# Implementación de ASA en modo transparente en un FP9300

## Contenido



## Introducción

Este documento describe cómo implementar un ASA Transparente en un FP9300. De forma predeterminada, cuando se implementa un ASA en un FP9300, el modo de firewall es el router. No existe la opción de seleccionar el modo transparente, ya que lo tenemos para la plantilla FTD.

Por otra parte, un firewall transparente es un firewall de capa 2 que actúa como un "bache en el cable" o un "firewall sigiloso" y no se ve como un salto de router a los dispositivos conectados. Sin embargo, al igual que cualquier otro firewall, se controla el control de acceso entre interfaces y se llevan a cabo todas las comprobaciones habituales del firewall.

### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modo transparente de ASA
- Arquitectura FP9300

#### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

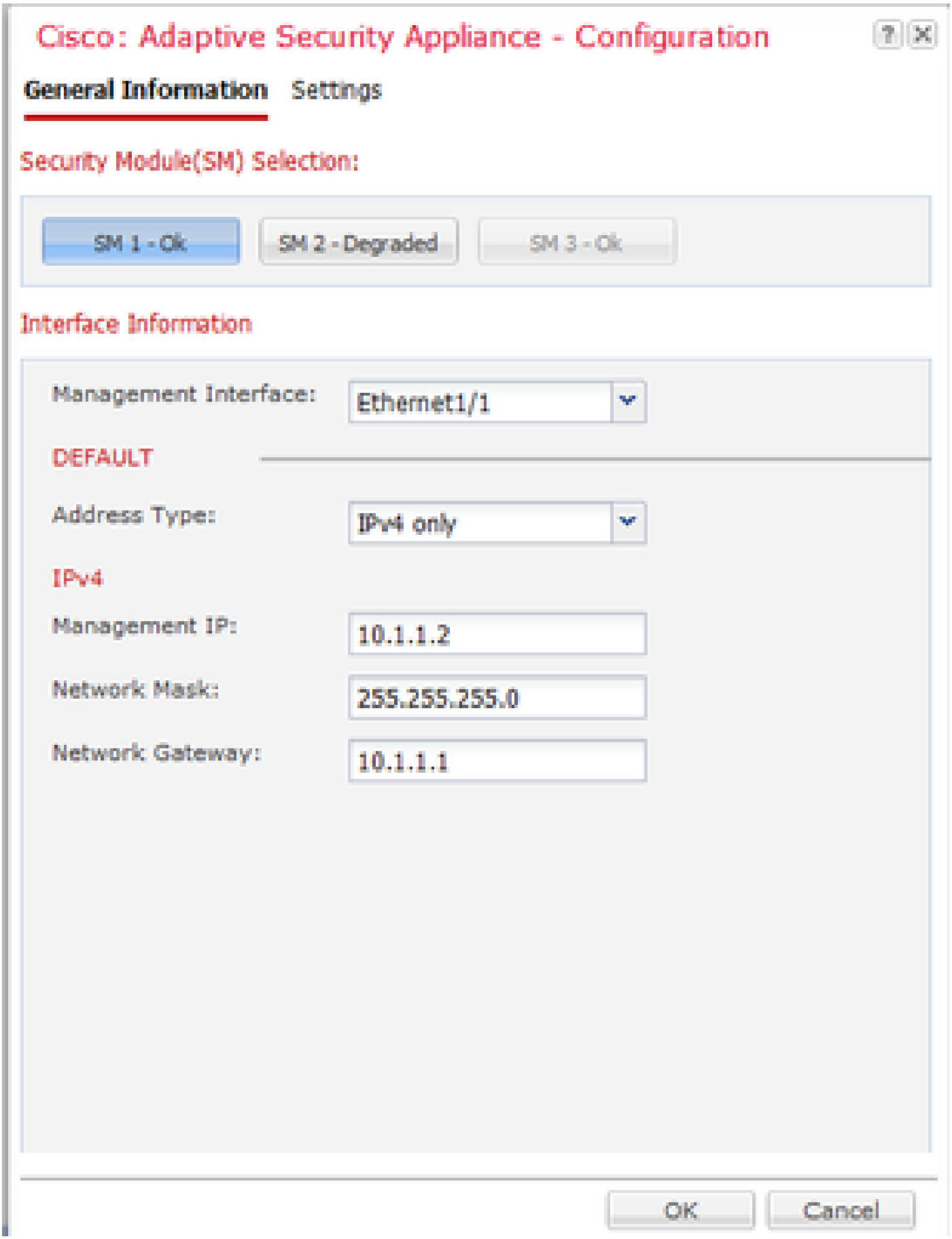
- FPR9K-SM-44 que ejecuta la versión FXOS 2.3.1.73
- Software ASA para FP9300 versión 9.6.1

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.

## Configurar

Al implementar un ASA, no existe la opción de seleccionar el modo Firewall tal como está al implementar FTD:




Una vez que se ha implementado el ASA, se configura previamente en el modo ruteado:

```
asa# show firewall
Firewall mode: Router

asa# show mode
Security context mode: single
```

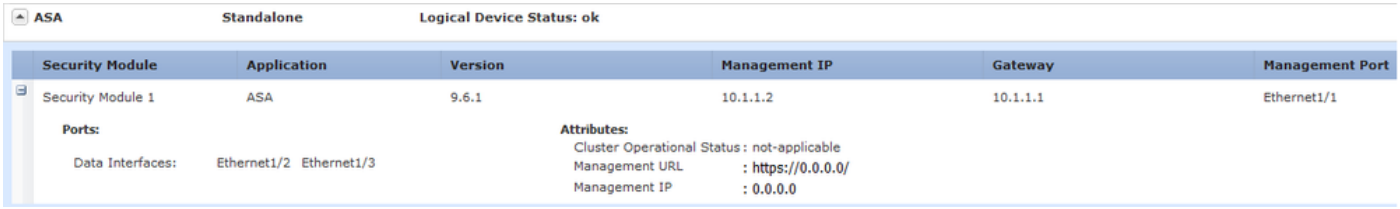
Como no existe la opción de configurar el modo de firewall desde el Administrador de chasis, debe hacerse desde la CLI de ASA:

```
asa(config)# firewall transparent

asa(config)# show firewall
Firewall mode: Transparent

asa(config)# wr mem
Building configuration...
Cryptochecksum: 746a107e aa0959e6 0f374a5f a004e35e
2070 bytes copied in 0.70 secs
[OK]
```

Después de guardar la configuración, se necesita una recarga, ya que se realiza con un dispositivo ASA incluso cuando el modo transparente ya está configurado en el dispositivo. Una vez que el dispositivo se ha iniciado, el dispositivo ya está configurado en modo transparente y toda la configuración se ha borrado como se esperaba, pero en el Administrador de chasis la configuración original que se implementó sigue apareciendo:

```
asa# show firewall
Firewall mode: Transparent

asa# show version | in up
Config file at boot was "startup-config"
asa up 1 min 30 secs
```

En el Administrador de chasis, se puede validar que la configuración del puerto de administración también se eliminó:




Es necesario realizar una reimplementación en la configuración de la interfaz de administración y en la configuración del clúster, si se aplica, desde el administrador de chasis hasta el dispositivo, como hicimos al principio de la implementación. El administrador de chasis vuelve a detectar el

dispositivo; en los primeros 5 minutos, se ve el estado del dispositivo como "El módulo de seguridad no responde", como se muestra en la imagen:


Después de un par de minutos, el dispositivo se reinicia:


# Verificación

Una vez que ASA está nuevamente en línea, se puede confirmar que el dispositivo está en modo transparente y con una dirección IP de administración con este comando de CLI:

```
asa# show firewall
Firewall mode: Transparent

asa# show ip
Management-only Interface: Ethernet1/1
System IP Address:
 ip address 10.1.1.3 255.255.255.0
Current IP Address:
 ip address 10.1.1.3 255.255.255.0


asa# show nameif
Interface       Name            Security
Ethernet1/1     management        0
```

La función de tener la capacidad de seleccionar un modo de firewall mientras se implementa un ASA desde el administrador de chasis se ha solicitado a través de los defectos CSCvc13164 y CSCvd91791.

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).