Pourquoi les entrées xlate de l'ASA ont-elles des valeurs d'inactivité plus longues que les délais d'attente configurés ?

Table des matières

[Introduction](#)
[Pourquoi les entrées xlate de l'appliance ASA (Adaptive Security Appliance) ont-elles des valeurs d'inactivité plus longues que les délais d'attente configurés ?](#)
[Informations connexes](#)

Introduction

Ce document explique pourquoi les entrées xlate avec des valeurs inactives sont plus longues que les délais d'attente configurés. Il fournit également des informations sur la façon de corréler et de voir les valeurs conn et xlate.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco.](#)

Q. Pourquoi les entrées xlate de l'appliance de sécurité adaptative (ASA) ont-elles des valeurs d'inactivité plus longues que les délais d'attente configurés ?

R. Voici un exemple qui montre les entrées xlate avec des valeurs d'inactivité plus longues que les délais d'attente configurés :

<#root>

ASA#

show xlate

```
26 in use, 16665 most used
Flags: D - DNS, e - extended, I - identity,
   I - dynamic, r - portmap, s - static,
   T - twice, N - net-to-net
TCP PAT from inside:10.20.33.2/54676 to outside:
   192.0.2.3/54676 flags ri idle 1:48:12
   timeout 0:00:30
TCP PAT from inside:10.20.33.2/54397 to outside:
   192.0.2.3/54397 flags ri idle 2:03:59
   timeout 0:00:30
TCP PAT from inside:10.20.33.2/54369 to outside:
   192.0.2.3/54369 flags ri idle 2:04:26
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/56695 to outside:
```

```
   192.0.2.3/56695 flags ri idle 0:09:22
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/55880 to outside:
   192.0.2.3/55880 flags ri idle 0:33:12
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/54431 to outside:
   192.0.2.3/54431 flags ri idle 2:03:23
   timeout 0:00:30
```

Si une connexion est soumise à une traduction (xlate) sur l'ASA, la traduction est d'abord construite, puis la connexion est construite, et enfin, la connexion est associée à cette traduction. Le délai d'inactivité de xlate ne commence que lorsque toutes les connexions associées pour ce xlate sont terminées.

Si vous corrélez le résultat de show xlate et de show conn, vous pouvez voir que les valeurs conn correspondent aux valeurs xlate qui ont été inactives pendant plus longtemps que le délai d'attente configuré. Voici un exemple .

Entrez la commande PAT (Port Address Translation) show xlate :

<#root>

ASA#

show xlate local port 54676

```
TCP PAT from inside:10.20.33.2/54676 to outside:192.0.2.3/54676 flags ri
   idle 1:48:12 timeout 0:00:30
```

Spécifiez ensuite le port dans la commande show conn pour trouver l'entrée de connexion associée :

<#root>

ASA#

show conn port 54676

```
TCP outside 192.168.22.3:443 events inside:10.20.33.2:54676, idle 0:03:52,
   bytes 1807, flags UIO
```

Cette connexion est associée à la traduction. Le port local 54676 est le même pour la connexion et l'entrée de traduction. Cette connexion TCP est présente jusqu'à ce qu'elle soit fermée par le protocole (TCP FINs ou paquets de réinitialisation), ou jusqu'à ce qu'elle expire par l'ASA (après le délai d'attente par défaut de 1 heure). Lorsque la connexion est interrompue, la traduction est également supprimée, mais cette suppression est retardée de quelques secondes.

Informations connexes

- Pare-feu de nouvelle génération Cisco ASA 5500
- Assistance et documentation techniques - Cisco Systems

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.