了解使用FQDN对象时在ASA上的DNS操作

目录

简介

本文档介绍使用FDQN对象时，思科自适应安全设备(ASA)上的域名系统(DNS)的操作。

先决条件

要求

Cisco建议您了解Cisco ASA。

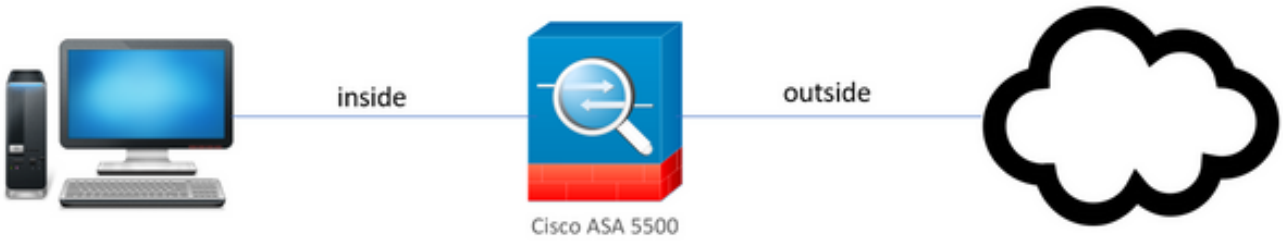
使用的组件

为了说明在模拟生产环境中在ASA上配置多个FQDN时的DNS工作原理，设置了一个ASAv，该ASAv具有一个面向互联网的接口和一个连接到ESXi服务器上托管的PC设备的接口。此模拟使用ASAv临时代码9.8.4(10)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图

拓扑设置如下所示。

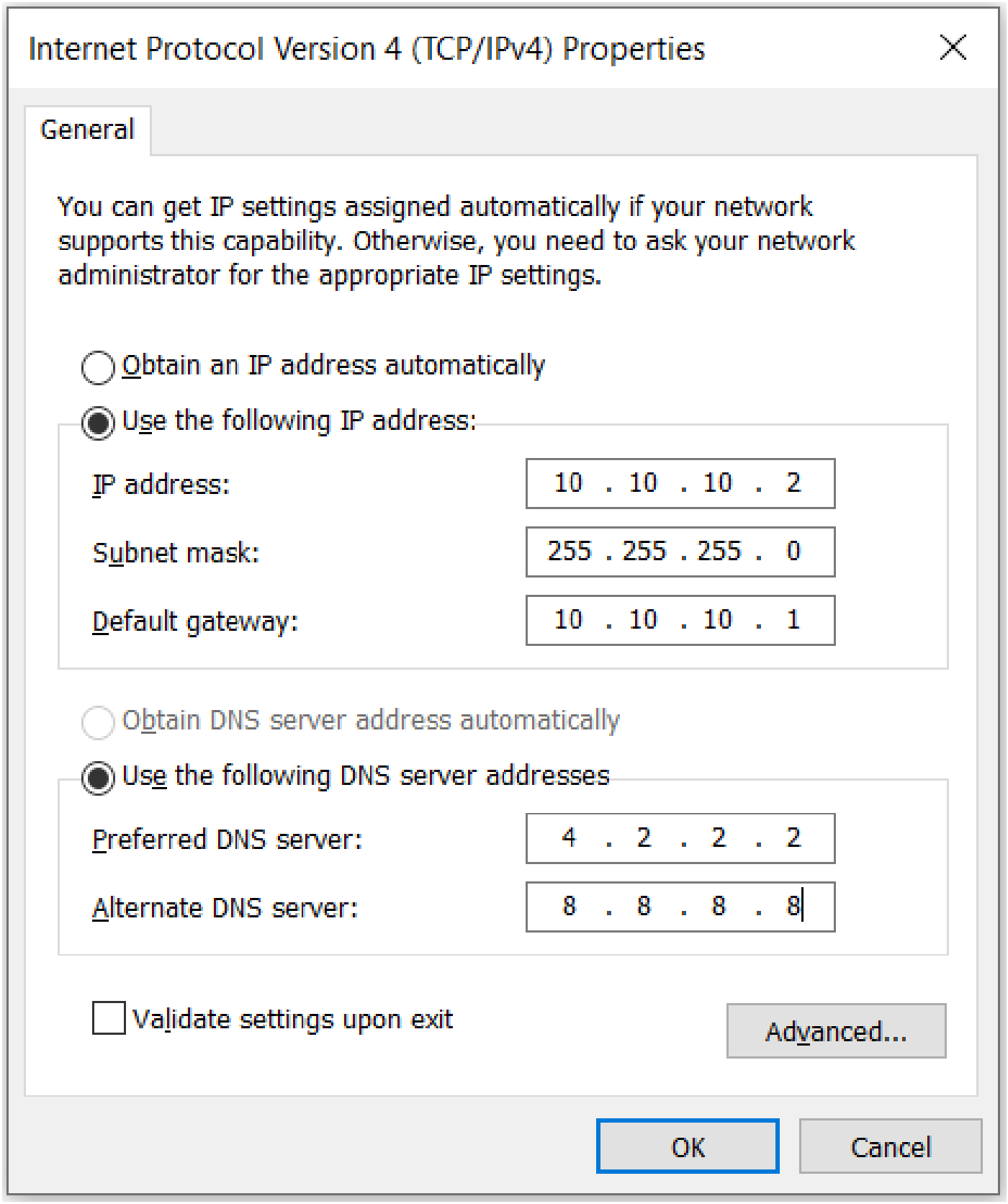


背景信息

在ASA上配置多个完全限定域名(FQDN)对象时，尝试访问FQDN对象中定义的任何URL的最终用户将观察ASA发送的多个DNS查询。本文档旨在更好地理解为什么会观察到此类行为。

配置

为进行DNS解析，客户端PC配置了这些IP、子网掩码和名称服务器。



在ASA上，配置了两个接口：一个安全级别为100的内部接口（PC连接到该接口），另一个外部接口（连接到互联网）。

```
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)#
```

这里，Gig0/1接口是接口IP为10.197.223.9的外部接口，而Gig0/3接口是接口IP为10.10.10.1的内部接口，并且连接到另一端的PC。

```
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
```

在ASA上配置DNS设置，如下所示：

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

为www.facebook.com、www.google.com、www.instagram.com和www.twitter.com配置4个FQDN对象。

```
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
```

在ASA外部接口上设置捕获，以捕获DNS流量。然后，从客户端PC尝试从浏览器访问 www.google.com。

你观察什么？请看数据包捕获。

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

此处我们看到，即使我们尝试仅解析www.google.com，也会发出针对所有FQDN对象的DNS查询。

现在看看DNS缓存如何用于ASA上的IP，了解为什么会发生这种情况。

- 在客户端PC的Web浏览器中键入www.google.com时，PC会发出DNS查询以获得解析为IP地址的URL。

- 然后，DNS服务器解析PC请求，并返回表明google.com位于指定位置的IP。
- 然后，PC发起到google.com解析IP地址的TCP连接。但是，当数据包到达ASA时，它没有表明允许或拒绝指定IP的ACL规则。
- 但是，ASA知道它有4个FQDN对象，并且任何FQDN对象都可能解析为相关的IP。
- 因此，ASA会针对所有FQDN对象发出DNS查询，因为它不知道哪个FQDN对象可以解析到相关的IP。（这就是观察到多个DNS查询的原因）。
- DNS服务器使用相应的IP地址解析FQDN对象。FQDN对象可以解析为客户端解析的同一公有IP地址。否则，ASA会为客户端尝试到达的不同IP地址创建动态访问列表条目，因此ASA最终丢弃数据包。例如，如果用户将google.com解析为203.0.113.1，并且ASA将其解析为203.0.113.2，则ASA会为203.0.113.2创建新的动态访问列表条目，用户将无法访问网站。
- 当下一次请求到达时（请求解析特定IP），如果该特定IP存储在ASA上，它不会再次查询所有FQDN对象，因为此时会存在动态ACL条目。
- 如果客户端担心ASA发送的大量DNS查询，请增加DNS计时器到期时间，并且假设终端主机尝试访问DNS缓存中的目标IP地址。如果PC请求的IP未存储在ASA DNS缓存中，则会发送DNS查询以解析所有FQDN对象。
- 如果要减少DNS查询的数量，一个可能的解决方法是减少FQDN对象的数量或定义要将FQDN解析到的整个公共IP范围，但这首先会破坏FQDN对象的用途。Cisco Firepower威胁防御(FTD)是处理此使用案例的更好解决方案。

验证

要验证每个FQDN对象解析到的ASA DNS缓存中存在哪些IP，可以使用命令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
```

相关信息

[思科技术支持和下载]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。