Ejemplo de Funciones de Bloqueo de Grupo ASA y Cisco IOS y Atributos AAA y Configuración de WebVPN

Contenido

Introducción

En este artículo se describen las funciones de bloqueo de grupo en el Cisco Adaptive Security Appliance (ASA) y en Cisco IOS® y se presenta el comportamiento de los diferentes atributos de autenticación, autorización y contabilidad (AAA). Para Cisco IOS, se explica la diferencia entre el bloque de grupo y los grupos de usuario-vpn junto con un ejemplo que utiliza ambas funciones complementarias al mismo tiempo. También hay un ejemplo de Cisco IOS WebVPN con dominios de autenticación.

Prerequisites

Requirements

Cisco recomienda que tenga un conocimiento básico de estos temas:

- Configuración de la CLI de ASA y configuración de VPN de capa de conexión segura (SSL)

- Configuración de VPN de acceso remoto en ASA y Cisco IOS

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software ASA, versión 8.4 y posteriores
- Cisco IOS, versión 15.1 y posteriores

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.

Configuraciones

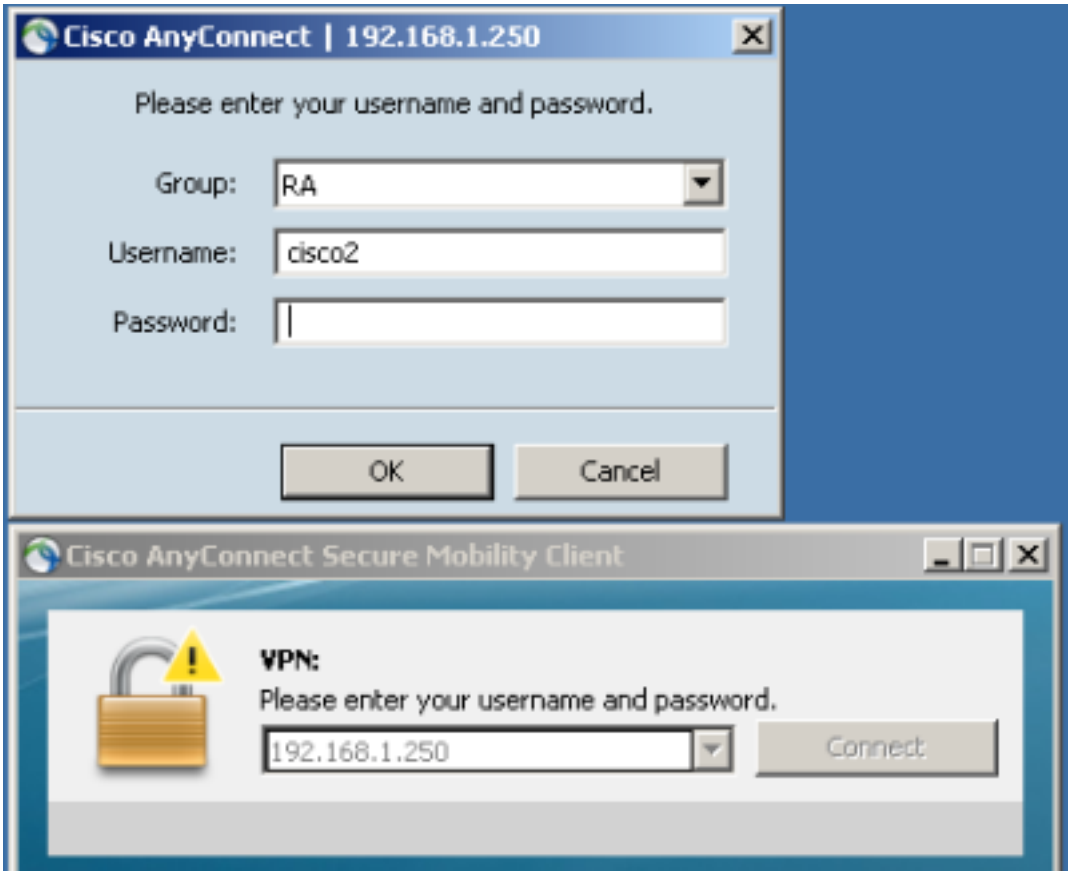
Bloqueo de grupo local ASA

Puede definir este atributo bajo el usuario o la política de grupo. Este es un ejemplo para el atributo de usuario 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
```

El usuario de Cisco puede utilizar solamente el grupo de túnel RA y el usuario de cisco2 puede utilizar solamente el grupo de túnel RA2.

Si el usuario de cisco2 elige el grupo de túnel RA, se deniega la conexión:

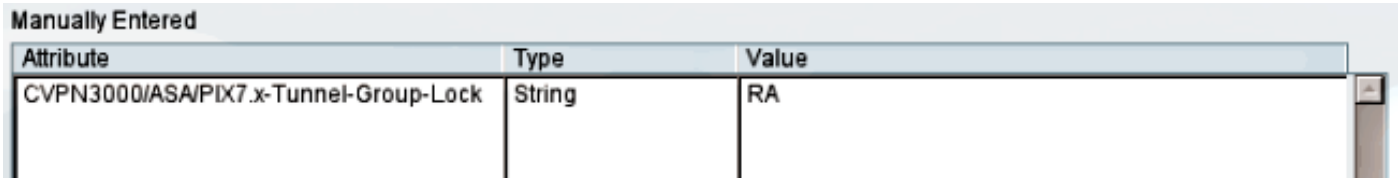



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

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

El atributo 3076/85 (Tunnel-Group-Lock) que devuelve el servidor AAA hace exactamente lo mismo. Se puede pasar junto con la autenticación del usuario o del atributo 25 del grupo de políticas (o Grupo de trabajo de ingeniería de Internet (IETF)) y bloquea al usuario en un grupo de túnel específico.

Este es un ejemplo de perfil de autorización en Cisco Access Control Server (ACS):



Cuando AAA devuelve el atributo, las depuraciones RADIUS lo indican:

```
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
```

El resultado es el mismo cuando se intenta acceder al grupo de túnel RA2 mientras se bloquea el grupo dentro del grupo de túnel RA:

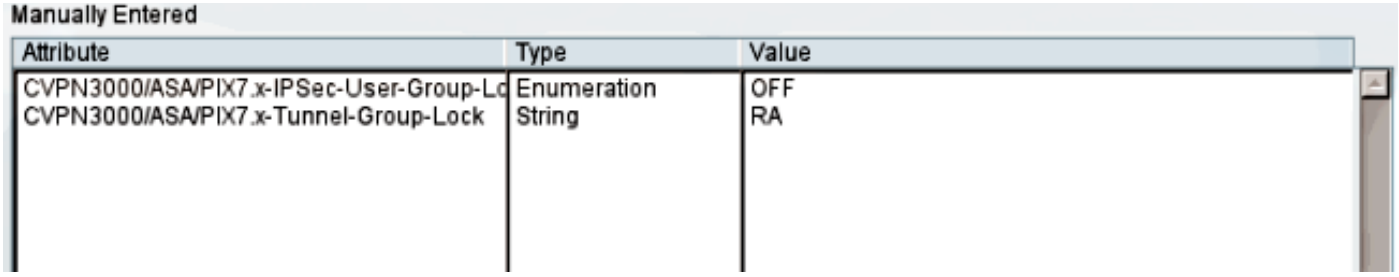
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

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

Este atributo también se toma del directorio VPN3000 heredado por el ASA. Todavía está presente en la guía de configuración 8.4 (aunque se elimina en una versión más reciente de la guía de configuración) y se describe como:

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

Parece que el atributo se podría utilizar para inhabilitar el bloqueo de grupo, incluso si el atributo Tunnel-Group-Lock está presente. Si intenta devolver el atributo configurado en 0 junto con Tunnel-Group-Lock (esto es solo autenticación de usuario), esto es lo que sucede. Parece extraño cuando intenta inhabilitar el bloqueo de grupo mientras devuelve un nombre de grupo de túnel específico:



Los depuradores muestran:

```
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
```

Esto produce el mismo resultado (se ha aplicado el bloqueo de grupo y no se ha tenido en cuenta IPSec-User-Group-Lock).

```
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
```

La política de grupo externa devolvió IPSec-User-Group-Lock=0 y también obtuvo Tunnel-Group-Lock=RA para la autenticación de usuario. Sin embargo, el usuario se ha bloqueado, lo que significa que se ha realizado el bloqueo de grupo.

Para la configuración opuesta, la política de grupo externa devuelve un nombre de grupo de túnel específico (Tunnel-Group-Lock) mientras intenta inhabilitar el bloqueo de grupo para un usuario específico (IPSec-User-Group-Lock=0), y el bloqueo de grupo todavía se ha aplicado para ese usuario.

Esto confirma que el atributo ya no se utiliza. Ese atributo se utilizó en la antigua serie VPN3000. Se ha abierto el Id. de bug Cisco CSCui34066.

Bloqueo de grupo local de Cisco IOS para Easy VPN

La opción local group-lock bajo la configuración de grupo en Cisco IOS funciona de manera diferente que en ASA. En el ASA, especifique el nombre del grupo de túnel al que está bloqueado el usuario. La opción de bloqueo de grupo de Cisco IOS (no hay argumentos) habilita la verificación adicional y compara el grupo proporcionado con el nombre de usuario (formato user@group) con IKEID (nombre de grupo).

Para obtener más información, consulte la Guía de Configuración de Easy VPN, Cisco IOS Release 15M&T.

Aquí tiene un ejemplo:

```
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
```

Esto muestra que la verificación de bloqueo de grupo está habilitada para GROUP1. Para GROUP1, el único usuario permitido es cisco1@GROUP1. Para GROUP2 (sin bloqueo de grupo), ambos usuarios pueden iniciar sesión.

Para una autenticación correcta, utilice cisco1@GROUP1 con 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 la autenticación, utilice cisco2@GROUP2 con 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

El **ipsec:user-vpn-group** es el atributo RADIUS devuelto por el servidor AAA, y sólo se puede aplicar para la autenticación de usuario (group-lock se utilizó para el grupo). Ambas características son complementarias y se aplican en diferentes etapas.

Para obtener más información, consulte la Guía de Configuración de Easy VPN, Cisco IOS Release 15M&T.

Funciona de forma diferente que el bloqueo de grupo y le permite alcanzar el mismo resultado. La diferencia es que el atributo debe tener un valor específico (como para el ASA) y que ese valor específico se compara con el nombre de grupo (IKEID) de la Asociación de Seguridad de Internet y del Protocolo de administración de claves (ISAKMP); si no coincide, la conexión falla. Esto es lo que sucede si cambia el ejemplo anterior para tener la autenticación AAA del cliente y inhabilita el bloqueo de grupo por ahora:

```
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 el atributo ipsec:user-vpn-group se define para el usuario y group-lock se define para el grupo.

En el ACS, hay dos usuarios, cisco1 y cisco2. Para el usuario de cisco1, se devuelve este atributo: **ipsec:user-vpn-group=GROUP1**. Para el usuario de cisco2, se devuelve este atributo: **ipsec:user-vpn-group=GROUP2**.

Cuando el usuario de cisco2 intenta iniciar sesión con GROUP1, se informa de este error:

```
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
```

Esto se debe a que el ACS para el usuario cisco2 devuelve **ipsec:user-vpn-group=GROUP2**, que es comparado por el IOS de Cisco con GROUP1.

De esta manera, se ha alcanzado el mismo objetivo que para el grupo bloqueado. Puede ver que ahora mismo, el usuario final no necesita proporcionar user@group como nombre de usuario, pero puede utilizar el usuario (sin @group).

Para group-lock, se debe utilizar cisco1@GROUP1, porque Cisco IOS eliminó la última parte (después de @) y la comparó con IKEID (nombre de grupo).

Para el ipsec:user-vpn-group, es suficiente con utilizar solamente cisco1 en Cisco VPN Client, porque ese usuario se define en el ACS y se devuelve el ipsec específico:user-vpn-group (en este caso, es =GROUP1) y ese atributo se compara con IKEID.

Cisco IOS AAA IPSec:user-vpn-group y Group-lock para Easy VPN

¿Por qué no debe utilizar ambas funciones al mismo tiempo?

Puede agregar de nuevo el bloqueo de grupo:

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

Aquí está el flujo:

1. El usuario VPN de Cisco configura la conexión GROUP1 y se conecta.
2. La fase de modo agresivo es exitosa, y Cisco IOS envía una solicitud xAuth para el nombre de usuario y la contraseña.
3. El usuario de Cisco VPN recibe un mensaje emergente e ingresa el nombre de usuario cisco1@GROUP1 con la contraseña correcta definida en el ACS.
4. Cisco IOS realiza una verificación para el bloqueo de grupo: elimina el nombre de grupo proporcionado en el nombre de usuario y lo compara con IKEID. Es un éxito.
5. Cisco IOS envía una solicitud AAA al servidor ACS (para el usuario cisco1@GROUP1).
6. ACS devuelve un RADIUS-Accept con **ipsec:user-vpn-group=GROUP1**.
7. Cisco IOS realiza una segunda verificación; esta vez, compara el grupo proporcionado por el atributo RADIUS con IKEID.

   Cuando falla en el Paso 4 (bloqueo de grupo), el error se registra inmediatamente después de proporcionar las credenciales:

```
*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
```

Cuando falla en el Paso 7 (ipsec:user-vpn-group), el error se devuelve después de que recibe el atributo RADIUS para la autenticación AAA:

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

Bloqueo de grupo de Webvpn de IOS

En el ASA, el Tunnel-Group-Lock se puede utilizar para todos los servicios VPN de acceso remoto (IPSec, SSL, WebVPN). Para el grupo de bloqueo de Cisco IOS y el grupo ipsec:user-vpn, sólo funciona para IPSec (servidor Easy VPN). Para agrupar usuarios específicos en contextos WebVPN específicos (y políticas de grupo asociadas), se deben utilizar dominios de autenticación.

Aquí tiene un ejemplo:

```
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
```

En el siguiente ejemplo, hay dos contextos: C1 y C2. Cada contexto tiene su propia política de grupo con configuraciones específicas. C1 permite el acceso a AnyConnect. La puerta de enlace se configura para escuchar ambos contextos: C1 y C2.

Cuando el usuario de cisco1 accede al contexto C1 con https://10.48.67.137/C1, el dominio de autenticación agrega **C1** y se autentica con el nombre de usuario cisco1@C1 definido localmente (list LIST):


```
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"
```

Cuando intenta iniciar sesión con cisco2 como nombre de usuario mientras accede al contexto C1 (https://10.48.67.137/C1), se informa de esta falla:

```
*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
```

Esto se debe a que no hay ningún usuario cisco2@C1 definido. el usuario de cisco no puede iniciar sesión en ningún contexto.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de Configuración de Easy VPN, Cisco IOS Release 15M&T
- Guía de configuración CLI VPN Cisco Serie ASA, 9.1
- Soporte Técnico y Documentación - Cisco Systems