Firepower Threat Defense Transparent Firewall Mode Advanced Conceptos y consejos para la resolución de problemas

Contenido

Introducción

Este documento describe una explicación detallada para comprender los conceptos y elementos básicos de una implementación de Firepower Threat Defense (FTD) en modo de firewall transparente (TFW). Este artículo también proporciona herramientas y tutoriales útiles para los problemas más comunes relacionados con la arquitectura de firewall transparente.

Colaborado por Cesar Lopez y editado por Yeraldin Sánchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del modo de firewall transparente de Cisco FTD

- Conceptos del protocolo de router con espera activa (HSRP)
- Protocolos de protocolo de resolución de direcciones (ARP) y protocolo de mensajes de control de Internet (ICMP)

Se recomienda encarecidamente leer la sección Modo de Firewall Transparente o Ruteado de la Guía de Configuración de Firepower para comprender mejor los conceptos descritos en este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 4120 FTD versión 6.3.0.4
- Cisco Firepower Management Center (FMC) versión 6.3.0.4
- Cisco ASR 1001 IOS-XE versión 16.3.9
- Cisco Catalyst 3850 IOS-XE versión 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Conceptos avanzados de firewall transparente

Tabla de dirección MAC

Mientras que un firewall en modo ruteado depende de la tabla de ruteo y la tabla ARP para determinar la interfaz de egreso y los datos necesarios para reenviar un paquete al salto siguiente, el modo TFW utiliza la tabla de dirección MAC para poder determinar la interfaz de egreso que se utiliza para enviar un paquete a su destino. El firewall observa el campo de dirección MAC de destino del paquete que se está procesando y busca una entrada que vincule esta dirección con una interfaz.

La tabla de direcciones MAC tiene estos campos.

```
> 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 - Este campo contiene el nombre de la interfaz desde la que se aprendió dinámicamente esta dirección MAC o se configuró estáticamente
- Dirección MAC: registro de dirección MAC para almacenar
- type - Método utilizado para aprender la entrada. Puede ser dinámico o estático
- Age(min) (Antigüedad): temporizador de desactivación en minutos que muestra el tiempo restante antes de que la entrada se marque como muerta. Este temporizador sólo se aplica a las entradas aprendidas dinámicamente
- bridge-group - ID del grupo de puentes al que pertenece la interfaz

La decisión de reenvío de paquetes es similar a un switch, pero hay una diferencia muy importante cuando se trata de una entrada que falta en la tabla MAC. En un switch, el paquete se

transmite a través de todas las interfaces excepto la interfaz de ingreso pero en TFW, Si se recibe un paquete y no hay entrada para la dirección MAC de destino, el paquete se descarta. Se descarta con el código de descarte de ruta de seguridad acelerada (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
```

Esta condición siempre ocurre para el primer paquete en un entorno con aprendizaje dinámico habilitado y sin entradas estáticas para un destino si la dirección MAC no se veía antes en un paquete como una dirección MAC de origen.

Una vez que se agrega la entrada a la tabla de direcciones MAC, se puede permitir que el siguiente paquete esté condicionado a las funciones de firewall habilitadas.

```
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
```

> **Precaución:** La búsqueda de MAC es la primera fase de las acciones realizadas por el firewall. Si se producen caídas constantes debido a las búsquedas fallidas de L2, se puede producir una pérdida de paquetes relevante y/o una inspección incompleta del motor de detección. La afectación se basa en el protocolo o la capacidad de la aplicación para retransmitir.

Sobre la base de lo anterior, siempre es preferible tener una entrada aprendida antes de cualquier transmisión. TFW tiene varios mecanismos para aprender una entrada.

Opciones de aprendizaje de la tabla de direcciones MAC

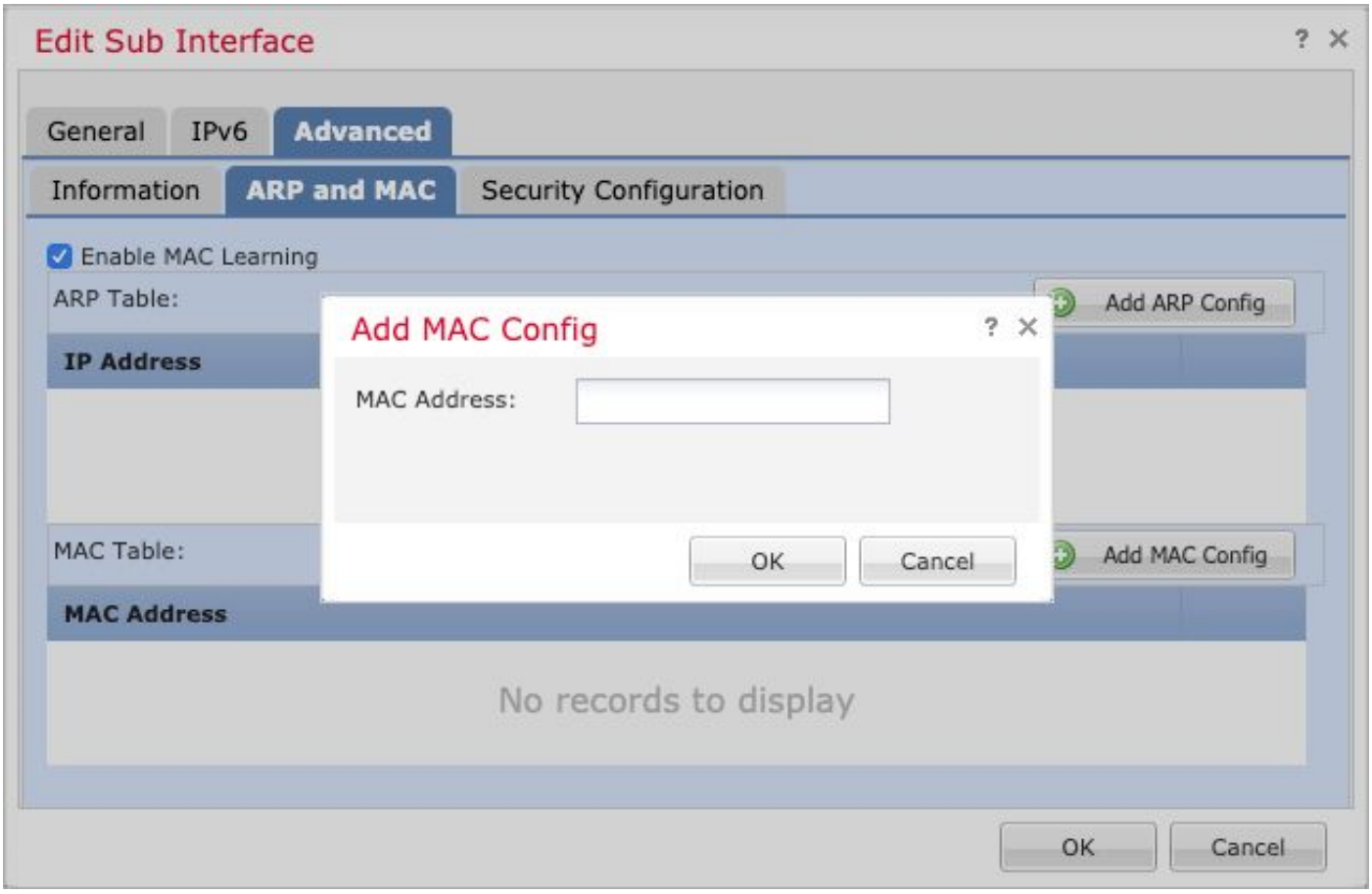
Entradas estáticas

Las direcciones MAC se pueden agregar manualmente para hacer que el firewall utilice siempre la misma interfaz para esa entrada específica. Esta es una opción válida para las entradas que no son susceptibles de cambio. Esta es una opción común cuando la MAC estática se sobrescribe en el nivel de configuración o por una función en el salto siguiente.

Por ejemplo, en un escenario en el que la dirección MAC de gateway predeterminada siempre

será la misma en un router de Cisco que se agregó manualmente a la configuración o si la dirección MAC virtual HSRP va a permanecer igual.

Para configurar las entradas estáticas en FTD administradas por FMC, puede hacer clic en **Edit Interface / Subinterface > Advanced > ARP y MAC** y hacer clic en **Add MAC Config**. Esto agrega una entrada para la interfaz específica que se está editando desde la sección **Dispositivos > Administración de dispositivos > Interfaces**.



Aprendizaje dinámico basado en la dirección MAC de origen

Este método es similar a lo que hace un switch para llenar la tabla de direcciones MAC. Si un paquete tiene una dirección MAC de origen que no forma parte de las entradas de la tabla MAC para la interfaz que recibió, se agrega una nueva entrada a la tabla.

Aprendizaje dinámico basado en la sonda ARP

Si un paquete llega con una dirección MAC de destino que no forma parte de la tabla MAC y la IP de destino forma parte de la misma red que la interfaz virtual de puente (BVI), el TFW intenta aprenderla enviando una solicitud ARP a través de todas las interfaces de grupo de puente. Si se recibe una respuesta ARP de cualquiera de las interfaces de grupo de bridges, se agrega a la tabla MAC. Tenga en cuenta que, como se mencionó anteriormente, aunque no hay respuesta a esa solicitud ARP, todos los paquetes se descartan con el código ASP *dst-l2_lookup-fail*.

Aprendizaje dinámico basado en sonda ICMP

Si un paquete llega con una dirección MAC de destino que no forma parte de la tabla MAC y la IP de destino NO forma parte de la misma red que la BVI, se envía una solicitud de eco ICMP con un

valor de Tiempo de vida (TTL) igual a 1. El firewall espera un mensaje ICMP Time Exceeded para aprender la dirección MAC del siguiente salto.

Temporizador de antigüedad de la tabla de direcciones MAC

El temporizador de antigüedad de la tabla de direcciones MAC se establece en 5 minutos para cada entrada aprendida. Este valor de tiempo de espera tiene dos etapas diferentes.

Tiempo de espera de la primera etapa

Durante los primeros 3 minutos, el valor de la antigüedad de la entrada MAC no se actualiza a menos que un paquete de respuesta ARP que pasa a través del firewall con la dirección MAC de origen sea igual a una entrada en la tabla de direcciones MAC. Esta condición excluye las respuestas ARP destinadas a las direcciones IP del grupo de puente. Esto significa que cualquier otro paquete que no sea una respuesta ARP a través del paquete se ignora durante los primeros 3 minutos.

En este ejemplo, hay un PC con una dirección IP de 10.10.10.5 que envía un ping a 10.20.20.5. La dirección IP del gateway para 10.20.20.5 es 10.20.20.3 con la dirección MAC 000.0c9f.f014.

El equipo de destino crea una actualización ARP cada 25 segundos, lo que provoca que los paquetes ARP constantes pasen a través del firewall.

```
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
```

Se utiliza una captura de paquetes que filtra los paquetes ARP para hacer coincidir estos paquetes.

```
> 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
```

La entrada para 000.0c9f.4014 permanece en 5 y nunca se sitúa por debajo de ese número.

```
> 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
```

Segundo período de tiempo de espera

Durante los últimos 2 minutos, la entrada entra en un período de tiempo en el que la dirección se considera antigua.

```
> 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
```

La entrada todavía no se elimina y si se detecta cualquier paquete con la dirección MAC de origen que coincida con la entrada de la tabla, incluidos los paquetes de caja, la entrada de antigüedad se actualiza de nuevo a 5 minutos.

En este ejemplo, se envía un ping dentro de estos 2 minutos para obligar al firewall a enviar su propio paquete 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
```

La entrada de la dirección MAC se devuelve a 5 minutos.

```
> 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
```

tabla ARP

En primer lugar, es esencial comprender que la tabla de direcciones MAC es completamente independiente de la tabla ARP. Mientras que los paquetes ARP enviados por el firewall para actualizar una entrada ARP pueden, al mismo tiempo, actualizar la tabla de direcciones MAC, estos procesos de actualización son tareas separadas y cada uno tiene sus propios tiempos de espera y condiciones.

Incluso si la tabla ARP no se utiliza para determinar el siguiente salto de salida como en el modo ruteado, es importante comprender el efecto de los paquetes ARP generados y destinados a la identidad de firewall que las IPs pueden tener en una implementación transparente.

Las entradas ARP se utilizan para fines de administración y sólo se agregan a la tabla si una función o tarea de administración lo requiere. Como ejemplo de una tarea de administración, si un grupo de puentes tiene una dirección IP, esta IP se puede utilizar para hacer ping al destino.

```
> 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 el destino está en la misma subred que la IP del grupo de puente, fuerza una solicitud ARP y si se recibe una respuesta ARP válida, la entrada IP/MAC se almacena en la tabla ARP.

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

A diferencia de la tabla de direcciones MAC, el temporizador que acompaña la interfaz/dirección IP/dirección MAC triplet es un valor creciente.

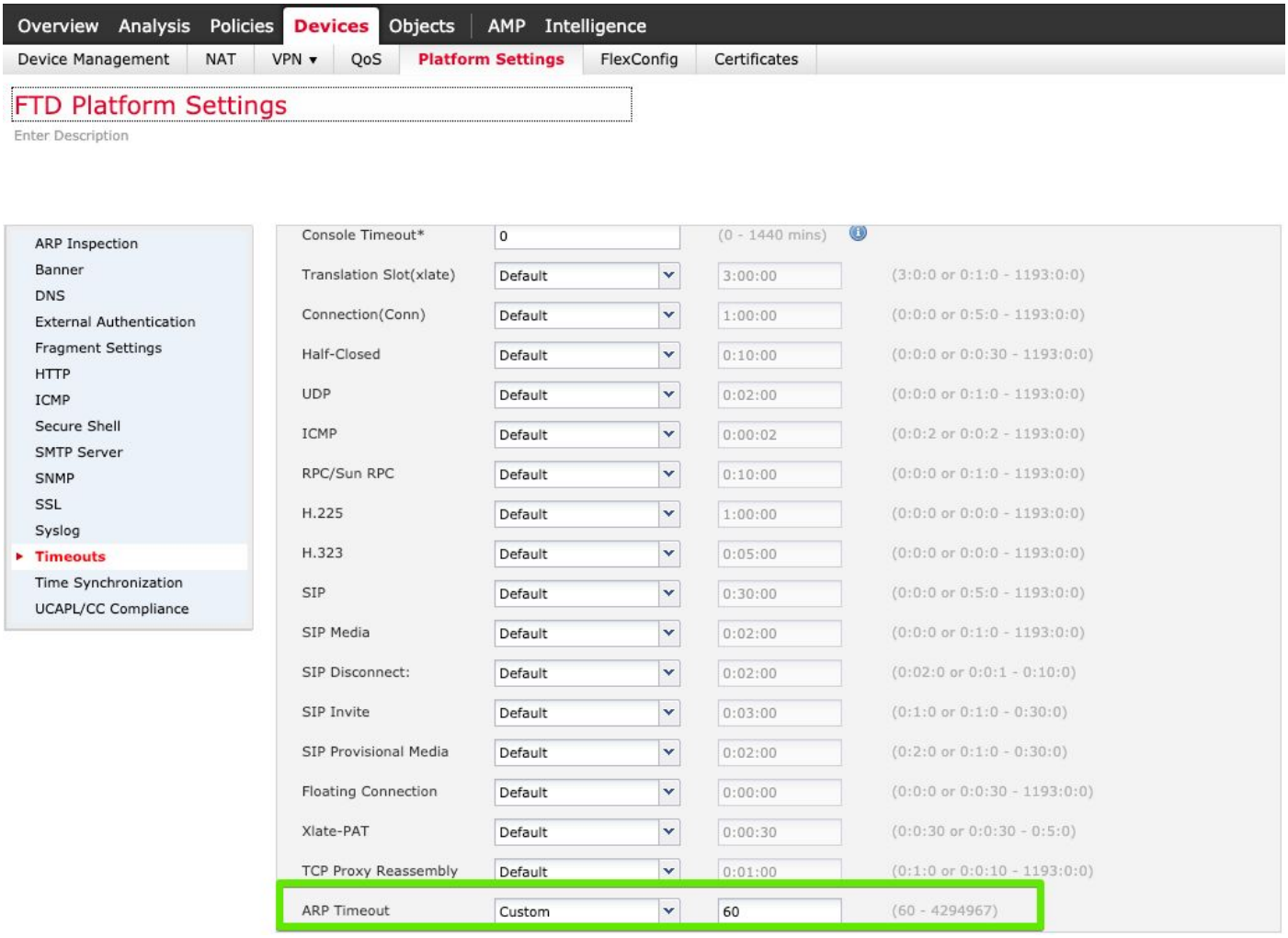
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Cuando el temporizador alcanza un *valor n - 30* donde *n* es el tiempo de espera configurado ARP (con un valor predeterminado de 14400 segundos), el firewall envía una solicitud ARP para actualizar la entrada. Si se recibe una respuesta ARP válida, se retiene la entrada y el temporizador vuelve a 0.

En este ejemplo, el tiempo de espera ARP se redujo a 60 segundos.

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

Este tiempo de espera está disponible para configurarse en la pestaña Dispositivos > Configuración de la plataforma > Tiempos de espera en FMC, como se muestra en la imagen.



Dado que el tiempo de espera es de 60 segundos, se envía una solicitud ARP cada 30 segundos (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
```

A continuación, la entrada ARP se actualiza cada 30 segundos.

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

Consejos para Troubleshooting

Dirección del tráfico

Una de las cosas más difíciles de rastrear en una TFW es la dirección del flujo de tráfico. Comprender cómo los flujos de tráfico ayudan a garantizar que el firewall reenvíe correctamente los paquetes al destino.

La determinación de la interfaz de entrada y salida correcta es una tarea más fácil en el modo enrutado, ya que hay varios indicadores de la participación del firewall, como la modificación de las direcciones MAC de origen y destino y la reducción del valor de Tiempo de vida (TTL) de una interfaz a otra.

Estas diferencias no están disponibles en una configuración de TFW. El paquete que llega a través de la interfaz de ingreso se ve igual que cuando sale del firewall en la mayoría de los casos.

Los problemas específicos como las solapas MAC en la red o los loops de tráfico podrían ser más difíciles de rastrear sin saber dónde ingresó el paquete y cuándo salió del firewall.

Para ayudar a diferenciar el ingreso de los paquetes de salida, la palabra clave trace se puede utilizar en las capturas de paquetes.

```
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: aumenta el búfer de captura en bytes. 33554432 es el valor máximo disponible. En modelos como 5500-X, appliances Firepower o máquinas virtuales, es seguro utilizar este valor de tamaño siempre y cuando no haya docenas de capturas ya configuradas.

trace: habilita la opción trace para la captura especificada.

trace-count - Permite un mayor número de seguimientos. 1000 es el máximo permitido y 128 es el valor predeterminado. Esto también es seguro siguiendo la misma recomendación que la opción de tamaño del búfer.

> **Consejo:** Si olvida agregar una de las opciones, puede agregarla sin tener que volver a escribir la captura completa haciendo referencia al nombre de captura y a la opción. Sin embargo, la nueva opción afecta solamente a los paquetes recién capturados, por lo que se debe utilizar **clear capture** *capname* para tener el nuevo efecto desde el paquete número 1. Ejemplo: **captura en traza**

Una vez capturados los paquetes, el comando **show capture** *cap_name* **trace** muestra los primeros rastros 1000 (si se aumentó el número de seguimiento) de los paquetes ingresados.

```
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
```

Este resultado es un ejemplo de los seguimientos de captura de paquetes de la interfaz externa. Esto significa que los números de paquete 1 y 3 ingresaron a la interfaz externa y el paquete

número 2 egresó la interfaz.

Se puede encontrar información adicional en este seguimiento como la Acción realizada para ese paquete y la razón de descarte en caso de que el paquete se descarte.

Para rastros más largos y si desea centrarse en un solo paquete, el comando **show capture** ***cap_name*** **trace packet-number** ***packet_***number se puede utilizar para mostrar el seguimiento de ese paquete específico.

Este es un ejemplo de un paquete permitido número 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
```

Seguimiento de MAC

TFW toma todas sus decisiones de reenvío en función de las direcciones MAC. Durante el análisis del flujo de tráfico, es esencial asegurarse de que las direcciones MAC utilizadas como origen y destino en cada paquete sean correctas en función de la topología de red.

La función de captura de paquetes le permite mostrar las direcciones MAC usadas usando la opción ***detail*** del **comando 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)
```

Una vez que haya localizado una dirección MAC interesante que requiera un seguimiento específico, los filtros de captura le permiten coincidir con ella.

```
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)
```

Este filtro es extremadamente útil cuando hay rastros de solapas MAC y desea encontrar los culpables.

Depuración de tabla de direcciones MAC

La depuración de la tabla de direcciones MAC se puede habilitar para revisar cada fase. La información proporcionada por esta depuración ayuda a comprender cuándo se aprende, actualiza y elimina una dirección MAC de la tabla.

Esta sección muestra ejemplos de cada fase y cómo leer esta información. Para habilitar los comandos debug en FTD, debe acceder a la CLI de diagnóstico.

> **Advertencia:** Las depuraciones pueden consumir recursos relevantes si la red está demasiado ocupada. Se recomienda utilizarlos en entornos controlados o durante las horas pico bajas. Se recomienda enviar estas depuraciones a un servidor Syslog si son demasiado verbosas.

```
> 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
```

Paso 1. Se aprende la dirección MAC. Cuando no se encuentra una entrada en la tabla MAC, esta dirección se agrega a la tabla. El mensaje de depuración informa la dirección y la interfaz donde se recibió.

```
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 la MAC se detecta a través del método ICMP, se muestra el siguiente mensaje. La entrada ingresa a la primera etapa del ciclo de tiempo de espera donde no actualiza su temporizador en base a las condiciones enumeradas en el Temporizador de Edad de la Tabla de Direcciones MAC.

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

Paso 2. Si ya se conoce una entrada, la depuración informa al respecto. La depuración también muestra mensajes de agrupamiento que son irrelevantes en configuraciones independientes o 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
```

Paso 3. Una vez que la entrada ha alcanzado la segunda etapa (2 minutos antes del tiempo de espera absoluto).

```
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
```

Paso 4. El firewall ahora espera que los nuevos paquetes originados con esa dirección actualicen la tabla. Si no hay más paquetes usando esa entrada durante esos 2 minutos, se elimina la dirección.

```
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.
```

Información Relacionada

- Guía de Firepower Management Center, versión 6.3 - Capítulo 3: Modo de firewall transparente o enrutado para Firepower Threat Defense
- Soporte Técnico y Documentación - Cisco Systems