DNS Doctoring sur l'exemple de configuration ASA

Contenu

Introduction

Ce document affiche comment le DNS Doctoring est utilisé sur l'appliance de sécurité adaptable (ASA) pour changer les adresses IP incluses dans des réponses de Système de noms de domaine (DNS) de sorte que les clients puissent se connecter à l'adresse IP correcte des serveurs.

Conditions préalables

Conditions requises

Le DNS Doctoring exige la configuration du Traduction d'adresses de réseau (NAT) sur l'ASA, aussi bien que l'activation de l'inspection de DN.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Exemples de DNS Doctoring

Serveur DNS sur 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 devrait distribuer une adresse IP privée, qui est la *vraie* adresse IP assignée au serveur d'applications. Ceci permet au client local pour se connecter directement au serveur d'applications.

Malheureusement, le client distant ne peut pas accéder au serveur d'applications avec l'adresse privée. En conséquence, le DNS Doctoring est configuré sur l'ASA pour changer l'adresse IP incluse dans le paquet de réponse de DN. Ceci s'assure que quand le client distant fait une demande de DN de www.abc.com, la réponse qu'ils obtiennent est pour l'adresse traduite du serveur d'applications. Sans mot clé de DN sur la déclaration NAT, les essais de client distant à connecter à 10.1.1.100, qui ne fonctionne pas parce que cette adresse ne peut pas être conduite sur l'Internet.

Serveur DNS sur 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 l'ISP ou le fournisseur de services semblable. Le serveur DNS devrait distribuer l'adresse IP publique, c.-à-d., l'adresse IP *traduite du* serveur d'applications. Ceci permet à tous les internautes pour accéder au serveur d'applications par l'intermédiaire de l'Internet.

Malheureusement, le client local ne peut pas accéder au serveur d'applications avec l'annonce publique. En conséquence, le DNS Doctoring est configuré sur l'ASA pour changer l'adresse IP incluse dans le paquet de réponse de DN. Ceci s'assure que quand le client local fait une demande de DN de www.abc.com, la réponse reçue est la vraie adresse du serveur d'applications. Sans mot clé de DN sur la déclaration NAT, les essais locaux de client à connecter à 198.51.100.100. Ceci ne fonctionne pas parce que ce paquet est envoyé à l'ASA, qui relâche le paquet.

VPN NAT et DNS Doctoring

Figure 3

Considérez une situation où il y a des réseaux qui superposent. En cette condition, l'adresse 10.1.1.100 vit du côté distant et du côté local. En conséquence, vous devez exécuter NAT sur le serveur local de sorte que le client distant puisse encore l'accéder à avec l'adresse IP 192.1.1.100. Afin d'obtenir ceci pour fonctionner correctement, le DNS Doctoring est exigé.

Le DNS Doctoring ne peut pas être exécuté dans cette fonction. Le mot clé de DN peut seulement

être ajouté à la fin d'un objet NAT ou de la source NAT. Deux fois Le NAT ne prend en charge pas le mot clé de DN. Il y a deux configurations possibles et chacun des deux échouent.

Configuration défectueuse 1 : Si vous configurez la ligne inférieure, elle traduit 10.1.1.1 à 192.1.1.1, non seulement pour le client distant, mais pour chacun sur l'Internet. Puisque 192.1.1.1 n'est pas Internet routable, personne sur l'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
```

Configuration défectueuse 2 : Si vous configurez la ligne NAT de DNS Doctoring après deux fois la ligne NAT nécessaire, ceci entraîne une situation où le DNS Doctoring ne fonctionne jamais. En conséquence, les essais de client distant pour accéder à www.abc.com avec l'adresse IP 10.1.1.100, 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
- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 > téléchargements logiciels
- Support et documentation techniques - Cisco Systems