Comprendre le fonctionnement de DNS sur ASA lorsque des objets FQDN sont utilisés

Table des matières

Introduction

Ce document décrit le fonctionnement du système de noms de domaine (DNS) sur Cisco Adaptive Security Appliance (ASA) lorsque des objets FDQN sont utilisés.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de Cisco ASA.

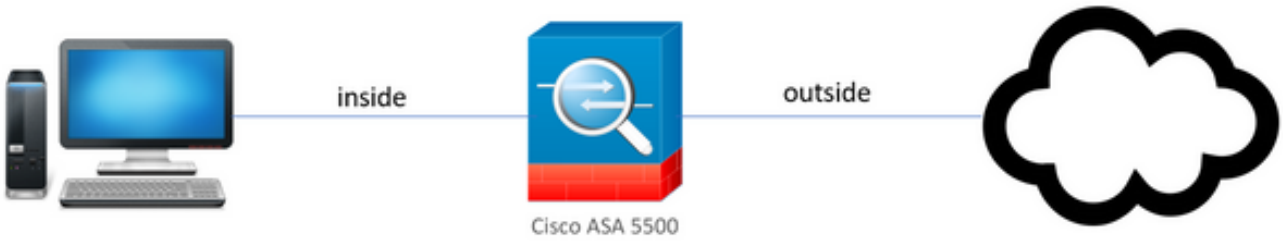
Composants utilisés

Afin d'élucider le fonctionnement du DNS lorsque plusieurs FQDN sont configurés sur l'ASA dans un environnement de production simulé, un ASAv avec une interface tournée vers Internet et une interface connectée à un périphérique PC hébergé sur le serveur ESXi a été configuré. Le code provisoire ASAv 9.8.4(10) a été utilisé pour cette simulation.

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.

Diagramme du réseau

La configuration de la topologie est illustrée ici.

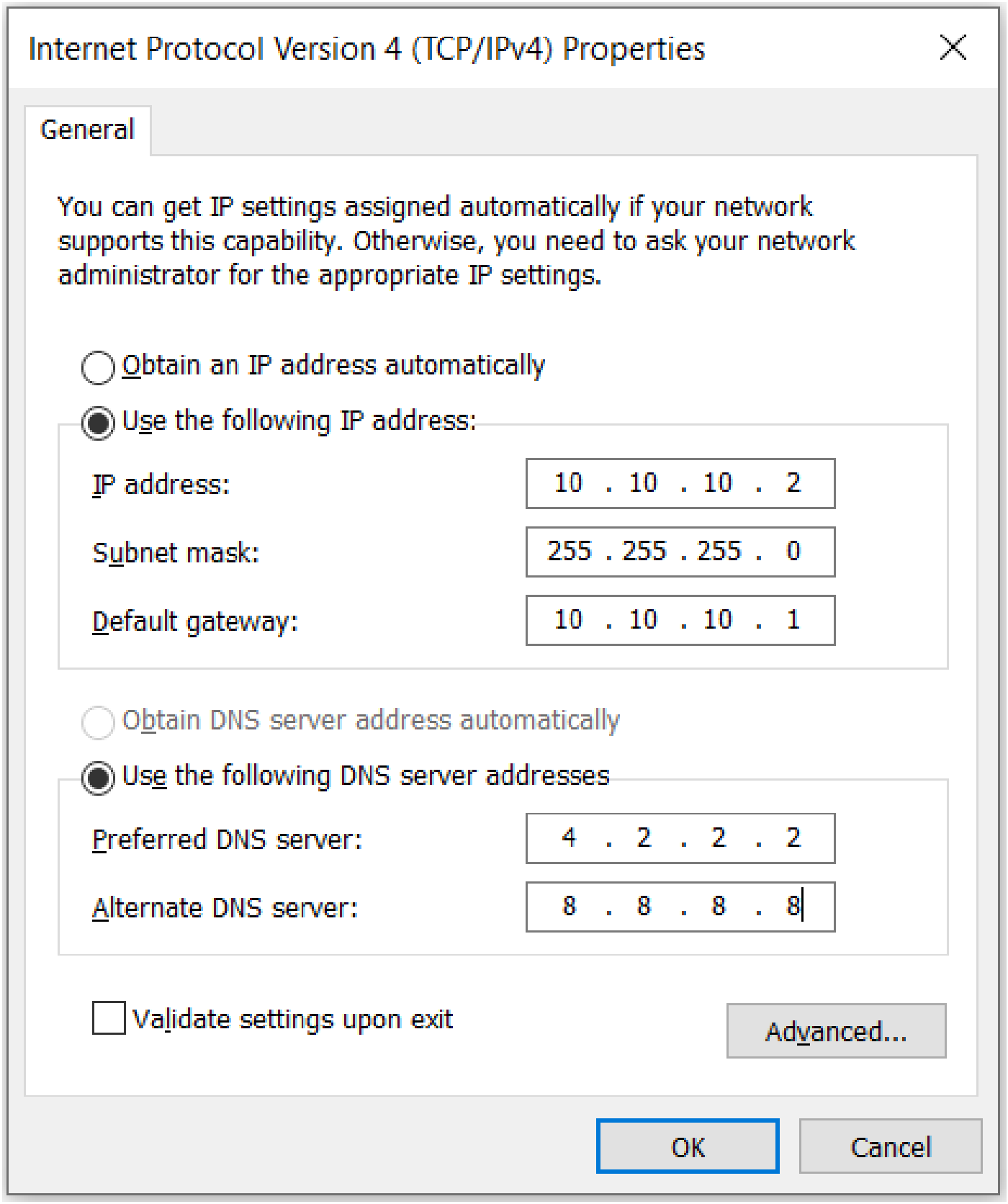


Informations générales

Lorsque plusieurs objets FQDN (Fully Qualified Domain Name) sont configurés sur un ASA, un utilisateur final qui tente d'accéder à l'une des URL définies dans les objets FQDN observe plusieurs requêtes DNS envoyées par l'ASA. Le présent document vise à mieux comprendre pourquoi un tel comportement est observé.

Configurer

Le PC client a été configuré avec ces adresses IP, masque de sous-réseau et serveurs de noms pour la résolution DNS.



Sur l'ASA, deux interfaces ont été configurées, 1 interface interne avec un niveau de sécurité de 100 auquel le PC était connecté et 1 interface externe qui a une connectivité à Internet.

```
ciscoasa(config-if)# sh int ip br
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         10.197.223.9    YES DHCP   up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         10.10.10.1      YES manual up                    up
GigabitEthernet0/4         unassigned      YES unset  administratively down up
GigabitEthernet0/5         unassigned      YES unset  administratively down up
GigabitEthernet0/6         unassigned      YES unset  administratively down down
GigabitEthernet0/7         unassigned      YES unset  administratively down up
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              unassigned      YES unset  up                    up
ciscoasa(config-if)#
```

Ici, l'interface Gig0/1 est l'interface externe avec une adresse IP d'interface de 10.197.223.9 et l'interface Gig0/3 est l'interface interne avec une adresse IP d'interface de 10.10.10.1 et connectée au PC à l'autre extrémité.

```
ciscoasa(config-if)# ping 10.197.222.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.197.222.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa(config-if)# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
```

Configurez la configuration DNS sur l'ASA comme indiqué ici :

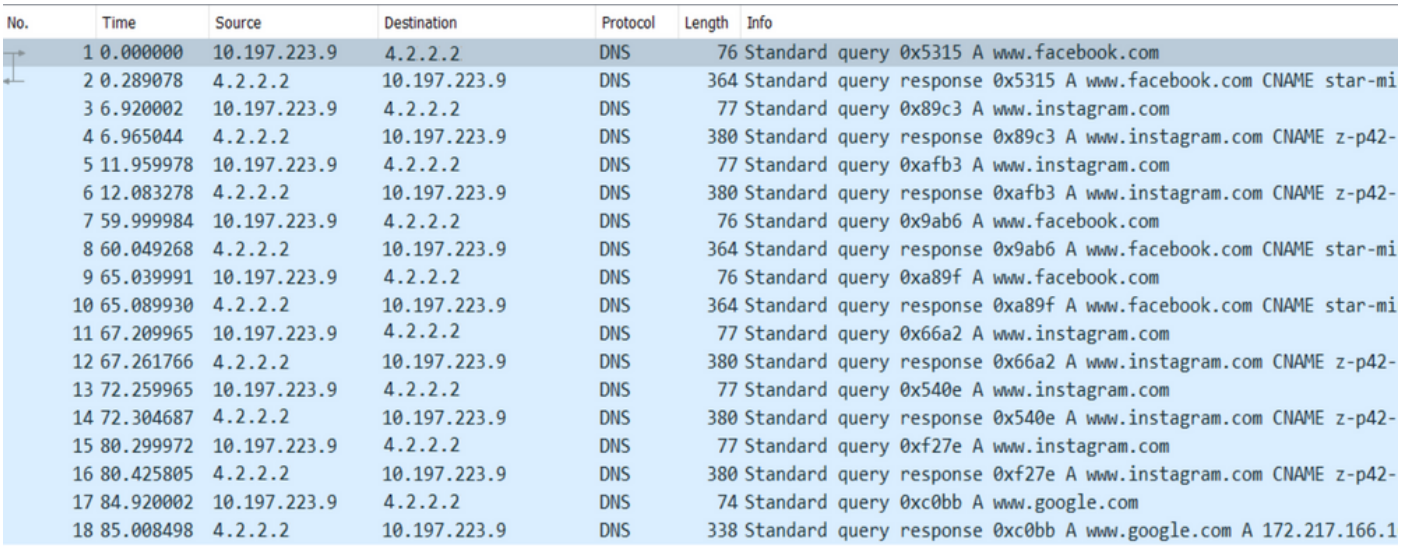
```
ciscoasa(config)# sh run dns
dns domain-lookup outside
DNS server-group DefaultDNS
    name-server 4.2.2.2
ciscoasa(config)#
```

Configurez 4 objets FQDN pour www.facebook.com, www.google.com, www.instagram.com et www.twitter.com.

```
ciscoasa(config)# sh run object
object network OBJ_GENERIC_ALL
 subnet 0.0.0.0 0.0.0.0
object network facebook.com
 fqdn www.facebook.com
object network twitter.com
 fqdn www.twitter.com
object network instagram.com
 fqdn www.instagram.com
object network google.com
 fqdn www.google.com
```

Configurez une capture sur l'interface externe ASA pour capturer le trafic DNS. Ensuite, à partir du PC client, essayez d'accéder à www.google.com à partir d'un navigateur.

Qu'observez-vous ? Examinez la capture de paquets.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.197.223.9	4.2.2.2	DNS	76	Standard query 0x5315 A www.facebook.com
2	0.289078	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0x5315 A www.facebook.com CNAME star-mi
3	6.920002	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x89c3 A www.instagram.com
4	6.965044	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x89c3 A www.instagram.com CNAME z-p42-
5	11.959978	10.197.223.9	4.2.2.2	DNS	77	Standard query 0xafb3 A www.instagram.com
6	12.083278	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0xafb3 A www.instagram.com CNAME z-p42-
7	59.999984	10.197.223.9	4.2.2.2	DNS	76	Standard query 0x9ab6 A www.facebook.com
8	60.049268	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0x9ab6 A www.facebook.com CNAME star-mi
9	65.039991	10.197.223.9	4.2.2.2	DNS	76	Standard query 0xa89f A www.facebook.com
10	65.089930	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0xa89f A www.facebook.com CNAME star-mi
11	67.209965	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x66a2 A www.instagram.com
12	67.261766	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x66a2 A www.instagram.com CNAME z-p42-
13	72.259965	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x540e A www.instagram.com
14	72.304687	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x540e A www.instagram.com CNAME z-p42-
15	80.299972	10.197.223.9	4.2.2.2	DNS	77	Standard query 0xf27e A www.instagram.com
16	80.425805	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0xf27e A www.instagram.com CNAME z-p42-
17	84.920002	10.197.223.9	4.2.2.2	DNS	74	Standard query 0xc0bb A www.google.com
18	85.008498	4.2.2.2	10.197.223.9	DNS	338	Standard query response 0xc0bb A www.google.com A 172.217.166.1

Ici, nous voyons que même si nous avons essayé de résoudre seulement www.google.com, il y a des requêtes DNS envoyées pour tous les objets FQDN.

Maintenant, examinez le fonctionnement de la mise en cache DNS pour les adresses IP sur l'ASA pour comprendre pourquoi cela se produit.

- Lorsque www.google.com est tapé dans le navigateur Web des ordinateurs clients, l'ordinateur envoie une requête DNS pour obtenir la résolution de l'URL en adresse IP.

- Le serveur DNS résout ensuite la requête des PC et renvoie une adresse IP qui indique google.com réside à l'emplacement spécifié.
- Le PC établit ensuite une connexion TCP à l'adresse IP résolue de google.com. Cependant, lorsque le paquet atteint l'ASA, il n'a pas de règle de liste de contrôle d'accès qui indique que l'IP spécifiée est autorisée ou refusée.
- Cependant, l'ASA sait qu'il a 4 objets FQDN et que n'importe lequel des objets FQDN pourrait éventuellement être résolu vers l'IP concernée.
- Par conséquent, l'ASA envoie des requêtes DNS pour tous les objets FQDN, car il ne sait pas quel objet FQDN peut être résolu vers l'adresse IP concernée (c'est pourquoi il y a plusieurs requêtes DNS observées).
- Le serveur DNS résout les objets FQDN avec leurs adresses IP correspondantes. L'objet FQDN peut être résolu avec la même adresse IP publique que celle résolue par le client. Sinon, l'ASA crée une entrée de liste d'accès dynamique pour une adresse IP différente de celle que le client tente d'atteindre, par conséquent l'ASA finit par abandonner le paquet. Par exemple, si l'utilisateur a résolu google.com en 203.0.113.1 et si l'ASA l'a résolu en 203.0.113.2, l'ASA crée une nouvelle entrée de liste d'accès dynamique pour 203.0.113.2 et l'utilisateur ne peut pas accéder au site Web.
- La prochaine fois qu'une requête arrive, qui demande la résolution d'une adresse IP particulière, si cette adresse IP particulière est stockée sur l'ASA, il ne demande pas à nouveau tous les objets FQDN puisque une entrée ACL dynamique serait maintenant présente.
- Si un client est préoccupé par le grand nombre de requêtes DNS envoyées par ASA, augmentez l'expiration du compteur DNS et à condition que les hôtes finaux tentent d'accéder aux adresses IP de destination qui se trouvent dans le cache DNS. Si le PC demande une adresse IP, qui n'est pas stockée dans le cache DNS ASA, des requêtes DNS sont envoyées pour résoudre tous les objets FQDN.
- Une solution de contournement possible pour cela, si vous voulez toujours réduire le nombre de requêtes DNS, serait soit de réduire le nombre d'objets FQDN, soit de définir toute la plage d'IP publiques vers lesquelles vous résoudrez le FQDN, ce qui cependant va à l'encontre de l'objectif d'un objet FQDN. Cisco Firepower Threat Defense (FTD) est une meilleure solution pour gérer ce cas d'utilisation.

Vérifier

Afin de vérifier quelles adresses IP sont présentes dans le cache DNS des ASA vers lequel chacun des objets FQDN est résolu, la commande ASA# sh dns peut être utilisée.

```
ciscoasa(config)# sh dns
Name: www.facebook.com
  Address: 157.240.192.35                          TTL 00:01:06
Name: www.google.com
  Address: 172.217.166.164                         TTL 00:04:44
Name: www.instagram.com
  Address: 157.240.16.174                          TTL 00:01:21
Name: www.twitter.com
  Address: 104.244.42.65                           TTL 00:06:37
  Address: 104.244.42.1                            TTL 00:05:26
```

Informations connexes

[Assistance technique et téléchargements Cisco]

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.