Configuration du service de gestion prêt à l'emploi FDM pour Secure Firewall 2100

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Diagramme du réseau
- Configurations

Vérifier

Informations connexes

Introduction

Ce document décrit comment configurer le service de gestion intégrée FDM (Secure Firewall Device Management) pour la gamme Secure Firewall 2100 avec FTD installé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall 2100, installation du logiciel FTD
- Configuration et dépannage de base de Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

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

- Cisco Secure Firewall série 2100
- Cisco FTD version 6.2.3

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.

Informations générales

L'objectif principal de ce document est de vous guider tout au long des étapes nécessaires à l'activation de la gestion FDM On-Box pour la gamme Secure Firewall 2100.

Vous avez deux options pour gérer le Secure Firewall Threat Defense (FTD) installé sur un pare-feu sécurisé de la gamme 2100 :

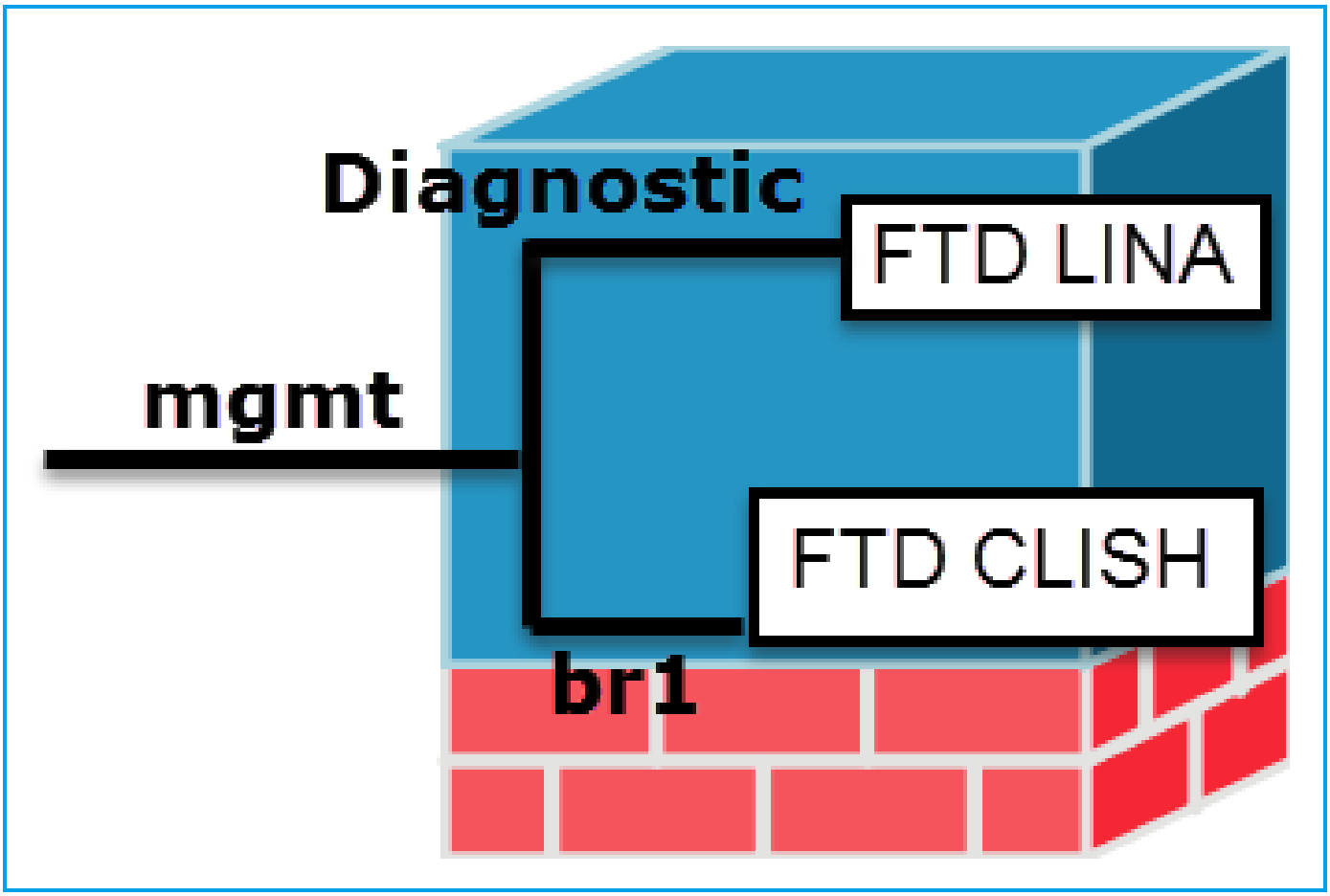
- La gestion intégrée FDM (Secure Firewall Device Management)
- Centre de gestion des pare-feu sécurisés de Cisco

Remarque : Un FTD installé sur un Secure Firewall 2100 ne peut pas être géré simultanément par FDM et FMC. L'activation de la gestion FDM « On-Box » sur le Secure Firewall 2100 FTD empêche la gestion via FMC, sauf si la gestion locale est désactivée et reconfigurée pour FMC. Inversement, l'enregistrement du FTD sur un FMC désactive automatiquement le service de gestion FDM On-Box sur le périphérique.

Utilisez l'outil de migration de pare-feu sécurisé (FMT) pour migrer en toute transparence la configuration d'un périphérique géré localement à l'aide de FDM vers un périphérique géré par le FMC, comme détaillé dans la Migration d'un périphérique géré par FDM vers Cisco Secure Firewall Threat Defense avec l'outil de migration

---

L'interface de gestion est divisée en 2 interfaces logiques, br1 (management0 sur les appliances 2100/4100/9300) et diagnostic :



	Gestion - br1/management0	Gestion - Diagnostic
Objectif	• Cette interface est utilisée afin d'attribuer l'IP FTD qui est utilisé pour la communication FTD/FMC. • Termine le sftunnel entre FMC/FTD. • Utilisé comme source pour les syslogs basés sur des règles. • Fournit un accès SSH et HTTPS au boîtier FTD.	• Fournit un accès à distance (par exemple, SNMP) au moteur ASA. • Utilisé comme source pour les messages syslog de niveau LINA, AAA, SNMP, etc.
Obligatoire	Oui, puisqu'il est utilisé pour la communication FTD/FMC (le sftunnel s'arrête dessus).	Non, et il n'est pas recommandé de le configurer. Il est recommandé d'utiliser une interface de données à la place (consultez la remarque ci-dessous).

Remarque : l'avantage de laisser l'adresse IP hors de l'interface de diagnostic est que vous pouvez placer l'interface de gestion sur le même réseau que n'importe quelle autre interface de données. Si vous configurez l'interface de diagnostic, son adresse IP doit se trouver sur le même réseau que l'adresse IP de gestion et elle compte comme une interface normale qui ne peut pas se trouver sur le même réseau que les autres interfaces de données. Étant

donné que l'interface de gestion nécessite un accès Internet pour les mises à jour, placer l'interface de gestion sur le même réseau qu'une interface FTD interne signifie que vous pouvez déployer la FTD avec seulement un commutateur sur le LAN et pointer l'interface interne comme passerelle par défaut pour l'interface de gestion (Ceci s'applique uniquement lorsque la FTD est déployée en mode routé).

Le FTD peut être installé dans un pare-feu sécurisé 2100. Le châssis exécute son propre système d'exploitation appelé Secure Firewall eXtensible Operating System (FXOS) pour contrôler les opérations de base du périphérique, tandis que le périphérique logique FTD est installé sur un module/lame.

Remarque : Vous pouvez utiliser l'interface graphique utilisateur (GUI) de FXOS appelée Secure Firewall Chassis Manager (FCM) ou l'interface de ligne de commande (CLI) de FXOS pour configurer les fonctions fchassis ; Cependant, le FCM de l'interface graphique n'est pas disponible lorsque le FTD est installé sur la gamme 2100, juste l'interface de ligne de commande FXOS.

Appliance Secure Firewall 21xx :

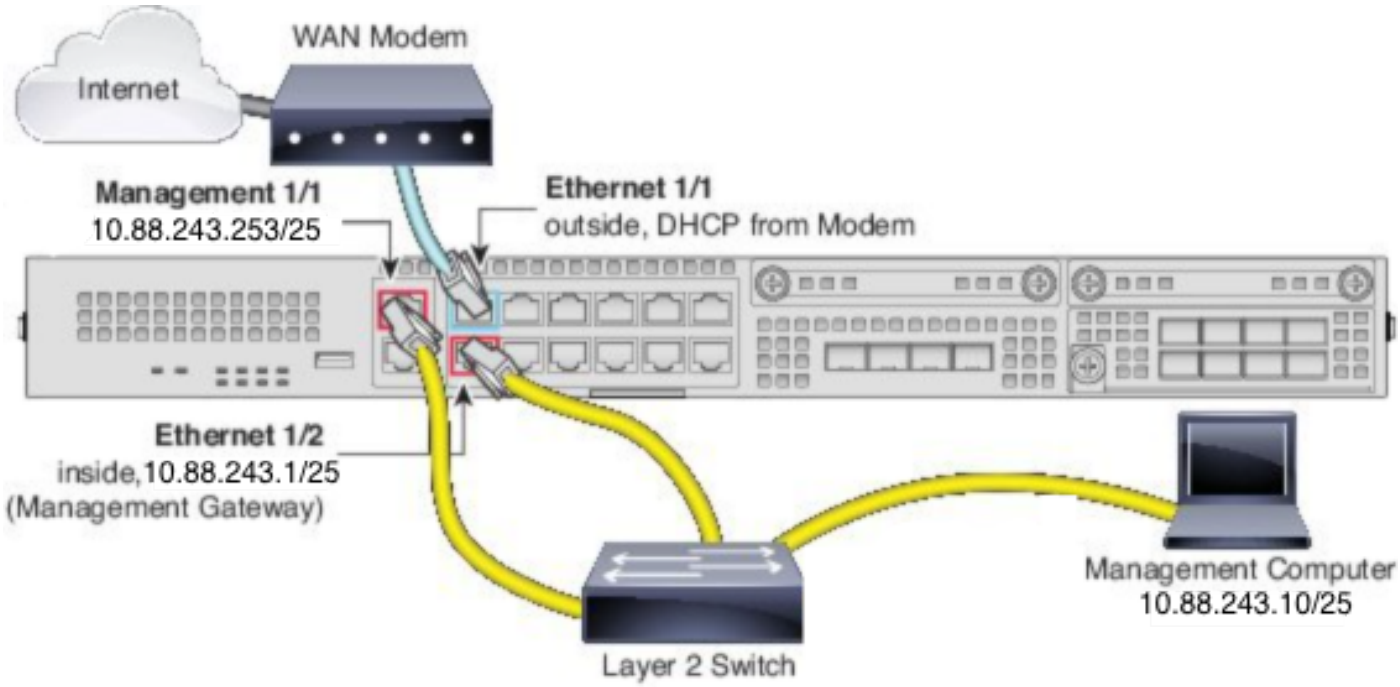


Remarque : sur le pare-feu sécurisé 2100, l'interface de gestion est partagée entre le châssis FXOS et le périphérique logique FTD.

Configurer

Diagramme du réseau

La configuration par défaut suppose que certaines interfaces de pare-feu sécurisé 2100 sont utilisées pour les réseaux intérieurs et extérieurs. La configuration initiale est plus facile à réaliser si vous connectez des câbles réseau aux interfaces en fonction de ces attentes. Pour câbler le pare-feu sécurisé 2100, reportez-vous à l'image suivante.



Remarque : l'image présente une topologie simple qui utilise un commutateur de couche 2. D'autres topologies peuvent être utilisées et votre déploiement peut varier en fonction de vos besoins de base en matière de connectivité réseau logique, de ports, d'adressage et de configuration.

Configurations

Afin d'activer la gestion FDM On-Box sur le pare-feu sécurisé de la gamme 2100 procédez comme suit.

1. Accédez au châssis 2100 via la console et connectez-vous à l'application FTD.

```
firepower# connect ftd
>
```

2. Configurez l'adresse IP de gestion FTD.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

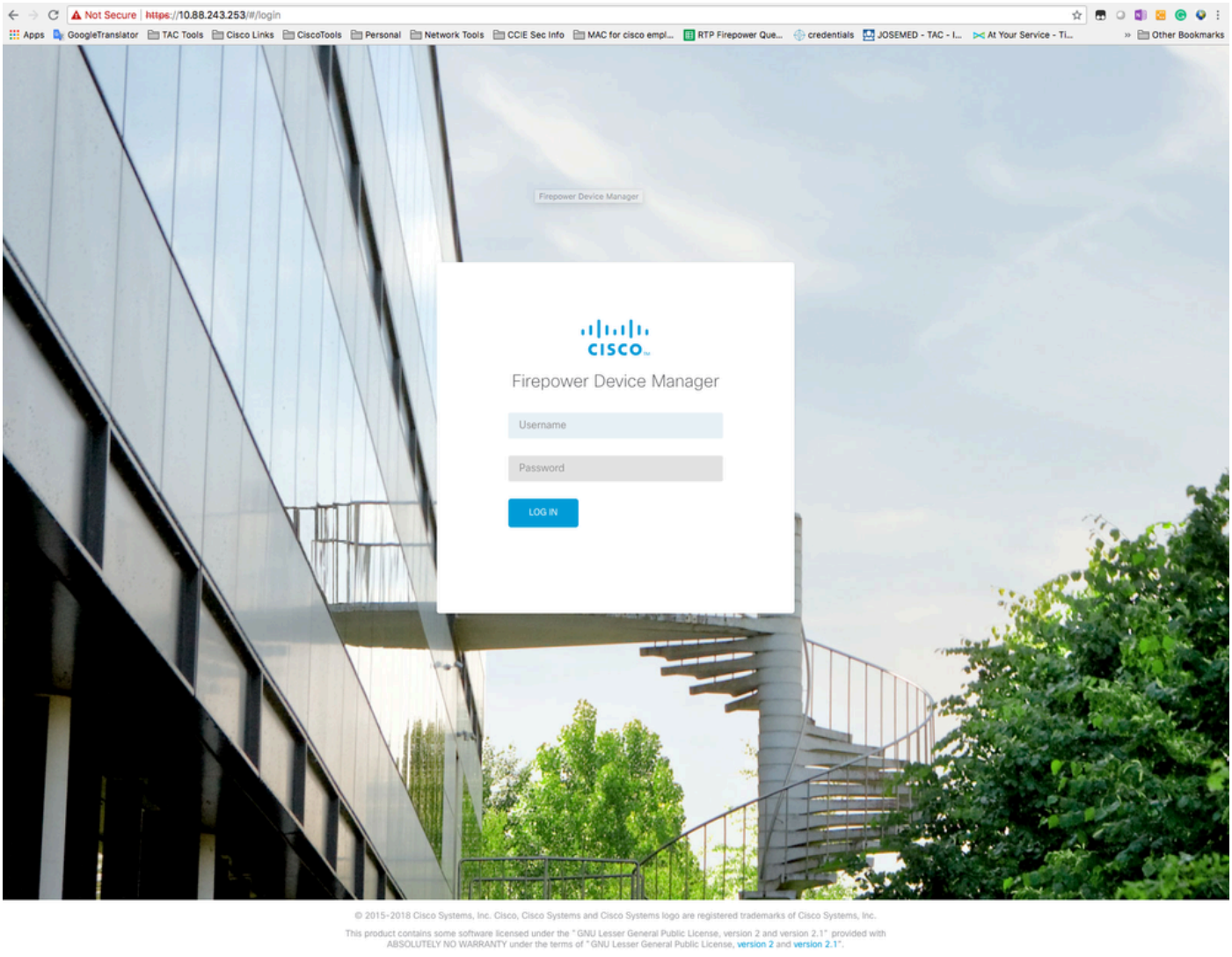
3. Configurez le type de gestion comme local.

```
>configure manager local
```

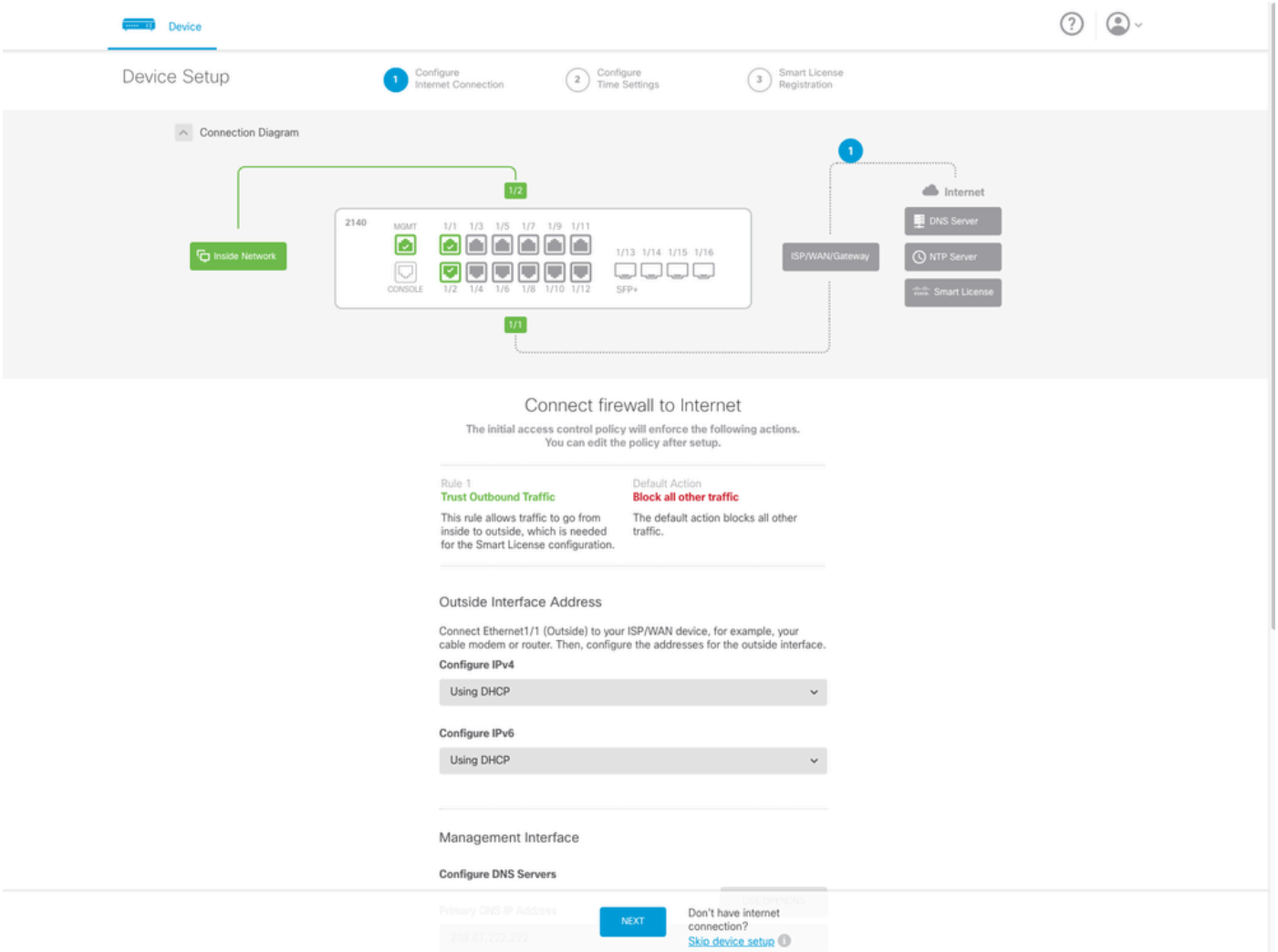
4. Configurez à partir de quelles adresses IP/sous-réseaux l’accès de gestion On-Box au FTD peut être autorisé.

```
>configure https-access-list 0.0.0.0/0
```

5. Ouvrez un navigateur et https dans l'adresse IP que vous avez configurée pour gérer le FTD. Cela peut ouvrir le gestionnaire FDM (On-Box).



6. Connectez-vous et utilisez les informations d'identification par défaut du pare-feu sécurisé, le nom d'utilisateur admin et le mot de passe Admin123.



Vérifier

1. Vérifiez les paramètres réseau que vous avez configurés pour le FTD avec la commande suivante.

```
> show network
===============[ System Information ]===============
Hostname                : firepower
DNS Servers             : 10.67.222.222
                          10.67.220.220
Management port         : 8305
IPv4 Default route
  Gateway               : 10.88.243.129

==================[ management0 ]===================
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:2C:C8:41:09:80
----------------------[ IPv4 ]----------------------
Configuration           : Manual
Address                 : 10.88.243.253
```

```
Netmask                   : 255.255.255.128
Broadcast                 : 10.88.243.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

2. Vérifiez le type de gestion que vous avez configuré pour le FTD avec la commande suivante.

```
> show managers
Managed locally.
```

Informations connexes

- Gestionnaire de périphériques Cisco Secure Firewall
- Guide de démarrage rapide de Cisco Secure Firewall Threat Defense pour la gamme 2100 à l'aide de Secure Firewall Management Center
- Configuration de l'interface de gestion Secure Firewall Threat Defense (FTD)
- Réinstallez la gamme Secure Firewall 2100.
- Migration d'un périphérique géré par FDM vers Cisco Secure Firewall Threat Defense avec l'outil de migration

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.