Entender os pacotes RST enviados pelo Cisco Secure Firewall

Contents

Introdução

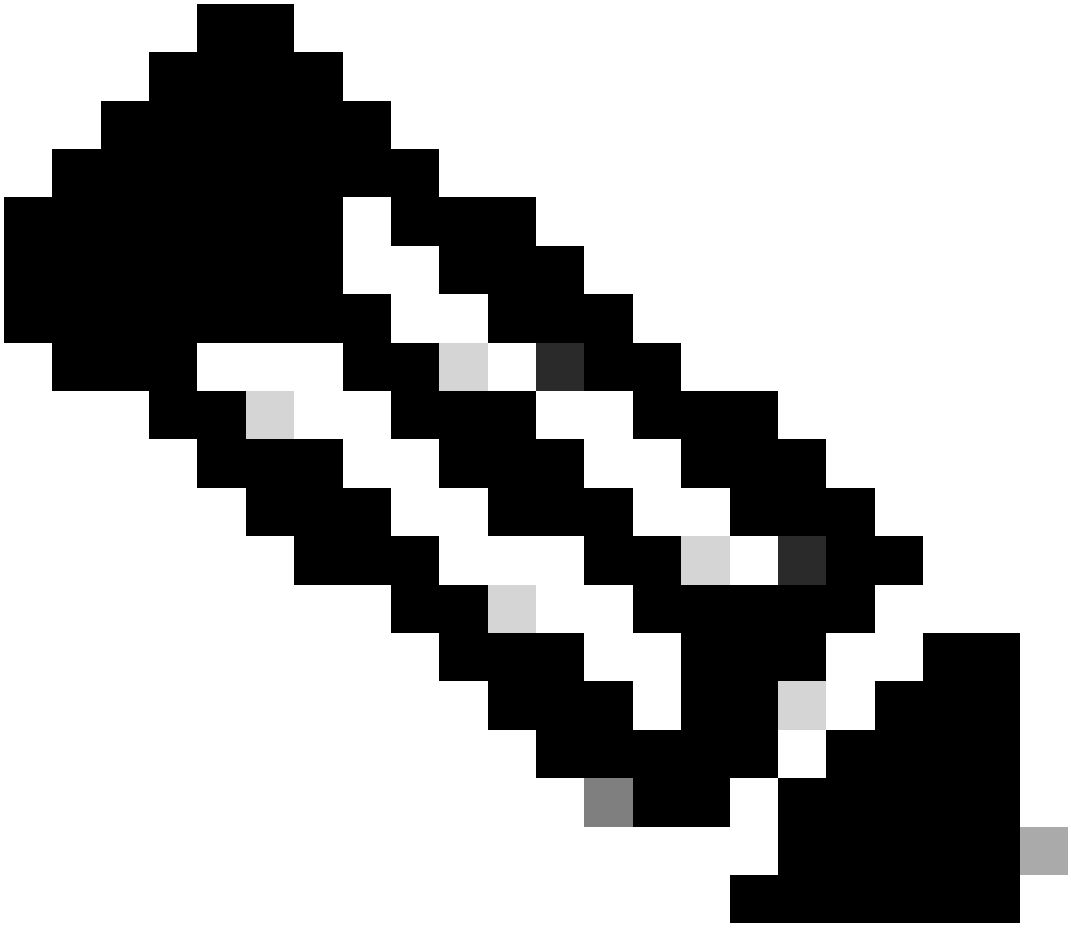
Este documento descreve o comportamento de um Cisco Firewall quando as redefinições de TCP são enviadas para sessões TCP que tentam passar pelo firewall.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxo de pacote ASA
- Fluxo de pacote FTD
- Capturas de pacotes ASA/FTD



Observação: esse comportamento descrito se aplica ao ASA e ao Secure Firewall Threat Defense.

Componentes Utilizados

As informações neste documento são baseadas neste software:

- ASA
- FTD Secure Firewall Threat Defense

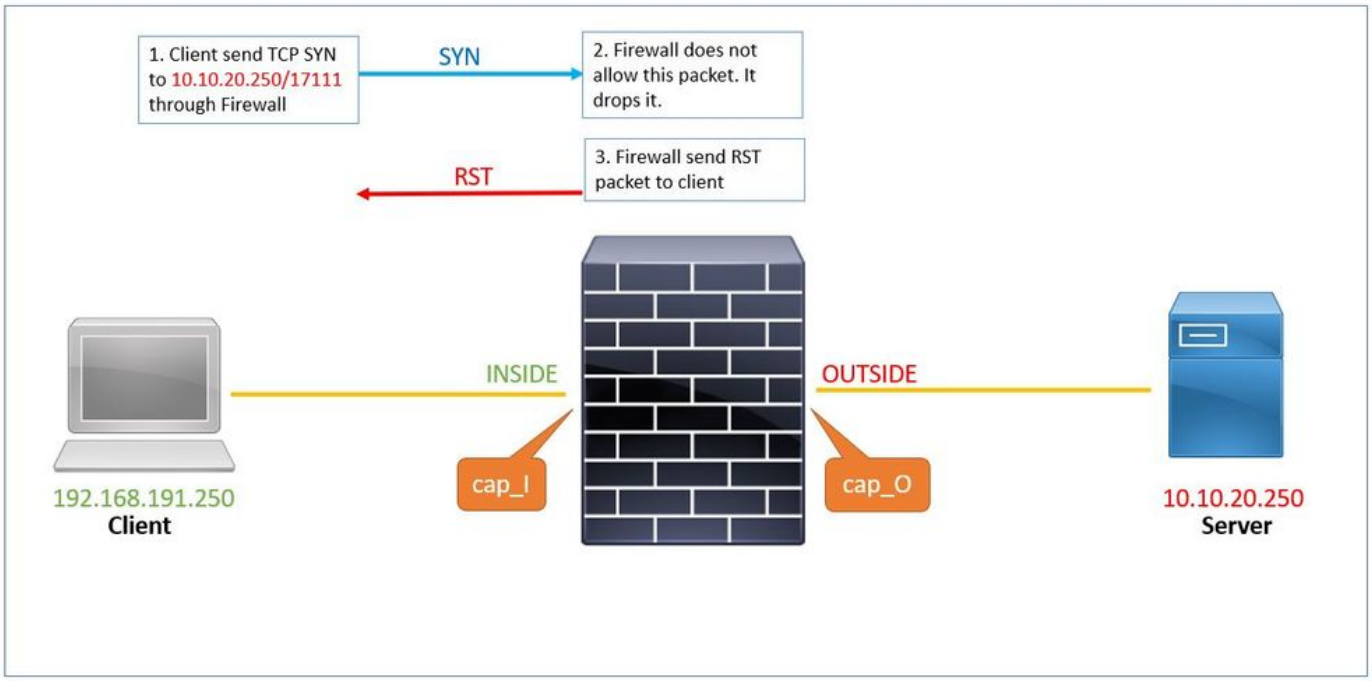
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Troubleshooting

O Firewall envia redefinições de TCP para sessões de TCP que tentam transitar pelo Firewall e são negadas pelo Firewall com base em listas de acesso. O Firewall também envia redefinições para pacotes que são permitidos por uma lista de acesso, mas que não pertencem a uma conexão que existe no firewall e, portanto, é negada pelo recurso stateful.

Estudo de caso 1: o serviço resetoutbound está habilitado e o tráfego de cliente para servidor é negado.

Por padrão, service **resetoutbound** está habilitado para todas as interfaces. Neste estudo de caso, não há nenhuma regra para permitir o tráfego de cliente para servidor.



Estas são as capturas configuradas no 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
```

O serviço resetoutbound está habilitado por padrão. Portanto, se a saída do show run service comando não exibir nada, isso significa que ele está habilitado:

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

1. O cliente envia TCP SYN ao servidor 10.10.20.250/17111 através do Firewall. Pacote número 1 nesta 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. Como não há ACL para permitir esse tráfego, o Firewall Seguro descarta esse pacote com acl-drop razão. Esse pacote é capturado na 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
```

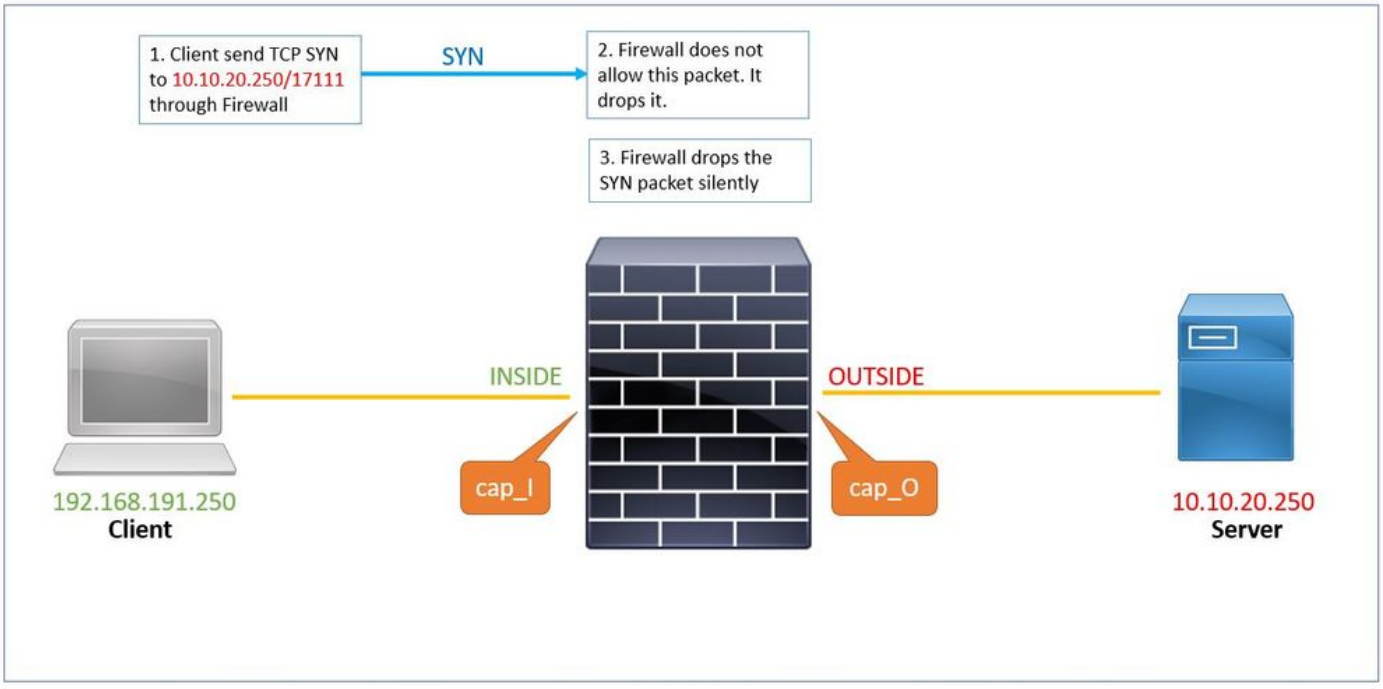
```
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. O firewall envia um pacote RST com o endereço ip do servidor como o endereço ip de origem. Pacote número 2 nesta 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
```

Estudo de caso 2: redefinição de serviço de saída não ativada e tráfego de cliente para servidor negado.

No Estudo de caso 2, não há nenhuma regra para permitir o tráfego de cliente para servidor e o serviço **resetoutbound** está desabilitado.



O comando show run service exibe que o serviço **resetoutbound** está desabilitado.

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

1. O cliente envia TCP ao servidor 10.10.20.250/17111 através do Firewall. Pacote número 1 nesta 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. Como não há ACL para permitir esse tráfego, o Firewall Seguro descarta esse pacote com acl-drop motivo. Esse pacote é capturado no **asp-drop capture**.

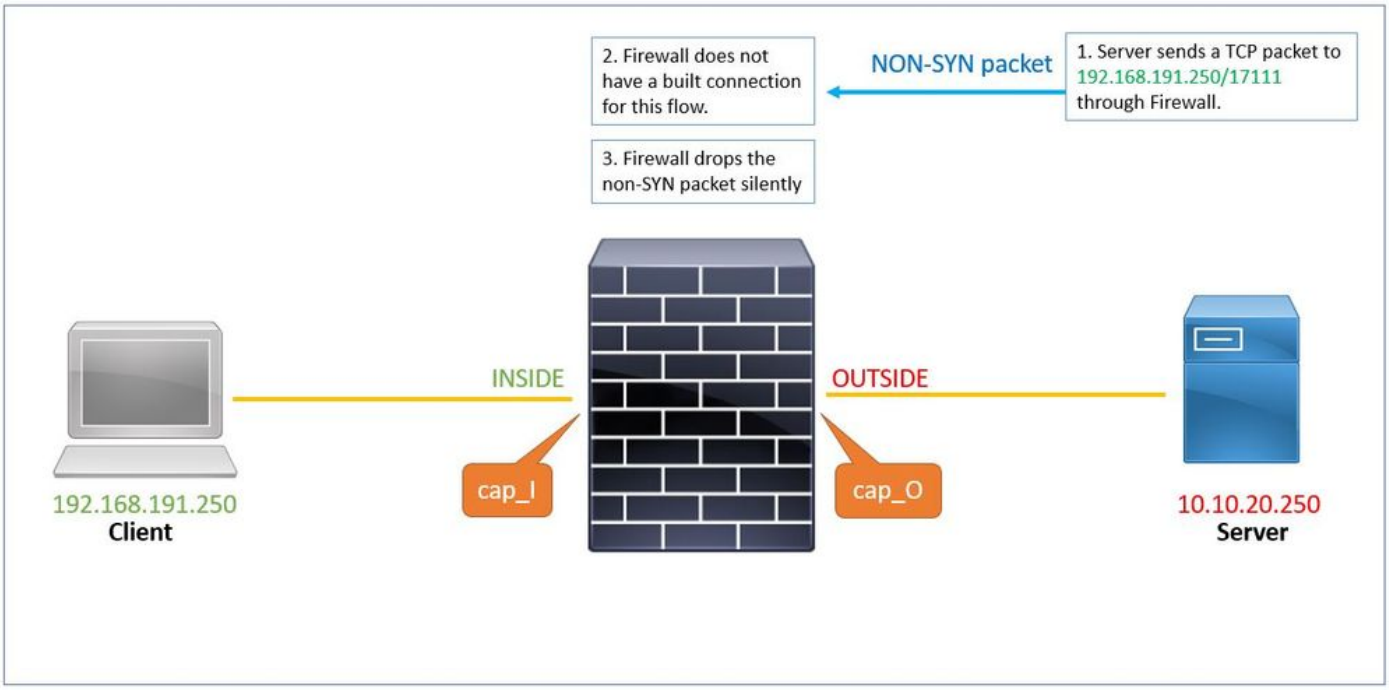
```
# show capture cap_I packet-number 1 trace det

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

3. O **asp-drop capture** mostra o pacote SYN, mas não há nenhum pacote RST enviado de volta cap_I capture via interface 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
```

Estudo de caso 3: Redefinição de serviço de saída desabilitada (por padrão) Redefinição de serviço desabilitada (por padrão)

Por padrão, o serviço **resetoutbound** está habilitado para todas as interfaces e o serviço resetoutbound está desabilitado.



1. O servidor envia um pacote TCP (SYN/ACK) ao cliente através do firewall. O firewall não tem uma conexão interna para esse fluxo.

```
# 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
```

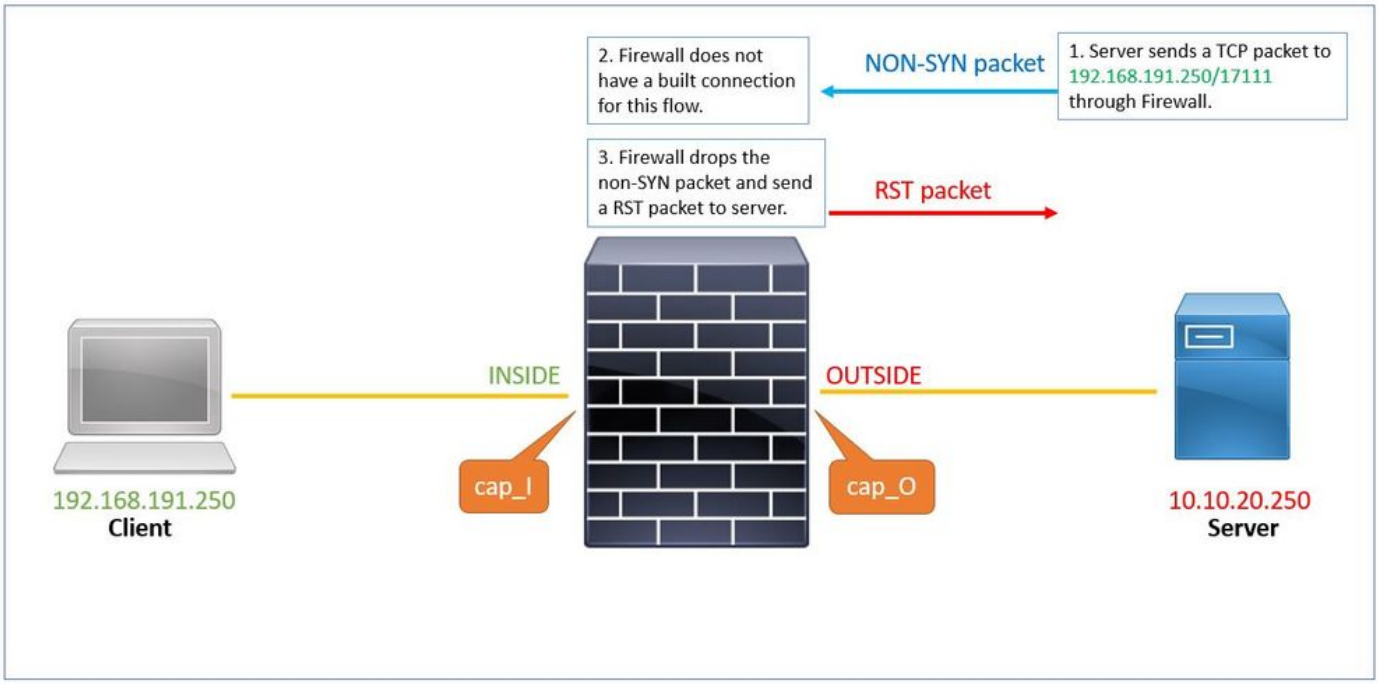
2. A redefinição não é enviada do Firewall para o servidor. Esse pacote SYN/ACK é descartado silenciosamente com razãotcp-not-syn. Ele é capturado asp-drop capture também.

```
# 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
```

Estudo de caso 4: Service resetoutbound disabled (por padrão) service resetoutbound disabled.

Por padrão, o serviço **resetoutbound** está desabilitado para todas as interfaces e o serviço **resetoutbound** também está desabilitado com o comando configuration.



A saída do show run service comando exibe que o serviço **resetoutbound** está desabilitado (por padrão) e o serviço **resetinbound** está desabilitado pelo comando de configuração.

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

1. O servidor envia um pacote TCP (SYN/ACK) ao cliente através do 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. O firewall não tem uma conexão integrada para esse fluxo e o descarta. O asp-drop captures mostra o pacote:

```
# show capture cap_O packet-number 1 trace detail
1: 00:32:26.434395 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)/
```

3. Desde a **reinicialização do** serviço, o firewall envia um pacote RST ao Servidor com o endereço ip de origem do cliente.

```
# show capture cap_O
1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
2: 00:32:26.434608 192.168.191.250.46118 > 10.10.20.250.17111: R 3490277959:3490277959(0) ack 347502458
```

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.