

# Implementazione di un'appliance ASA in modalità trasparente all'interno di un FP9300

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

## Introduzione

Questo documento descrive come distribuire un'ASA trasparente in un FP9300. Per impostazione predefinita, quando un ASA viene distribuito in un FP9300, la modalità firewall è Router e non è possibile selezionare la modalità trasparente come nel modello FTD.

Un firewall trasparente, d'altra parte, è un firewall di layer 2 che funziona come un "bump in the wire" (urto sul filo) o un "firewall stealth" (nascosto) e non viene visto come un router hop verso i dispositivi connessi. Tuttavia, come qualsiasi altro firewall, il controllo degli accessi tra le interfacce è controllato e sono in atto tutti i normali controlli del firewall.

## Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Modalità ASA trasparente
- Architettura FP9300

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FPR9K-SM-44 con FXOS versione [2.3.1.73](#)
- Software ASA per FP9300 versione [9.6.1](#)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

Quando si distribuisce un'ASA, non è possibile selezionare la modalità firewall così come è quando si distribuisce l'[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

Una volta distribuita, l'ASA è preconfigurata in modalità di routing:

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

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

Poiché non è disponibile un'opzione per configurare la modalità firewall da **Chassis Manager**, occorre farlo dalla CLI dell'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]
```

Dopo aver salvato la configurazione, è necessario ricaricare il dispositivo come se si trattasse di un accessorio ASA, anche se la modalità trasparente è già stata impostata sul dispositivo. Una

volta avviato il dispositivo, è già impostato in modalità trasparente e tutta la configurazione è stata cancellata come previsto, ma in Gestione chassis la configurazione originale distribuita continua a essere visualizzata:

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

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

In Chassis Manager è possibile verificare che anche la configurazione della porta di gestione sia stata rimossa:



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
<b>Ports:</b>		<b>Attributes:</b>			
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable			
		Management URL : https://0.0.0.0/			
		Management IP : 0.0.0.0			

È necessario eseguire una reinstallazione nella configurazione dell'interfaccia di gestione e nella configurazione del cluster, se applicabile, da Gestione chassis al dispositivo, come è stato fatto all'inizio dell'installazione. Chassis Manager individua nuovamente il dispositivo; nei primi 5 minuti viene visualizzato lo stato del dispositivo come "Modulo di sicurezza che non risponde", come mostrato nell'immagine:



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
<b>Ports:</b>		<b>Attributes:</b>				
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable				
		Management URL : https://0.0.0.0/				
		Management IP : 0.0.0.0				

Dopo alcuni minuti, il dispositivo viene riavviato:



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
<b>Ports:</b>		<b>Attributes:</b>				
Data Interfaces: Ethernet1/2 Ethernet1/3		Cluster Operational Status: not-applicable				
		Management URL : https://0.0.0.0/				
		Management IP : 0.0.0.0				

## Verifica

Una volta che l'ASA è tornata online, è possibile verificare che il dispositivo sia in modalità trasparente e con un indirizzo IP di gestione con questo comando dalla 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 funzionalità che consente di selezionare una modalità firewall mentre un'ASA viene distribuita da Chassis Manager è stata richiesta tramite i difetti [CSCvc13164](#) e [CSCvd91791](#).