# Deploy ASA in Transparent Mode Within a FP9300

## Contents



## Introduction

This document describes how to deploy an ASA Transparent in a FP9300. By default when an ASA is deployed within a FP9300 the Firewall mode is Router, there is no option to select Transparent mode as we have it for the FTD template.

A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire”, or a “stealth firewall”, and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.

### Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- ASA Transparent Mode
- FP9300 Architecture

#### Components Used

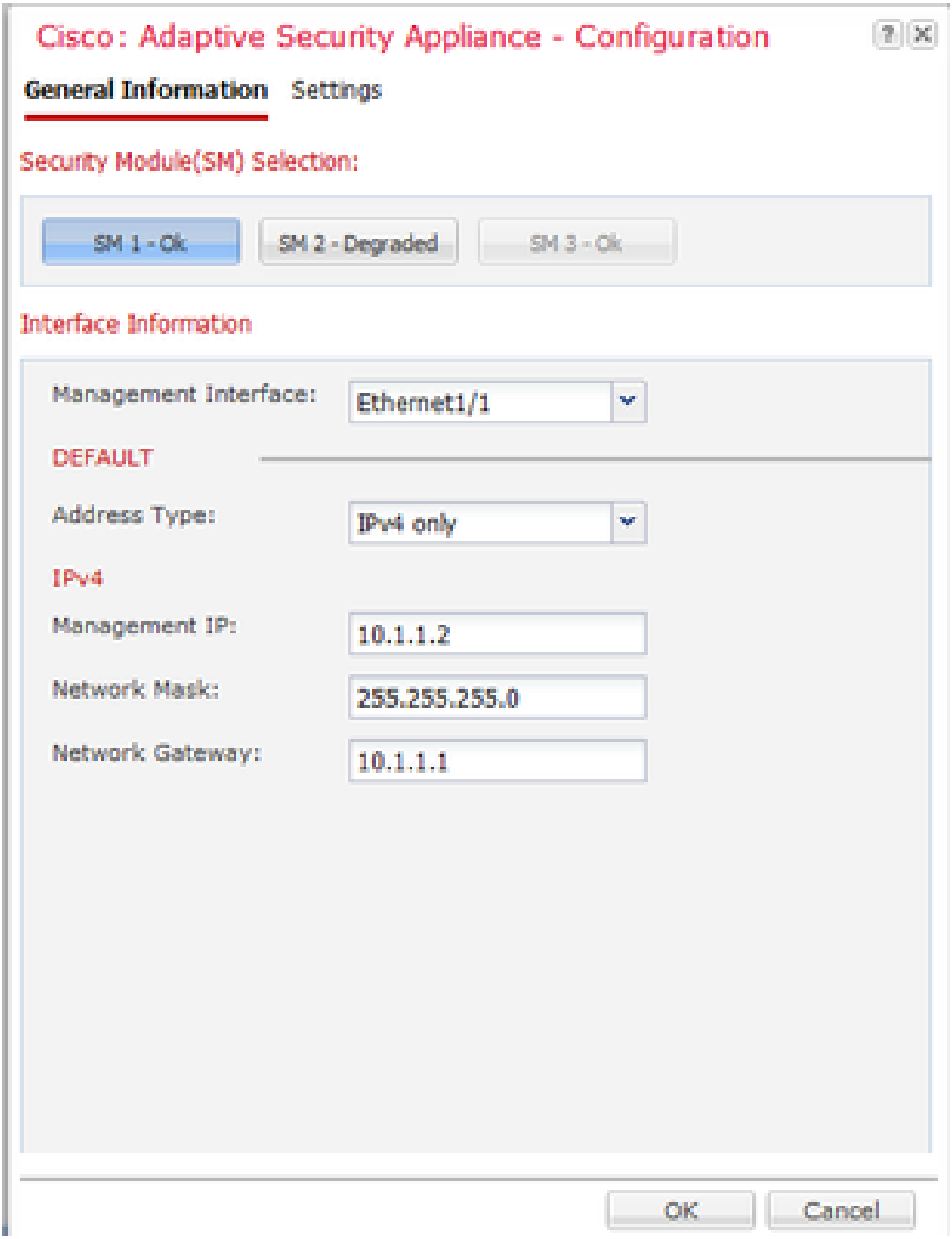
The information in this document is based on these software and hardware versions:

- FPR9K-SM-44 running FXOS version 2.3.1.73
- ASA software for FP9300 version 9.6.1

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, ensure that you understand the potential impact of any command.

## Configure

When Deploying an ASA there is no option to select the Firewall mode as it is when deploying FTD:




Once the ASA has been deployed, it is preconfigured in routed mode:

```
asa# show firewall
Firewall mode: Router

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

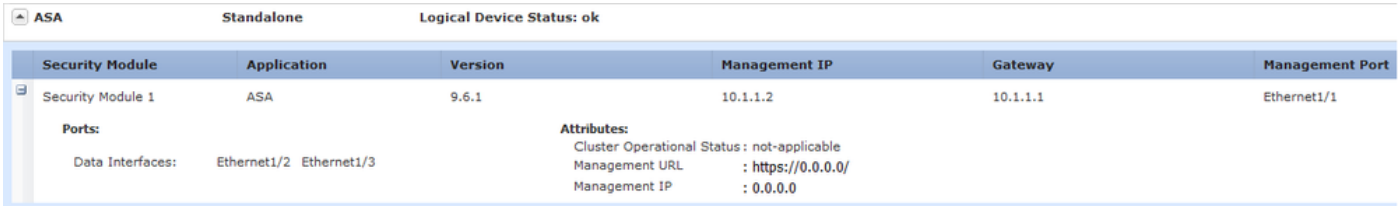
As there is no option to configure the Firewall mode from the **Chassis Manager,** it needs to be done from the ASA CLI:

```
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]
```

After the configuration is saved, a reload is needed as it is done with an ASA appliance even when the transparent mode is already setup on the device. Once the device has booted up, the device is already setup in transparent mode and all the configuration has been cleared as expected, but in the Chassis Manager the original configuration that was deployed still appears:

```
asa# show firewall
Firewall mode: Transparent

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

On the Chassis Manager, it can be validated that the **management port** configuration was also removed:




A re-deploy needs to be performed in the Management interface configuration and the Cluster configuration, if it applies, from the Chassis Manager to the device as we did at the beginning of the deployment. The Chassis Manager re-discovers the device; in the first 5 minutes it is seen the status of the device as "Security module not responding" as shown in the image:


After a couple of minutes, the device is restarted:


# Verify

Once the ASA is back online, it can be confirmed that the device is in transparent mode and with a Management IP address with this command from 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
```

The feature to have the ability to select a firewall mode while an ASA is deployed from the Chassis Manager has been requested through the defects CSCvc13164 and CSCvd91791.