Firepower Threat Defense Modo de firewall transparente Conceitos avançados e dicas de solução de problemas

Contents

Introduction

Este documento descreve uma explicação detalhada para entender os principais conceitos e elementos de uma implantação do Firepower Threat Defense (FTD) no modo de firewall transparente (TFW). Este artigo também fornece ferramentas e avanços úteis para os problemas mais comuns relacionados à arquitetura de firewall transparente.

Contribuído por Cesar Lopez e editado por Yeraldin Sánchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do modo de firewall transparente do Cisco FTD

- Conceitos do Hot Standby Router Protocol (HSRP)
- Protocolo de Resolução de Endereços (ARP - Address Resolution Protocol) e Protocolos ICMP (Internet Control Message Protocol)

Éaltamente recomendável que a seção do Guia de Configuração do Firepower Transparent or Routed Firewall Mode seja lida para compreender melhor os conceitos descritos neste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower 4120 FTD versão 6.3.0.4
- Cisco Firepower Management Center (FMC) versão 6.3.0.4
- Cisco ASR1001 IOS-XE versão 16.3.9
- Cisco Catalyst 3850 IOS-XE versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conceitos avançados do firewall transparente

Tabela de endereço MAC

Embora um firewall no modo roteado dependa da tabela de roteamento e da tabela ARP para determinar a interface de saída e os dados necessários para encaminhar um pacote ao próximo salto, o modo TFW usa a tabela de endereços MAC para poder determinar a interface de saída usada para enviar um pacote ao seu destino. O firewall examina o campo de endereço MAC de destino do pacote que está sendo processado e procura uma entrada que vincule esse endereço a uma interface.

A tabela de endereços MAC tem estes 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 contém o nome da interface de onde esse endereço MAC foi aprendido dinamicamente ou configurado estaticamente
- Endereço MAC - registro de endereço MAC a ser armazenado
- type - Método usado para aprender a entrada. Pode ser dinâmico ou estático
- Age(min) - Temporizador decremental em minutos exibindo o tempo restante antes que a entrada seja marcada como inoperante. Este temporizador aplica-se somente a entradas aprendidas dinamicamente
- bridge-group - ID do grupo de bridge ao qual a interface pertence

A decisão de encaminhamento de pacotes é semelhante a um switch, mas há uma diferença muito importante quando se trata de uma entrada ausente na tabela MAC. Em um switch, o pacote é transmitido por todas as interfaces, exceto pela interface de entrada, mas em TFW. Se

um pacote é recebido e não há entrada para o endereço MAC de destino, o pacote é descartado. Ele é descartado com o código de queda do 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
```

Essa condição sempre acontece para o primeiro pacote em um ambiente com aprendizado dinâmico habilitado e sem entradas estáticas para um destino se o endereço MAC não fosse visto antes em um pacote como um endereço MAC de origem.

Quando a entrada é adicionada à tabela de endereços MAC, o próximo pacote pode ser condicionado aos recursos de firewall ativados.

```
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
```

> **Caution**: A Pesquisa de MAC é a primeira fase das ações tomadas pelo firewall. Ter quedas constantes devido a consultas L2 com falha pode resultar em perda de pacotes relevante e/ou inspeção incompleta do mecanismo de detecção. O efeito depende do protocolo ou da capacidade de aplicação para retransmitir.

Com base no acima mencionado, é sempre preferível ter uma entrada aprendida antes de qualquer transmissão. O TFW tem vários mecanismos para aprender uma entrada.

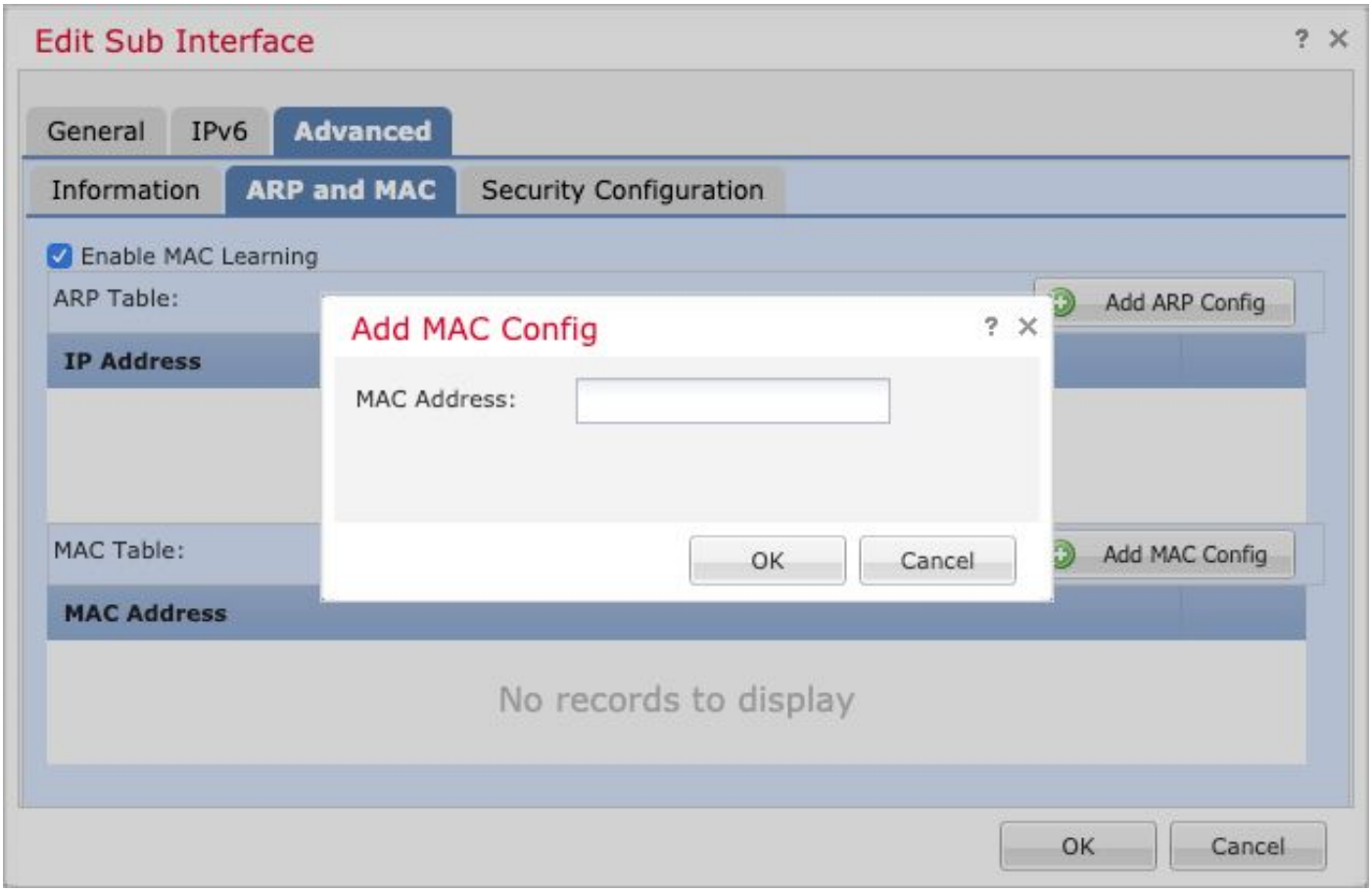
Opções de aprendizado da tabela de endereços MAC

Entradas estáticas

Os endereços MAC podem ser adicionados manualmente para fazer com que o firewall sempre use a mesma interface para essa entrada específica. Esta é uma opção válida para entradas que não são susceptíveis de alteração. Essa é uma opção comum quando o MAC estático é sobrescrito no nível de configuração ou por um recurso no próximo salto.

Por exemplo, em um cenário em que o endereço MAC do gateway padrão será sempre o mesmo em um roteador Cisco que foi adicionado manualmente à configuração ou se o endereço MAC virtual do HSRP permanecerá o mesmo.

Para configurar entradas estáticas no FTD gerenciado pelo FMC, você pode clicar em **Edit Interface / Subinterface > Advanced > ARP e MAC** e clicar em **Add MAC Config**. Isso adiciona uma entrada para a interface específica que está sendo editada da seção **Dispositivos > Gerenciamento de dispositivos > Interfaces**.



Aprendizado dinâmico com base no endereço MAC origem

Esse método é semelhante ao que um switch faz para preencher a tabela de endereços MAC. Se um pacote tiver um endereço MAC de origem que não faça parte das entradas da tabela MAC para a interface recebida, uma nova entrada será adicionada à tabela.

Aprendizado dinâmico baseado na sonda ARP

Se um pacote chega com um endereço MAC de destino que não faz parte da tabela MAC e o IP de destino faz parte da mesma rede da BVI (Bridge Virtual Interface), o TFW tenta aprender a enviar uma solicitação ARP através de todas as interfaces do grupo de bridge. Se uma resposta ARP for recebida de qualquer uma das interfaces do grupo de bridge, ela será adicionada à tabela MAC. Observe que, como foi mencionado acima, enquanto não há resposta para essa solicitação ARP, todos os pacotes são descartados com o código ASP *dst-l2_lookup-fail*.

Aprendizado dinâmico baseado no ICMP Probe

Se um pacote chega com um endereço MAC de destino que não faz parte da tabela MAC e o IP de destino NÃO faz parte da mesma rede que o BVI, uma solicitação de eco ICMP é enviada com um valor Time-to-Live (TTL) igual a 1. O firewall espera que uma mensagem ICMP Time Exceeded conheça o endereço MAC do próximo salto.

Temporizador de Tempo de existência da tabela de endereços MAC

O temporizador de idade da tabela de endereços MAC é definido como 5 minutos para cada entrada aprendida. Esse valor de tempo limite tem dois estágios diferentes.

Tempo limite de existência primeiro estágio

Durante os primeiros 3 minutos, o valor de Idade da entrada MAC não é atualizado a menos que um pacote de resposta ARP que passa pelo firewall com o endereço MAC de origem seja igual a uma entrada na tabela de endereços MAC. Essa condição exclui as respostas ARP destinadas aos endereços IP do grupo de bridge. Isso significa que qualquer outro pacote que não seja uma resposta ARP através da caixa é ignorado durante os primeiros 3 minutos.

Neste exemplo, há um PC com um endereço IP 10.10.10.5 enviando um ping para 10.20.20.5. O endereço IP do gateway para 10.20.20.5 é 10.20.20.3 com o endereço MAC 0000.0c9f.f014.

O PC de destino cria uma atualização ARP a cada 25 segundos, fazendo com que pacotes ARP constantes passem pelo 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
```

Um pacote de filtragem de pacotes ARP é usado para corresponder a esses pacotes.

```
> 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
```

A entrada para 000.0c9f.4014 permanece em 5 e nunca vai abaixo desse 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
```

Tempo limite de existência segundo estágio

Durante os últimos 2 minutos, a entrada cai em um período em que o endereço é considerado obsoleto.

```
> 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
```

A entrada ainda não foi removida e se algum pacote com o endereço MAC de origem correspondente à entrada da tabela, incluindo pacotes prontos para uso, for detectado, a entrada Age será atualizada de volta para 5 minutos.

Neste exemplo, um ping é enviado dentro desses 2 minutos para forçar o firewall a enviar seu próprio pacote 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
```

A entrada do endereço MAC é definida novamente como 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
```

tabela ARP

Primeiro, é essencial entender que a tabela de endereços MAC é totalmente independente da tabela ARP. Embora os pacotes ARP enviados pelo firewall para atualizar uma entrada ARP possam, ao mesmo tempo, atualizar a tabela de endereços MAC, esses processos de atualização são tarefas separadas e cada uma tem seus próprios intervalos e condições.

Mesmo que a tabela ARP não seja usada para determinar o próximo salto de saída como no modo roteado, é importante entender o efeito dos pacotes ARP gerados e destinados à identidade de firewall que os IPs podem ter em uma implantação transparente.

As entradas ARP são usadas para fins de gerenciamento e só são adicionadas à tabela se um recurso de gerenciamento ou tarefa o exigir. Como exemplo de uma tarefa de gerenciamento, se

um grupo de bridge tem um endereço IP, esse IP pode ser usado para fazer ping no 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
```

Se o destino estiver na mesma sub-rede que o IP do grupo de bridge, ele forçará uma solicitação ARP e se uma resposta ARP válida for recebida, a entrada IP/MAC será armazenada na tabela ARP.

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

Diferentemente da tabela de endereços MAC, o temporizador que acompanha a interface/endereço IP/triplet de endereço MAC é um valor crescente.

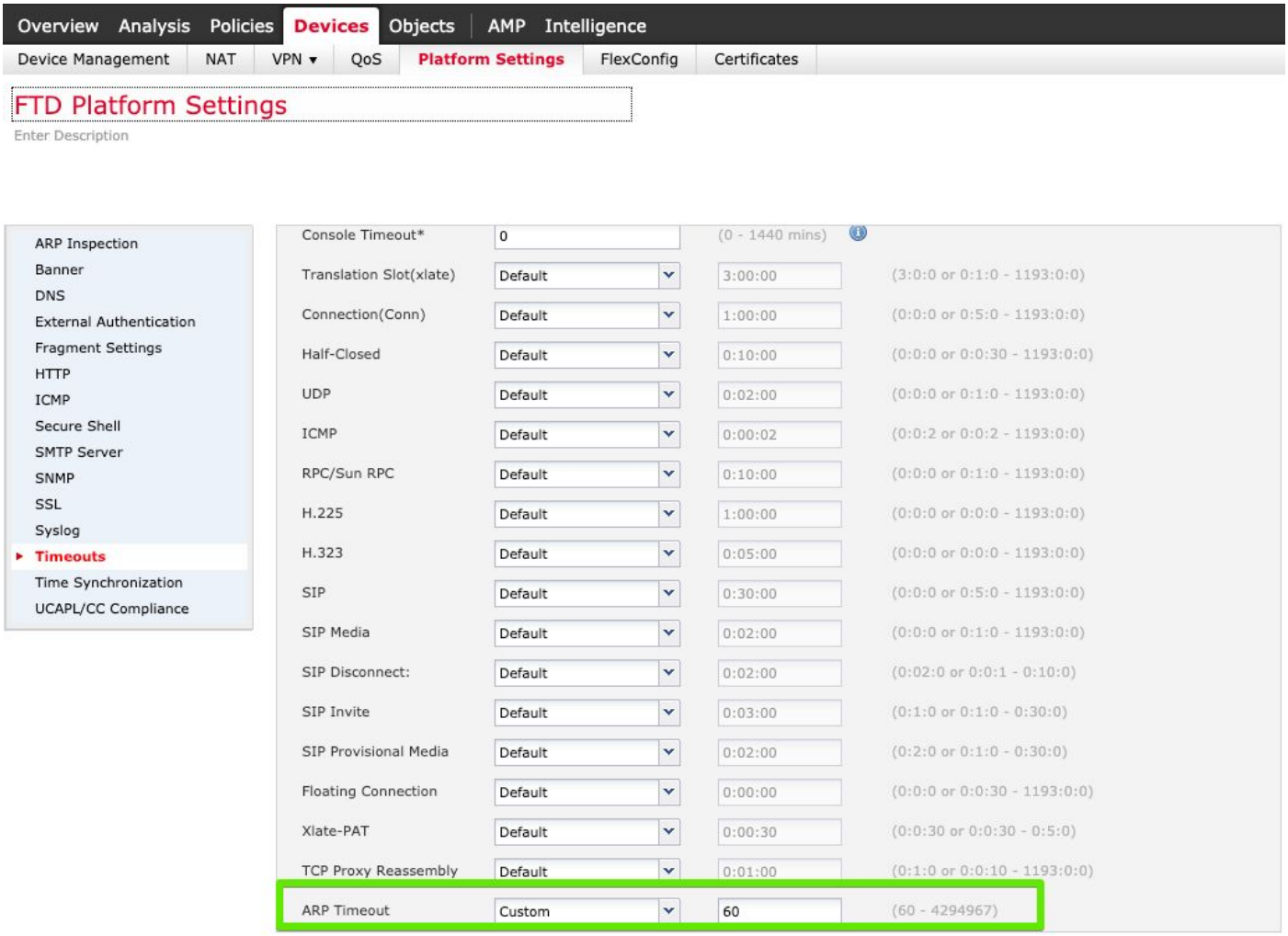
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Quando o temporizador atinge um valor *n - 30* em que *n* é o tempo limite configurado ARP (com um padrão de 14400 segundos), o firewall envia uma solicitação ARP para atualizar a entrada. Se uma resposta ARP válida for recebida, a entrada será mantida e o temporizador retornará para 0.

Neste exemplo, o tempo limite ARP foi reduzido para 60 segundos.

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

Esse tempo limite está disponível para ser configurado na guia **Devices > Platform Settings > Timeouts** no FMC, como mostrado na imagem.



Como o tempo limite é de 60 segundos, uma solicitação ARP é enviada a 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 entrada ARP é atualizada a 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
```

Dicas de solução de problemas

Direção de tráfego

Uma das coisas mais difíceis de rastrear em um TFW é a direção do fluxo de tráfego. Entender como o tráfego flui ajuda a garantir que o firewall esteja encaminhando corretamente os pacotes ao destino.

A determinação da interface de entrada e saída certa é uma tarefa mais fácil no modo roteado, pois há vários indicadores do envolvimento do firewall, como a modificação dos endereços MAC de origem e de destino e a redução do valor de Time-To-Live (TTL) de uma interface para a outra.

Essas diferenças não estão disponíveis em uma configuração TFW. O pacote que passa pela interface de ingresso é igual ao quando sai do firewall na maioria dos casos.

Problemas específicos, como flaps MAC na rede ou loops de tráfego, podem ser mais difíceis de rastrear sem saber onde o pacote entrou e quando saiu do firewall.

Para ajudar a diferenciar a entrada de pacotes de saída, a palavra-chave trace pode ser usada em capturas de pacotes.

```
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 o buffer de captura em bytes. 33554432 é o valor máximo disponível. Em modelos como 5500-X, Firepower Appliances ou máquinas virtuais, é seguro usar esse valor de tamanho desde que não haja dezenas de capturas já configuradas.

trace - Ativa a opção de rastreamento para o capturado especificado.

trace-count - Permite um número maior de rastreamentos. 1000 é o máximo permitido e 128 é o padrão. Isso também é seguro seguindo a mesma recomendação que para a opção de tamanho do buffer.

> **Tip**: Caso se esqueça de adicionar uma das opções, você pode adicioná-la sem ter que gravar a captura inteira novamente, fazendo referência ao nome da captura e à opção. No entanto, a nova opção afeta somente os pacotes recém-capturados, de modo que um *capname de captura clara* deve ser usado para ter o novo efeito desde o pacote número 1. Exemplo: **captura no rastreamento**

Depois que os pacotes tiverem sido capturados, o comando **show capture** *cap_name* **trace** exibirá os primeiros 1000 (se o número de rastreamento tiver sido aumentado) rastreamentos dos pacotes em ingresso.

```
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
```

Essa saída é um exemplo dos rastreamentos de captura de pacotes da interface externa. Isso significa que os pacotes 1 e 3 incluíram a interface externa e o pacote número 2 exibiram a interface.

Informações adicionais podem ser encontradas nesse rastreamento, como a Ação tomada para esse pacote e o motivo de descarte, caso o pacote seja descartado.

Para rastreamentos mais longos e se você quiser se concentrar em um único pacote, o comando **show capture** *cap_name* **trace packet-number** *packet_*number pode ser usado para exibir o rastreamento desse pacote específico.

Este é um exemplo de um número de pacote permitido 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
```

Rastreamento de MAC

O TFW toma todas as suas decisões de encaminhamento com base nos endereços MAC. Durante a análise do fluxo de tráfego, é essencial garantir que os endereços MAC usados como origem e destino em cada pacote estejam corretos com base na topologia de rede.

O recurso de captura de pacotes permite exibir os endereços MAC usados usando a opção ***detail*** do 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)
```

Depois de localizar um endereço MAC interessante e que exija rastreamento específico, os filtros de captura permitem que você faça correspondência com ele.

```
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)
```

Esse filtro é extremamente útil quando há rastreamentos de oscilações de MAC e você deseja encontrar o(s) culpado(s).

Depuração da tabela de endereços Mac

A depuração da tabela de endereços MAC pode ser habilitada para revisar cada fase. As informações fornecidas por essa depuração ajudam a entender quando um endereço MAC é aprendido, atualizado e removido da tabela.

Esta seção mostra exemplos de cada fase e como ler essas informações. Para habilitar os comandos debug no FTD, você deve acessar a CLI de diagnóstico.

> **aviso:** As depurações podem consumir recursos relevantes se a rede estiver muito ocupada. Recomenda-se a sua utilização em ambientes controlados ou em horários de pico baixos. É recomendável enviar essas depurações a um servidor Syslog se elas forem muito graves.

```
> 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
```

Etapa 1. O endereço MAC é aprendido. Quando uma entrada já não é encontrada na tabela MAC, esse endereço é adicionado à tabela. A mensagem de depuração informa o endereço e a interface onde foi recebida.

```
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.
!!!!
```

Se o MAC for aprendido através do método ICMP, a próxima mensagem será exibida. A entrada entra no primeiro estágio do ciclo de tempo limite em que não atualiza seu temporizador com base nas condições listadas no Temporizador de Tempo de existência da tabela de endereços MAC.

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

Etapa 2. Se uma entrada já for conhecida, a depuração informará sobre ela. A depuração também exibe mensagens de cluster que são irrelevantes em configurações independentes 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
```

Etapa 3. Quando a entrada tiver atingido o segundo estágio (2 minutos antes do tempo limite

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
```

Etapa 4. O firewall agora espera que novos pacotes originados com esse endereço atualizem a tabela. Se não houver mais pacotes usando essa entrada durante esses 2 minutos, o endereço será removido.

```
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.
```

Informações Relacionadas

- Guia do Firepower Management Center, Versão 6.3 - Capítulo 3: Modo de firewall transparente ou roteado para Firepower Threat Defense
- Suporte Técnico e Documentação - Cisco Systems