Bereitstellung von ASA im transparenten Modus innerhalb eines FP9300

Inhalt

Einführung

In diesem Dokument wird die Bereitstellung eines ASA Transparent in einem FP9300 beschrieben. Wenn eine ASA in einem FP9300 bereitgestellt wird, ist der Firewall-Modus standardmäßig Router. Es gibt keine Option, den transparenten Modus auszuwählen, wie er für die FTD-Vorlage vorgesehen ist.

Eine transparente Firewall dagegen ist eine Layer-2-Firewall, die wie ein "Bump in the Wire" oder eine "Stealth-Firewall" funktioniert und nicht als Router-Hop auf verbundene Geräte angesehen wird. Wie bei jeder anderen Firewall wird die Zugriffskontrolle zwischen den Schnittstellen jedoch gesteuert, und es werden alle üblichen Firewall-Prüfungen durchgeführt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Transparenter ASA-Modus
- Architektur des FP9300

Verwendete Komponenten

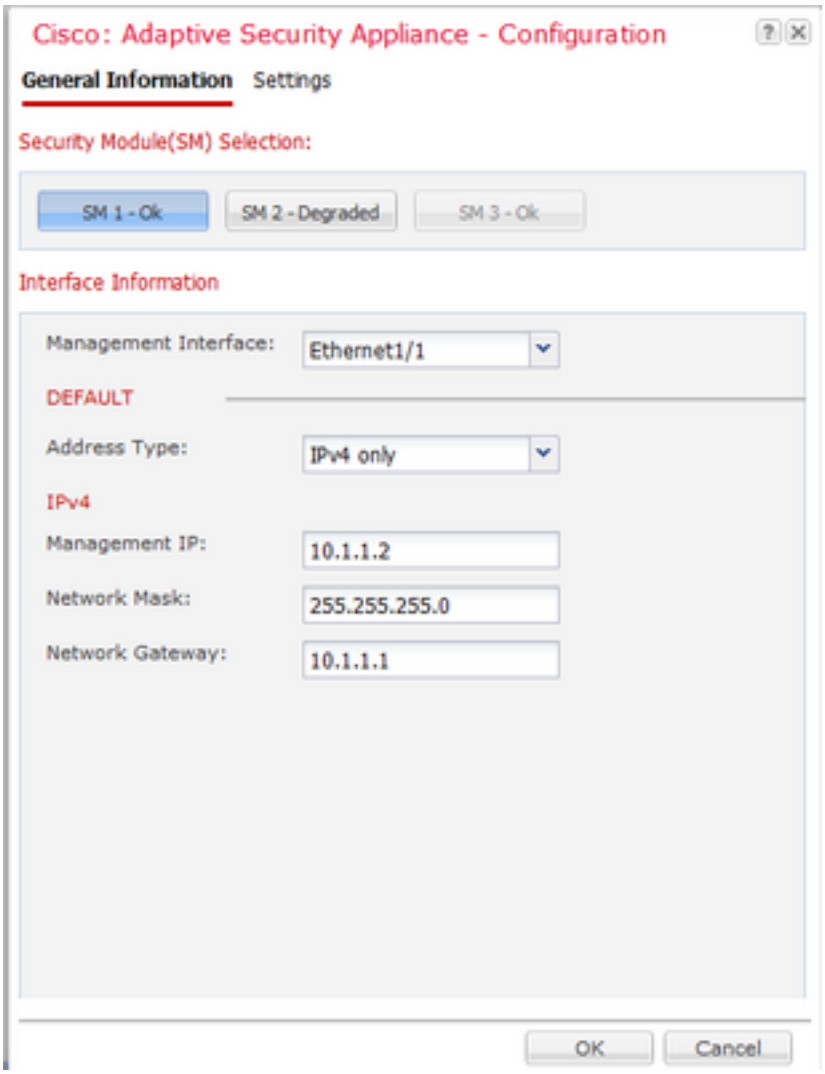
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- FPR9K-SM-44 mit FXOS-Version 2.3.1.73
- ASA Software für FP9300 Version 9.6.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Bei der Bereitstellung einer ASA gibt es keine Option, den Firewall-Modus bei der Bereitstellung von FTD auszuwählen:



Sobald die ASA bereitgestellt wurde, wird sie im Routing-Modus vorkonfiguriert:

```
asa# show firewall
Firewall mode: Router

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

Da es keine Option zum Konfigurieren des Firewall-Modus über den **Chassis Manager** gibt, muss dieser über die ASA-CLI erfolgen:

```
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]
```

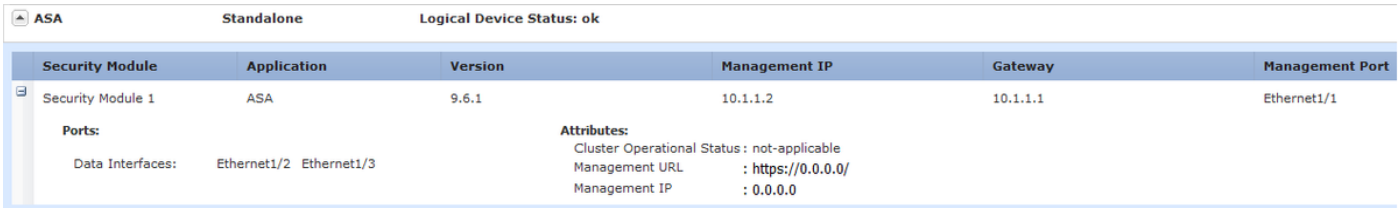
Nach dem Speichern der Konfiguration ist ein Neuladen wie bei einer ASA-Appliance erforderlich, selbst wenn der transparente Modus bereits auf dem Gerät eingerichtet ist. Nachdem das Gerät

gestartet wurde, wird das Gerät bereits im transparenten Modus eingerichtet, und alle Konfigurationen wurden wie erwartet gelöscht. Im Chassis Manager wird jedoch die ursprüngliche Konfiguration angezeigt, die bereitgestellt wurde:

```
asa# show firewall
Firewall mode: Transparent

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

Im Chassis Manager kann überprüft werden, ob die **Management-Port**-Konfiguration ebenfalls entfernt wurde:



Eine erneute Bereitstellung muss in der Management-Schnittstellenkonfiguration und, falls zutreffend, in der Cluster-Konfiguration vom Chassis Manager zum Gerät erfolgen, wie bereits zu Beginn der Bereitstellung. Der Chassis Manager erkennt das Gerät erneut. in den ersten 5 Minuten wird der Status des Geräts als "Sicherheitsmodul reagiert nicht" angezeigt, wie im Bild gezeigt:

Nach einigen Minuten wird das Gerät neu gestartet:

Überprüfen

Wenn die ASA wieder online ist, kann mit dem folgenden Befehl aus der CLI bestätigt werden, dass sich das Gerät im transparenten Modus befindet und eine Management-IP-Adresse hat:

```
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
```

Die Funktion zur Auswahl eines Firewall-Modus während der Bereitstellung einer ASA über den Chassis Manager wurde durch die Fehler CSCvc13164 und CSCvd91791 angefordert.