

ASA: Tramas Ethernet enormes de recepción y que transmiten

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Soporte de Trama Jumbo en el ASA](#)

[¿Qué si el ASA no se configura para las Tramas gigantes y recibe una trama Jumbo?](#)

[¿Qué si el ASA recibe con éxito una trama Jumbo pero intenta mandarle una interfaz con un MTU inferior?](#)

[Información Relacionada](#)

[Introducción](#)

Este documento provee información sobre cómo el Adaptive Security Appliance (ASA) recibe y transmite tramas Ethernet jumbo.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

[Soporte de Trama Jumbo en el ASA](#)

Habilitar el soporte de Trama Jumbo requiere las versiones de software y hardware adaptantes específicas del dispositivo de seguridad (ASA), así como una reinicialización. Para más

información sobre los modelos y las versiones soportados, así como cómo habilitar las Tramas gigantes, refiera a la sección de la guía de configuración ASA 8.4, [habilitando el soporte de Trama Jumbo \(modelos soportados\)](#).

Observe que después de habilitar el soporte de Trama Jumbo y de reiniciar el ASA, estas medidas adicionales se deben tomar para hacer el uso completo de las Tramas gigantes:

- El MTU de las interfaces ASA se debe aumentar con el **comando mtu** en el modo de la sub-configuración de la interfaz de modo que el ASA transmita las Tramas gigantes.
- El ASA se debe configurar para ajustar el TCP MSS para que haya conexiones TCP a un valor más alto que el valor por defecto. Si esto no se hace, las tramas Ethernet que contienen los datos de TCP no serán más grandes de 1500 bytes. El TCP MSS se debe ajustar a 120 bytes menos que la configuración más baja según el MTU de interfaz. Si el MTU de interfaz es 9216, después el MSS se debe configurar a 9096. Esto se puede hacer con el comando de los **tcpmss** de la conexión del **sysopt**.

¿Qué si el ASA no se configura para las Tramas gigantes y recibe una trama Jumbo?

El comando **enorme de la trama-reserva** permite no sólo la transmisión de los jumbo, pero también a la recepción. Sin el soporte de Trama Jumbo habilitado, el ASA caerá los paquetes que son demasiado grandes. Estos descensos se cuentan conforme a la estadística "gigante" en la **salida de la interfaz de la demostración**:

```
ASA# show interface Interface GigabitEthernet0/0 "inside", is up, line protocol is up Hardware is bcm56801 rev 01, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps) Input flow control is unsupported, output flow control is on MAC address 5475.d029.8916, MTU 1500 IP address 10.36.29.1, subnet mask 255.255.0.0 499 packets input, 52146 bytes, 0 no buffer Received 63 broadcasts, 0 runts, 5 giants <---- HERE
```

¿Qué si el ASA recibe con éxito una trama Jumbo pero intenta mandarle una interfaz con un MTU inferior?

Para recibir una trama Jumbo, el ASA debe tener el comando de la reserva de la trama Jumbo, pero no necesita necesariamente hacer el MTU aumentar (porque eso afecta solamente al tamaño de la transmisión máxima para la interfaz, no la recepción).

Si el ASA recibe con éxito una trama Jumbo, pero esa trama es entonces demasiado grande transmitir hacia fuera la interfaz de egreso, estas situaciones pueden ocurrir dependiendo de la configuración del don't fragment (DF) mordida en el encabezado IP del paquete:

- Si el bit DF se fija en el encabezado IP, el ASA caerá el paquete y enviará un mensaje del código 4 del tipo 3 ICMP de nuevo al remitente.
- Si el bit DF no se fija, el ASA hará fragmentos del paquete y transmitirá los fragmentos hacia fuera la interfaz de egreso.

Ésta es una sesión CLI ASA que utiliza a las capturas de paquetes para mostrar el ASA que recibe una trama Jumbo en la interfaz interior (con un tamaño de 4014 bytes) que es demasiado grande transmitir hacia fuera la interfaz de egreso (el exterior tiene un MTU de 1500). **En este caso el bit DF no se fija en el encabezado IP.** El paquete se hace fragmentos en la salida hacia fuera la interfaz exterior:

```
ASA# show cap in detail 20 packets captured 1: 11:30:30.308913 0017.0f17.af80 5475.d029.8916
0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (ttl 255, id 48872) 2:
11:30:30.309920 5475.d029.8916 0017.0f17.af80 0x0800 1514: 10.23.124.1 > 10.99.103.6: icmp: echo
reply (wrong icmp csum) (frag 48872:1480@0+) (ttl 255) 3: 11:30:30.309935 5475.d029.8916
0017.0f17.af80 0x0800 1514: 10.23.124.1 > 10.99.103.6: (frag 48872:1480@1480+) (ttl 255) 4:
11:30:30.309935 5475.d029.8916 0017.0f17.af80 0x0800 1054: 10.23.124.1 > 10.99.103.6: (frag
48872:1020@2960) (ttl 255) ... ASA# show cap out detail 30 packets captured 1: 11:30:30.309035
5475.d029.8917 001a.a185.847f 0x0800 1514: 10.23.124.142 > 10.23.124.1: icmp: echo request
(wrong icmp csum) (frag 48872:1480@0+) (ttl 255) 2: 11:30:30.309035 5475.d029.8917
001a.a185.847f 0x0800 1514: 10.23.124.142 > 10.23.124.1: (frag 48872:1480@1480+) (ttl 255) 3:
11:30:30.309050 5475.d029.8917 001a.a185.847f 0x0800 1054: 10.23.124.142 > 10.23.124.1: (frag
48872:1020@2960) (ttl 255) 4: 11:30:30.309859 001a.a185.847f 5475.d029.8917 0x0800 1514:
10.23.124.1 > 10.23.124.142: icmp: echo reply (wrong icmp csum) (frag 48872:1480@0+) (ttl 255)
5: 11:30:30.309859 001a.a185.847f 5475.d029.8917 0x0800 1514: 10.23.124.1 > 10.23.124.142: (frag
48872:1480@1480+) (ttl 255) 6: 11:30:30.309859 001a.a185.847f 5475.d029.8917 0x0800 1054:
10.23.124.1 > 10.23.124.142: (frag 48872:1020@2960) (ttl 255)
```

Esto es un ejemplo que muestra un ASA que recibe una trama Jumbo en la interfaz interior demasiado grande para transmitir hacia fuera la interfaz de egreso, y el paquete tiene el conjunto de bits DF. Se cae el paquete y el mensaje de error del código 4 del tipo 3 ICMP se transmite hacia el host interior:

```
ASA# show cap in detail 6 packets captured 1: 11:42:10.147422 0017.0f17.af80 5475.d029.8916
0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (DF) (ttl 255, id 48887) 2:
11:42:10.147605 5475.d029.8916 0017.0f17.af80 0x0800 70: 10.99.29.1 > 10.99.103.6: icmp:
10.23.124.1 unreachable - need to frag (mtu 1500) (ttl 72, id 56194) 3: 11:42:10.150199
0017.0f17.af80 5475.d029.8916 0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (DF)
(ttl 255, id 48888) 4: 11:42:12.146476 0017.0f17.af80 5475.d029.8916 0x0800 4014: 10.99.103.6 >
10.23.124.1: icmp: echo request (DF) (ttl 255, id 48889) 5: 11:42:12.146553 5475.d029.8916
0017.0f17.af80 0x0800 70: 10.99.29.1 > 10.99.103.6: icmp: 10.23.124.1 unreachable - need to frag
(mtu 1500) (ttl 72, id 45247) 6: 11:42:12.152427 0017.0f17.af80 5475.d029.8916 0x0800 4014:
10.99.103.6 > 10.23.124.1: icmp: echo request (DF) (ttl 255, id 48890) 6 packets shown ASA# show
cap out detail 0 packet captured 0 packet shown ASA#
```

[Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)