瞭解使用FQDN對象時ASA上的DNS操作

目錄

簡介

本檔案介紹使用FDQN對象時，網域名稱系統(DNS)在思科調適型安全裝置(ASA)上的運作方式。

必要條件

需求

思科建議您瞭解Cisco ASA。

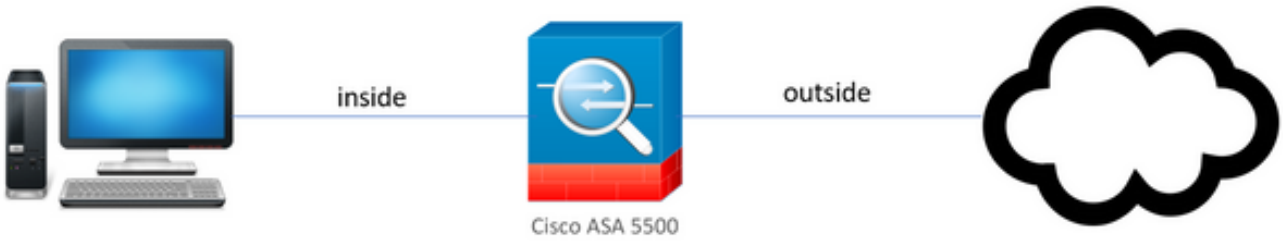
採用元件

為了說明在模擬生產環境中在ASA上配置多個FQDN時DNS的運行情況，設定了一個ASAv，該ASAv具有一個面向網際網路的介面和一個連線到ESXi伺服器上託管的PC裝置的介面。此模擬使用ASAv臨時代碼9.8.4(10)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表

拓撲設定如下所示。

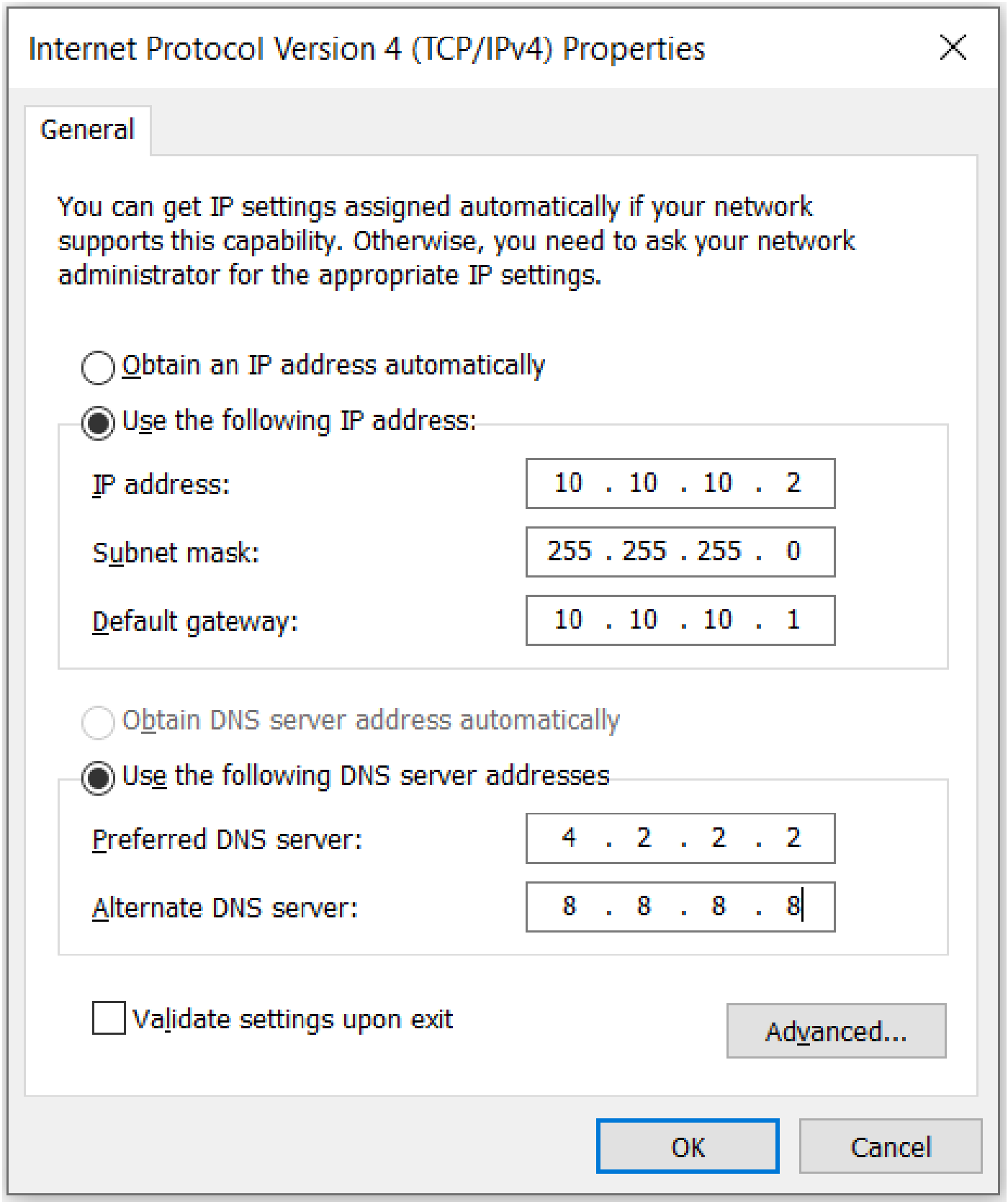


背景資訊

在ASA上配置多個完全限定的域名(FQDN)對象時，嘗試訪問FQDN對象中定義的任何URL的終端使用者將觀察ASA傳送的多個DNS查詢。本文旨在更好地瞭解為什麼會觀察到這種行為。

設定

客戶端PC配置了這些IP、子網掩碼和名稱伺服器以進行DNS解析。



在ASA上配置了兩個介面：一個內部介面，其安全級別為100,PC連線到該介面；一個外部介面，其連線到網際網路。

```
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)#
```

這裡，Gig0/1介面是介面IP為10.197.223.9的外部介面，而Gig0/3介面是介面IP為10.10.10.1的內部介面，並且連線到另一端的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設定，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)#
```

為www.facebook.com、www.google.com、www.instagram.com和www.twitter.com配置4個FQDN對象。

```
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外部介面上設定捕獲以捕獲DNS流量。然後在客戶端PC上，嘗試從瀏覽器訪問 www.google.com。

你觀察什麼？請看一下封包擷取。

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

此處我們發現，即使我們嘗試只解析www.google.com，也會針對所有FQDN對象發出DNS查詢。

現在，請檢視DNS快取如何用於ASA上的IP，以瞭解發生這種情況的原因。

- 在客戶端PC的Web瀏覽器中鍵入www.google.com時，PC會發出DNS查詢，以獲取URL解析為IP地址。
- 然後，DNS伺服器會解析PC請求，並返回一個IP，表明google.com位於指定位置。

- 然後PC發起與google.com解析IP地址的TCP連線。但是，當資料包到達ASA時，它沒有表明允許或拒絕指定IP的ACL規則。
- 但是，ASA知道它有4個FQDN對象，並且任何FQDN對象都可能解析為相關IP。
- 因此，ASA會傳送所有FQDN對象的DNS查詢，因為它不知道哪個FQDN對象可以解析到相關的IP。（這就是觀察到多個DNS查詢的原因）。
- DNS伺服器使用相應的IP地址解析FQDN對象。FQDN對象可以解析為客戶端解析的同一公共IP地址。否則，ASA會為與客戶端嘗試到達的IP地址不同的IP地址建立動態訪問清單條目，因此ASA最終丟棄資料包。例如，如果使用者將google.com解析為203.0.113.1，並且ASA將其解析為203.0.113.2，則ASA會為203.0.113.2建立新的動態訪問清單條目，使用者將無法訪問該網站。
- 下次當請求到達時（請求特定IP的解析度），如果該特定IP儲存在ASA上，它將不再查詢所有FQDN對象，因為此時將存在動態ACL條目。
- 如果客戶端擔心ASA傳送的大量DNS查詢，請增加DNS計時器到期時間，並且如果終端主機嘗試訪問DNS快取中的目標IP地址。如果PC請求的IP不儲存在ASA DNS快取中，則會傳送DNS查詢以解析所有FQDN對象。
- 如果要減少DNS查詢數量，一個可能的解決方法是減少FQDN對象數量或定義將將FQDN解析到的整個公共IP範圍，但這首先會破壞FQDN對象的用途。Cisco Firepower威脅防禦(FTD)是處理此使用案例的更好解決方案。

驗證

為了驗證每個FQDN對象解析到的ASA DNS快取中存在哪些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
```

相關資訊

思科技術支援和下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。