Concepts avancés et conseils de dépannage relatifs au mode pare-feu transparent Firepower Threat Defense

Contenu

Introduction

Ce document décrit une explication détaillée pour comprendre les concepts et les éléments de base d'un déploiement Firepower Threat Defense (FTD) en mode TFW (Transparent Firewall). Cet article fournit également des outils et des procédures pas à pas utiles pour résoudre les problèmes les plus courants liés à l'architecture de pare-feu transparent.

Contribué par Cesar Lopez et édité par Yeraldin Sánchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances en mode de pare-feu transparent Cisco FTD

- Concepts du protocole HSRP (Hot Standby Router Protocol)
- Protocoles ARP (Address Resolution Protocol) et ICMP (Internet Control Message Protocol)

Il est fortement recommandé de lire la section Guide de configuration Firepower Mode transparent ou mode pare-feu routé pour mieux comprendre les concepts décrits dans ce document.

Components Used

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

- Cisco Firepower 4120 FTD version 6.3.0.4
- Cisco Firepower Management Center (FMC) version 6.3.0.4
- Cisco ASR1001 IOS-XE version 16.3.9
- Cisco Catalyst 3850 IOS-XE version 16.9.3

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.

Concepts avancés du pare-feu transparent

Table d'adresses MAC

Alors qu'un pare-feu en mode routé s'appuie sur la table de routage et la table ARP pour déterminer l'interface de sortie et les données nécessaires pour transférer un paquet au tronçon suivant, le mode TFW utilise la table d'adresses MAC pour déterminer l'interface de sortie utilisée pour envoyer un paquet à sa destination. Le pare-feu examine le champ d'adresse MAC de destination du paquet traité et recherche une entrée reliant cette adresse à une interface.

La table d'adresses MAC comporte ces champs.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Outside 0050.56a5.6d52 dynamic 1 1
Inside 0000.0c9f.f014 dynamic 3 1
```

- Interface : ce champ contient le nom de l'interface à partir de laquelle cette adresse MAC a été apprise dynamiquement ou configurée de manière statique.
- Adresse MAC : enregistrement d'adresse MAC à stocker
- type : méthode utilisée pour apprendre l'entrée. Il peut être dynamique ou statique
- Age(min) - Minuteur de décrément en minutes affichant le temps restant avant que cette entrée soit marquée comme morte. Ce compteur s'applique uniquement aux entrées d'apprentissage dynamique
- bridge-group - ID de groupe de ponts auquel appartient l'interface

La décision de transfert de paquets est similaire à celle d'un commutateur, mais il y a une différence très importante lorsqu'il s'agit d'une entrée manquante dans la table MAC. Dans un commutateur, le paquet est diffusé via toutes les interfaces, à l'exception de l'interface d'entrée, mais dans TFW, si un paquet est reçu et qu'il n'y a pas d'entrée pour l'adresse MAC de destination, le paquet est abandonné. Il est ignoré avec le code de suppression ASP (Accelerated

Security Path) *dst-l2_lookup-fail*.

```
FTD63# show cap icmpin trace pack 1

7 packets captured

1: 00:20:22.338391 802.1Q vlan#20 P0 10.10.10.5 > 20.20.20.5 icmp: echo request
Result:
input-interface: Inside
input-status: up
input-line-status: up
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```

Cette condition se produit toujours pour le premier paquet d'un environnement avec apprentissage dynamique activé et sans entrée statique pour une destination si l'adresse MAC n'était pas vue auparavant dans un paquet comme adresse MAC source.

Une fois l'entrée ajoutée à la table d'adresses MAC, le paquet suivant peut être conditionné aux fonctions de pare-feu activées.

```
FTD63# show cap icmpin trace pack 2

7 packets captured

2: 00:20:27.329206 802.1Q vlan#20 P0 10.10.10.5 > 20.20.20.5 icmp: echo request
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc Outside
```

> **Attention** : La recherche MAC est la première phase des actions entreprises par le pare-feu. Les pertes constantes dues à des recherches de couche 2 échouées peuvent entraîner une perte de paquets appropriée et/ou une inspection incomplète du moteur de détection. L'affectation dépend de la capacité du protocole ou de l'application à retransmettre.

Compte tenu de ce qui précède, il est toujours préférable d'avoir une entrée apprise avant toute transmission. TFW a plusieurs mécanismes pour apprendre une entrée.

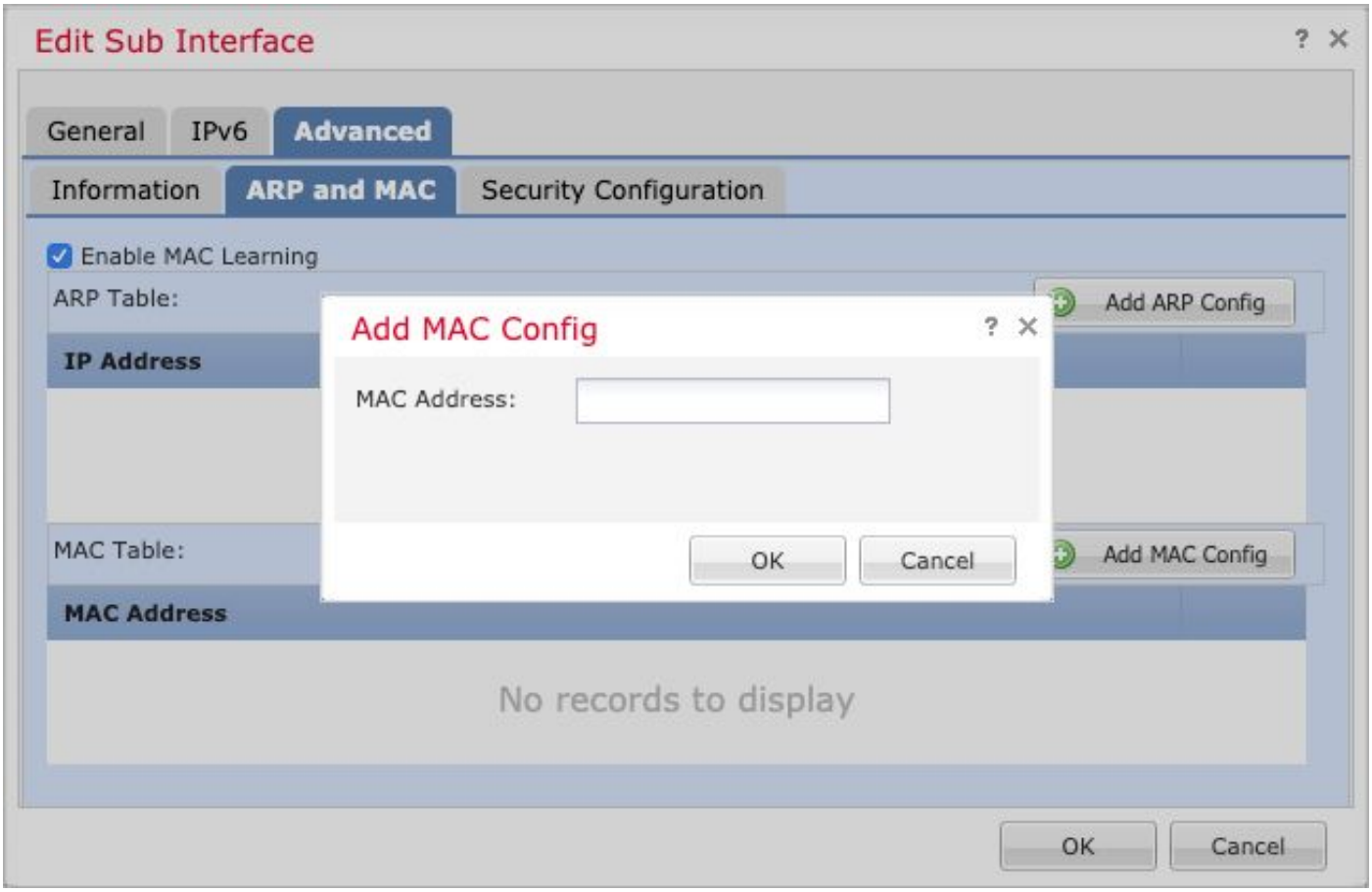
Options d'apprentissage de la table d'adresses MAC

Entrées statiques

Les adresses MAC peuvent être ajoutées manuellement pour que le pare-feu utilise toujours la même interface pour cette entrée spécifique. Cette option est valide pour les entrées qui ne sont pas susceptibles de modification. Il s'agit d'une option courante lorsque l'adresse MAC statique est écrasée au niveau de configuration ou par une fonction au saut suivant.

Par exemple, dans un scénario où l'adresse MAC de la passerelle par défaut sera toujours la même sur un routeur Cisco qu'elle a été ajoutée manuellement à la configuration ou si l'adresse MAC virtuelle HSRP restera la même.

Afin de configurer des entrées statiques dans FTD géré par FMC, vous pouvez cliquer sur **Edit Interface / Subinterface > Advanced > ARP and MAC** et sur **Add MAC Config**. Ceci ajoute une entrée pour l'interface spécifique qui est modifiée à partir de la section **Périphériques > Gestion des périphériques > Interfaces**.



Apprentissage dynamique basé sur l'adresse MAC source

Cette méthode est similaire à celle utilisée par un commutateur pour remplir la table d'adresses MAC. Si un paquet a une adresse MAC source qui ne fait pas partie des entrées de la table MAC pour l'interface qu'il a reçue, une nouvelle entrée est ajoutée à la table.

Apprentissage dynamique basé sur la sonde ARP

Si un paquet arrive avec une adresse MAC de destination qui ne fait pas partie de la table MAC et que l'adresse IP de destination fait partie du même réseau que l'interface virtuelle de pont (BVI), le TFW tente de l'apprendre en envoyant une requête ARP via toutes les interfaces de groupe de ponts. Si une réponse ARP est reçue de l'une des interfaces du groupe de pontage, elle est ajoutée à la table MAC. Notez que, comme il a été mentionné ci-dessus, bien qu'il n'y ait pas de réponse à cette requête ARP, tous les paquets sont abandonnés avec le code ASP *dst-l2_lookup-fail*.

Apprentissage dynamique basé sur la sonde ICMP

Si un paquet arrive avec une adresse MAC de destination qui ne fait pas partie de la table MAC et que l'adresse IP de destination NE fait PAS partie du même réseau que l'interface BVI, une requête d'écho ICMP est envoyée avec une valeur de durée de vie égale à 1. Le pare-feu attend qu'un message ICMP Time Exceeded (Délai dépassé) apprenne l'adresse MAC du tronçon

suivant.

Minuteur d'âge de la table d'adresses MAC

Le compteur Age de la table d'adresses MAC est défini sur 5 minutes pour chaque entrée apprise. Cette valeur de délai d'attente comporte deux étapes différentes.

Délai d'expiration du premier stade

Au cours des 3 premières minutes, la valeur Age de l'entrée MAC n'est pas actualisée à moins qu'un paquet de réponse ARP passant par le pare-feu avec l'adresse MAC source soit égal à une entrée dans la table d'adresses MAC. Cette condition exclut les réponses ARP destinées aux adresses IP du groupe de ponts. Cela signifie que tout autre paquet qui n'est pas une réponse ARP prête à l'emploi est ignoré au cours des 3 premières minutes.

Dans cet exemple, il existe un PC dont l'adresse IP est 10.10.10.5 envoyant une requête ping à 10.20.20.5. L'adresse IP de la passerelle pour 10.20.20.5 est 10.20.20.3 avec l'adresse MAC 0000.0c9f.f014.

L'ordinateur de destination crée une mise à jour ARP toutes les 25 secondes, ce qui entraîne l'acheminement des paquets ARP constants par le pare-feu.

```
FTD63# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 3 1
Outside 0050.56a5.6d52 dynamic 5 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 4 1
```

Un filtrage de paquets des paquets ARP est utilisé pour faire correspondre ces paquets.

```
> show capture

capture arp type raw-data ethernet-type arp interface Inside [Capturing - 1120 bytes]

>show capture arp

12 packets captured

1: 23:04:52.142524 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
2: 23:04:52.142952 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
3: 23:04:52.145057 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
4: 23:04:52.145347 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
5: 23:05:16.644574 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
6: 23:05:16.644940 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
7: 23:05:16.646756 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
8: 23:05:16.647015 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
9: 23:05:41.146614 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
10: 23:05:41.146980 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
11: 23:05:41.148734 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
12: 23:05:41.149009 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
```

L'entrée 000.0c9f.4014 reste à 5 et ne descend jamais en dessous de ce nombre.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 3 1
Outside 0050.56a5.6d52 dynamic 5 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 4 1
```

Délai d'expiration en deuxième étape

Au cours des 2 dernières minutes, l'entrée tombe dans une période où l'adresse est considérée comme obsolète.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 5 1
Outside 0050.56a5.6d52 dynamic 3 1
Inside 0000.0c9f.f014 dynamic 2 1
Outside 40a6.e833.2a05 dynamic 3 1
```

L'entrée n'est pas encore supprimée et si un paquet dont l'adresse MAC source correspond à l'entrée de table, y compris les paquets prêts à l'emploi, est détecté, l'entrée Age est rétablie à 5 minutes.

Dans cet exemple, une requête ping est envoyée au cours de ces 2 minutes pour forcer le pare-feu à envoyer son propre paquet ARP.

```
> ping 10.20.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

L'entrée d'adresse MAC est rétablie à 5 minutes.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 4 1
Outside 0050.56a5.6d52 dynamic 2 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 5 1
```

Table ARP

Tout d’abord, il est essentiel de comprendre que la table d’adresses MAC est entièrement indépendante de la table ARP. Bien que les paquets ARP envoyés par le pare-feu pour actualiser une entrée ARP puissent, en même temps, actualiser la table d'adresses MAC, ces processus d'actualisation sont une tâche distincte et chacun a ses propres délais d'expiration et conditions.

Même si la table ARP n'est pas utilisée pour déterminer le tronçon suivant de sortie comme en mode routé, il est important de comprendre l'effet des paquets ARP générés et destinés aux IP

d'identité de pare-feu dans un déploiement transparent.

Les entrées ARP sont utilisées à des fins de gestion et ne sont ajoutées à la table que si une fonction ou une tâche de gestion l'exige. Par exemple, si un groupe de ponts possède une adresse IP, cette adresse IP peut être utilisée pour envoyer une requête ping à la destination.

```
> show ip
Management-only Interface: Ethernet1/4
System IP Address:
no ip address
Current IP Address:
no ip address
Group : 1
Management System IP Address:
ip address 10.20.20.4 255.255.255.0
Management Current IP Address:
ip address 10.20.20.4 255.255.255.0
```

Si la destination se trouve dans le même sous-réseau que l'adresse IP du groupe de ponts, elle force une requête ARP et si une réponse ARP valide est reçue, l'entrée IP/MAC est stockée dans la table ARP.

```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 6
```

Contrairement à la table d'adresses MAC, le compteur qui accompagne le triplet interface/adresse IP/adresse MAC est une valeur croissante.

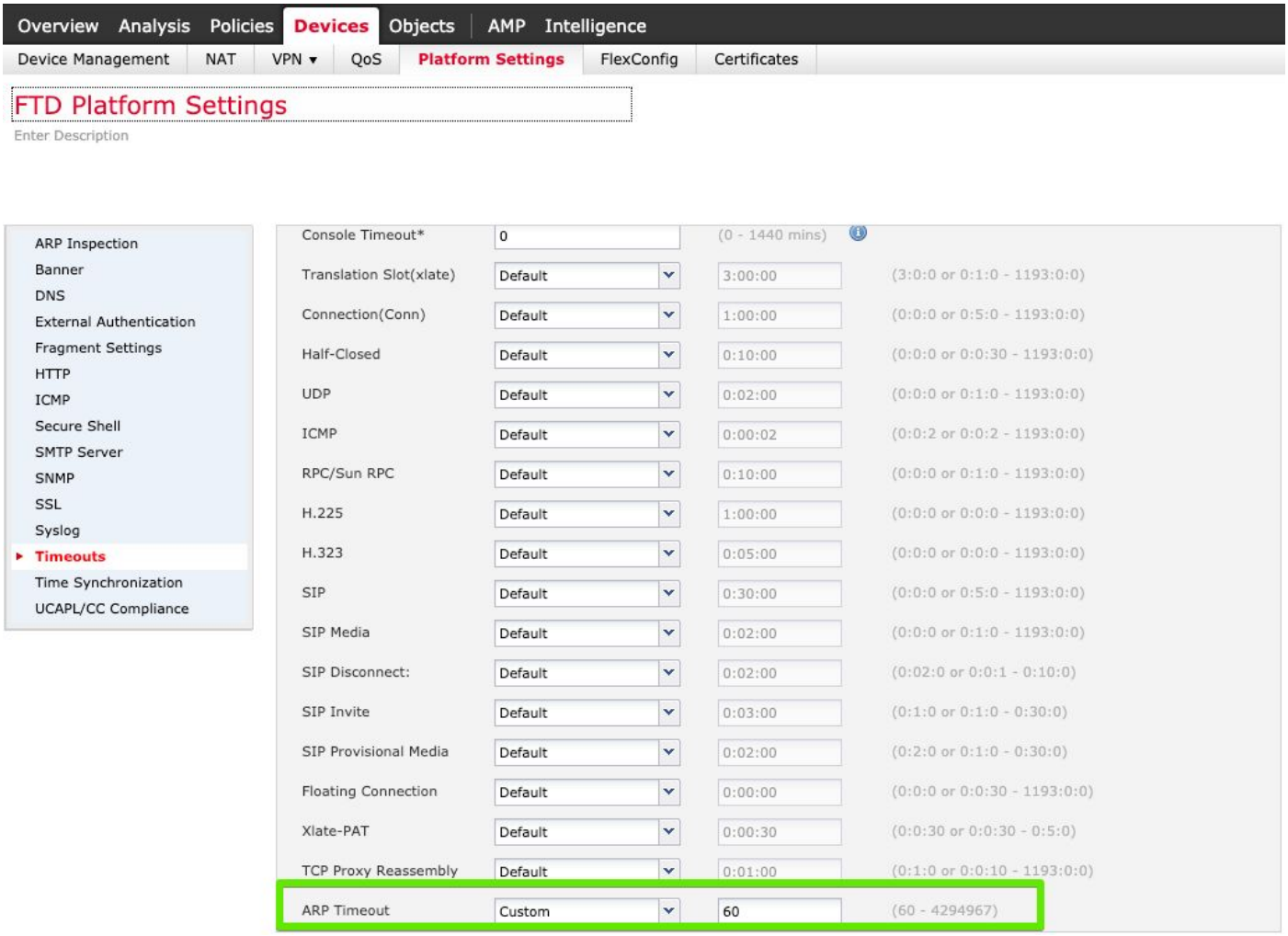
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Lorsque le temporisateur atteint une valeur *n - 30* où *n* est le délai d'expiration configuré ARP (avec une valeur par défaut de 14 400 secondes), le pare-feu envoie une requête ARP pour actualiser l'entrée. Si une réponse ARP valide est reçue, l'entrée est conservée et le compteur revient à 0.

Dans cet exemple, le délai ARP a été réduit à 60 secondes.

```
> show running-config arp
arp timeout 60
arp rate-limit 32768
```

Ce délai d'attente peut être configuré dans l'onglet **Devices > Platform Settings > Timeouts** de FMC, comme illustré dans l'image.



Comme le délai d'attente est de 60 secondes, une requête ARP est envoyée toutes les 30 secondes (60 - 30 = 30).

```
> show capture arp

8 packets captured

1: 21:18:16.779729 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
2: 21:18:16.780111 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
3: 21:18:46.779744 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
4: 21:18:46.780126 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
5: 21:19:16.779744 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
6: 21:19:16.780111 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
7: 21:19:46.779729 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
8: 21:19:46.780126 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
```

L'entrée ARP est ensuite actualisée toutes les 30 secondes.

```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 29
>show arp
Inside 10.20.20.3 0000.0c9f.f014 0
```

Conseils de dépannage

Direction du trafic

Une des choses les plus difficiles à suivre sur un TFW est la direction du flux de trafic. Comprendre comment le trafic circule permet de s'assurer que le pare-feu transfère correctement les paquets vers la destination.

La détermination de la bonne interface d'entrée et de sortie est une tâche plus facile en mode routé, car il existe plusieurs indicateurs de l'implication du pare-feu, tels que la modification des adresses MAC source et de destination et la réduction de la valeur de durée de vie (TTL) d'une interface à l'autre.

Ces différences ne sont pas disponibles sur une configuration TFW. Dans la plupart des cas, le paquet qui passe par l'interface d'entrée est identique à celui qui sort du pare-feu.

Des problèmes spécifiques, tels que les volets MAC dans le réseau ou les boucles de trafic, peuvent être plus difficiles à suivre sans savoir où le paquet est entré et quand il a quitté le pare-feu.

Pour aider à différencier les entrées des paquets de sortie, le mot clé trace peut être utilisé dans les captures de paquets.

```
capture in interface inside buffer 33554432 trace trace-count 1000 match tcp host 10.10.220.42
host 10.10.241.225
capture out interface outside buffer 33554432 trace trace-count 1000 match tcp host 10.10.220.42
host 10.10.241.225
```

buffer - Augmente le tampon de capture en octets. 33554432 est la valeur maximale disponible. Dans les modèles tels que 5500-X, les appliances Firepower ou les machines virtuelles, il est sûr d'utiliser cette valeur de taille tant qu'il n'y a pas de douzaines de captures déjà configurées.

trace - Active l'option trace pour le capturé spécifié.

trace-count - Permet un nombre plus élevé de traces. 1000 est le maximum autorisé et 128 est le maximum par défaut. Ceci est également sûr en suivant la même recommandation quant à l'option de taille de tampon.

> **Astuce** : Si vous oubliez d'ajouter l'une des options, vous pouvez l'ajouter sans avoir à réécrire la capture entière en référençant le nom de la capture et l'option. Cependant, la nouvelle option n'affecte que les paquets nouvellement capturés, de sorte qu'un ***nom*** de ***casque de capture clair*** doit être utilisé pour avoir le nouvel effet depuis le paquet numéro 1. Exemple : **capture dans trace**

Une fois les paquets capturés, la commande **show capture *cap_name* trace** affiche les 1 000 premières traces (si le numéro de trace a été augmenté) des paquets entrants.

```
FTD63# show capture out trace
1: 16:34:56.940960 802.1Q vlan#7 P0 10.10.241.225 > 10.10.220.38 icmp: time exceeded in-transit
Result: input-interface: outside input-status: up input-line-status: up Action: drop Drop-
reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed 2: 16:34:57.143959 802.1Q vlan#7 P0
10.10.220.42 > 10.10.241.225 icmp: echo request 3: 16:34:57.146476 802.1Q vlan#7 P0
10.10.241.225 > 10.10.220.42 icmp: echo reply Result: input-interface: outside input-status: up
input-line-status: up Action: drop Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```

Ce résultat est un exemple des traces de capture de paquets d'interface externe. Cela signifie que les numéros de paquet 1 et 3 ont saisi l'interface externe et que le numéro de paquet 2 a quitté

l'interface.

Des informations supplémentaires peuvent être trouvées dans cette trace, telles que l'action prise pour ce paquet et la raison de rejet au cas où le paquet serait abandonné.

Pour des traces plus longues et si vous voulez vous concentrer sur un seul paquet, la commande **show capture** *cap_name* **trace packet-number** *packet_*numberpeut être utilisée pour afficher la trace de ce paquet spécifique.

Voici un exemple de numéro de paquet autorisé 10.

```
FTD63# show capture in detail trace packet-number 10

10: 20:55:31.118218 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98 802.1Q vlan#20 P0
10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos 0xc0] [ttl 1] (id 0) Phase: 1 Type:
L2-EGRESS-IFC-LOOKUP Subtype: Destination MAC L2 Lookup Result: ALLOW Config: Additional
Information: Destination MAC lookup resulted in egress ifc Outside Phase: 2 Type: CAPTURE
Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 3 Type: ACCESS-
LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase:
4 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id
2562905, using existing flow Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional
Information: Snort Verdict: (fast-forward) fast forward this flow Phase: 6 Type: CAPTURE
Subtype: Result: ALLOW Config: Additional Information: MAC Access list Result: input-interface:
Inside input-status: up input-line-status: up Action: allow
```

Suivi MAC

TFW prend toutes ses décisions de transfert en fonction des adresses MAC. Lors de l’analyse du flux de trafic, il est essentiel de s’assurer que les adresses MAC utilisées comme source et destination sur chaque paquet sont correctes en fonction de la topologie du réseau.

La fonction de capture de paquets vous permet d'afficher les adresses MAC utilisées à l'aide de l'option ***detail*** de la commande **show capture**.

```
FTD63# show cap i detail

98 packets captured

   1: 20:55:06.938473 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98
      802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985:  [udp sum ok] udp 52 [tos 0xc0]
[ttl 1] (id 0)
   2: 20:55:09.805561 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98
      802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985:  [udp sum ok] udp 52 [tos 0xc0]
[ttl 1] (id 0)
```

Une fois que vous avez trouvé une adresse MAC intéressante qui nécessite un suivi spécifique, les filtres de capture vous permettent de la faire correspondre.

```
FTD63# capture in type raw-data trace interface inside match mac 0000.0c9f.f014 ffff.ffff.ffff
any

FTD63# show capture

capture in type raw-data trace interface inside [Capturing - 114 bytes] match mac 0000.0c9f.f014
ffff.ffff.ffff any
```

```
FTD63# show cap in detail 98 packets captured 1: 20:55:06.938473 0000.0c9f.f014 0100.5e00.0066
0x8100 Length: 98 802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos
0xc0] [ttl 1] (id 0) 2: 20:55:09.805561 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98 802.1Q
vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos 0xc0] [ttl 1] (id 0)
```

Ce filtre est extrêmement utile lorsqu'il y a des traces de volets MAC et que vous voulez trouver le ou les coupables.

Débogage de table d'adresses MAC

Le débogage de la table d'adresses MAC peut être activé pour examiner chaque phase. Les informations fournies par ce débogage permettent de comprendre quand une adresse MAC est apprise, actualisée et supprimée de la table.

Cette section présente des exemples de chaque phase et explique comment lire ces informations. Pour activer les commandes debug sur FTD, vous devez accéder à l'interface de ligne de commande de diagnostic.

> **Avertissement :** Les débogages peuvent consommer des ressources pertinentes si le réseau est trop occupé. Il est recommandé de les utiliser dans des environnements contrôlés ou pendant les heures de pointe. Il est recommandé d'envoyer ces débogages à un serveur Syslog si ceux-ci sont trop détaillés.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FTD63# debug mac-address-table
debug mac-address-table enabled at level 1
```

Étape 1. L'adresse MAC est apprise. Lorsqu'une entrée n'est pas trouvée dans la table MAC, cette adresse est ajoutée à la table. Le message de débogage informe l'adresse et l'interface où il a été reçu.

```
FTD63# ping 10.20.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
add_l2fwd_entry: Going to add MAC 0000.0c9f.f014.
add_l2fwd_entry: Added MAC 0000.0c9f.f014 into bridge table thru Inside.
set_l2: Found MAC entry 0000.0c9f.f014 on Inside.
!add_l2fwd_entry: Going to add MAC 00fc.baf3.d680.
add_l2fwd_entry: Added MAC 00fc.baf3.d680 into bridge table thru Inside.
!!!!
```

Si l’adresse MAC est apprise via la méthode ICMP, le message suivant s’affiche. L'entrée entre dans la première étape du cycle d'expiration où elle n'actualise pas son compteur en fonction des conditions répertoriées dans le compteur d'âge de la table d'adresses MAC.

```
learn_from_icmp_error: Learning from icmp error.
```

Étape 2. Si une entrée est déjà connue, le débogage en informe. Le débogage affiche également des messages de mise en grappe qui ne sont pas pertinents dans les configurations autonomes ou HA.

```
set_l2: Found MAC entry 0000.0c9f.f014 on Inside.
l2fwd_refresh: Sending clustering LU to refresh MAC 0000.0c9f.f014.
l2fwd_refresh: Failed to send clustering LU to refresh MAC 0000.0c9f.f014
```

Étape 3. Une fois que l'entrée a atteint la deuxième étape (2 minutes avant le délai absolu).

```
FTD63# show mac-add
interface                  mac  address          type       Age(min)    bridge-group
-------------------------------------------------------------------------------------------
----
Inside                     00fc.baf3.d700       dynamic      3           1
Outside                    0050.56a5.6d52       dynamic      4           1
Inside                     0000.0c9f.f014       dynamic      2           1
Outside                    40a6.e833.2a05       dynamic      3           1

FTD63# l2fwd_clean:MAC 0000.0c9f.f014 entry aged out.
l2fwd_timeout:MAC entry timed out
```

Étape 4. Le pare-feu attend maintenant que de nouveaux paquets provenant de cette adresse actualisent la table. S'il n'y a plus de paquets utilisant cette entrée pendant ces 2 minutes, l'adresse est supprimée.

```
FTD63# show mac-address-table
interface mac address type Age(min) bridge-group
-------------------------------------------------------------------------------------------
----
Inside 0000.0c9f.f014 dynamic 1 1
Outside 40a6.e833.2a05 dynamic 3 1
FTD63# l2fwd_clean:Deleting MAC 0000.0c9f.f014 entry due to timeout.
delete_l2_fromPC: Deleting MAC 0000.0c9f.f014 due to freeing up of entry
l2fwd_clean:Deleted MAC 0000.0c9f.f014 from NP.
```

Informations connexes

- Guide Firepower Management Center, version 6.3 - Chapitre 3 : Mode pare-feu transparent ou routé pour la défense contre les menaces Firepower
- Support et documentation techniques - Cisco Systems