

Déployez l'ASA en mode transparent dans un FP9300

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Vérifiez](#)

Introduction

Ce document décrit comment déployer une ASA transparente dans un FP9300. Par défaut quand une ASA est déployée dans un FP9300 le mode de Pare-feu est routeur, là n'est aucune option de sélectionner le mode transparent car nous le prenons pour le modèle FTD.

Un Pare-feu transparent, d'autre part, est un Pare-feu de la couche 2 qui agit comme un « bosse sur le fil », ou un « pare-feu furtif », et n'est pas vu comme saut de routeur aux périphériques connectés. Cependant, comme n'importe quel autre Pare-feu, le contrôle d'accès entre les interfaces est commandé, et tous les contrôles habituels de Pare-feu sont en place.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Mode transparent ASA
- Architecture FP9300

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FPR9K-SM-44 exécutant la [version 2.3.1.73](#) FXOS
- Logiciel ASA pour la [version 9.6.1](#) FP9300

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Configurez

Quand déployer une ASA là n'est aucune option de sélectionner le mode de Pare-feu car il est en déployant [FTD](#) :

Cisco: Adaptive Security Appliance - Configuration

General Information Settings

Security Module(SM) Selection:

SM 1 - Ok SM 2 - Degraded SM 3 - Ok

Interface Information

Management Interface: Ethernet1/1

DEFAULT

Address Type: IPv4 only

IPv4

Management IP: 10.1.1.2

Network Mask: 255.255.255.0

Network Gateway: 10.1.1.1

OK Cancel

Une fois que l'ASA a été déployée, elle est préconfigurée en mode conduit :

```
asa# show firewall
Firewall mode: Router
```

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

Car il n'y a aucune option de configurer le mode de Pare-feu du **gestionnaire de châssis**, il doit être fait de l'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]
```

Après que la configuration soit enregistrée, une recharge est nécessaire comme elle est faite avec une appliance ASA même lorsque le mode transparent est déjà installé sur le périphérique. Une

fois que le périphérique a initialisé, le périphérique est déjà installé en mode transparent et toute la configuration a été effacée comme prévue, mais dans le gestionnaire de châssis la configuration d'origine qui était déployée toujours apparaît :

```
asa# show firewall
Firewall mode: Transparent
```

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

Sur le gestionnaire de châssis, il peut valider que la configuration de port de gestion a été également retirée :

Security Module	Application	Version	Management IP	Gateway	Management Port
Security Module 1	ASA	9.6.1	10.1.1.2	10.1.1.1	Ethernet1/1
Ports:		Attributes:			
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable			
		Management URL : https://0.0.0.0/			
		Management IP : 0.0.0.0			

Un redéploiement doit être exécuté en configuration d'interface de gestion et configuration du cluster, s'il s'applique, du gestionnaire de châssis au périphérique comme nous avons fait au début du déploiement. Le gestionnaire de châssis redécouvre le périphérique ; dans les 5 premiers minute l'est vu le statut du périphérique en tant que « module de Sécurité ne répondant pas » suivant les indications de l'image :

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	ASA	9.6.1	10.1.1.3	10.1.1.1	Ethernet1/1	Security module not responding
Ports:		Attributes:				
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable				
		Management URL : https://0.0.0.0/				
		Management IP : 0.0.0.0				

Après quelques minutes, le périphérique est redémarré :

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	ASA	9.6.1	10.1.1.3	10.1.1.1	Ethernet1/1	starting
Ports:		Attributes:				
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable				
		Management URL : https://0.0.0.0/				
		Management IP : 0.0.0.0				

Vérifiez

Une fois que l'ASA est de retour en ligne, il peut confirmer que le périphérique est en mode transparent et avec une adresse IP de Gestion avec cette commande 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 caractéristique pour avoir la capacité de sélectionner un mode de Pare-feu tandis qu'une ASA est déployée du gestionnaire de châssis a été demandée par les défauts [CSCvc13164](#) et [CSCvd91791](#).