Firepower Threat Defense Transparent Firewall Mode geavanceerde concepten en tips voor probleemoplossing

Inhoud

Inleiding

Dit document beschrijft een gedetailleerde uitleg om de kernconcepten en -elementen te begrijpen van een FTD-implementatie (Firepower Threat Defense) in de TFW-modus (Transparent Firewall). Dit artikel biedt ook bruikbare gereedschappen en doorvoerfuncties voor de meest voorkomende problemen met betrekking tot de transparante firewallarchitectuur.

Bijgedragen door Cesar Lopez en bewerkt door Yeraldin Sánchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco FTD transparante kennis over firewallmodus

- Heet Standby Router Protocol (HSRP)-concepten
- Adresresolutie Protocol (ARP) en Internet Control Message Protocol (ICMP)-protocollen

Het is sterk aanbevolen om de sectie Firepower Configuration Guide Transparent of Routed Firewall Mode te lezen om de concepten die in dit document worden beschreven beter te begrijpen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 4120 FTD versie 6.3.0.4
- Cisco Firepower Management Center (FMC) versie 6.3.0.4
- Cisco ASR 1001 IOS-XE versie 16.3.9
- Cisco Catalyst 3850 IOS-XE versie 16.9.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Geavanceerde concepten voor transparante firewall

MAC-adrestabel

Terwijl een firewall in routed Mode op de routingtabel en ARP-tabel steunt om de egress-interface en de benodigde gegevens te bepalen om een pakket naar de volgende hop door te sturen, gebruikt de TFW-modus de MAC-adrestabel om de egress-interface te kunnen bepalen die wordt gebruikt om een pakket naar de bestemming te verzenden. De firewall kijkt naar het van bestemming MAC adresveld van het pakket dat wordt verwerkt en zoekt naar een ingang die dit adres met een interface verbindt.

De MAC-adrestabel heeft deze velden.

```
> 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 - Dit veld houdt de interfacenaam in van waar dit MAC-adres dynamisch is geleerd of statistisch is ingesteld
- MAC-adres - MAC-adresrecord bij opslag
- type - Methode die wordt gebruikt om de ingang te leren. Het kan dynamisch of statisch zijn
- Leeftijd (min.) - Vertraagde timer in minuten met de resterende tijd voordat de ingang is gemarkeerd als dood. Deze timer is alleen van toepassing op dynamisch inzendingen leren
- bridge group - Bridge Group-ID waarvan de interface deel uitmaakt

De Packet Forwarding-beslissing is gelijk aan een schakelaar maar er is een zeer belangrijk verschil wanneer het op een ontbrekende ingang in de MAC-tabel komt. In een schakelaar, wordt het pakket door alle interfaces behalve de ingangsinterface maar in TFW uitgezonden, Als een pakket wordt ontvangen en er geen ingang voor het bestemming MAC-adres is, wordt het pakket

ingetrokken. Het wordt weggegooid met de code Accelerated Security Path (ASP) *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
```

Deze voorwaarde gebeurt altijd voor het eerste pakket op een omgeving met dynamisch leren ingeschakeld en zonder statische items voor een bestemming als het MAC-adres niet eerder in een pakket was gezien als een bron-MAC-adres.

Zodra het punt aan de MAC-adrestabel is toegevoegd, kan het volgende pakket worden toegestaan, mits het wordt geconditioneerd aan de geselecteerde firewallfuncties.

```
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
```

> **Voorzichtig:** MAC Lookup is de eerste fase in de acties die door de firewall worden ondernomen. Het hebben van constante druppels wegens mislukte L2 raadpleging kan resulteren in relevant pakketverlies en/of onvolledige inspectie van de detectiemotor. De beïnvloeding is afhankelijk van de protocol- of toepassingscapaciteit om opnieuw te verzenden.

Op basis van het bovenstaande verdient het altijd de voorkeur een vermelding te laten aanleren vóór elke overdracht. TFW heeft meerdere mechanismen om een inzending te leren.

MAC-adrestafelopties

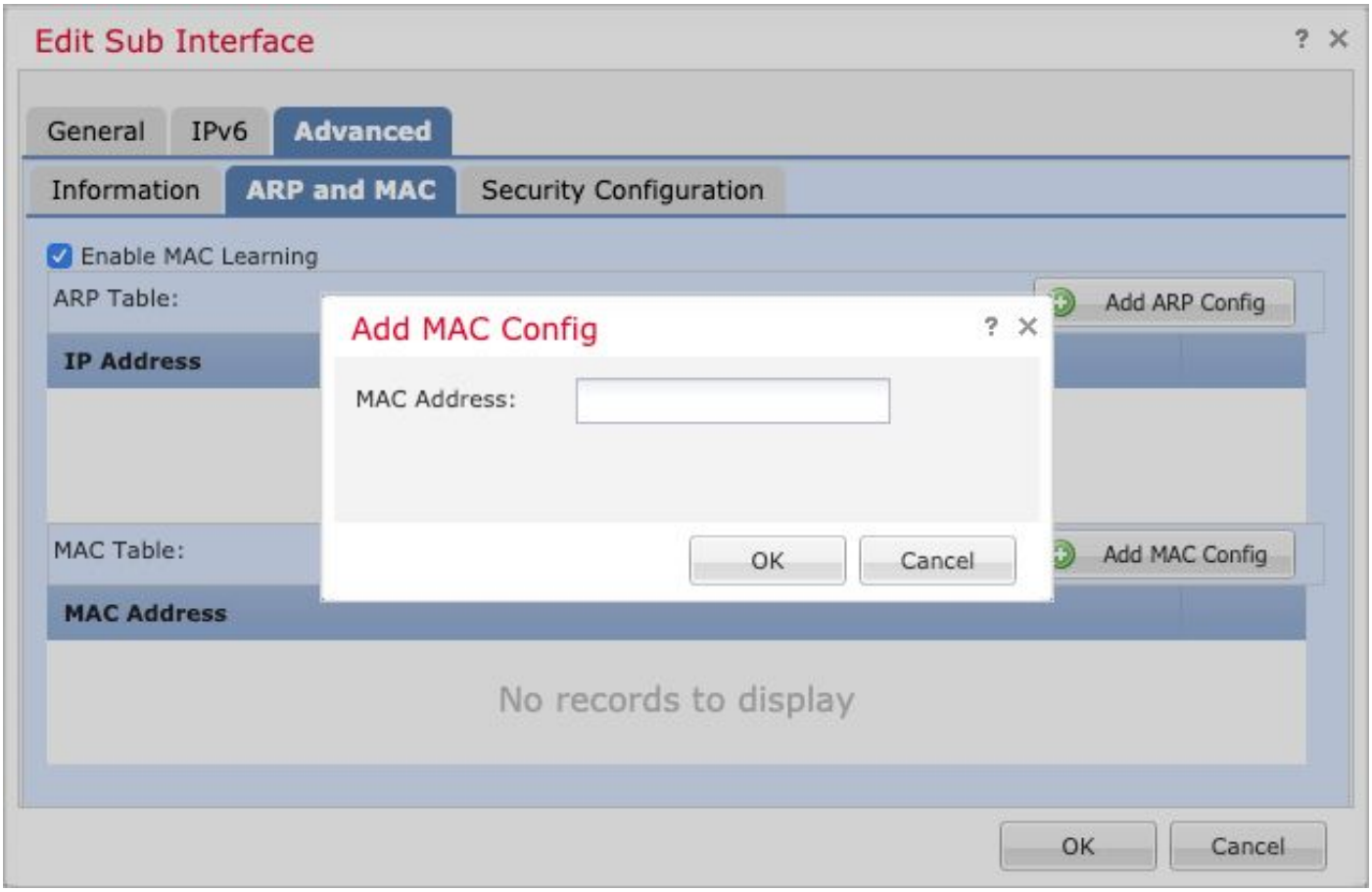
Statische vermeldingen

MAC-adressen kunnen handmatig worden toegevoegd om de firewall altijd dezelfde interface te laten gebruiken voor die specifieke ingang. Dit is een geldige optie voor items die niet kunnen worden gewijzigd. Dit is een veelvoorkomende optie wanneer de statische MAC op het configuratieniveau of door een optie bij de volgende hop wordt overschreven.

Bijvoorbeeld in een scenario waar het standaard MAC-adres van de gateway altijd hetzelfde zal zijn op een Cisco-router die handmatig aan de configuratie is toegevoegd of wanneer het HSRP

virtuele MAC-adres hetzelfde zal blijven.

Om statische ingangen in FTD te configureren die door FMC worden beheerd, kunt u klikken op **Bewerken Interface / Subinterface > Geavanceerd > ARP en MAC** en op **Add MAC Config** klikken. Dit voegt een ingang voor de specifieke interface toe die van **Apparaten > het** gedeelte **van het Apparaatbeheer > Interfaces** wordt bewerkt.



Dynamisch leren gebaseerd op BronMAC-adres

Deze methode is vergelijkbaar met wat een switch doet om de MAC-adrestabel te vullen. Als een pakket een bron-MAC-adres heeft dat geen deel uitmaakt van de MAC-tabel-items voor de interface die het is ontvangen, wordt er een nieuw item toegevoegd aan de tabel.

Dynamic Learning Based op ARP Probe

Als een pakket arriveert met een MAC-adres van de bestemming dat geen deel uitmaakt van de MAC-tabel en de bestemming IP deel uitmaakt van hetzelfde netwerk als de Bridge Virtual Interface (BVI), probeert het TFW te leren door een ARP-verzoek te verzenden via alle bridge-groepsinterfaces. Als een ARP-antwoord van een van de bridge group interfaces wordt ontvangen, wordt het vervolgens toegevoegd aan de MAC-tabel. Merk op dat, zoals het hierboven vermeld werd, terwijl er geen antwoord op dat ARP verzoek is, alle pakketten met ASP code *dst-l2_lookup-fail* worden geworpen.

Dynamisch leren op basis van ICMP-test

Als een pakket arriveert met een bestemmings-MAC-adres dat geen deel uitmaakt van de MAC-tabel en de bestemming IP GEEN deel uitmaakt van hetzelfde netwerk als de BVI, wordt een

ICMP-echo-verzoek verzonden met een Time-to-Live (TTL)-waarde is gelijk aan 1. De firewall verwacht dat een ICMP-bericht dat de tijd overschrijdt, het volgende-hop-MAC-adres leert.

MAC-adresonderhandelingstitel

De timer voor de MAC-adrestabel Age wordt op 5 minuten ingesteld voor elke geleerde ingang. Deze timeout waarde heeft twee verschillende fasen.

Time-out leeftijd eerste fase

Tijdens de eerste 3 minuten, wordt de waarde van het MAC-ingangstijdperk niet ververst tenzij een ARP-antwoordpakket dat door de firewall met het bron-MAC-adres gaat, gelijk is aan een ingang in de MAC-adrestabel. Deze voorwaarde sluit de ARP-antwoorden uit die bestemd zijn voor de IP-adressen van de Bridge Group. Dit betekent dat een ander pakje dat geen door-de-doos ARP antwoord is in de eerste 3 minuten wordt genegeerd.

In dit voorbeeld, is er een PC met een IP adres van 10.10.10.5 die een ping naar 10.20.20.5 verzenden. Het IP-adres van de gateway voor 10.20.20.5 is 10.20.20.3 met MAC-adres 000.0c9f.f014.

De bestemming PC maakt elke 25 seconden een ARP update die constante ARP pakketten veroorzaakt om door de firewall te gaan.

```
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
```

Er wordt een pakket met het filteren van ARP-pakketten gebruikt om deze pakketten aan te passen.

```
> 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
```

De vermelding voor 000.0c9f.4014 blijft op 5 en blijft nooit onder dat getal.

```
> 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
```

Tweede fase van de leeftijdsperiode

In de laatste 2 minuten valt de vermelding in een periode waarin het adres als verouderd wordt beschouwd.

```
> 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
```

De ingang wordt nog niet verwijderd en als om het even welk pakket met het BronMAC-adres dat het tabelitem aansluit, inclusief de pakketten-the-box, wordt gedetecteerd, wordt de Age-ingang teruggebracht naar 5 minuten.

In dit voorbeeld, wordt een ping verzonden binnen deze 2 minuten om de firewall te dwingen om zijn eigen ARP pakket te verzenden.

```
> 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
```

De MAC-adresingang wordt teruggezet op 5 minuten.

```
> 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
```

ARP-tabel

Eerst is het essentieel om te begrijpen dat de MAC-adrestabel volledig onafhankelijk is van de ARP-tabel. Terwijl de ARP-pakketten die door de firewall worden verzonden om een ARP-ingang te verfrissen, tegelijkertijd de MAC-adrestabel verfrissen, zijn deze verfrissingsprocessen een afzonderlijke taak en hebben elk zijn eigen tijdelijke status en voorwaarden.

Zelfs als de ARP tabel niet wordt gebruikt om de stap next-hop te bepalen zoals in routed mode, is het belangrijk om het effect van de ARP-pakketten te begrijpen die gegenereerd zijn en die bestemd zijn voor de firewall-identiteit van IPs in een transparante implementatie kan hebben.

De ARP-vermeldingen worden gebruikt voor beheerdoeleinden en worden alleen aan de tabel toegevoegd als een beheerfunctie of -taak dit vereist. Als voorbeeld van een beheertaak, als een Bridge Group een IP-adres heeft, kan deze IP worden gebruikt om de bestemming te pingelen.

```
> 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
```

Als de bestemming in zelfde voorwerp als de Bridge Group IP is, dwingt het een ARP-verzoek en als een geldig ARP-antwoord wordt ontvangen, wordt de IP/MAC-ingang in de ARP-tabel opgeslagen.

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

In tegenstelling tot de MAC-adrestabel is de timer die het interface/IP-adres/MAC-adrestriplet begeleidt een stijgende waarde.

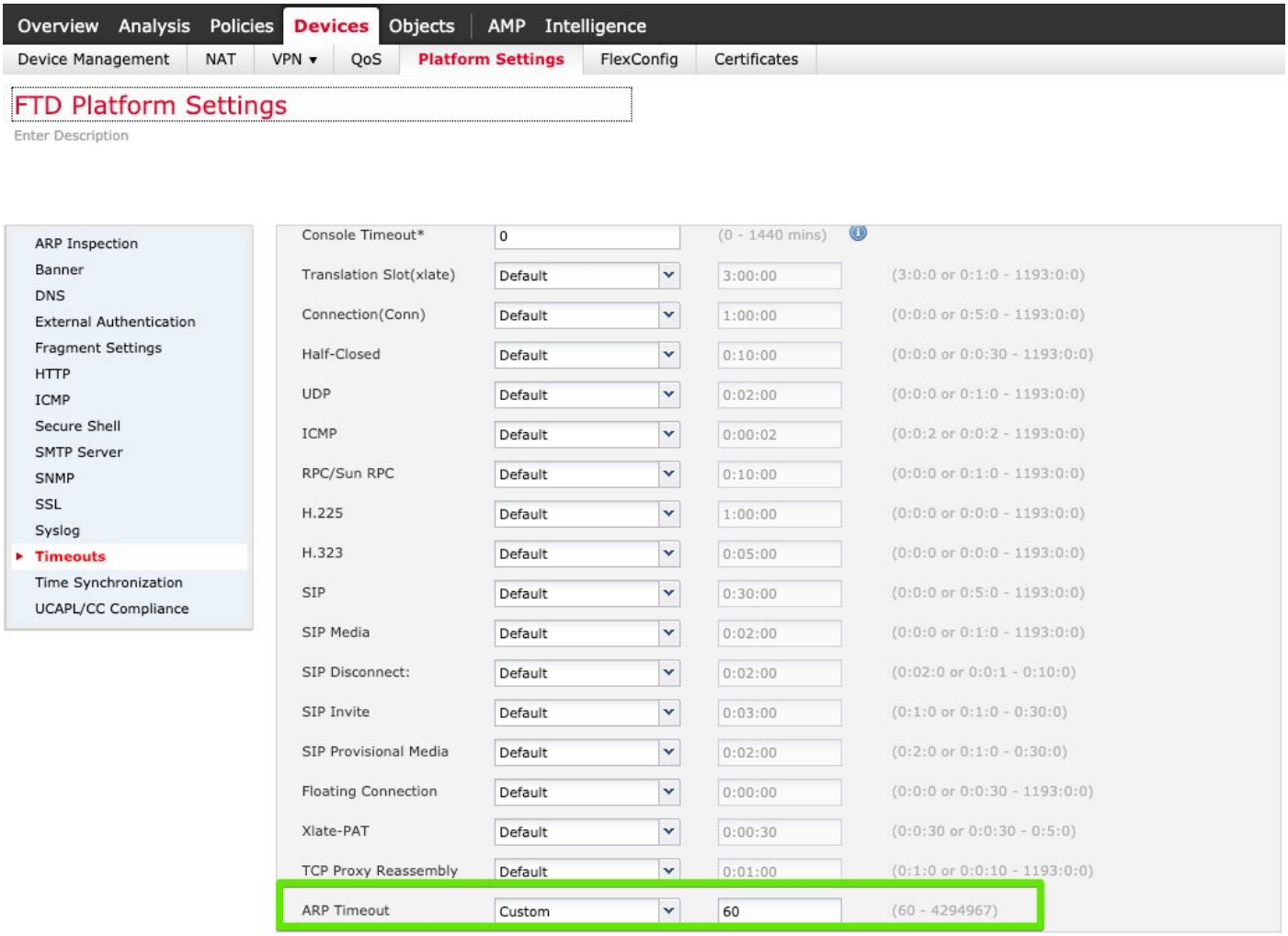
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Wanneer de timer een *n - 30*-waarde bereikt waar *n* de ARP geconfigureerde time-out is (met een standaard van 14400 seconden), stuurt de firewall een ARP-verzoek om de ingang te verfrissen. Als een geldig ARP-antwoord wordt ontvangen, wordt de entry gehouden en de timer gaat terug naar 0.

In dit voorbeeld, werd de ARP tijd teruggebracht tot 60 seconden.

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

Deze tijdelijke versie is beschikbaar voor configuratie op **Apparaten > Platform Settings > Time-outs** tabblad in FMC, zoals in de afbeelding wordt getoond.



Aangezien de timeout 60 seconden is, wordt er elke 30 seconden een ARP-verzoek verzonden (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
```

De ARP ingang wordt dan ververst elke 30 seconden.

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

Tips voor probleemoplossing

Verkeersrichting

Een van de moeilijkste dingen om op een TFW te achterhalen is de verkeersstroomrichting. Het begrijpen van hoe de verkeersstromen helpen om de firewall goed te verzekeren de pakketten aan de bestemming door te sturen.

Het bepalen van de juiste instap- en spanningsinterface is een makkelijke taak op Routed Mode omdat er meerdere indicatoren zijn van de firewallbetrokkenheid zoals de bron en de bestemming MAC-adreswijziging en de reductie van de Time-To-Live (TTL)-waarde van de ene interface naar de andere.

Deze verschillen zijn niet beschikbaar bij een TFW-instelling. Het pakket dat door de ingangsinterface komt ziet er hetzelfde uit als wanneer de firewall in de meeste gevallen wordt verlaten.

De specifieke problemen zoals MAC flaps in het netwerk of de lijnen van het verkeer zouden moeilijker te volgen kunnen zijn zonder te weten waar het pakket binnendrong en wanneer het de firewall verliet.

Om ingangen te onderscheiden van gelijkspakketten, kan het sleutelwoord in pakketopnamen worden gebruikt.

```
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 - verhoogt de opnamefbuffer in bytes. 33554432 is de maximaal beschikbare waarde. In modellen zoals 5500-X, FirePOWER-apparaten of virtuele machines is het veilig om deze groottewaarde te gebruiken zolang er geen tientallen beelden zijn geconfigureerd.

overtrekken - hiermee kan de optie overtrekken voor de gespecificeerde opgenomen video worden ingeschakeld.

aantal sporen: maakt een hoger aantal sporen mogelijk. 1000 is het maximum toegestaan en 128 is de standaard. Dit is ook veilig volgens dezelfde aanbeveling als voor de buffergrootteoptie.

> **Tip**: Als u een van de opties vergeet toe te voegen, kunt u deze toevoegen zonder de gehele opname opnieuw te moeten schrijven door de naam van de opname en de optie te verwijzen. De nieuwe optie beïnvloedt echter alleen de nieuw opgenomen pakketten, zodat een **duidelijke** *Capname* moet worden gebruikt om het nieuwe effect te hebben sinds paknummer 1. Voorbeeld: **traceren**

Nadat pakketten zijn opgenomen, **toont** de opdracht **het** *cap_name* **spoor** de eerste 1000 (als het spooraantal werd verhoogd) sporen van de samengeperste pakketten weer.

```
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
```

Deze uitvoer is een voorbeeld van de sporen van de externe interface-pakketvastlegging. Dit

betekent dat de pakketnummers 1 en 3 op de externe interface en pakketnummer 2 op de interface werden gedrukt.

Aanvullende informatie kan in dit spoor worden gevonden zoals de Actie die voor dat pakket is genomen en de Drop-rede voor het geval dat het pakket wordt ingetrokken.

Voor langere sporen en als u zich op één pakje wilt concentreren, kan de opdracht **Opname** *cap_name* **pakketnummer** *pakje*_Packet-number gebruiken om de overtrek voor dat specifieke pakje weer te geven.

Dit is een voorbeeld van een toegestaan pakketnummer 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
```

MAC-tracering

TFW neemt al haar verzendingsbesluiten op basis van MAC-adressen. Tijdens de analyse van de verkeersstroom, is het van essentieel belang om te verzekeren dat de MAC adressen die als bron en bestemming op elk pakket worden gebruikt correct op de netwerktopologie zijn gebaseerd.

Met de optie pakketvastlegging kunt u de MAC-adressen weergeven die gebruikt worden met de detailoptie uit de opdracht **Geeft** op.

```
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)
```

Zodra u een interessant MAC-adres hebt gevonden dat specifieke tracering vereist, kunnen de opnamefilters u toestaan om het aan te passen.

```
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)
```

Deze filter is uiterst nuttig wanneer er sporen van MAC-flaps zijn en u de schuldige(n) wilt vinden.

Debug van Mac-adrestabel

Debug van de MAC-adrestabel kan worden ingeschakeld om elke fase te bekijken. De informatie die door dit debug wordt verstrekt helpt te begrijpen wanneer een adres van MAC wordt geleerd, verfrist en uit de tabel verwijderd.

In dit deel worden voorbeelden gegeven van elke fase en hoe deze informatie te lezen. Om debug-opdrachten op FTD mogelijk te maken, moet u naar de diagnostische CLI gaan.

> **Waarschuwing**: Debugs kunnen relevante bronnen gebruiken als het netwerk te druk is. Aanbevolen wordt ze te gebruiken in gecontroleerde omgevingen of tijdens lage piekuren. Het wordt aanbevolen om deze apparaten naar een Syslog server te sturen als ze te lang zijn.

```
> 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
```

Stap 1. Het MAC-adres wordt geleerd. Wanneer een punt niet in de MAC-tabel staat, wordt dit adres aan de tabel toegevoegd. Het debug-bericht stelt het adres en de interface in waar het is ontvangen.

```
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.
!!!!
```

Als de MAC door de ICMP-methode wordt geleerd, wordt het volgende bericht weergegeven. Het punt gaat het eerste stadium van het timeout programma in waar het zijn timer niet verfrist op basis van de voorwaarden in de MAC-adressenlijst Timer.

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

Stap 2. Als een bericht al bekend is, verschijnt het geluid ervan. Debug toont ook clusterberichten die niet relevant zijn in standalone of HA-instellingen.

```
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
```

Stap 3. Zodra de ingang de tweede fase heeft bereikt (2 minuten vóór de absolute onderbreking).

```
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
```

Stap 4 . De firewall verwacht nu nieuwe pakketten die met dat adres zijn meegeleverd, om de tabel te verfrissen. Als die vermelding tijdens die twee minuten niet meer wordt gebruikt, wordt het adres verwijderd.

```
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.
```

Gerelateerde informatie

- Firepower Management Center Guide, versie 6.3 - Hoofdstuk 3: Firewallmodus transparant of Routed for Firepower Threat Defense
- Technische ondersteuning en documentatie – Cisco Systems