPN-grupo), o erro é retornado depois que recebe o atributo RADIUS para a autenticação de AAA:

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

Fechamento do grupo IO Webvpn

No ASA, o Túnel-Grupo-fechamento pode ser usado para todos os serviços do acesso remoto VPN (IPsec, SSL, WebVPN). Para o grupo-fechamento do Cisco IOS e o IPsec: USER-VPN-grupo, trabalha somente para o IPsec (Easy VPN Server). Os usuários específicos do grupo-fechamento em contextos específicos WebVPN (e em grupo-políticas anexadas), domínios da 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 exemplo seguinte, há dois contextos: C1 e C2. Cada contexto tem sua própria grupo-política com ajustes específicos. O C1 permite o acesso de AnyConnect. O gataway é configurado a fim escutar ambos os contextos: C1 e C2.

Quando os acessos de usuário cisco1 o contexto C1 com https://10.48.67.137/C1, o domínio da autenticação adicionarem o **C1** e o autenticarem contra (LISTA da lista) o username localmente definido de 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 entrar com cisco2 como um username quando você alcançar o contexto C1 (https://10.48.67.137/C1), esta falha está relatado:

```
*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
```

Isto é porque não há nenhum cisco2@C1 definido pelo utilizador. o usuário de Cisco não pode entrar a nenhum contexto.

Verificar

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

Troubleshooting

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

Informações Relacionadas

- Guia de configuração de VPN fácil, Cisco IOS Release 15M&T

- Guia de configuração de CLI da série VPN de Cisco ASA, 9.1
- Suporte Técnico e Documentação - Cisco Systems