FQDNオブジェクトを使用する場合のASAでのDNSの動作について

内容

はじめに

このドキュメントでは、FDQNオブジェクトを使用する場合のCisco適応型セキュリティアプライアンス(ASA)でのドメインネームシステム(DNS)の動作について説明します。

前提条件

要件

Cisco ASAに関する知識があることが推奨されます。

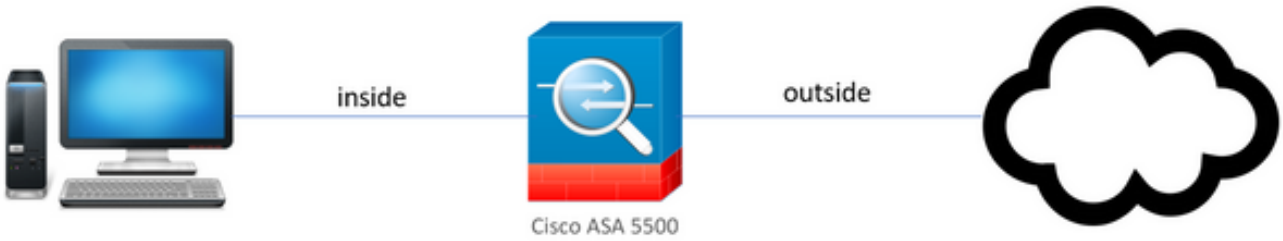
使用するコンポーネント

シミュレートされた実稼働環境のASAで複数のFQDNが設定されている場合のDNSの動作を明らかにするために、1つのインターフェイスがインターネットに面し、1つのインターフェイスがESXiサーバでホストされるPCデバイスに接続されたASAvをセットアップしました。このシミュレーションでは、ASAv中間コード9.8.4(10)が使用されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

トポロジの設定を次に示します。

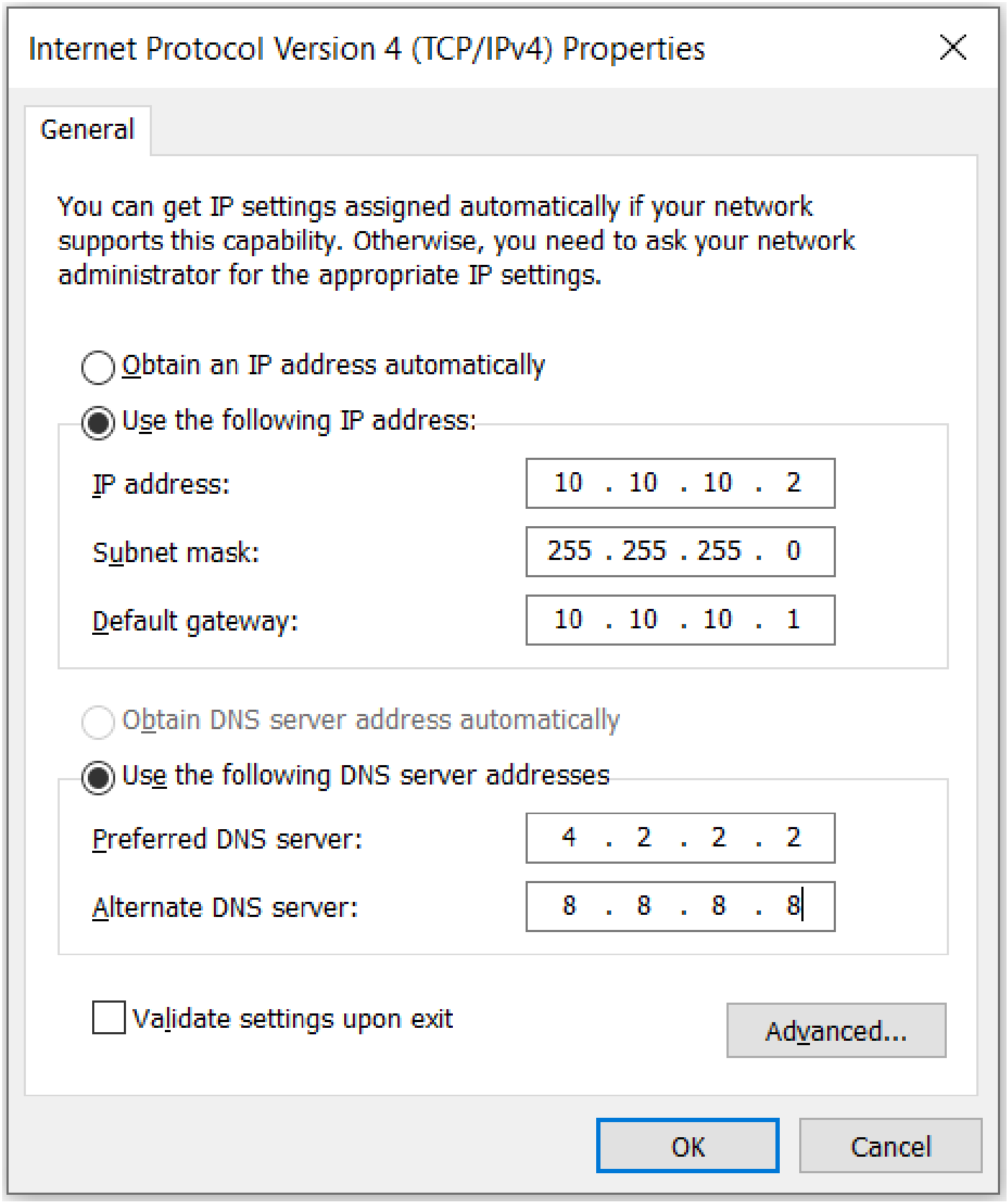


背景説明

ASAで複数の完全修飾ドメイン名(FQDN)オブジェクトが設定されている場合、FQDNオブジェクトで定義されているいずれかのURLにアクセスしようとするエンドユーザは、ASAによって送信された複数のDNSクエリを確認します。このドキュメントの目的は、このような動作が観察される理由について、より詳細に理解することです。

設定

クライアントPCは、DNS解決のためにこれらのIP、サブネットマスク、およびネームサーバで設定されました。



ASAでは、2つのインターフェイスが設定されています。1つはPCが接続されたセキュリティレベル100の内部インターフェイス、もう1つはインターネットに接続できる外部インターフェイスです。

```
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)#
```

Gig0/1インターフェイスはインターフェイスIPが10.197.223.9の外部インターフェイスで、Gig0/3インターフェイスはインターフェイスIPが10.10.10.1の内部インターフェイスで、もう一方の端のPCに接続されています。

```
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
```

次に示すように、ASAでDNS設定を行います。

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

www.facebook.com、www.google.com、www.instagram.com、およびwww.twitter.comに対して4つのFQDNオブジェクトを設定します。

```
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
```

DNSトラフィックをキャプチャするために、ASAのOutsideインターフェイスでキャプチャを設定します。次に、クライアントPCで、ブラウザからwww.google.comへのアクセスを試みます。

何を観察しますか。パケットキャプチャを見てください。

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

ここでは、www.google.comのみを解決しようとしたにもかかわらず、すべてのFQDNオブジェクトに対して送信されるDNSクエリがあることがわかります。

次に、ASA上のIPに対するDNSキャッシングの仕組みを見て、これが発生する理由を理解します。

- クライアントPCのWebブラウザにwww.google.comと入力すると、PCからDNSクエリが送信され、IPアドレスに解決されたURLが取得されます。

- DNSサーバはPCの要求を解決し、google.comが指定された場所にあることを示すIPを返します。

- 次に、PCはgoogle.comの解決済みIPアドレスへのTCP接続を開始します。ただし、パケットがASAに到達すると、指定されたIPが許可または拒否されることを示すACLルールは存在しません。

- ただし、ASAは4つのFQDNオブジェクトを持ち、FQDNオブジェクトのいずれかが該当するIPに解決される可能性があることを認識しています。

- したがって、ASAはすべてのFQDNオブジェクトに対してDNSクエリを送信します。これは、関係するIPに解決できるFQDNオブジェクトがASAで認識されないためです（これが複数のDNSクエリが観察される理由です）。

- DNSサーバは、FQDNオブジェクトを対応するIPアドレスで解決します。FQDNオブジェクトは、クライアントが解決したのと同じパブリックIPアドレスに解決できます。そうしないと、ASAはクライアントが到達しようとしているIPアドレスとは異なるIPアドレスのダイナミックアクセスリストエントリを作成するため、ASAはパケットを廃棄してしまいます。たとえば、ユーザがgoogle.comを203.0.113.1に解決し、ASAが203.0.113.2に解決した場合、ASAは203.0.113.2の新しいダイナミックアクセスリストエントリを作成するため、ユーザはWebサイトにアクセスできません。

- 次に要求が到着したとき、その要求は特定のIPの解決を要求します。その特定のIPがASAに保存されている場合、ダイナミックACLエントリが存在することになるため、その要求はすべてのFQDNオブジェクトに対してクエリを再実行しません。

- クライアントがASAによって送信される大量のDNSクエリについて懸念している場合は、DNSタイマーの有効期限を長くします。ただし、エンドホストがDNSキャッシュにある宛先IPアドレスにアクセスを試みる場合に限ります。PCがASA DNSキャッシュに保存されていないIPを要求すると、すべてのFQDNオブジェクトを解決するためにDNSクエリが送信されます。

- この問題を回避するには、DNSクエリの数を引き続き削減する場合は、FQDNオブジェクトの数を減らすか、FQDNを解決するパブリックIPの全範囲を定義します。ただし、最初はFQDNオブジェクトの目的が達成されません。シスコのFirepower脅威対策(FTD)は、このユースケースを処理するためのより優れたソリューションです。

確認

各FQDNオブジェクトが解決されるASAのDNSキャッシュにどのIPが存在するかを確認するには、コマンドASA# sh dnsを使用できます。

```
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
```

関連情報

[シスコテクニカルサポートおよびダウンロード]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。