Explicación de los paquetes RST enviados por Secure Firewall

Contenido

Introducción

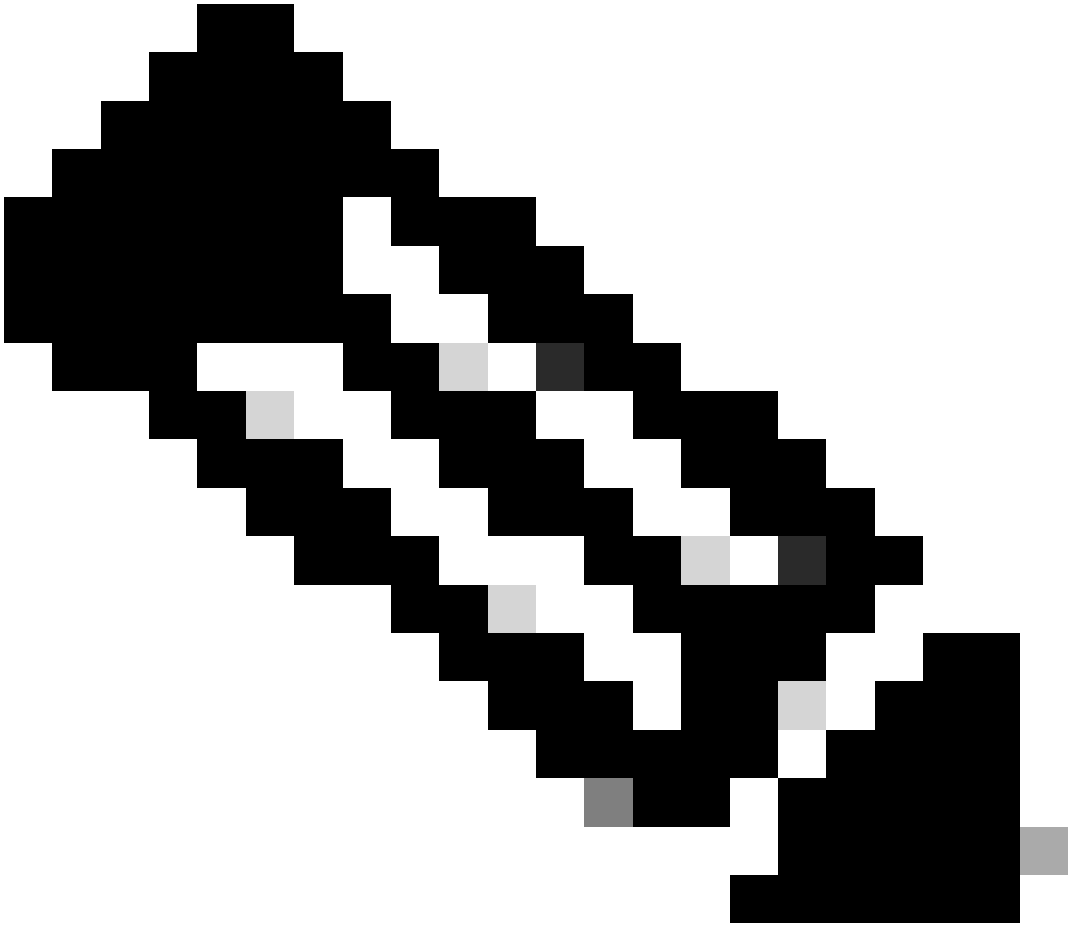
Este documento describe el comportamiento de un firewall de Cisco cuando se envían restablecimientos de TCP para las sesiones de TCP que intentan transitar el firewall.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- flujo de paquetes ASA
- flujo de paquetes FTD
- Capturas de paquetes ASA/FTD



Nota: Este comportamiento descrito se aplica a ASA y a Secure Firewall Threat Defence.

Componentes Utilizados

La información de este documento se basa en este software:

- ASA
- Firewall seguro Threat Defence FTD

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

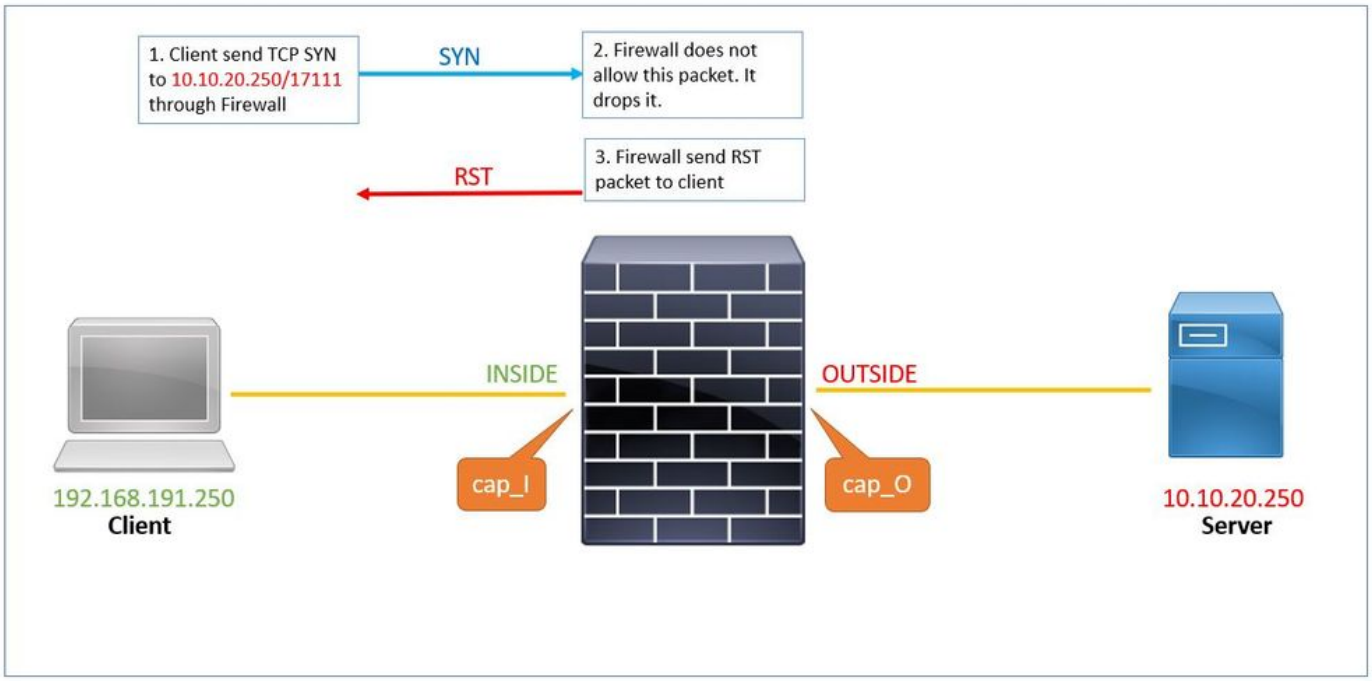
Troubleshoot

El cortafuegos envía reinicios de TCP para las sesiones TCP que intentan transitar por el

cortafuegos y que éste deniega en función de las listas de acceso. El firewall también envía restablecimientos para los paquetes permitidos por una lista de acceso, pero que no pertenecen a una conexión que existe en el firewall y que, por lo tanto, es denegada por la función stateful.

Caso práctico 1: el servicio resetoutbound está activado y se deniega el tráfico cliente-servidor.

De forma predeterminada, service **resetoutbound** está habilitado para todas las interfaces. En este caso práctico, no existe ninguna regla que permita el tráfico cliente-servidor.



Estas son las capturas configuradas en el Firewall:

```
# show capture
capture cap_I type raw-data trace trace-count 50 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture cap_O type raw-data trace trace-count 50 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture asp type asp-drop all [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
```

El servicio resetoutbound está habilitado de forma predeterminada. Por lo tanto, si el resultado del show run service comando no muestra nada, significa que está habilitado:

```
# show run service ...
```

1. El cliente envía TCP SYN al servidor 10.10.20.250/17111 a través del firewall. Paquete número 1 en esta captura:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

2. Dado que no hay ninguna ACL que permita este tráfico, Secure Firewall descarta este paquete con acl-drop motivo. Este paquete se captura en la captura asp-drop.

```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74
192.168.191.250.46118 > 10.10.20.250.17111: S [tcp sum ok] 3490277958:3490277958(0) win 29200 <mss 1380
    (DF) (ttl 49, id 60335)

<output removed>

Subtype: log
Result: DROP
Config:
access-group allow_all global
access-list allow_all extended deny ip any any
Additional Information:

<output removed>

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
```

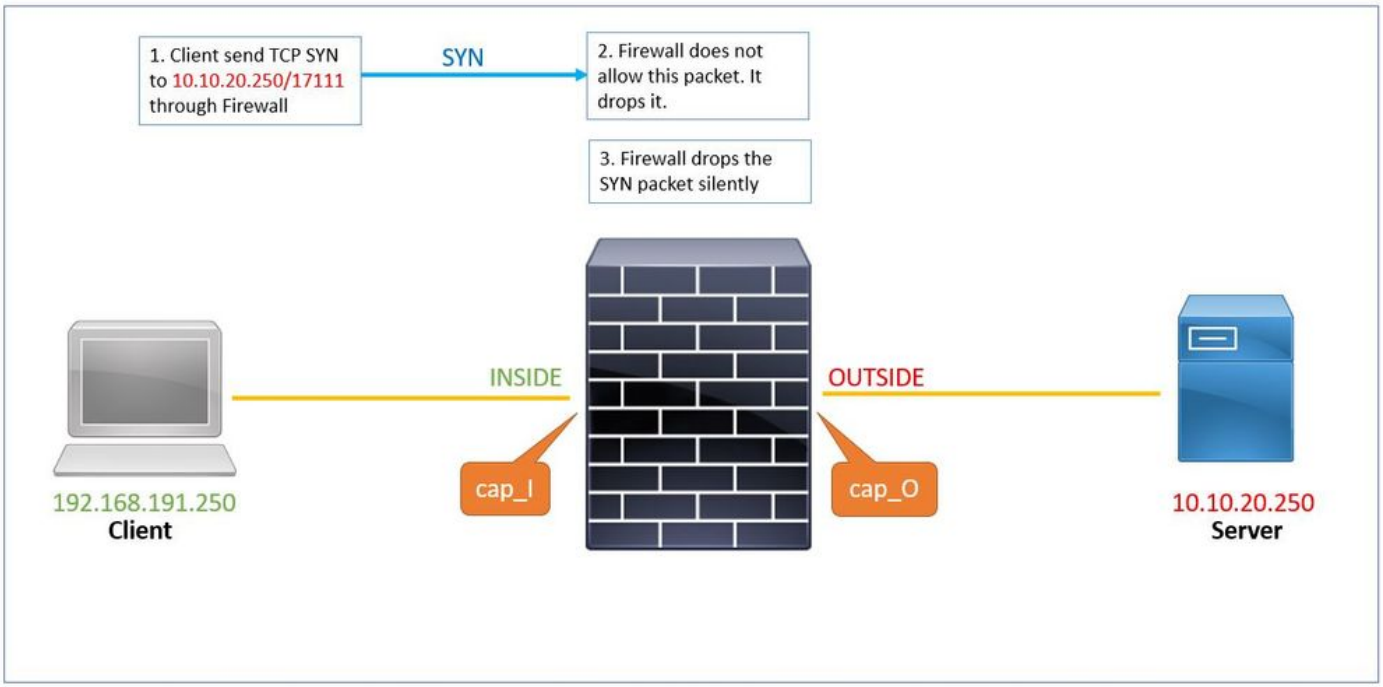
```
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. El firewall envía un paquete RST con la dirección IP del servidor como dirección IP de origen. Paquete número 2 en esta captura:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
        timestamp 2096884214 0,nop,wscale 7>
2: 19:48:55.512806 10.10.20.250.17111 > 192.168.191.250.46118: R 0:0(0) ack 3490277959 win 29200
```

Caso práctico 2: el servicio resetoutbound no está habilitado y se deniega el tráfico cliente-servidor.

En el caso práctico 2, no hay ninguna regla para permitir el tráfico cliente-servidor y el servicio **resetoutbound** está desactivado.



El show run service comando muestra que service **resetoutbound** está inhabilitado.

```
# show run service
no service resetoutbound
```

1. El cliente envía TCP TCP al servidor 10.10.20.250/17111 a través del firewall. Paquete número 1 en esta captura:

```
# show capture cap_I

1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200
<mss 1380,sackOK,timestamp 2096884214 0,nop,wscale 7>
```

2. Dado que no hay ninguna ACL que permita este tráfico, Secure Firewall descarta este paquete con acl-drop motivo. Este paquete se captura en el **asp-drop capture**.

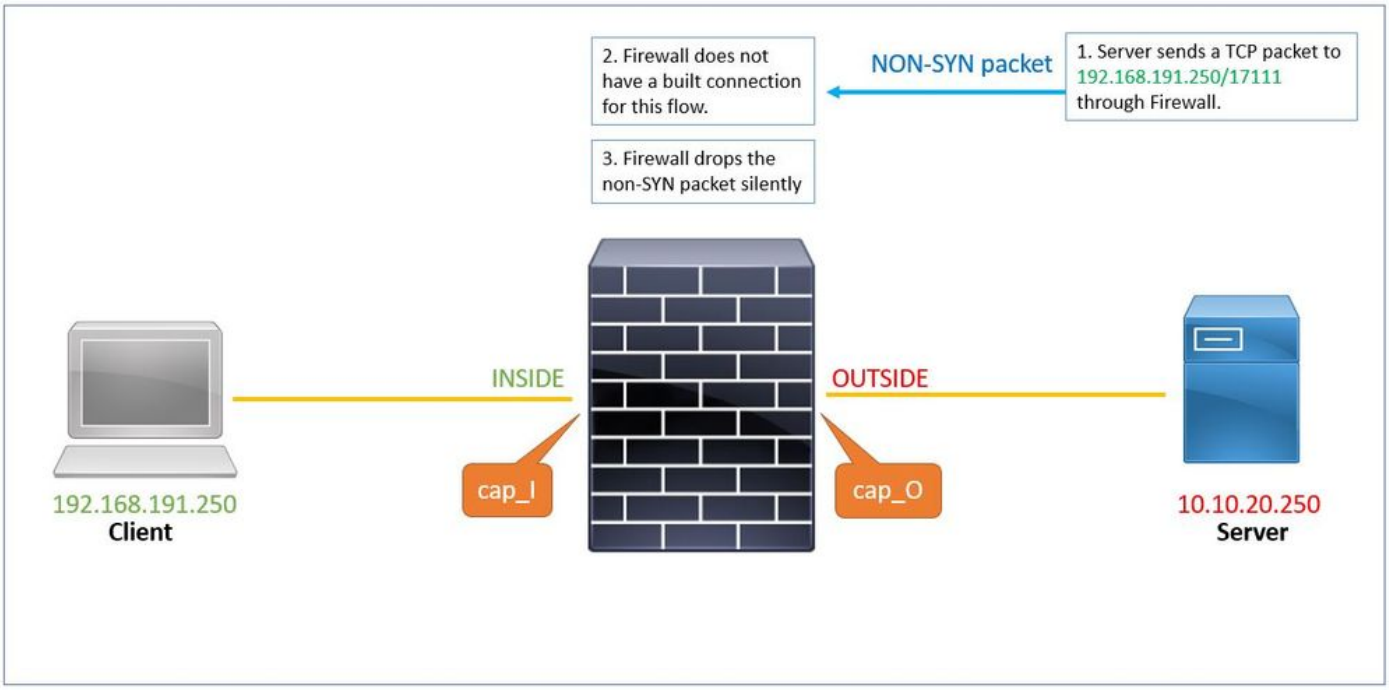
```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74 192.168.191.250.46118 > 10.10.20.250
```

3. La **asp-drop capture** muestra el paquete SYN pero no hay ningún paquete RST enviado de vuelta cap_I capturevía interfaz interna:

```
# show cap cap_I
1: 23:58:32.850755 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms

# show cap asp
1: 23:58:32.850999 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

Caso práctico 3: Service resetoutbound disabled (predeterminado) service resetinbound disabled (predeterminado)

De forma predeterminada, service **resetoutbound** está habilitado para todas las interfaces y service **resetinbound** está deshabilitado.



1. El servidor envía un paquete TCP (SYN/ACK) al cliente a través del firewall. El firewall no tiene una conexión integrada para este flujo.

```
# show capture cap_O

1: 00:22:35.111993 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

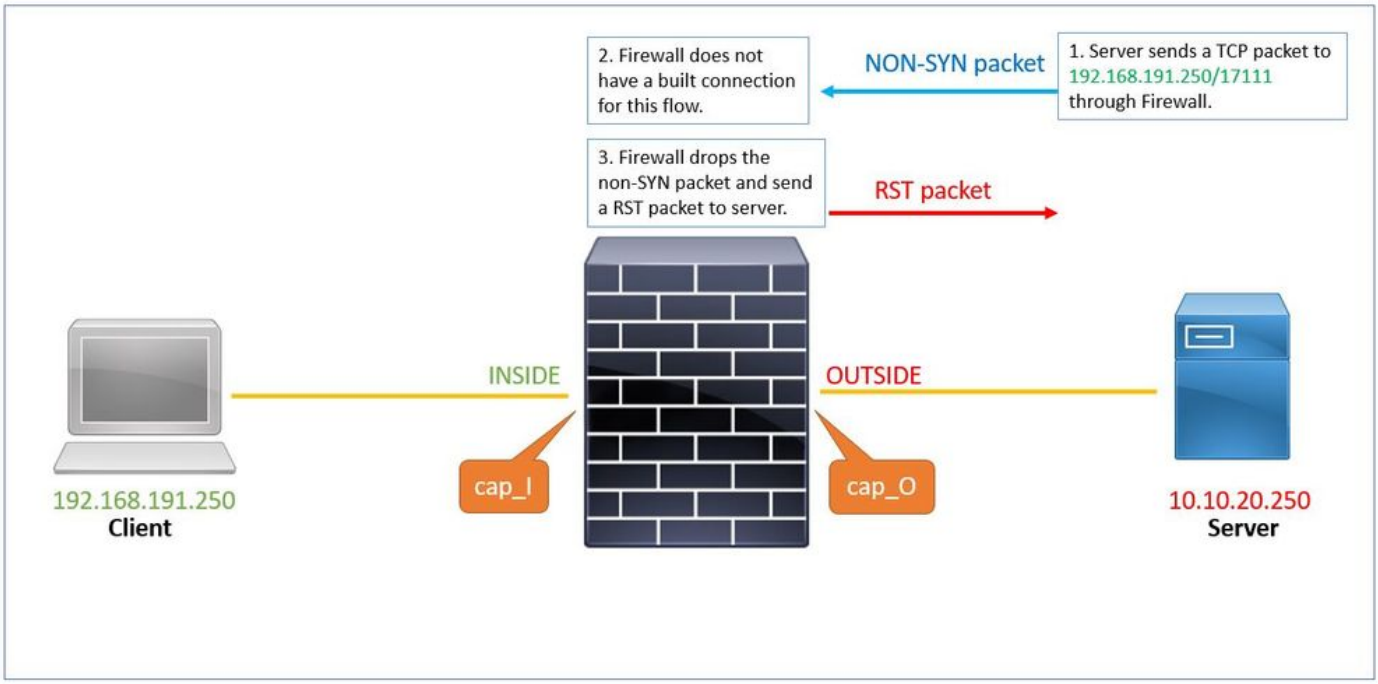
2. El restablecimiento no se envía del firewall al servidor. Este paquete SYN/ACK se descarta silenciosamente con la razón tcp-not-syn. Se captura también en asp-drop capture.

```
# show capture cap_O packet-number 1 trace detail
1: 00:22:35.111993 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
</pre
```

```
# show capture asp

1: 00:22:35.112176 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

Caso práctico 4: Servicio resetoutbound disabled (predeterminado) servicio resetinbound disabled.

De forma predeterminada, service **resetinbound** está inhabilitado para todas las interfaces y service **resetinbound** también está inhabilitado con el comando de configuración.



La salida del show run service comando muestra que el servicio **resetoutbound** está inhabilitado (de forma predeterminada) y el servicio **resetinbound** está inhabilitado por el comando de configuración.

```
# show run service
service resetinbound
```

1. El servidor envía un paquete TCP (SYN/ACK) al cliente a través del firewall.

```
# show cap cap_O

1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

2. El firewall no tiene una conexión integrada para este flujo y lo descarta. El asp-drop captures muestra el paquete:

```
# show capture cap_O packet-number 1 trace detail
1: OO:32:26.434395 a2c7.1eOO.003e OO50.56b3.1ef5 Ox08OO Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(O) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
```

3. Desde el servicio **resetinbound**, el firewall envía un paquete RST al servidor con la dirección IP de origen del cliente.

```
# show capture cap_O
1: OO:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(O) ack 349027795
2: OO:32:26.434608 192.168.191.250.46118 > 10.10.20.250.17111: R 3490277959:3490277959(O) ack 347502458
```

Información Relacionada

- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).