FQDN 개체를 사용할 때 ASA에서 DNS 작동 이해

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소
- 네트워크 다이어그램

배경 정보

구성

다음을 확인합니다.

관련 정보

소개

이 문서에서는 FDQN 개체를 사용할 때 Cisco ASA(Adaptive Security Appliance)에서 DNS(Domain Name System)의 작동을 설명합니다.

사전 요구 사항

요구 사항

Cisco ASA에 대한 지식이 있는 것이 좋습니다.

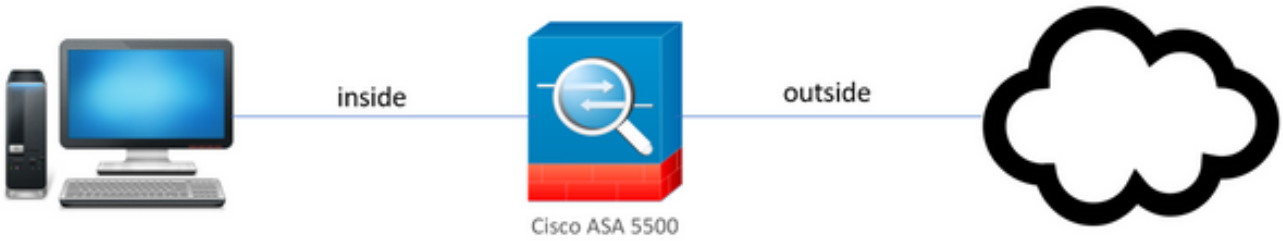
사용되는 구성 요소

시뮬레이션된 프로덕션 환경에서 ASA에 여러 FQDN이 구성된 경우 DNS의 작동을 확인하기 위해 인터넷과 마주하는 인터페이스 하나와 ESXi 서버에 호스팅된 PC 디바이스에 연결되는 인터페이스 하나가 있는 ASAv가 설정되었습니다. ASAv 중간 코드 9.8.4(10)가 이 시뮬레이션에 사용되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

토폴로지 설정이 여기에 표시됩니다.

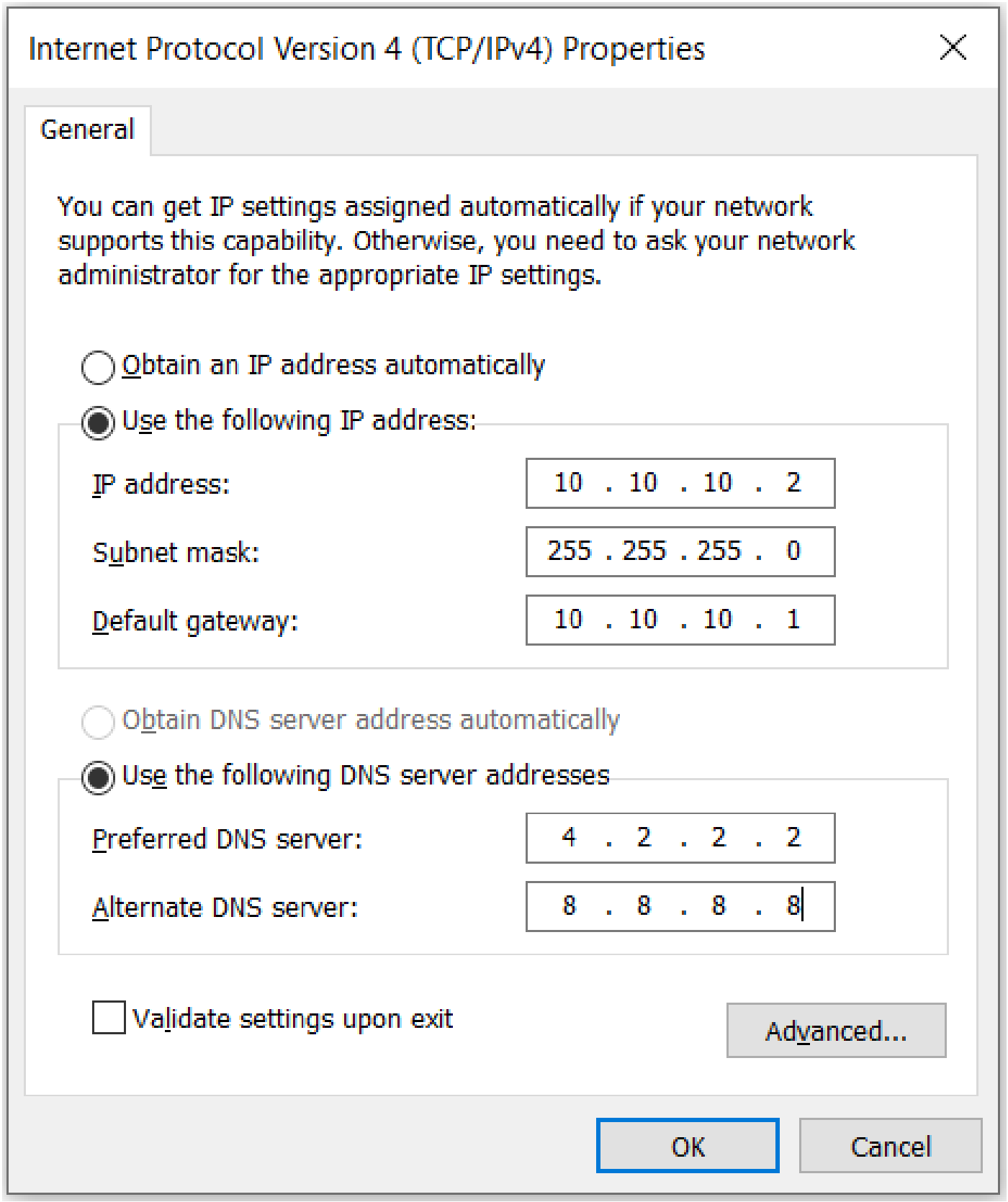


배경 정보

ASA에 여러 FQDN(Fully Qualified Domain Name) 객체가 구성된 경우, FQDN 객체에 정의된 URL에 액세스를 시도하는 최종 사용자는 ASA에서 전송된 여러 DNS 쿼리를 관찰하게 됩니다. 이 문서는 그러한 행동이 왜 관찰되는지에 대한 더 나은 이해를 제공하는 것을 목표로 한다.

구성

클라이언트 PC는 DNS 확인을 위해 이러한 IP, 서브넷 마스크 및 이름 서버로 구성되었습니다.



ASA에서는 2개의 인터페이스가 구성되었습니다. 즉, PC가 연결된 보안 수준이 100인 내부 인터페이스 1개와 인터넷에 연결된 외부 인터페이스 1개가 구성되었습니다.

```
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)#
```

여기서 Gig0/1 인터페이스는 인터페이스 IP가 10.197.223.9인 외부 인터페이스이고, Gig0/3 인터페이스는 인터페이스 IP가 10.10.10.1이고 다른 쪽 끝의 PC에 연결된 내부 인터페이스입니다.

```
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
```

다음과 같이 ASA에서 DNS 설정을 구성합니다.

```
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, www.twitter.com에 대해 4개의 FQDN 객체를 구성합니다.

```
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 트래픽을 캡처하도록 ASA 외부 인터페이스에 캡처를 설정합니다. 그런 다음 클라이언트 PC에서 브라우저에서 www.google.com에 액세스하십시오.

무엇을 관찰합니까? 패킷 캡처를 살펴봅니다.

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

여기서는 www.google.com만 확인하려고 했지만, 모든 FQDN 개체에 대해 DNS 쿼리가 전송되는 것을 확인할 수 있습니다.

이제 ASA의 IP에 대해 DNS 캐싱이 어떻게 작동하는지 살펴보고 이러한 현상이 발생하는 이유를 알아보십시오.

- 클라이언트 PC 웹 브라우저에 www.google.com을 입력하면 PC는 DNS 쿼리를 보내 URL을 IP 주소로 확인합니다.

- 그런 다음 DNS 서버는 PC 요청을 확인하고 지정된 위치에 google.com이 상주한다는 IP를 반환합니다.
- 그런 다음 PC는 google.com의 확인된 IP 주소에 대한 TCP 연결을 시작합니다. 그러나 패킷이 ASA에 도달하면 지정된 IP가 허용 또는 거부됨을 나타내는 ACL 규칙이 없습니다.
- 그러나 ASA는 4개의 FQDN 개체를 가지고 있으며 FQDN 개체 중 하나를 관련 IP로 확인할 수 있음을 알고 있습니다.
- 따라서 ASA는 어떤 FQDN 개체를 관련 IP로 확인할 수 있는지 모르기 때문에 모든 FQDN 개체에 대한 DNS 쿼리를 보냅니다(여러 DNS 쿼리가 관찰되는 이유).
- DNS 서버는 해당 IP 주소로 FQDN 개체를 확인합니다. FQDN 객체는 클라이언트에서 확인된 것과 동일한 공용 IP 주소로 확인될 수 있습니다. 그렇지 않으면 ASA는 클라이언트가 도달하려고 시도하는 IP 주소가 아닌 다른 IP 주소에 대한 동적 액세스 목록 항목을 생성합니다. 따라서 ASA는 결국 패킷을 삭제합니다. 예를 들어, 사용자가 google.com을 203.0.113.1로 확인하고 ASA가 203.0.113.2로 확인하면 ASA는 203.0.113.2에 대한 새 동적 액세스 목록 항목을 생성하며 사용자는 웹 사이트에 액세스할 수 없습니다.
- 다음에 특정 IP의 확인을 요청하는 요청이 도착하면, 해당 특정 IP가 ASA에 저장되어 있는 경우 동적 ACL 항목이 있으므로 모든 FQDN 객체를 다시 쿼리하지 않습니다.
- 클라이언트가 ASA에서 보낸 많은 수의 DNS 쿼리에 대해 우려하는 경우 DNS 타이머 만료를 늘리고, 제공된 종단 호스트가 DNS 캐시에 있는 대상 IP 주소에 액세스하려고 시도합니다. PC에서 ASA DNS 캐시에 저장되지 않은 IP를 요청하는 경우, 모든 FQDN 객체를 확인하기 위해 DNS 쿼리가 전송됩니다.
- DNS 쿼리 수를 계속 줄이려면 FQDN 개체의 수를 줄이거나 FQDN을 확인할 공용 IP의 전체 범위를 정의해야 합니다. 그러나 이 경우 FQDN 개체의 목적을 처음부터 달성할 수 없습니다. Cisco Firepower FTD(Threat Defense)는 이 활용 사례를 처리하는 데 더 적합한 솔루션입니다.

다음을 확인합니다.

각 FQDN 개체가 확인되는 ASA DNS 캐시에 어떤 IP가 있는지 확인하기 위해 ASA# sh dns 명령을 사용할 수 있습니다.

```
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
```

관련 정보

Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.