Dépannage du proxy sur Cisco Secure Firewall Management Center (FMC)

Table des matières

Introduction

Ce document décrit la configuration d'un proxy sur FMC pour permettre aux utilisateurs de se connecter à Internet via un serveur intermédiaire, améliorant ainsi la sécurité et parfois les performances. Cet article vous guide tout au long des étapes de configuration d'un proxy sur FMC et fournit des conseils de dépannage pour les problèmes courants.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Proxy

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMC 7.4.x

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.

Configuration

Configurez le proxy http du réseau sur l'interface utilisateur graphique FMC :

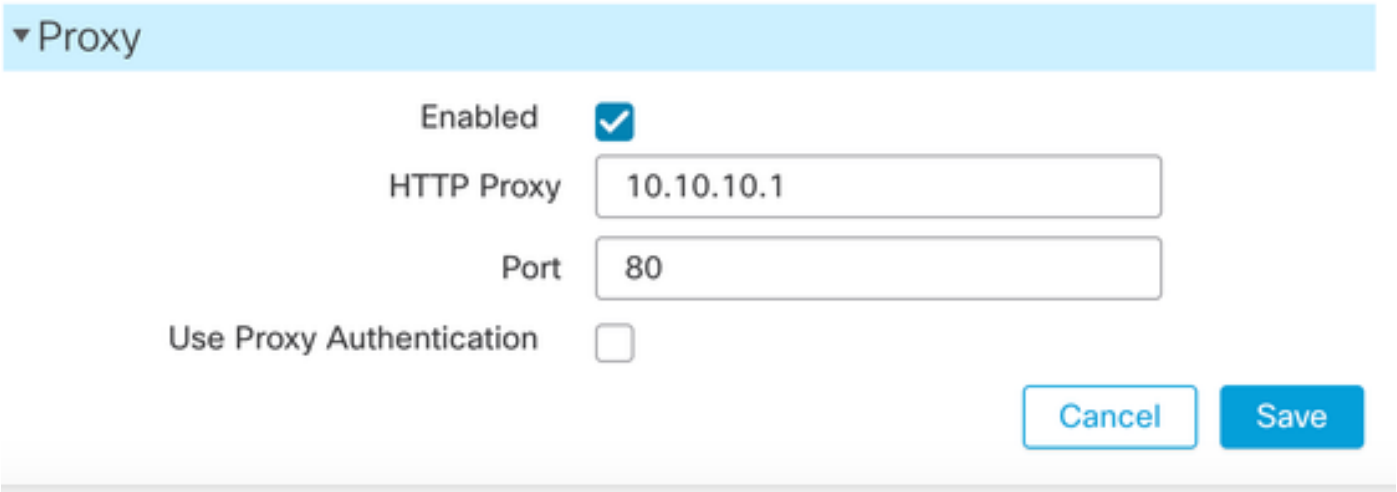
Connectez-vous à l'interface utilisateur graphique de FMC > Choisissez System > Configuration, puis sélectionnez Management Interfaces.

Remarque : Les proxys qui utilisent l'authentification NT LAN Manager (NTLM) ne sont pas pris en charge. Si vous utilisez Smart Licensing, le nom de domaine complet du proxy ne peut pas comporter plus de 64 caractères.

Dans la zone Proxy, configurez les paramètres du proxy HTTP.

Le centre de gestion est configuré pour se connecter directement à Internet sur les ports TCP/443 (HTTPS) et TCP/80 (HTTP). Vous pouvez utiliser un serveur proxy auquel vous pouvez vous authentifier via HTTP Digest.

- Cochez la case Activé.
- Dans le champ Proxy HTTP, saisissez l'adresse IP ou le nom de domaine complet de votre serveur proxy.
- Dans le champ Port, saisissez un numéro de port.
- Fournissez les informations d'authentification en choisissant Utiliser l'authentification proxy, puis fournissez un nom d'utilisateur et un mot de passe.
- Cliquez sur Save.



Remarque: Pour le mot de passe proxy, vous pouvez utiliser les caractères spéciaux A-Z, a-z et 0-9.

Dépannage

Accédez à l'ILC FMC et au mode expert, puis vérifiez iprep_proxy.conf pour vous assurer que les paramètres de proxy sont corrects :

```
<#root>

admin@fmc:~$

cat /etc/sf/iprep_proxy.conf


iprep_proxy {
PROXY_HOST 10.10.10.1;
PROXY_PORT 80;
}
```

Vérifiez les connexions actives pour vérifier la connexion proxy active :

```
<#root>

admin@fmc:~$

netstat -na | grep 10.10.10.1


tcp 0 0 10.40.40.1:40220 10.10.10.1:80

ESTABLISHED
```

À l'aide de la commande curl, vérifiez à la fois les détails de la requête et la réponse du proxy. Si vous recevez la réponse : HTTP/1.1 200 Connection established, cela indique que le FMC envoie et reçoit correctement le trafic via le proxy.

<#root>

admin@fmc:~$

curl -x http://10.10.10.1:80 -I https://tools.cisco.com

HTTP/1.1 200 Connection established

Si vous avez configuré le nom d'utilisateur et le mot de passe du proxy, vérifiez l'authentification et la réponse du proxy :

```
curl -u proxyuser:proxypass --proxy http://proxy.example.com:80 https://example.com
```

Vérification

Établissement de connexion réussi via le proxy

Lors de l'exécution d'une commande curl avec un proxy, telle que curl -x http://proxy:80 -I https://tools.cisco.com, une série d'interactions réseau attendues se produisent, qui peuvent être observées via la capture de paquets (tcpdump). Ceci est une vue d'ensemble de haut niveau du processus, enrichie de sorties tcpdump réelles :

Initiation de la connexion TCP :
Le client (FMC) initie une connexion TCP au serveur proxy sur le port 80 en envoyant un paquet SYN. Le proxy répond avec un SYN-ACK et le client termine la connexion avec un ACK. Ceci établit la session TCP sur laquelle la communication HTTP se poursuit.

Exemple de sortie tcpdump :

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Requête HTTP CONNECT :
Une fois la connexion TCP établie, le client envoie une requête HTTP CONNECT au proxy, lui

demandant de créer un tunnel vers le serveur HTTPS cible (tools.cisco.com:443). Cette demande permet au client de négocier une session TLS de bout en bout via le proxy.

Exemple de tcpdump (HTTP décodé) :

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Accusé de réception d'établissement de connexion :
Le proxy répond avec une réponse HTTP/1.1 200 Connection established, indiquant que le tunnel vers le serveur cible a été créé avec succès. Cela signifie que le proxy agit désormais comme un relais, en transférant le trafic chiffré entre le client et tools.cisco.com.

Exemple de tcpdump :

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

Communication HTTPS via le tunnel :
À la suite de la réponse CONNECT, le client initie la connexion SSL/TLS directement avec tools.cisco.com sur le tunnel établi. Puisque ce trafic est chiffré, le contenu n'est pas visible dans le tcpdump, mais les longueurs de paquets et les minutages sont observables, y compris les paquets Hello du client TLS et Hello du serveur.

Exemple de tcpdump :

```
10:20:59.123456 IP client.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > client.54321: Flags [P.], length 1514 (Server Hello)
```

Gestion de la redirection HTTP (302 trouvé) :
Dans le cadre de la communication HTTPS, le client demande la ressource à partir de tools.cisco.com. Le serveur répond avec une redirection HTTP/1.1 302 Found vers une autre URL (https://tools.cisco.com/healthcheck), que le client peut suivre en fonction des paramètres de

boucle et du but de la requête. Bien que cette redirection se produise au sein de la session TLS chiffrée et ne soit pas directement visible, il s'agit d'un comportement normal qui peut être observé si le trafic TLS est déchiffré.

Le trafic de redirection chiffré se présente comme suit :

```
10:21:00.123000 IP client.54321 > proxy.80: Flags [P.], length 517 (Encrypted Application Data)
10:21:00.123045 IP proxy.80 > client.54321: Flags [P.], length 317 (Encrypted Application Data)
```

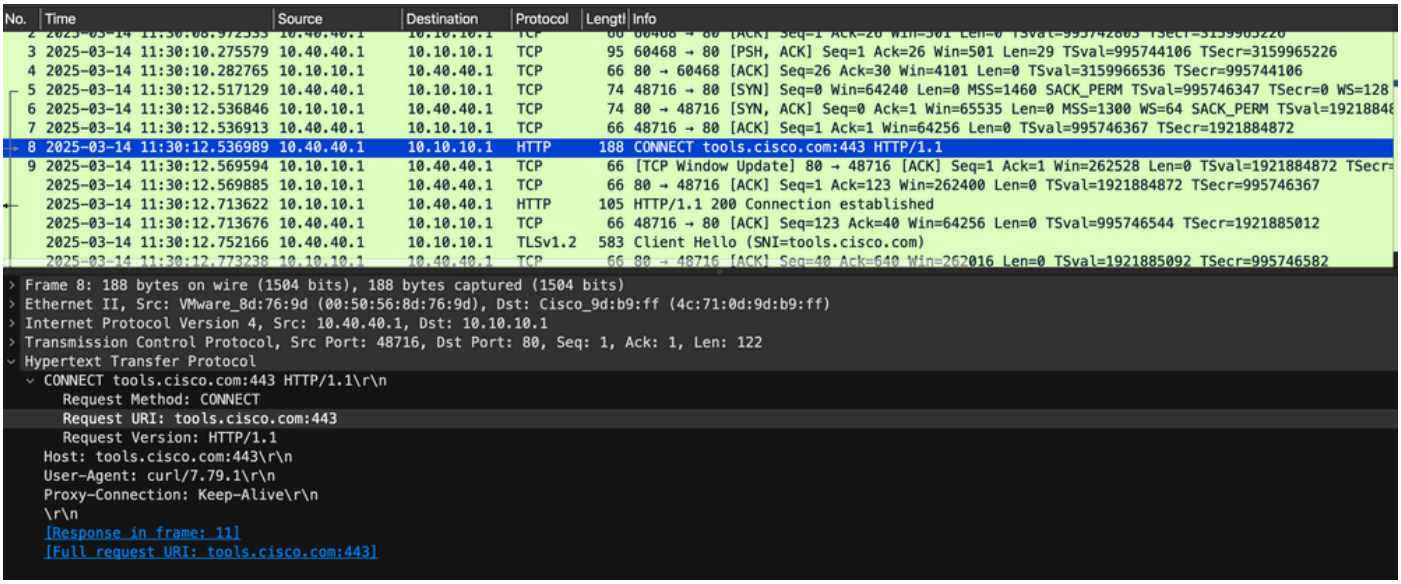
Déconnexion de la connexion :
Une fois l'échange terminé, le client et le proxy ferment gracieusement la connexion TCP en échangeant des paquets FIN et ACK, ce qui garantit la fermeture correcte de la session.

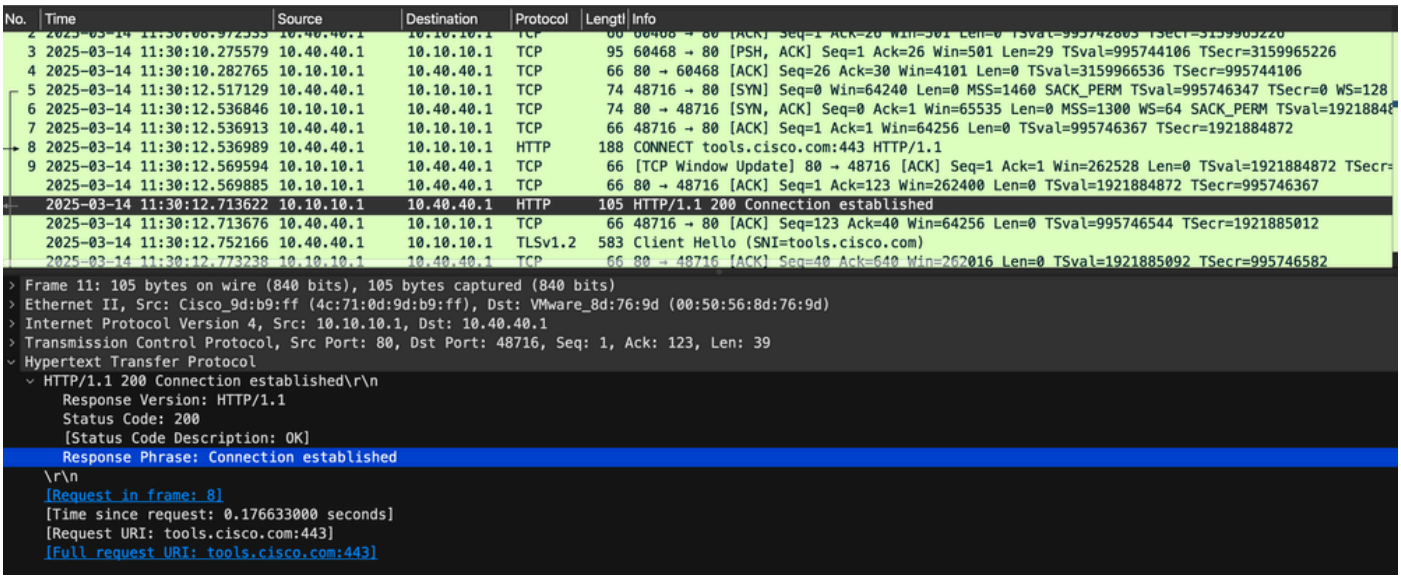
Exemple de sortie tcpdump :

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

Conseil : En analysant le résultat de tcpdump, vous pouvez vérifier que la requête HTTPS via le proxy explicite suit le flux attendu : Connexion TCP, requête CONNECT, établissement de tunnel, connexion TLS, communication chiffrée (y compris les redirections possibles) et fermeture progressive de la connexion. Cela confirme que l'interaction proxy/client fonctionne correctement et permet d'identifier les problèmes dans le flux, tels que les échecs de tunneling ou de négociation SSL.

Le FMC (10.40.40.1) établit une connexion TCP réussie avec le proxy (10.10.10.1) sur le port 80, suivie d'une connexion HTTP au serveur (72.163.4.161) sur le port 443. Le serveur répond avec un message HTTP 200 Connection established. La connexion TLS se termine et les données circulent correctement. Enfin, la connexion TCP se termine en douceur (FIN).





Problèmes identifiés

Restrictions ACL proxy

En cas de problème d'autorisation (comme une liste d'accès sur le proxy), vous pouvez observer cela via la capture de paquets (tcpdump). Ceci est une explication générale du scénario de défaillance, avec des exemples de résultats tcpdump :

Initiation de la connexion TCP :
Le client (Firepower) commence par établir une connexion TCP au proxy sur le port 80. La connexion TCP (SYN, SYN-ACK, ACK) s'effectue correctement, ce qui signifie que le proxy est accessible.

Exemple de sortie tcpdump :

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Requête HTTP CONNECT :
Une fois connecté, le client envoie une requête HTTP CONNECT au proxy, lui demandant de créer un tunnel vers tools.cisco.com:443.

Exemple de tcpdump (HTTP décodé) :

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Réponse d'erreur du proxy :

Au lieu d'autoriser le tunnel, le proxy refuse la demande, probablement en raison d'une liste de contrôle d'accès (ACL) qui n'autorise pas ce trafic. Le proxy répond avec une erreur du type 403 Forbidden ou 502 Bad Gateway.

Exemple de sortie tcpdump indiquant une erreur :

<#root>

```
HTTP/1.1
```

403

```
 Forbidden
Content-Type: text/html
Content-Length: 123
Connection: close
```

Déconnexion de la connexion :
Après l'envoi du message d'erreur, le proxy ferme la connexion et les deux côtés échangent des paquets FIN/ACK.

Exemple de sortie tcpdump :

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

Conseil : À partir de tcpdump, vous pouvez voir que bien que la connexion TCP et la requête HTTP CONNECT aient réussi, le proxy a refusé la configuration du tunnel. Cela indique généralement que le proxy dispose d'une liste de contrôle d'accès ou d'une restriction d'autorisation empêchant le trafic de passer.

Échec du téléchargement du proxy (délai d'attente/transfert incomplet)

Dans ce scénario, FMC se connecte avec succès au proxy et démarre le téléchargement du fichier, mais le transfert expire ou échoue. Cela est généralement dû à l'inspection du proxy, aux délais d'attente ou aux limites de taille de fichier sur le proxy.

Initiation de la connexion TCP
FMC initie une connexion TCP au proxy sur le port 80, et la connexion s'effectue correctement.
Exemple de sortie tcpdump :

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Requête HTTP CONNECT
FMC envoie une requête HTTP CONNECT au proxy pour atteindre la cible externe.
Exemple de tcpdump (HTTP décodé) :

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

Établissement de tunnel et échange TLS
Le proxy répond avec la connexion HTTP/1.1 200 établie, ce qui permet à la connexion TLS de commencer.

Exemple de sortie tcpdump :

<#root>

```
HTTP/1.1
```

```
200

 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Délai d'attente ou téléchargement incomplet
Après le lancement du transfert de fichiers, le téléchargement est bloqué ou ne se termine pas, ce qui entraîne un délai d'attente. La connexion reste inactive.
Raisons possibles :

- Délais d'inspection ou filtrage du proxy.
- Délais d'expiration proxy pour les transferts longs.
- Limites de taille de fichier imposées par le proxy.

Exemple de tcpdump montrant l'inactivité :

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440

# FMC sending data


# No response from proxy, connection goes idle...


# After a while, FMC may close the connection or retry.
```


Conseil : FMC lance le téléchargement mais ne parvient pas à se terminer en raison de délais d'attente ou de transferts incomplets, souvent provoqués par le filtrage par proxy ou des restrictions de taille de fichier.

Échec du téléchargement du fichier proxy (problème MTU)

Dans ce cas, FMC se connecte au proxy et commence à télécharger des fichiers, mais la session échoue en raison de problèmes de MTU. Ces problèmes entraînent la fragmentation ou l'abandon de paquets, en particulier avec des fichiers volumineux ou des échanges SSL/TLS.

Initiation de la connexion TCP
FMC initie une connexion TCP avec le proxy, ce qui réussit.
Exemple de sortie tcpdump :

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Requête HTTP CONNECT et établissement du tunnel
FMC envoie une requête HTTP CONNECT, et le proxy répond, ce qui permet d'établir le tunnel.
Exemple de tcpdump (HTTP décodé) :

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

Début de la connexion TLS
FMC et tools.cisco.com commencent à négocier SSL/TLS, et les paquets initiaux sont échangés.
Exemple de sortie tcpdump :

<#root>

```
HTTP/1.1
```

200

```
 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Fragmentation ou abandon de paquets en raison de MTU
Lorsque FMC ou le serveur tente d'envoyer des paquets volumineux, les problèmes de MTU entraînent la fragmentation ou l'abandon des paquets, ce qui entraîne des échecs de transfert de fichiers ou de négociation TLS.
Cela se produit généralement lorsque le MTU entre FMC et le proxy (ou entre le proxy et Internet) est mal défini ou trop petit.
Exemple de tcpdump montrant une tentative de fragmentation :

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440
```

 # Large packet

```
10:21:00.456123 IP proxy.80 > fmc.54321: Flags [R], seq X, win 0, length 0
```

```
# Proxy resets connection due to MTU issue
```

Conseil : Le problème de MTU entraîne l'abandon ou la fragmentation des paquets, ce qui perturbe la connexion TLS ou entraîne l'échec des téléchargements de fichiers. Cela se produit généralement lorsque l'inspection SSL ou la fragmentation de paquets se produit en raison de paramètres MTU incorrects.

Dans un scénario d'échec, FMC obtient CONNECT sans HTTP 200, avec des retransmissions et des FIN confirmant l'absence d'échange TLS/données, peut-être en raison de problèmes de MTU ou d'un problème de proxy/amont.

Lorsque vous utilisez curl, vous pouvez rencontrer divers codes de réponse HTTP indiquant des problèmes côté serveur ou des erreurs d'authentification. Voici une liste des codes d'erreur les plus courants et de leur signification :

Code HTTP	Signification	Motif
400	Requête incorrecte	Syntaxe de demande incorrecte
401	Non Autorisé	Identifiants manquants ou incorrects
403	Interdit	Accès refusé
404	Non trouvé	Ressource introuvable
500	Internal Error	Erreur du serveur
502	Passerelle incorrecte	Mauvaise communication du serveur
503	Service non disponible	Surcharge ou maintenance du serveur
504	Délai de passerelle	Délai entre les serveurs

Références

Notes de version de Cisco Secure Firewall Threat Defense, version 7.4.x

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.