Comprender el funcionamiento de DNS en ASA cuando se utilizan objetos FQDN

Contenido

Introducción

Este documento describe el funcionamiento del Sistema de nombres de dominio (DNS) en Cisco Adaptive Security Appliance (ASA) cuando se utilizan objetos FDQN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de Cisco ASA.

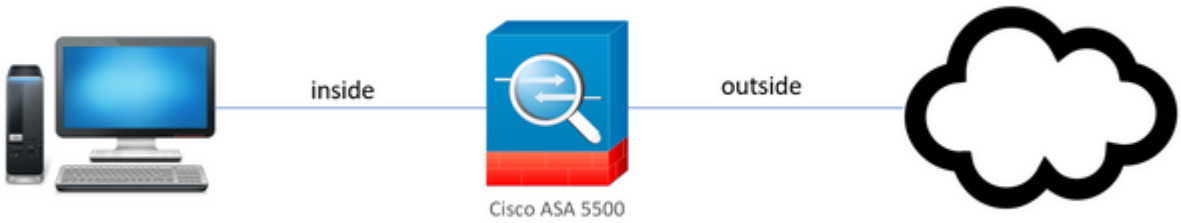
Componentes Utilizados

Para elucidar el funcionamiento del DNS cuando se configuran varios FQDN en el ASA en un entorno de producción simulado, se configuró un ASAv con una interfaz orientada a Internet y una interfaz conectada a un dispositivo de PC alojado en el servidor ESXi. Para esta simulación se utilizó el código provisional ASAv 9.8.4(10).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red

Aquí se muestra la configuración de la topología.

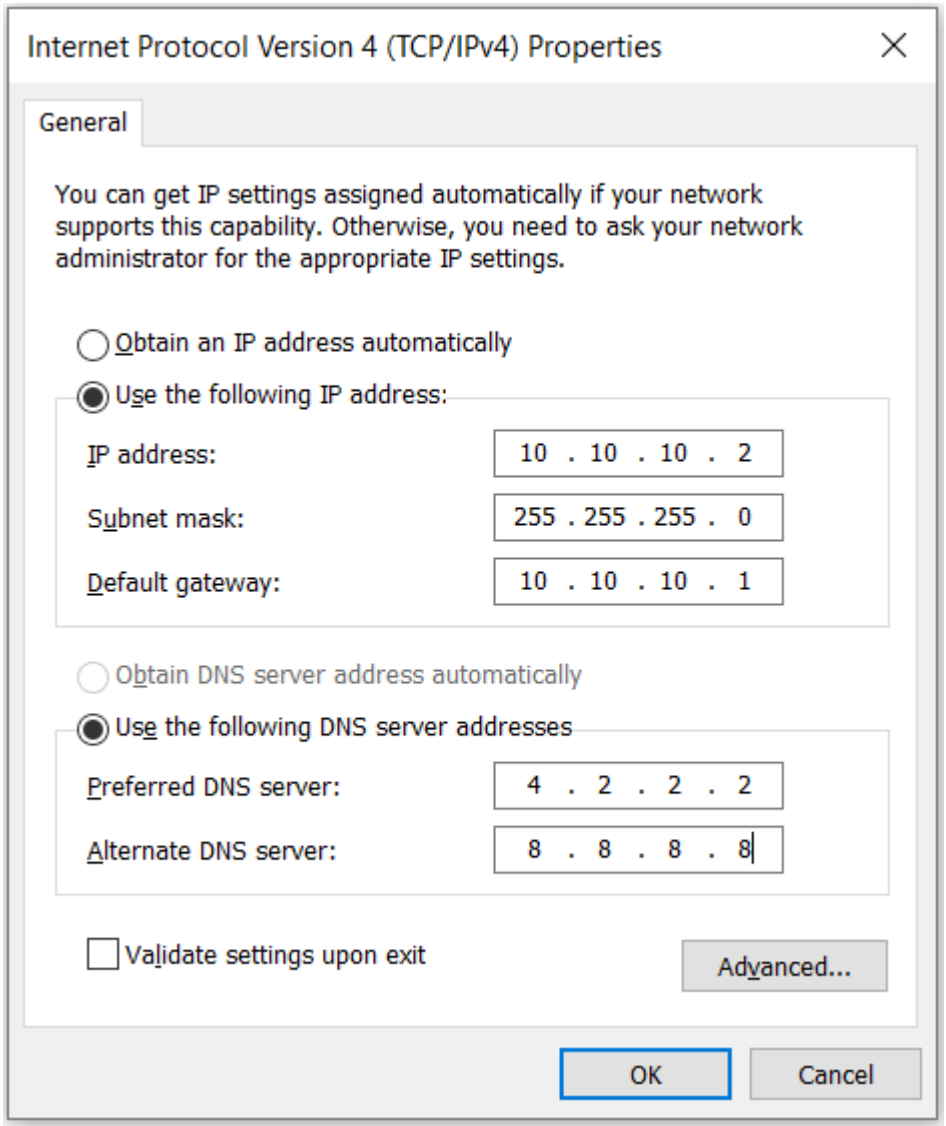


Antecedentes

Cuando se configuran varios objetos de nombre de dominio completo (FQDN) en un ASA, un usuario final que intente acceder a cualquiera de las URL definidas en los objetos FQDN observará varias consultas DNS enviadas por el ASA. Este documento tiene como objetivo proporcionar una mejor comprensión de por qué se observa este tipo de comportamiento.

Configurar

El equipo cliente se configuró con estos IP, máscara de subred y servidores de nombres para la resolución DNS.



En ASA, se configuraron dos interfaces, una interfaz interna con un nivel de seguridad de 100 a la que se conectó el PC y una interfaz externa que tiene conectividad a 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)#
```

Aquí la interfaz Gig0/1 es la interfaz externa con una IP de interfaz de 10.197.223.9 y la interfaz Gig0/3 es la interfaz interna con una IP de interfaz de 10.10.10.1 y conectada al PC en el otro extremo.

```
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
```

Configure la configuración de DNS en el ASA como se muestra aquí:

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

Configure 4 objetos FQDN para www.facebook.com, www.google.com, www.instagram.com y 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
```

Configure una captura en la interfaz externa de ASA para capturar el tráfico DNS. A continuación, desde el PC cliente, intente acceder a www.google.com desde un navegador.

¿Qué observas? Eche un vistazo a la captura de paquetes.

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.f
2	0.289078	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0x531
3	6.920002	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x89c3 A www.i
4	6.965044	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x89c
5	11.959978	10.197.223.9	4.2.2.2	DNS	77	Standard query 0xafb3 A www.i
6	12.083278	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0xafb
7	59.999984	10.197.223.9	4.2.2.2	DNS	76	Standard query 0x9ab6 A www.f
8	60.049268	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0x9ab
9	65.039991	10.197.223.9	4.2.2.2	DNS	76	Standard query 0xa89f A www.f
10	65.089930	4.2.2.2	10.197.223.9	DNS	364	Standard query response 0xa89
11	67.209965	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x66a2 A www.i
12	67.261766	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x66a
13	72.259965	10.197.223.9	4.2.2.2	DNS	77	Standard query 0x540e A www.i
14	72.304687	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0x540
15	80.299972	10.197.223.9	4.2.2.2	DNS	77	Standard query 0xf27e A www.i
16	80.425805	4.2.2.2	10.197.223.9	DNS	380	Standard query response 0xf27
17	84.920002	10.197.223.9	4.2.2.2	DNS	74	Standard query 0xc0bb A www.g
18	85.008498	4.2.2.2	10.197.223.9	DNS	338	Standard query response 0xc0b

Aquí vemos que aunque intentamos resolver solamente www.google.com, se envían consultas DNS para todos los objetos FQDN.

Ahora eche un vistazo a cómo funciona el almacenamiento en caché de DNS para las IP en ASA para entender por qué sucede esto.

- Cuando se escribe www.google.com en el explorador web de los PC cliente, el PC envía una consulta DNS para que la URL se resuelva en una dirección IP.
- El servidor DNS resuelve la solicitud de los PC y devuelve una dirección IP que indica que google.com reside en la ubicación especificada.
- El PC inicia una conexión TCP a la dirección IP resuelta de google.com. Sin embargo, cuando el paquete llega al ASA, no tiene una regla ACL que establezca que la IP especificada se permite o se niega.
- Sin embargo, ASA sabe que tiene 4 objetos FQDN y que cualquiera de los objetos FQDN podría resolverse en la IP en cuestión.
- Por lo tanto, ASA envía consultas DNS para todos los objetos FQDN, ya que no sabe qué objeto FQDN puede resolver a la IP en cuestión. (Esta es la razón por la que se observan varias consultas DNS).
- El servidor DNS resuelve los objetos FQDN con sus direcciones IP correspondientes. El objeto FQDN se puede resolver en la misma dirección IP pública que resolvió el cliente. De lo contrario, el ASA crea una entrada de lista de acceso dinámica para una dirección IP diferente de la que el cliente intenta alcanzar, de ahí que el ASA termine descartando el paquete. Por ejemplo, si el usuario resolvió google.com a 203.0.113.1 y si ASA lo resuelve a 203.0.113.2, ASA crea una nueva entrada de lista de acceso dinámica para 203.0.113.2 y el usuario no puede acceder al sitio web.
- La próxima vez que llegue una solicitud, que solicite la resolución de una IP en particular, si esa IP en

particular está almacenada en el ASA, no volverá a consultar todos los objetos FQDN ya que ahora estaría presente una entrada de ACL dinámica.

- Si un cliente está preocupado por el gran número de consultas DNS enviadas por ASA, aumente el vencimiento del temporizador DNS y los hosts finales provistos intenten acceder a las direcciones IP de destino que están allí en la memoria caché DNS. Si el equipo solicita una dirección IP, que no está almacenada en la caché DNS de ASA, se envían consultas DNS para resolver todos los objetos FQDN.

- Una solución alternativa posible para esto, si desea reducir aún el número de consultas DNS, sería reducir el número de objetos FQDN o definir todo el rango de IP públicas a las que resolvería el FQDN, lo que sin embargo derrota el propósito de un objeto FQDN en primer lugar. Cisco Firepower Threat Defense (FTD) es una solución más eficaz para este caso práctico.

Verificación

Para verificar qué IP están presentes en la memoria caché DNS de ASA a la que se resuelve cada uno de los objetos FQDN, se puede utilizar el comando **ASA# sh dns**.

```
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
```

Información Relacionada

Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).