Configuration des adresses MAC virtuelles pour FTD HA

Table des matières

Introduction	
Conditions préalables	
Exigences	
Composants utilisés	
Informations générales	
Configuration	
Vérification	

Introduction

Ce document décrit comment configurer des adresses MAC virtuelles sur une paire haute disponibilité (HA) FTD (Firewall Threat Defense).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protection pare-feu contre les menaces (FTD)
- Centre de gestion du pare-feu sécurisé (FMC)

Composants utilisés

- FMC version virtuelle 7.2.8
- FTD version virtuelle 7.2.7

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La configuration d'adresses MAC virtuelles sur une paire FTD HA est bénéfique pour la disponibilité d'un réseau. Les adresses MAC virtuelles permettent au FTD principal et secondaire de maintenir des adresses MAC cohérentes, ce qui empêche certaines interruptions du trafic.

Si aucune adresse MAC virtuelle n'est configurée, chaque unité de la paire haute disponibilité

démarre à l'aide de ses adresses MAC gravées. Dans le cas où l'unité secondaire démarre sans détecter l'unité principale, elle devient l'unité active et utilise ses adresses MAC gravées. Lorsque l'unité principale est mise en ligne, l'unité secondaire obtient les adresses MAC de l'unité principale, ce qui peut entraîner des interruptions du réseau. De nouvelles adresses MAC sont également utilisées si l'unité principale est remplacée par un nouveau matériel. La configuration d'adresses MAC virtuelles sur les périphériques vous protège contre cette interruption. En effet, l'unité secondaire connaît les adresses MAC des unités principales à tout moment et continue d'utiliser les adresses MAC correctes lorsqu'elle est le périphérique actif, même si elle se met en ligne avant l'unité principale.



Remarque : les termes adresse MAC virtuelle et adresse MAC d'interface peuvent être utilisés de manière interchangeable.

Pour plus d'informations sur les avantages de cette configuration, reportez-vous à ce guide.

Configuration

1. Dans l'interface utilisateur graphique de FMC, accédez à la page Devices et modifiez la paire HA en cliquant sur l'icône du crayon à l'extrême droite.

Fi 💀	rewall Management Center Overview Analysis	Policies Devices Objects	Integration	1			Deploy Q 🍯	🖇 🧔 admin 🔹 🏤 SECURE
View By: All (2)	Group • • Error (0) • Warning (0) • Offline (0) • Normal (2)	Deployment Pending (0) • Up	grade (0) 🔹	Snort 3 (2)				Deployment History Q. Search Device Add •
Collaose A								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (1)							
	FTD_HA High Availability							×
	FTD Primary 192.168.192.13(Primary, Active) Short 3 192.168.192.13 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	e9	I
	FTD Secondary 192.168.192.16(Secondary, Standby) Snott 3 192.168.192.16 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	49	:

Paire FTD HA

2. Sous l'onglet Haute disponibilité, localisez la zone intitulée Adresses MAC d'interface. Cliquez sur l'icône + pour accéder à l'éditeur.

FTD Primary 192.168.192.1 Cisco Firepower Threat Defense for VMWare	3										Cancel
Summary High Availability Device	Routing Interfaces	Inline Sets DHCP	VTEP								
High Availability Configuration											
High Availability Link					State Link						
Interface			GigabitEthernet0/0		Interface					GigabitE	(thernet0/0
Logical Name			fover_link		Logical Name						fover_link
Primary IP			1.1.1.1		Primary IP						1.1.1.1
Secondary IP			1.1.1.2		Secondary IP						1.1.1.2
Subnet Mask			255.255.255.0		Subnet Mask					255	255.255.0
IPsec Encryption			Disabled		Statistics						٩
Monitored Interfaces											
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6			Active Link-Local IPv6		Standby Link-Local IP	ve	Monitoring	
Inside	10.10.75.254									•	/
diagnostic										•	/
Outside	10.10.10.231									•	/
Calleurs Triages Oritoria				— Г	Interface MAC Addresse						
Failure Limit	Failure of 1 Interfaces									+	
Peer Poll Time			1 sec		Physical Interface		Active Mac Addre	155	Standby Mac Addr	035	
Peer Hold Time			15 sec				No reco	rds to display			
Interface Poll Time			5 sec								
Interface Hold Time			25 sec								
				L							

Boîte de dialogue Adresses MAC des interfaces

3. Dans l'éditeur, sélectionnez l'interface physique et configurez les adresses Mac de l'interface active/veille. Cliquez sur OK lorsque vous avez terminé.

Add Interface Mac Address
Physical Interface:*
GigabitEthernet0/1
Active Interface Mac Address:*
dead.beef.0001
Standby Interface Mac Address:*
dead.beef.0002
Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab
Cancel OK

Création d'adresse MAC d'interface



Remarque : lors de la configuration des adresses MAC virtuelles, il est utile de respecter une convention standard. Les adresses au sein des interfaces doivent être des adresses MAC valides, mais elles peuvent être de nature arbitraire. L'utilisation d'une convention standard facilite la gestion lors de la vérification des tables d'adresses MAC en amont ou en aval. Le formatage des adresses MAC nécessite 12 chiffres hexadécimaux avec des points séparant chaque ensemble de 4 chiffres.

4. Répétez le processus pour toutes les interfaces restantes nécessitant des configurations d'adresses Mac virtuelles.

5. Vérifiez que les configurations sont correctes.

Interface MAC Addresses			+
Physical Interface	Active Mac Address	Standby Mac Address	
GigabitEthernet0/1	dead.beef.0001	dead.beef.0002	/1
GigabitEthernet0/2	dead.beef.0003	dead.beef.0004	/1

Configuration des adresses Mac des interfaces

6. Enregistrez et déployez les configurations sur la paire FTD HA.

Vérification

À partir de chacun des périphériques exécutant des configurations, les adresses Mac virtuelles apparaissent maintenant.

DFT principal (actif) :

firepower	r# show run grep failover	
failover		
failover	lan unit primary	
failover	lan interface fover_link GigabitEthernet0/0	
failover	replication http	
failover	<pre>mac address GigabitEthernet0/1 dead.beef.0001</pre>	dead.beef.0002
failover	<pre>mac address GigabitEthernet0/2 dead.beef.0003</pre>	dead.beef.0004
failover	link fover_link GigabitEthernet0/0	
failover	interface ip fover_link 1.1.1.1 255.255.255.0	standby 1.1.1.2

Afficher les résultats du basculement Exécuter

> show interface "Inside"
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address dead.beef.0001, MTU 1500
IP address 10.10.75.254, subnet mask 255.255.255.0
1639 packets input, 108958 bytes, 0 no buffer

Afficher les résultats internes de l'interface

```
> show interface "Outside"
Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address dead.beef.0003, MTU 1500
IP address 10.10.10.231, subnet mask 255.255.255.0
```

Afficher les résultats externes de l'interface

FTD secondaire (en veille) :

Afficher les résultats du basculement Exécuter

> show interface "Inside" Interface GigabitEthernet0/1 "Inside", is up, line protocol is up Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps) Input flow control is unsupported, output flow control is unsupported MAC address dead.beef.0002, MTU 1500

Afficher les résultats internes de l'interface

```
> show interface "Outside"
```

Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address dead.beef.0004, MTU 1500

Afficher les résultats externes de l'interface

Cela confirme que la configuration a réussi.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.