

Configuración de varias instancias en Secure Firewall serie 3100

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración para la versión 7.4.1+](#)

Introducción

Este documento describe cómo configurar Multi-Instance en Secure Firewall 3100 Series que ejecuta la versión 7.4+.

Prerequisites

Conocimiento del sistema operativo extensible (FXOS) y de la interfaz gráfica de usuario (GUI) del centro de administración de firewalls (FMC).

Requirements

Acceso a:

- Acceso a la consola de Secure Firewall serie 3100
- Acceso a GUI de FMC

Componentes Utilizados

- Cisco Secure Firewall Management Center con más de 7.4
- Cisco Secure Firewall serie 3100
 - Excepto 3105*

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En el modo de varias instancias, puede implementar varias instancias de contenedor en un único

chasis que actúen como dispositivos completamente independientes.


Configuración para la versión 7.4.1+

Paso 1. Conéctese al puerto de la consola del chasis.

El puerto de la consola se conecta a la CLI de FXOS.

Paso 2. Inicie sesión con el nombre de usuario admin y la contraseña Admin123.

Se le solicitará que cambie la contraseña la primera vez que inicie sesión en FXOS.

 Nota: Si la contraseña ya se ha cambiado y no la conoce, debe recrear la imagen del dispositivo para restablecer la contraseña predeterminada. Consulte [la guía de resolución de problemas](#) de [FXOS](#) para el [procedimiento image](#).

Paso 3. Compruebe el modo actual, Native o Container. Si el modo es nativo, puede continuar con este procedimiento para convertir al modo de varias instancias (contenedor).

```
firepower# show system detail
```

Ejemplo:

```
firepower# show system detail

Systems:
  Name: firepower
  Mode: Stand Alone
  System IP Address: 0.0.0.0
  System IPv6 Address: ::
  System Owner:
  System Site:
  Deploy Mode: Native
  Description for System:
```

Mostrar estado de varias instancias

Paso 4. Conéctese a la CLI de Threat Defence.

```
firepower# connect ftd
```

Ejemplo:



```
firepower# connect ftd
>
```

Conexión a FTD

Paso 5. La primera vez que inicie sesión en Threat Defence, se le solicitará que acepte el Acuerdo de licencia del usuario final (CLUF). A continuación, se le presentará la secuencia de comandos de instalación de CLI.

El script de configuración permite establecer la dirección IP de la interfaz de gestión y otros parámetros. Sin embargo, cuando se convierte al modo de instancia múltiple, los únicos ajustes que se conservan son los siguientes.

- Contraseña de administrador (que se establece al iniciar sesión)
- Servidores DNS
- Buscar dominios

La dirección IP de administración y la puerta de enlace se restablecen como parte del comando de modo de instancia múltiple. Después de convertir al modo de varias instancias, puede cambiar la configuración de administración en la CLI de FXOS. [Consulte Cambio de la configuración de administración del chasis en la CLI de FXOS.](#)

Paso 6. Habilite el modo de instancias múltiples, establezca la configuración de la interfaz de administración del chasis e identifique el centro de administración. Puede utilizar IPv4 o IPv6. Después de ingresar el comando, se le pedirá que borre la configuración y reinicie. EnterERASE(mayúsculas). El sistema se reinicia y, como parte del cambio de modo, borra la configuración con la excepción de la configuración de red de administración que estableció en el comando y la contraseña de administración. El nombre de host del chasis está configurado como "modelo de firepower".

IPv4:

```
configure multi-instance network
ipv4ip_addressnetwork_maskgateway_ip_addressmanager_name
{hostname | dirección_ipv4 | DONTRESOLVE} registration_keynat_id
```

IPv6:

```
configure multi-instance network ipv6ipv6_addressprefix_length
gateway_ip_addressmanagermanager_name {hostname | ipv6_address | DONTRESOLVE}
registration_keynat_id
```

Consulte estos componentes del gerente:

- {nombre del host | dirección_ipv4 | DONTRESOLVE} : especifica el FQDN o la dirección IP del centro de administración. Al menos uno de los dispositivos, ya sea el centro de administración o el chasis, debe tener una dirección IP accesible para establecer el canal de comunicación bidireccional cifrado mediante SSL entre los dos dispositivos. Si no especifica un nombre de host o dirección IP del administrador en este comando, ingrese DONTRESOLVE; en este caso, el chasis debe tener una dirección IP o nombre de host accesible, y debe especificar thenat_id.
- registration_key: introduzca una clave de registro única de su elección que también especifique en el centro de administración cuando registre el chasis. La clave de registro no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A-Z, a-z, 0-9) y el guión (-).
- nat_id: especifica una cadena única de su elección que también se especifica en el centro de administración cuando se registra el chasis cuando un lado no especifica una dirección IP o nombre de host alcanzable. Es obligatorio si no especifica una dirección de administrador o un nombre de host; sin embargo, se recomienda que establezca siempre el ID de NAT aunque especifique un nombre de host o una dirección IP. El ID de NAT no debe superar los 37 caracteres. Los caracteres válidos incluyen caracteres alfanuméricos (A-Z, a-z, 0-9) y el guión (-). Este ID no se puede utilizar para ningún otro dispositivo que se registre en el centro de gestión.

Para volver a cambiar el modo al modo de dispositivo, debe utilizar el sistema CLI de FXOS y enterscope y después establecer el modo de implementación nativo. [Consulte Cambio de la configuración de administración del chasis en la CLI de FXOS.](#)

Ejemplo:


```
> configure multi-instance network ipv4 10.88.146.203 255.255.255.0 10.88.146.1
manager fmc1 10.88.243.100 cisco123 natid1
WARNING: This command will discard any FTD configuration (except admin's credentials). Make sure you backup your content
. All previous content will be lost. System is going to be re-initialized. Type ERASE to confirm:ERASE
Continue...
Validation check...
Checking startup version and csp file ...
Converting to MI mode, device will be rebooted and re-initialized...
>
Broadcast message from root@firepower (Sun Jan 22 00:10:14 2023):


All shells being terminated due to system /sbin/reboot

Broadcast message from root@firepower (Sun Jan 22 00:10:15 2023):

System is restarted due to deploy mode changed
```

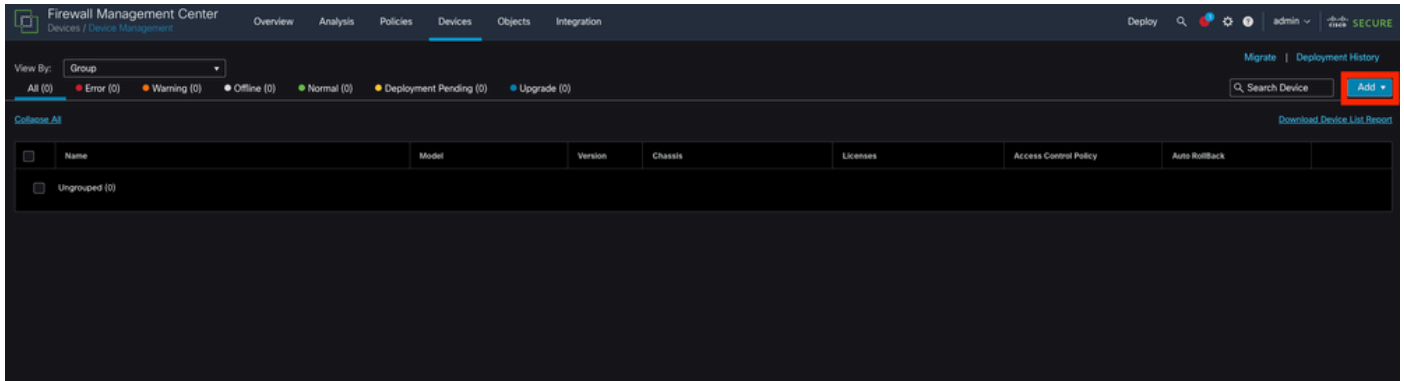
Cambio al modo multiinstancia

 Nota: Añada el chasis de varias instancias al centro de gestión. El centro de gestión y el chasis comparten una conexión de gestión independiente mediante la interfaz de gestión del

 chasis. Puede utilizar el centro de administración para configurar todos los ajustes del chasis, así como las instancias. No se admite la configuración ni el administrador de chasis de firewall seguro en la CLI de FXOS.

Paso 7. En el centro de administración, agregue el chasis mediante la dirección IP o el nombre de host de administración del chasis.

- Elija Devices>Device Management y luego Add>Chassis.



Adición del chasis al CSP

Add Chassis



i This operation is only supported on 3100, 4100 & 9300 chassis

Hostname/IP Address†

Chassis name

Registration key*

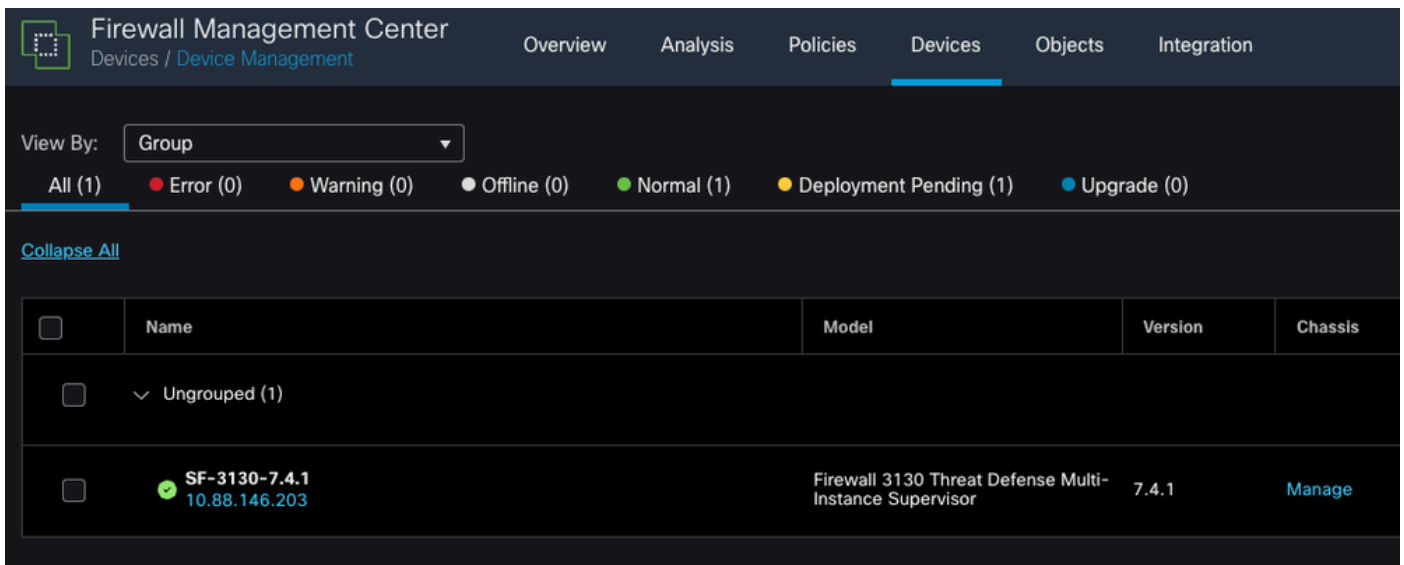
Device Group

Unique NAT ID†

† Either host or NAT ID is required.

Parámetros de configuración del chasis

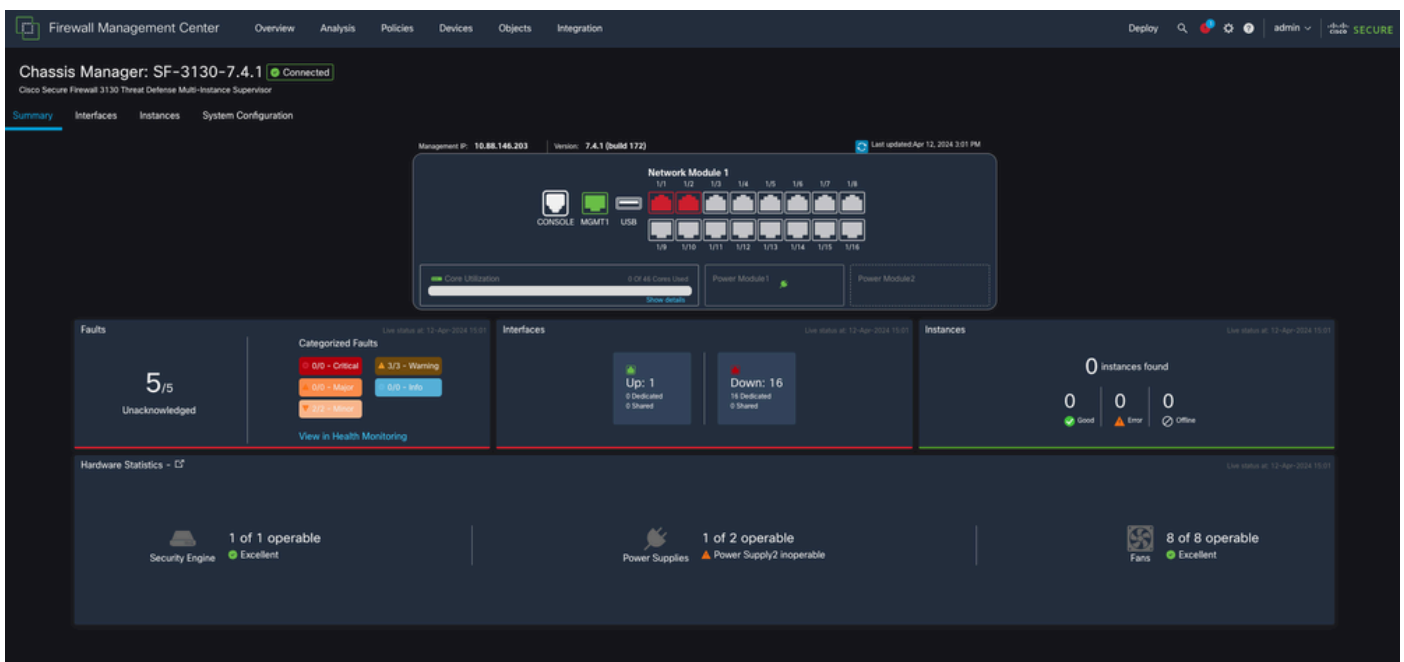
- Una vez agregado el chasis al FMC, consulte el dispositivo en la lista de dispositivos del FMC.



Chassis añadido en el FMC

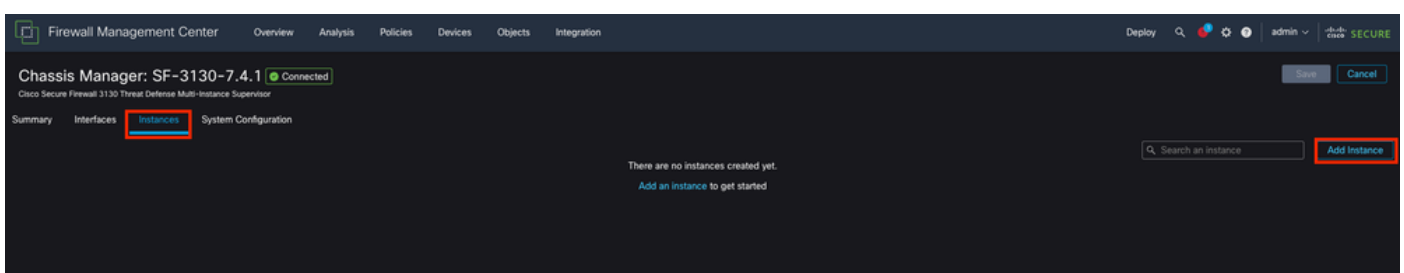
Paso 8. Para ver y configurar el chassis, haga clic en Administrar en la columna Chassis o haga clic en Editar(✎).

La página Administrador de chassis se abre para que el chassis acceda a la página Resumen.



Gestión de chassis

Paso 9. Seleccione el botón Instancias y, a continuación, Agregar instancia para crear una nueva instancia en el chassis.



Paso 10. Siga las instrucciones del asistente para finalizar la instalación de la instancia.

1. Acepte el acuerdo

The screenshot shows a dark-themed window titled "Add Instance" with a progress bar at the top containing five steps: 1 Agreement, 2 Instance Configuration, 3 Interface Assignment, 4 Device Management, and 5 Summary. The "Agreement" step is active. The main content area displays the following text:

End User License Agreement
Effective: May 10, 2022
Secure Firewall Terms and Conditions

By clicking 'Accept' below or using this Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and applicable Product Specific Terms available at:

<https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>

You also acknowledge that you have read the Cisco Privacy Statement at:

<https://www.cisco.com/c/en/us/about/legal/privacy-full.html>

If you are a Cisco partner accepting on behalf of an end customer, you must inform the end customer that the EULA applies to such end customer's use of the Cisco Technology and provide the end customer with access to all relevant terms. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'Accept' and do not use the Cisco Technology.

I understand and accept the agreement.

At the bottom right, there are two buttons: "Cancel" and "Next". The "Next" button is highlighted with a red box.

Aceptar acuerdo

2. Configurar los parámetros de instancia

Add Instance ? X

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Display Name*
SF-3130-741-Instance

Device Version*
7.4.1.172

Resource Profile*
Default-Medium +

Permit Expert mode for CLI

IPv4 IPv6 Both

IPv4

Management IP*
10.88.146.198

Network Mask*
255.255.255.0

Network Gateway*
10.88.146.1

Search Domain

FQDN

Firewall Mode*
Routed

DNS Servers
172.18.108.34

Device SSH Password*
.....

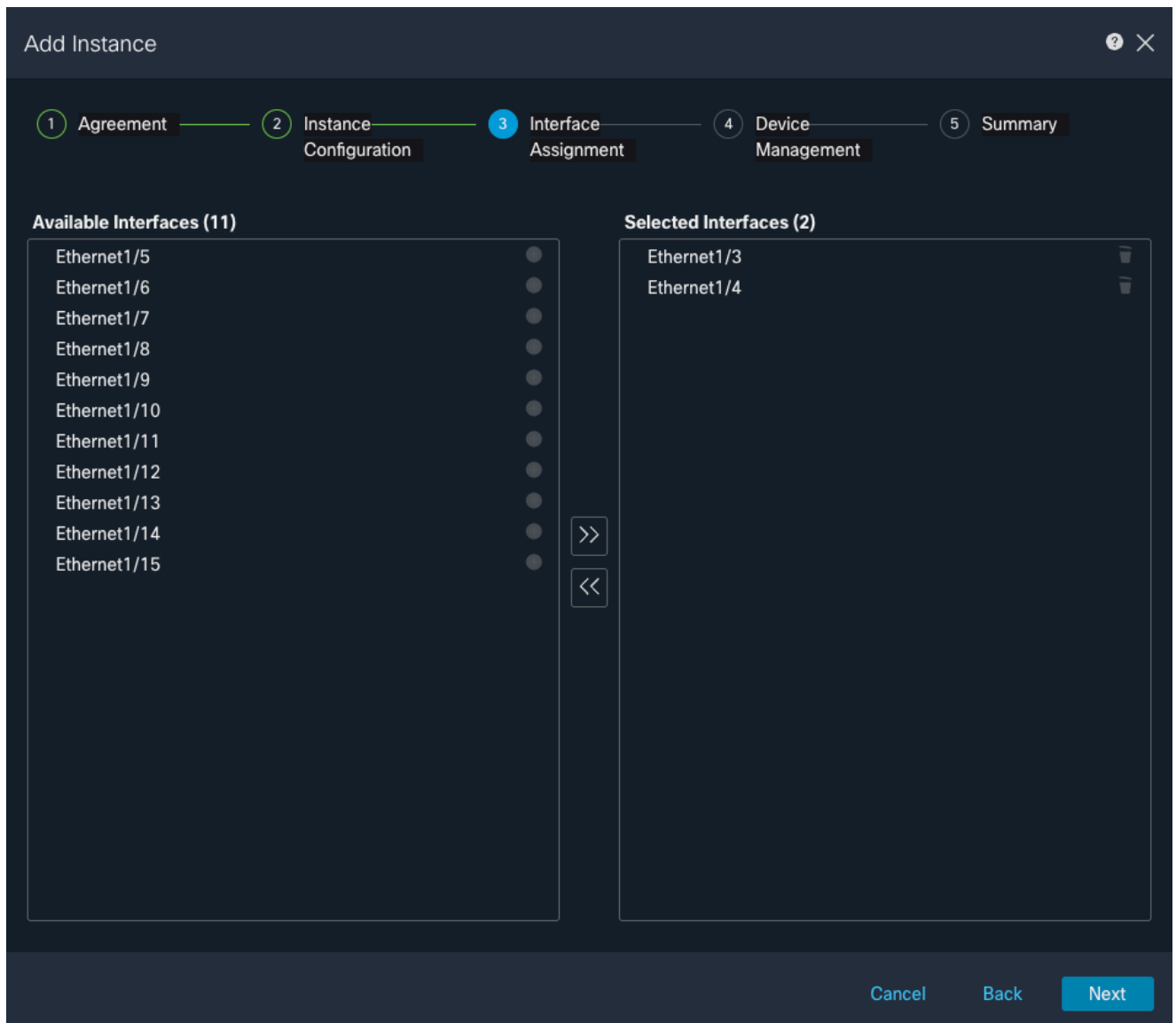
Confirm Password*
.....

Show Password

Cancel Back **Next**

Parámetros de instancia

3. Selección de interfaz.



Asignación de interfaz

4. Gestión de dispositivos.

Add Instance ? X

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Device Group
Select... ▼

Access Control Policy*
ACP ▼ +

Platform Settings
Instance x ▼ +

Smart Licensing

- Carrier
- Malware Defense
- IPS
- URL

Cancel Back **Next**

Gestión de dispositivos

5. Summary

Add Instance



- 1 Agreement
- 2 Instance Configuration
- 3 Interface Assignment
- 4 Device Management
- 5 Summary

Instance Configuration

Name: asdvav
Version: 7.4.1.172
Resource Profile: Default-Small
IP: 10.88.243.13
Mask: 255.255.255.0
Gateway: 10.88.243.1
Mode: routed
Password: *****
FQDN:
DNS Servers:
Search Domain:
Expert Mode: disabled

Device Management - This info is required only during instance creation.

Access Policy: ACP
Device Group:
Platform Policy: Instance
Licenses: Carrier, Malware Defense, IPS, URL

Interface Assignment - 2 dedicated and 0 shared interfaces attached [Show All](#)

Cancel

Back

Save

Resumen de la instancia

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).