Comprendre les paquets RST envoyés par Cisco Secure Firewall

Table des matières

Introduction

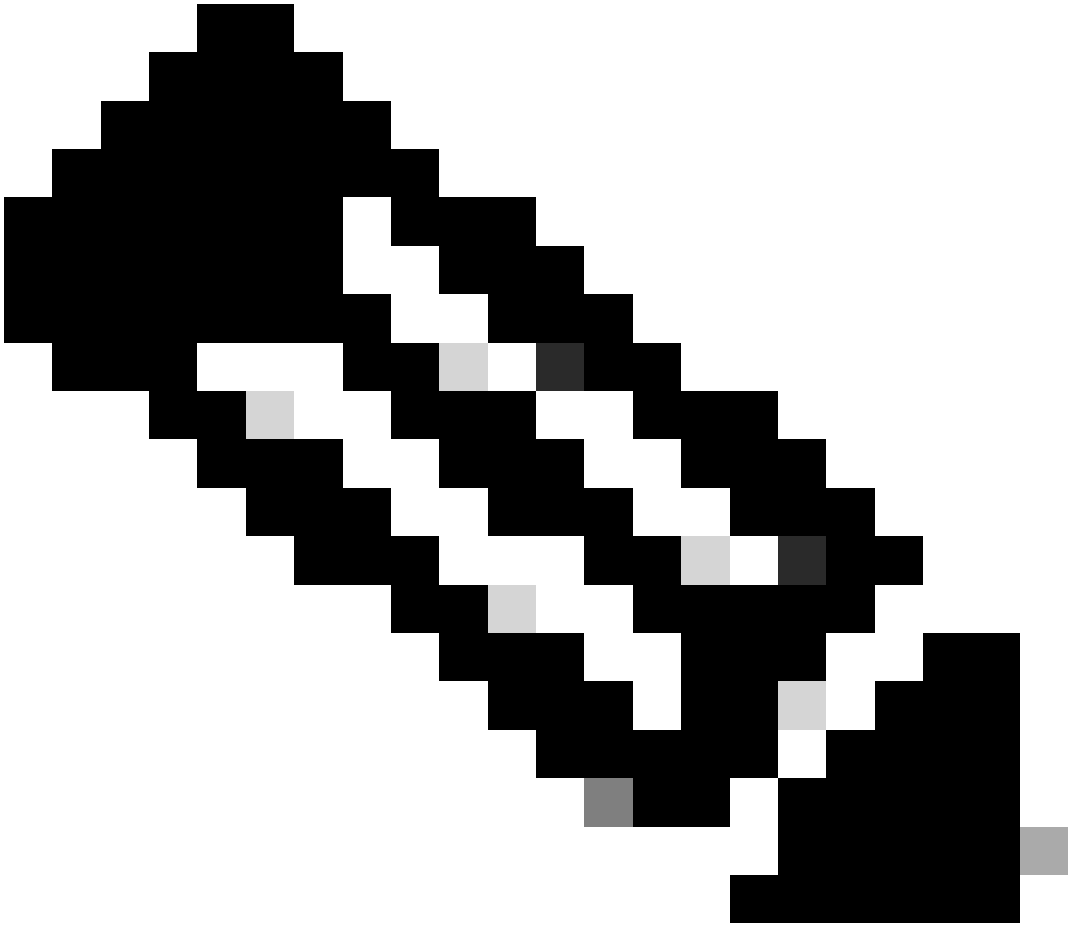
Le présent document décrit le comportement d'un pare-feu de Cisco lorsque des réinitialisations TCP sont envoyées pour les sessions TCP qui tentent de passer par le pare-feu.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Flux de paquets ASA
- Flux de paquets FTD
- Captures de paquets ASA/FTD



Remarque : ce comportement décrit s'applique à ASA et à Secure Firewall Threat Defense.

Composants utilisés

Les informations contenues dans ce document sont basées sur ce logiciel :

- ASA
- Protection pare-feu FTD

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

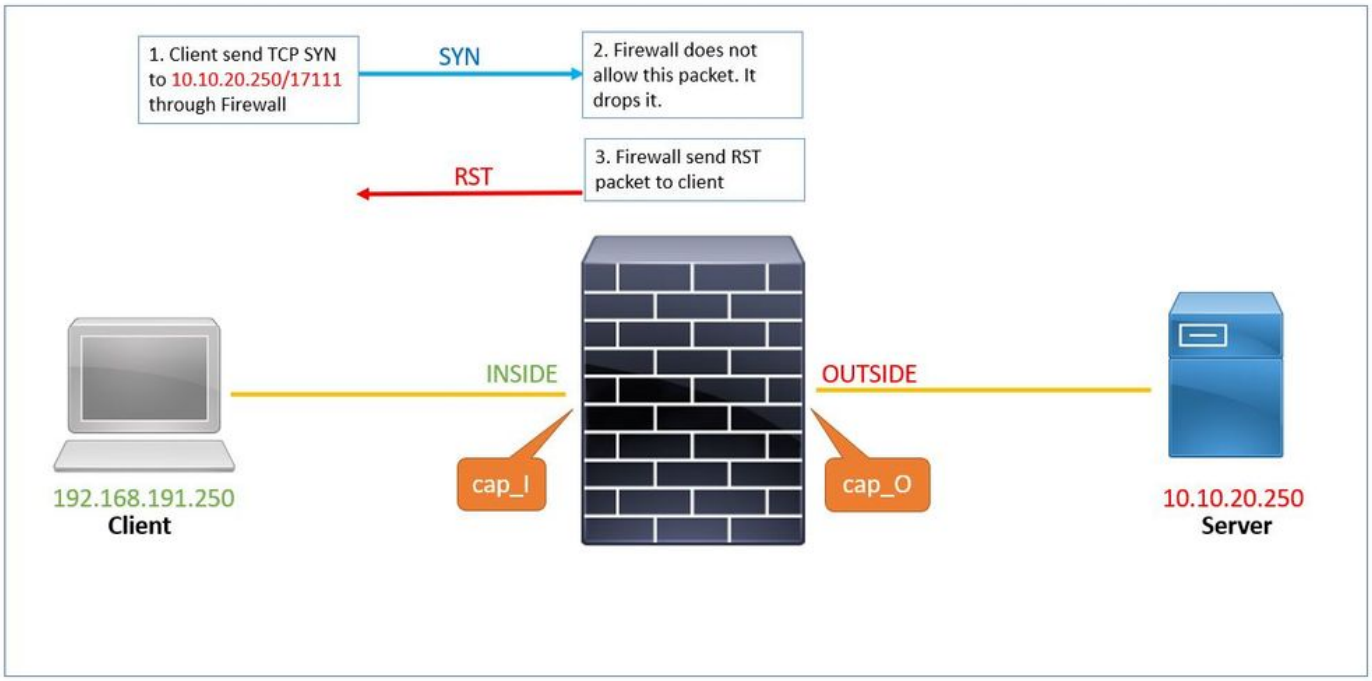
Dépannage

Le pare-feu envoie des réinitialisations TCP pour les sessions TCP qui tentent de transiter par le

pare-feu et qui sont refusées par le pare-feu en fonction des listes d'accès. Le pare-feu envoie également des réinitialisations pour les paquets qui sont autorisés par une liste d'accès, mais qui n'appartiennent pas à une connexion qui existe dans le pare-feu et qui est donc refusée par la fonctionnalité avec état.

Étude de cas 1 : le service resetoutbound est activé et le trafic client-serveur est refusé.

Par défaut, le service **resetoutbound** est activé pour toutes les interfaces. Dans cette étude de cas, il n'existe aucune règle autorisant le trafic client-serveur.



Voici les captures configurées dans le pare-feu :

```
# 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
```

La réinitialisation sortante du service est activée par défaut. Par conséquent, si la sortie de la show run service commande n'affiche rien, cela signifie qu'elle est activée :

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

1. Le client envoie TCP SYN au serveur 10.10.20.250/17111 via le pare-feu. Paquet numéro 1 dans cette capture :

```
# 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. Puisqu'il n'y a pas de liste de contrôle d'accès pour autoriser ce trafic, le pare-feu sécurisé abandonne ce paquet avec acl-drop raison. Ce paquet est capturé dans la capture 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
```

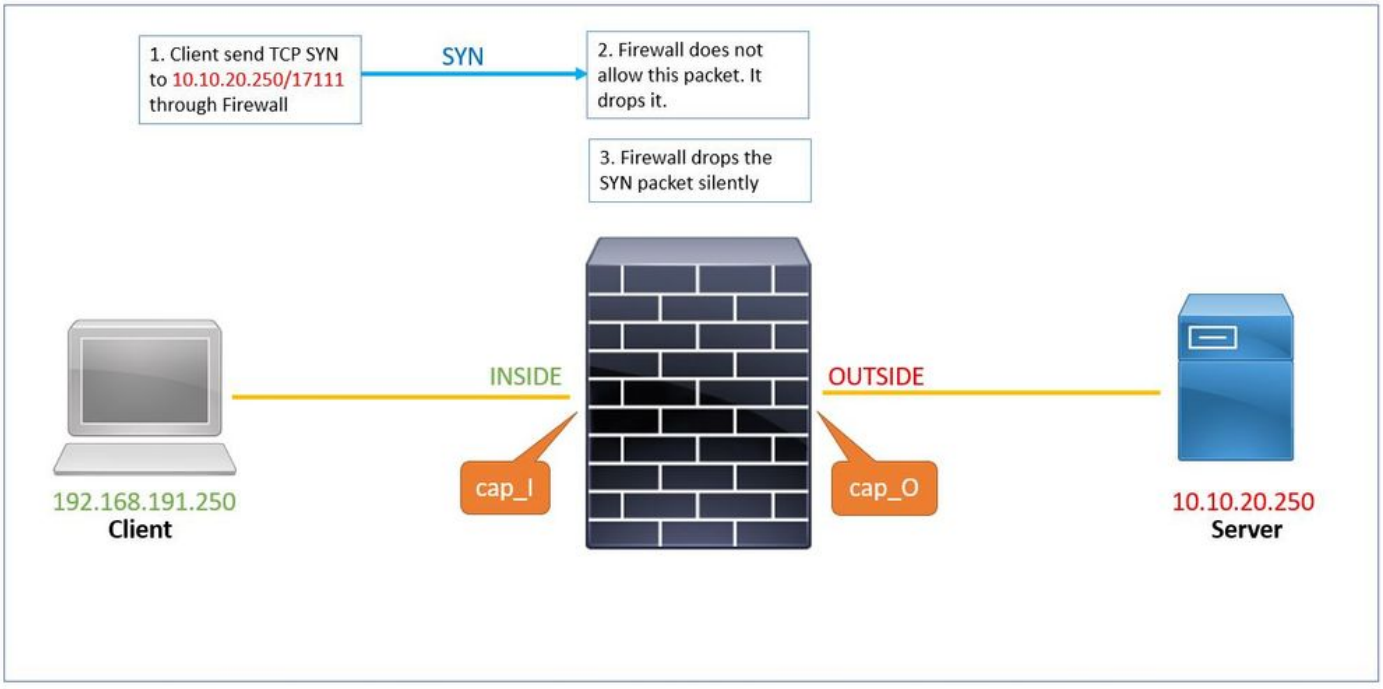
```
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. Le pare-feu envoie un paquet RST avec l'adresse IP du serveur comme adresse IP source. Paquet numéro 2 dans cette capture :

```
# 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
```

Étude de cas 2 : réinitialisation du service en sortie non activée et refus du trafic client-serveur.

Dans l'étude de cas 2, il n'existe aucune règle autorisant le trafic client-serveur et le service **resetoutbound** est désactivé.



La commandeshow run service affiche que le service **resetoutbound** est désactivé.

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

1. Le client envoie TCP TCP au serveur 10.10.20.250/17111 via le pare-feu. Paquet numéro 1 dans cette capture :

```
# 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. Puisqu'il n'y a pas de liste de contrôle d'accès pour autoriser ce trafic, le pare-feu sécurisé abandonne ce paquet avec acl-drop raison. Ce paquet est capturé dans le **asp-drop capture**.

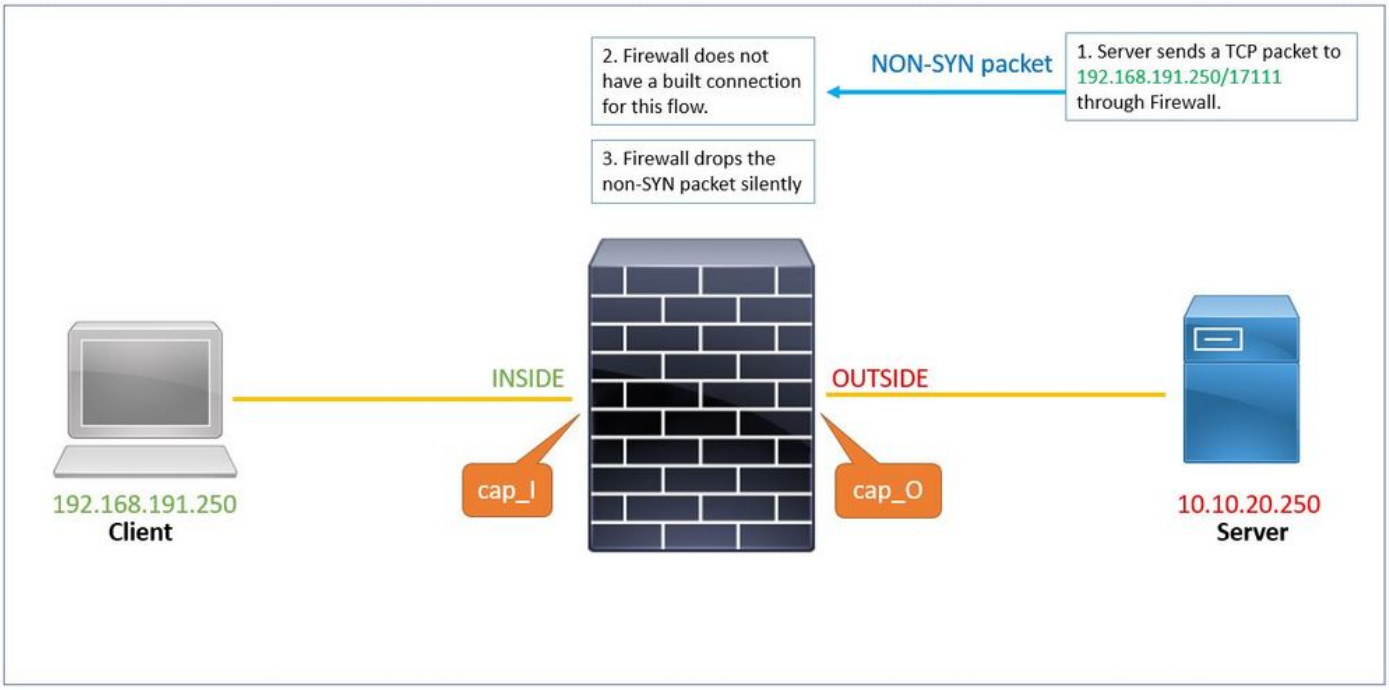
```
# show capture cap_I packet-number 1 trace det

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** montre le paquet SYN, mais aucun paquet RST n'est renvoyé cap_I capture via l'interface interne :

```
# 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
```

Étude de cas 3 : Service resetoutbound disabled (par défaut) service resetinbound disabled (par défaut)

Par défaut, le service **resetoutbound** est activé pour toutes les interfaces et le service **resetoutbound** est désactivé.



1. Le serveur envoie un paquet TCP (SYN/ACK) au client via le pare-feu. Le pare-feu n'a pas de connexion intégrée pour ce flux.

```
# 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
```

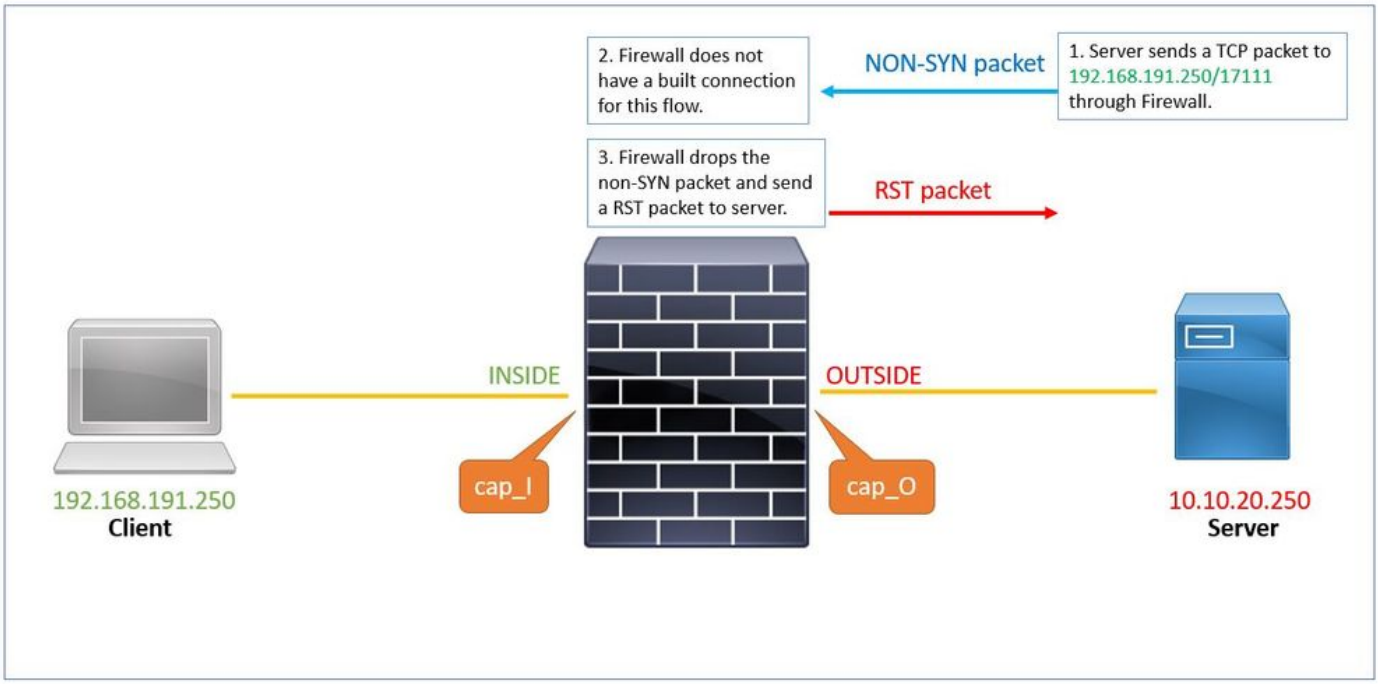
2. La réinitialisation n'est pas envoyée du pare-feu au serveur. Ce paquet SYN/ACK est abandonné en silence avec la raison tcp-not-syn. Il est également capturé asp-drop capture dans.

```
# 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
```

Étude de cas 4 : Service resetoutbound disabled (par défaut) service resetinbound disabled.

Par défaut, le service **resetoutbound** est désactivé pour toutes les interfaces et le service **resetoutbound** est également désactivé avec la commande de configuration.



Le résultat de cette show run service commande indique que le service **resetoutbound** est désactivé (par défaut) et que le service **resetinbound** est désactivé par la commande de configuration.

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

1. Le serveur envoie un paquet TCP (SYN/ACK) au client via le pare-feu.

```
# 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. Le pare-feu n'a pas de connexion intégrée pour ce flux et le supprime. La asp-drop captures affiche le paquet :

```
# 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. Depuis la **réinitialisation du** service, le pare-feu envoie un paquet RST au serveur avec l'adresse IP source du client.

```
# 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
```

Informations connexes

- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.