

Exemple de configuration du doctoring DNS sur ASA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Exemples de doctoring DNS](#)

[Serveur DNS à l'intérieur de l'ASA](#)

[Serveur DNS à l'extérieur de l'ASA](#)

[NAT VPN et doctoring DNS](#)

[Informations connexes](#)

Introduction

Ce document montre comment le doctoring DNS est utilisé sur l'appareil de sécurité adaptatif (ASA) pour modifier les adresses IP intégrées dans les réponses DNS (Domain Name System) afin que les clients puissent se connecter à l'adresse IP correcte des serveurs.

Conditions préalables

Exigences

Le doctoring DNS nécessite la configuration de la traduction d'adresses de réseau (NAT) sur l'ASA, ainsi que l'activation de l'inspection DNS.

Composants utilisés

Les informations contenues dans ce document sont basées sur l'appliance de sécurité adaptative.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Exemples de doctoring DNS

Serveur DNS à l'intérieur de l'ASA

Figure 1

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Dans la Figure 1, le serveur DNS est contrôlé par l'administrateur local. Le serveur DNS doit distribuer une adresse IP privée, qui est l'adresse IP réelle attribuée au serveur d'applications. Cela permet au client local de se connecter directement au serveur d'applications.

Malheureusement, le client distant ne peut pas accéder au serveur d'applications avec l'adresse privée. Par conséquent, DNS Doctoring est configuré sur l'ASA pour modifier l'adresse IP intégrée dans le paquet de réponse DNS. Cela garantit que lorsque le client distant fait une requête DNS pour `www.abc.com`, la réponse qu'il obtient est pour l'adresse traduite du serveur d'applications. Sans le mot clé DNS sur l'instruction NAT, le client distant tente de se connecter à `10.1.1.100`, ce qui ne fonctionne pas car cette adresse ne peut pas être routée sur Internet.

Serveur DNS à l'extérieur de l'ASA

Figure 2

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Dans la Figure 2, le serveur DNS est contrôlé par le FAI ou un fournisseur de services similaire. Le serveur DNS doit distribuer l'adresse IP publique, c'est-à-dire l'adresse IP traduite du serveur d'applications. Cela permet à tous les utilisateurs Internet d'accéder au serveur d'applications via Internet.

Malheureusement, le client local ne peut pas accéder au serveur d'applications avec l'adresse publique. Par conséquent, DNS Doctoring est configuré sur l'ASA pour modifier l'adresse IP intégrée dans le paquet de réponse DNS. Cela garantit que lorsque le client local effectue une requête DNS pour `www.abc.com`, la réponse reçue est l'adresse réelle du serveur d'applications. Sans le mot clé DNS sur l'instruction NAT, le client local tente de se connecter à `198.51.100.100`.

Cela ne fonctionne pas car ce paquet est envoyé à l'ASA, qui abandonne le paquet.

NAT VPN et doctoring DNS

Figure 3

Imaginez une situation où des réseaux se chevauchent. Dans cette condition, l'adresse 10.1.1.100 se trouve à la fois sur le côté distant et sur le côté local. Par conséquent, vous devez exécuter la fonction NAT sur le serveur local afin que le client distant puisse toujours y accéder avec l'adresse IP 192.1.1.100. Pour que cela fonctionne correctement, le doctoring DNS est requis.

DNS Doctoring ne peut pas être effectué dans cette fonction. Le mot clé DNS peut uniquement être ajouté à la fin d'une NAT d'objet ou d'une NAT source. La NAT à deux reprises ne prend pas en charge le mot clé DNS. Il existe deux configurations possibles et toutes deux échouent.

Échec de la configuration 1 : si vous configurez le résultat, il traduit 10.1.1.1 en 192.1.1.1, non seulement pour le client distant, mais pour tous les utilisateurs d'Internet. 192.1.1.1 n'étant pas routable sur Internet, personne sur Internet ne peut accéder au serveur local.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
    REMOTE_CLIENT REMOTE_CLIENT
```

Échec de la configuration 2 : Si vous configurez la ligne NAT de doctoring DNS après la ligne NAT double nécessaire, cela entraîne une situation où le doctoring DNS ne fonctionne jamais. Par conséquent, le client distant tente d'accéder à www.abc.com avec l'adresse IP 10.1.1.100, ce qui ne fonctionne pas.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
    REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Informations connexes

- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Appareils de sécurité adaptatifs Cisco ASA 5500 > Téléchargements de logiciels](#)
- [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.