Concetti avanzati e suggerimenti per la risoluzione dei problemi relativi alla modalità firewall trasparente di Firepower Threat Defense

Sommario

Introduzione

Questo documento descrive una spiegazione dettagliata per comprendere i concetti e gli elementi fondamentali di una distribuzione Firepower Threat Defense (FTD) in modalità Transparent Firewall (TFW). In questo articolo vengono inoltre forniti utili strumenti e procedure dettagliate per i problemi più comuni relativi all'architettura del firewall trasparente.

Contributo di Cesar Lopez e curato da Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza modalità firewall trasparente FTD Cisco

- Nozioni base sul protocollo HSRP (Hot Standby Router Protocol)
- Protocolli Address Resolution Protocol (ARP) e Internet Control Message Protocol (ICMP)

Si consiglia vivamente di leggere la sezione Modalità firewall trasparente della guida alla configurazione di Firepower per una migliore comprensione dei concetti descritti in questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Concetti avanzati di Transparent Firewall

Tabella indirizzi MAC

Mentre un firewall in modalità routing si basa sulla tabella di routing e sulla tabella ARP per determinare l'interfaccia di uscita e i dati necessari per inoltrare un pacchetto all'hop successivo, la modalità TFW utilizza la tabella degli indirizzi MAC per essere in grado di determinare l'interfaccia di uscita utilizzata per inviare un pacchetto alla sua destinazione. Il firewall cerca il campo dell'indirizzo MAC di destinazione del pacchetto in fase di elaborazione e cerca una voce che colleghi questo indirizzo a un'interfaccia.

La tabella degli indirizzi MAC contiene questi campi.

```
> 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
```

- Interfaccia: questo campo contiene il nome dell'interfaccia da cui l'indirizzo MAC è stato appreso dinamicamente o configurato staticamente.
- Indirizzo MAC - Record indirizzo MAC da archiviare
- type - Metodo utilizzato per apprendere la voce. Può essere dinamico o statico
- Age(min) - Timer decrementale in minuti che visualizza il tempo rimasto prima che la voce venga contrassegnata come inattiva. Questo timer si applica solo alle voci di apprendimento dinamico
- bridge-group - ID gruppo bridge a cui appartiene l'interfaccia

La decisione di inoltro del pacchetto è simile a quella di uno switch, ma c'è una differenza molto importante quando si tratta di una voce mancante nella tabella MAC. In uno switch, il pacchetto

viene trasmesso tramite tutte le interfacce ad eccezione dell'interfaccia in entrata, ma in TFW. Se si riceve un pacchetto e non vi è alcuna voce per l'indirizzo MAC di destinazione, il pacchetto viene scartato. Viene scartato con il codice di rilascio 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
```

Questa condizione si verifica sempre per il primo pacchetto in un ambiente con l'apprendimento dinamico abilitato e senza voci statiche per una destinazione se l'indirizzo MAC non è stato visto in precedenza in un pacchetto come indirizzo MAC di origine.

Una volta aggiunta la voce alla tabella degli indirizzi MAC, è possibile autorizzare il pacchetto successivo in base alle funzionalità del firewall abilitate.

```
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
```

> **Attenzione:** Ricerca MAC è la prima fase delle azioni intraprese dal firewall. La presenza di cadute costanti dovute a ricerche L2 non riuscite può causare la perdita di pacchetti rilevanti e/o l'ispezione incompleta del motore di rilevamento. L'effetto dipende dalla capacità del protocollo o dell'applicazione di ritrasmettere.

In base a quanto sopra indicato, è sempre preferibile avere una voce appresa prima di qualsiasi trasmissione. TFW dispone di più meccanismi per imparare una voce.

Opzioni di apprendimento della tabella degli indirizzi MAC

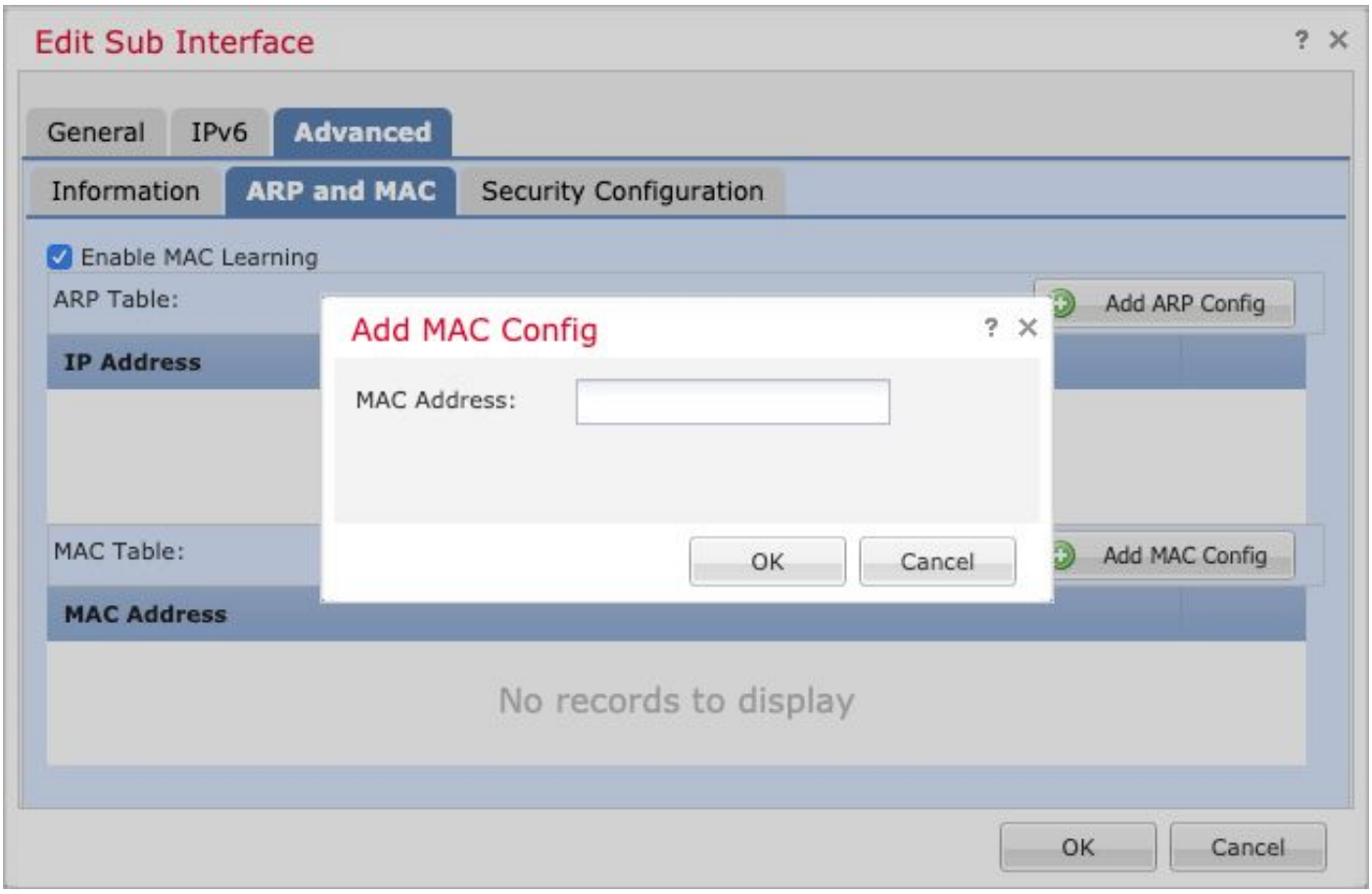
Voci statiche

Gli indirizzi MAC possono essere aggiunti manualmente per fare in modo che il firewall utilizzi sempre la stessa interfaccia per quella voce specifica. Questa opzione è valida per le voci che non possono essere modificate. Questa è un'opzione comune quando l'indirizzo MAC statico viene sovrascritto al livello di configurazione o da una funzione all'hop successivo.

Ad esempio, in uno scenario in cui l'indirizzo MAC del gateway predefinito sarà sempre lo stesso

su un router Cisco come è stato aggiunto manualmente alla configurazione o se l'indirizzo MAC virtuale del gateway HSRP rimarrà lo stesso.

Per configurare le voci statiche in FTD gestito da FMC, è possibile fare clic su **Edit Interface / Subinterface > Advanced > ARP and MAC** (Modifica interfaccia/sottointerfaccia > Avanzate > ARP e MAC) e fare clic su **Add MAC Config** (Aggiungi configurazione MAC). In questo modo viene aggiunta una voce per l'interfaccia specifica che si sta modificando dalla sezione **Dispositivi > Gestione dispositivi > Interfacce**.



Apprendimento dinamico basato sull'indirizzo MAC di origine

Questo metodo è simile a quello utilizzato da uno switch per popolare la tabella degli indirizzi MAC. Se un pacchetto ha un indirizzo MAC di origine che non fa parte delle voci della tabella MAC per l'interfaccia che è stata ricevuta, viene aggiunta una nuova voce alla tabella.

Apprendimento dinamico basato su sonda ARP

Se un pacchetto arriva con un indirizzo MAC di destinazione che non fa parte della tabella MAC e l'IP di destinazione fa parte della stessa rete dell'interfaccia virtuale del bridge (BVI), il TFW tenta di apprendere che sta inviando una richiesta ARP tramite tutte le interfacce del gruppo di bridge. Se si riceve una risposta ARP da una delle interfacce del gruppo di bridge, questa viene aggiunta alla tabella MAC. Si noti che, come indicato in precedenza, in assenza di risposta a tale richiesta ARP, tutti i pacchetti vengono scartati con il codice ASP *dst-l2_lookup-fail*.

Apprendimento dinamico basato su sonda ICMP

Se un pacchetto arriva con un indirizzo MAC di destinazione che non fa parte della tabella MAC e

l'IP di destinazione NON fa parte della stessa rete della BVI, viene inviata una richiesta echo ICMP con un valore TTL (Time-to-Live) pari a 1. Il firewall si aspetta un messaggio ICMP "Tempo scaduto" per imparare l'indirizzo MAC dell'hop successivo.

Timer durata tabella indirizzi MAC

Il timer di validità della tabella degli indirizzi MAC è impostato su 5 minuti per ogni voce appresa. Questo valore di timeout prevede due stadi diversi.

Timeout validità prima fase

Durante i primi 3 minuti, il valore Age della voce MAC non viene aggiornato a meno che un pacchetto di risposta ARP che passa attraverso il firewall con l'indirizzo MAC di origine non sia uguale a una voce nella tabella degli indirizzi MAC. Questa condizione esclude le risposte ARP destinate agli indirizzi IP del gruppo di bridge. Ciò significa che qualsiasi altro pacchetto che non sia una risposta ARP completa viene ignorato nei primi 3 minuti.

Nell'esempio, è presente un PC con indirizzo IP 10.10.10.5 che invia un ping a 10.20.20.5. L'indirizzo IP del gateway per 10.20.20.5 è 10.20.20.3 con indirizzo MAC 000.0c9f.f014.

Il PC di destinazione crea un aggiornamento ARP ogni 25 secondi causando il passaggio di pacchetti ARP costanti attraverso il 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
```

I pacchetti ARP di filtro acquisizione pacchetti vengono utilizzati per trovare una corrispondenza con questi pacchetti.

```
> 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 voce per 000.0c9f.4014 rimane 5 e non va mai al di sotto di tale numero.

```
> 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
```

Timeout durata seconda fase

Negli ultimi 2 minuti, la voce rientra in un periodo di tempo in cui l'indirizzo è considerato scaduto.

```
> 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 voce non viene ancora rimossa e se viene rilevato un pacchetto con l'indirizzo MAC di origine corrispondente alla voce della tabella, inclusi i pacchetti "to the box", la voce Age viene aggiornata a 5 minuti.

Nell'esempio, viene inviato un ping entro questi 2 minuti per forzare il firewall a inviare il proprio pacchetto 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 voce relativa all'indirizzo MAC è impostata su 5 minuti.

```
> 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
```

tabella ARP

In primo luogo, è essenziale capire che la tabella degli indirizzi MAC è completamente indipendente dalla tabella ARP. Mentre i pacchetti ARP inviati dal firewall per aggiornare una voce ARP possono, allo stesso tempo, aggiornare la tabella degli indirizzi MAC, questi processi di aggiornamento sono attività separate e ognuno ha i propri timeout e condizioni.

Anche se la tabella ARP non viene usata per determinare l'hop successivo in uscita come in

modalità di routing, è importante capire l'effetto dei pacchetti ARP generati e destinati all'identità firewall che gli IP possono avere in un'implementazione trasparente.

Le voci ARP vengono utilizzate a scopo di gestione e vengono aggiunte alla tabella solo se una funzione o un task di gestione lo richiede. Come esempio di attività di gestione, se un gruppo di bridge dispone di un indirizzo IP, questo IP può essere utilizzato per eseguire il ping della destinazione.

```
> 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 la destinazione si trova nella stessa subnet dell'indirizzo IP del gruppo di bridge, viene forzata una richiesta ARP e, se viene ricevuta una risposta ARP valida, la voce IP/MAC viene memorizzata nella tabella ARP.

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

A differenza della tabella degli indirizzi MAC, il timer che accompagna la tripletta interfaccia/indirizzo IP/indirizzo MAC è un valore crescente.

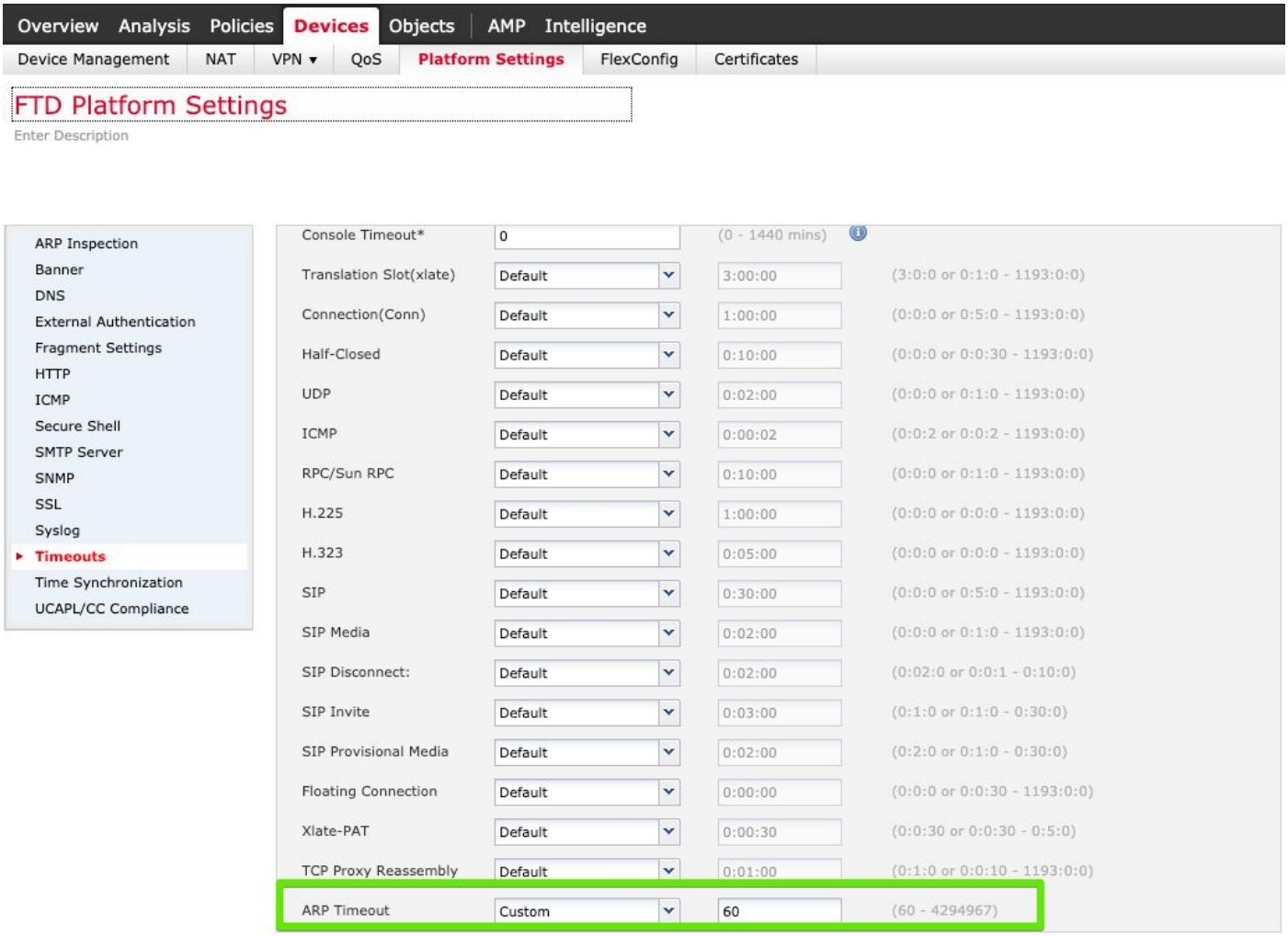
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Quando il timer raggiunge un valore *n - 30* dove *n* è il timeout configurato per ARP (con un valore predefinito di 14400 secondi), il firewall invia una richiesta ARP per aggiornare la voce. Se si riceve una risposta ARP valida, la voce viene sospesa e il timer torna a 0.

In questo esempio, il timeout ARP è stato ridotto a 60 secondi.

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

Questo timeout è disponibile per la configurazione nella scheda **Dispositivi > Impostazioni piattaforma > Timeout** in FMC, come mostrato nell'immagine.



Poiché il timeout è di 60 secondi, viene inviata una richiesta ARP ogni 30 secondi (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
```

La voce ARP viene quindi aggiornata ogni 30 secondi.

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

Suggerimenti per la risoluzione dei problemi

Direzione traffico

Una delle cose più difficili da rintracciare su un TFW è la direzione del flusso del traffico.

Comprendere come i flussi di traffico aiutino a garantire che il firewall inoltri correttamente i pacchetti alla destinazione.

Determinare l'interfaccia corretta in entrata e in uscita è un'operazione più semplice nella modalità Routed, in quanto esistono diversi indicatori del coinvolgimento del firewall, ad esempio la modifica degli indirizzi MAC di origine e di destinazione e la riduzione del valore TTL (Time-To-Live) da un'interfaccia all'altra.

Queste differenze non sono disponibili in una configurazione TFW. Nella maggior parte dei casi, il pacchetto che attraversa l'interfaccia in entrata ha lo stesso aspetto di quando esce dal firewall.

Problemi specifici come i link ai link MAC nella rete o i loop di traffico potrebbero essere più difficili da tracciare senza sapere dove il pacchetto è entrato e quando è uscito dal firewall.

Per distinguere l'ingresso dai pacchetti in uscita, la parola chiave trace può essere usata nelle acquisizioni dei pacchetti.

```
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 il buffer di acquisizione in byte. 33554432 è il valore massimo disponibile. In modelli come 5500-X, appliance Firepower o macchine virtuali, è sicuro utilizzare questo valore di dimensioni purché non vi siano decine di acquisizioni già configurate.

trace: abilita l'opzione trace per l'oggetto recuperato specificato.

trace-count: consente un numero maggiore di tracce. Il valore massimo consentito è 1000, il valore predefinito è 128. Anche questo è sicuro seguendo lo stesso consiglio dell'opzione dimensione buffer.

> **Suggerimento**: Se dimenticate di aggiungere una delle opzioni, potete aggiungerla senza dover riscrivere l'intera acquisizione facendo riferimento al nome e all'opzione. Tuttavia, poiché la nuova opzione influisce solo sui pacchetti appena acquisiti, per ottenere il nuovo effetto dal numero di pacchetto 1 è necessario utilizzare **clear capture *capname***. Esempio: **acquisire in traccia**

Dopo l'acquisizione dei pacchetti, il comando **show capture *cap_name* trace** visualizza le prime 1000 tracce (se il numero di traccia è stato aumentato) dei pacchetti in entrata.

```
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
```

Questo output è un esempio delle tracce di acquisizione dei pacchetti dell'interfaccia esterna. I numeri 1 e 3 entrano quindi nell'interfaccia esterna, mentre il numero 2 esce dall'interfaccia.

In questa traccia sono disponibili ulteriori informazioni, ad esempio l'azione intrapresa per il

pacchetto e il motivo dell'eliminazione, in caso il pacchetto venga scartato.

Per tracce più lunghe e se si desidera evidenziare un singolo pacchetto, il comando **show capture** ***cap_name*** **trace packet-number** ***packet_***number può essere usato per visualizzare la traccia per quel pacchetto specifico.

Questo è un esempio di pacchetto autorizzato numero 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
```

Tracciamento MAC

TFW prende tutte le decisioni relative all'inoltro in base agli indirizzi MAC. Durante l'analisi del flusso di traffico, è essenziale verificare che gli indirizzi MAC utilizzati come origine e destinazione su ciascun pacchetto siano corretti in base alla topologia di rete.

La funzione di acquisizione del pacchetto consente di visualizzare gli indirizzi MAC utilizzati usando l'opzione ***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 volta individuato un indirizzo MAC interessante che richiede un tracciamento specifico, i filtri di acquisizione consentono di farvi corrispondere.

```
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)
```

Questo filtro è estremamente utile quando ci sono tracce di flap MAC e si desidera trovare il colpevole (i colpevoli).

Debug della tabella degli indirizzi Mac

Il debug della tabella degli indirizzi MAC può essere abilitato per l'analisi di ciascuna fase. Le informazioni fornite da questo debug consentono di capire quando un indirizzo MAC viene appreso, aggiornato e rimosso dalla tabella.

In questa sezione vengono illustrati alcuni esempi di ciascuna fase e viene spiegato come leggere queste informazioni. Per abilitare i comandi di debug su FTD, è necessario accedere alla CLI di diagnostica.

> **Avviso:** Se la rete è occupata, i debug possono richiedere l'utilizzo di risorse rilevanti. Si consiglia di utilizzarli in ambienti controllati o durante le ore di punta. Si consiglia di inviare questi debug a un server Syslog se sono troppo dettagliati.

```
> 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
```

Passaggio 1. Viene appreso l'indirizzo MAC. Quando non viene trovata alcuna voce nella tabella MAC, questo indirizzo viene aggiunto alla tabella. Il messaggio di debug informa l'indirizzo e l'interfaccia su cui è stato ricevuto.

```
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 l'indirizzo MAC viene acquisito tramite il metodo ICMP, viene visualizzato il messaggio successivo. La voce entra nella prima fase del ciclo di timeout in cui non aggiorna il proprio timer in base alle condizioni elencate nel timer Age della tabella degli indirizzi MAC.

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

Passaggio 2. Se una voce è già nota, il comando debug ne informa la Commissione. Il debug visualizza anche i messaggi di clustering che sono irrilevanti nelle impostazioni standalone 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
```

Passaggio 3. Dopo aver raggiunto la seconda fase (2 minuti prima del timeout assoluto).

```
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
```

Passaggio 4. Il firewall ora si aspetta che i nuovi pacchetti provenienti da tale indirizzo aggiornino la tabella. Se non ci sono più pacchetti che usano quella voce durante quei 2 minuti, l'indirizzo viene rimosso.

```
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.
```

Informazioni correlate

- Guida di Firepower Management Center, versione 6.3 - Capitolo 3: Modalità firewall trasparente o con routing per Firepower Threat Defense
- Documentazione e supporto tecnico – Cisco Systems