Entender a operação do DNS no ASA quando objetos FQDN são usados

Contents

Introduction

Este documento descreve a operação do Domain Name System (DNS) no Cisco Adaptive Security Appliance (ASA) quando objetos FDQN são usados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Cisco ASA.

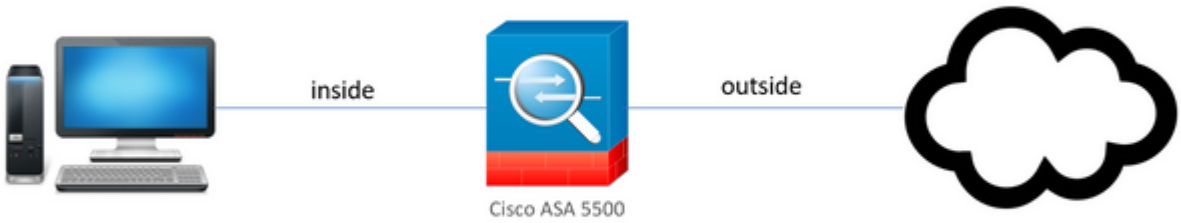
Componentes Utilizados

Para elucidar o funcionamento do DNS quando vários FQDNs são configurados no ASA em um ambiente de produção simulado, foi configurado um ASAv com uma interface voltada para a Internet e uma interface conectada a um dispositivo PC hospedado no servidor ESXi. O código provisório ASAv 9.8.4(10) foi usado para esta simulação.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

A configuração da topologia é mostrada aqui.

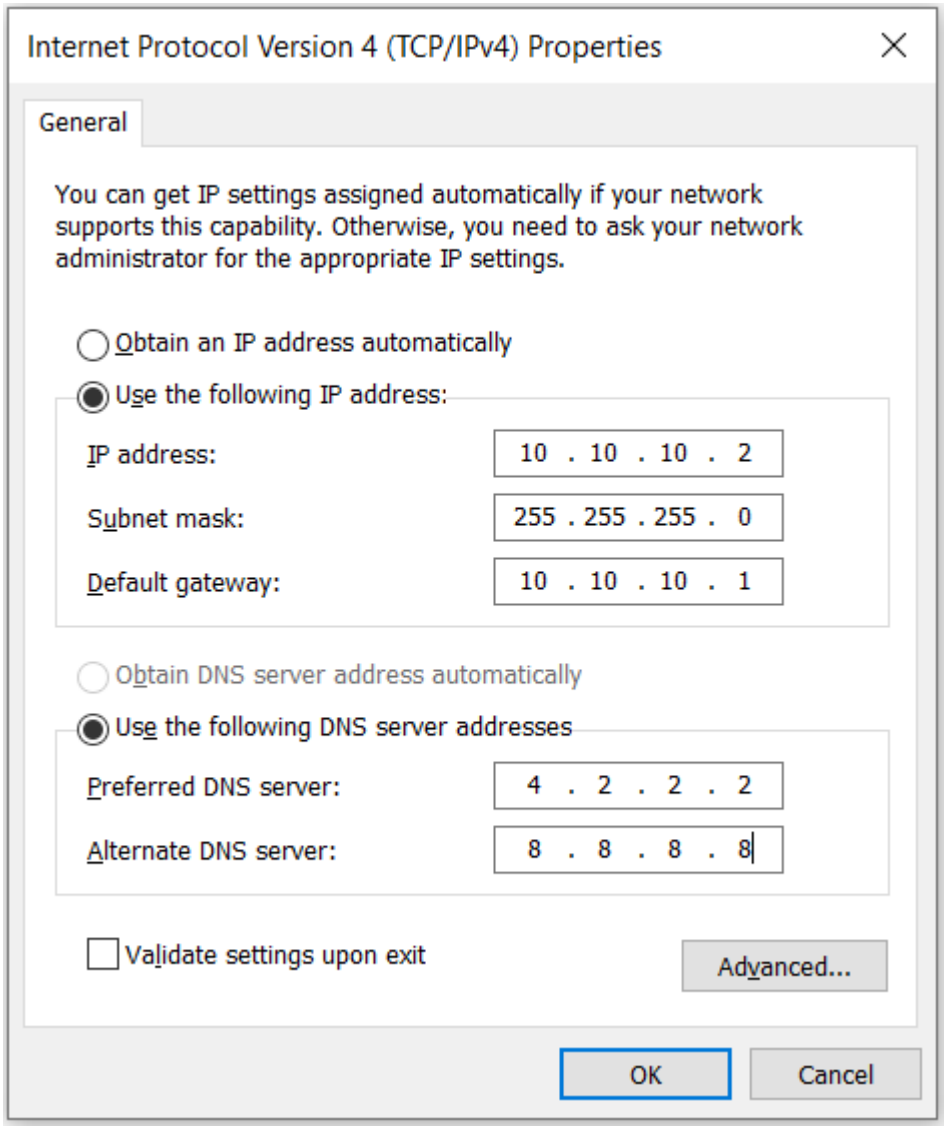


Informações de Apoio

Quando vários objetos Fully Qualified Domain Name (FQDN) são configurados em um ASA, um usuário final que tenta acessar qualquer URL definida nos objetos FQDN observaria várias consultas DNS enviadas pelo ASA. Este documento tem como objetivo fornecer uma melhor compreensão da razão pela qual tal comportamento é observado.

Configurar

O PC cliente foi configurado com esses IP, máscara de sub-rede e servidores de nome para resolução DNS.



No ASA, foram configuradas duas interfaces, uma interface interna com um nível de segurança de 100 ao qual o PC estava conectado e uma interface externa com conectividade com 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)#
```

Aqui a interface Gig0/1 é a interface externa com um IP de interface de 10.197.223.9 e a interface Gig0/3 é a interface interna com um IP de interface de 10.10.10.1 e conectada ao PC na outra extremidade.

```
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 o DNS no ASA conforme mostrado aqui:

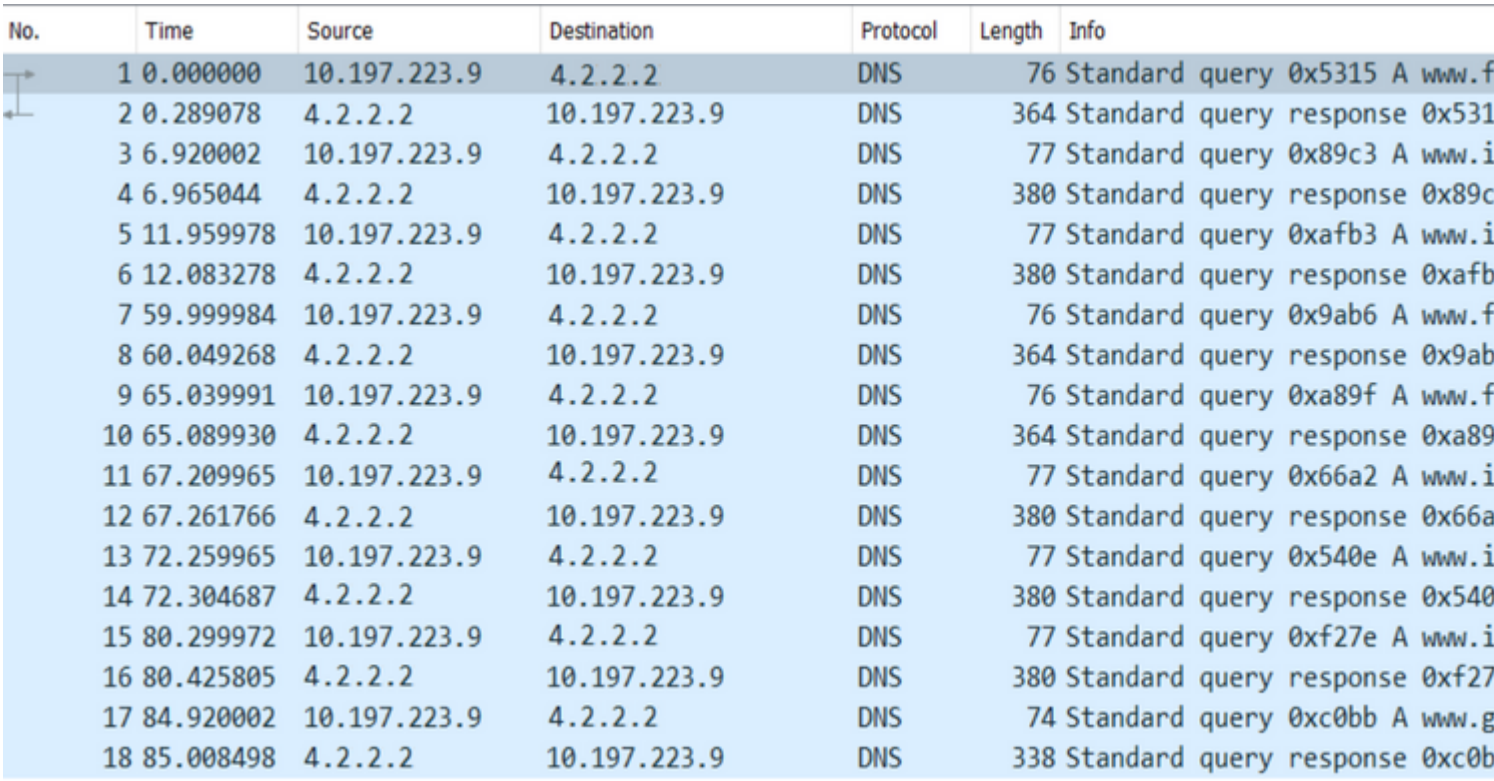
```
ciscoasa(config)# sh run dns
dns domain-lookup outside
DNS server-group DefaultDNS
    name-server 4.2.2.2
ciscoasa(config)#
```

Configure 4 objetos FQDN para www.facebook.com, www.google.com, www.instagram.com e 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 uma captura na interface externa do ASA para capturar o tráfego DNS. Em seguida, no PC cliente, tente acessar www.google.com de um navegador.

O que você observa? Observe a captura de pacotes.



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

Aqui vemos que, embora tentemos resolver apenas www.google.com, há consultas DNS enviadas para todos os objetos FQDN.

Agora, observe como o cache DNS funciona para IPs no ASA para entender por que isso acontece.

- Quando www.google.com é digitado no navegador da Web dos PCs clientes, o PC envia uma consulta DNS para obter o URL resolvido para um endereço IP.
- O servidor DNS então resolve a solicitação dos PCs e retorna um IP que afirma que google.com reside no local especificado.
- Em seguida, o PC inicia uma conexão TCP com o endereço IP resolvido do google.com. No entanto, quando o pacote alcança o ASA, ele não tem uma regra de ACL que declare que o IP especificado é permitido ou negado.
- O ASA, no entanto, sabe que tem 4 objetos FQDN e que qualquer um dos objetos FQDN poderia ser resolvido para o IP em questão.
- Portanto, o ASA envia consultas DNS para todos os objetos FQDN, pois não sabe qual objeto FQDN pode resolver para o IP em questão. (É por isso que há várias consultas DNS observadas).
- O servidor DNS resolve os objetos FQDN com seus endereços IP correspondentes. O objeto FQDN pode ser resolvido para o mesmo endereço IP público que foi resolvido pelo cliente. Caso contrário, o ASA cria uma entrada de lista de acesso dinâmica para um endereço IP diferente daquele que o cliente tenta alcançar, portanto, o ASA acaba descartando o pacote. Por exemplo, se o usuário resolveu google.com para 203.0.113.1 e se o ASA resolveu para 203.0.113.2, o ASA cria uma nova entrada de lista de acesso dinâmica para 203.0.113.2 e o usuário não consegue acessar o site.
- Na próxima vez que uma solicitação chegar, ela solicitará a resolução de um IP específico, se esse IP específico estiver armazenado no ASA, ele não consultará todos os objetos FQDN novamente, pois uma entrada de ACL dinâmica estaria presente agora.

- Se um cliente estiver preocupado com o grande número de consultas DNS enviadas pelo ASA, aumente a expiração do temporizador DNS e, desde que os hosts finais tentem acessar os endereços IP de destino que estão no cache DNS. Se o PC solicitar um IP, não armazenado no cache DNS do ASA, as consultas DNS serão enviadas para resolver todos os objetos FQDN.

- Uma solução possível para isso, se você ainda quiser reduzir o número de consultas DNS, seria reduzir o número de objetos FQDN ou definir todo o intervalo de IPs públicos para os quais você resolveria o FQDN, o que, no entanto, anula a finalidade de um objeto FQDN em primeiro lugar. O Cisco Firepower Threat Defense (FTD) é uma solução melhor para lidar com esse caso de uso.

Verificar

Para verificar quais IPs estão presentes no cache DNS dos ASAs para os quais cada um dos objetos FQDN é resolvido, o comando **ASA# sh dns** pode ser usado.

```
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
```

Informações Relacionadas

[Suporte técnico e downloads da Cisco]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.