Verständnis des Betriebs von DNS auf ASA bei Verwendung von FQDN-Objekten

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Netzwerkdiagramm](#)
[Hintergrundinformationen](#)
[Konfigurieren](#)
[Überprüfung](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Betrieb des Domain Name System (DNS) auf der Cisco Adaptive Security Appliance (ASA) bei Verwendung von FDQN-Objekten beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco ASA verfügen.

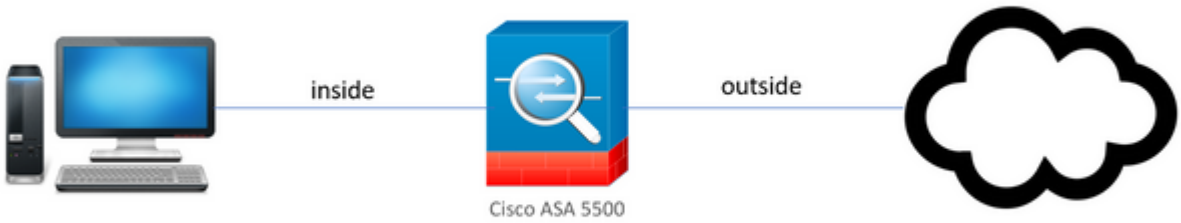
Verwendete Komponenten

Um die Funktionsweise des DNS bei der Konfiguration mehrerer FQDNs auf der ASA in einer simulierten Produktionsumgebung zu verdeutlichen, wurde eine ASAv mit einer Schnittstelle zum Internet und einer Schnittstelle, die mit einem auf dem ESXi-Server gehosteten PC-Gerät verbunden ist, eingerichtet. Für diese Simulation wurde der ASAv-Zwischencode 9.8.4(10) verwendet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Die Topologie-Konfiguration ist hier dargestellt.

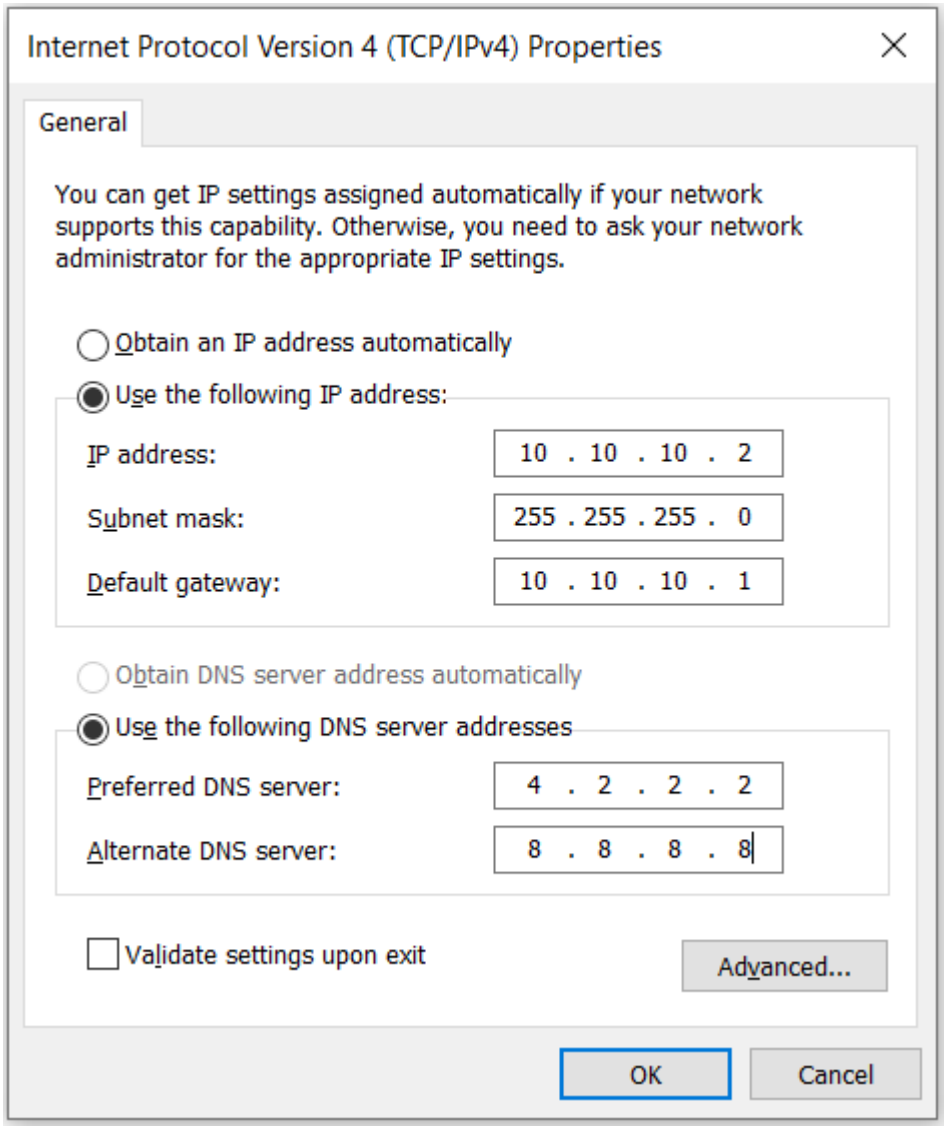


Hintergrundinformationen

Wenn auf einem ASA mehrere vollqualifizierte Domänennamensobjekte (FQDN) konfiguriert werden, überwacht ein Endbenutzer, der versucht, auf eine der in den FQDN-Objekten definierten URLs zuzugreifen, mehrere von der ASA gesendete DNS-Abfragen. Ziel dieses Dokuments ist es, besser zu verstehen, warum ein solches Verhalten beobachtet wird.

Konfigurieren

Auf dem Client-PC wurden diese IP-Adressen, Subnetzmasken und Namensserver für die DNS-Auflösung konfiguriert.



Auf der ASA wurden zwei Schnittstellen konfiguriert: eine interne Schnittstelle mit einer Sicherheitsstufe von 100, mit der der PC verbunden war, und eine externe Schnittstelle, die über eine Verbindung zum Internet verfügt.

```
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)#
```

Hier ist die Gig0/1-Schnittstelle die externe Schnittstelle mit einer Schnittstellen-IP-Adresse von 10.197.223.9, und die Gig0/3-Schnittstelle ist die interne Schnittstelle mit einer Schnittstellen-IP-Adresse von 10.10.10.1 und mit dem PC am anderen Ende verbunden.

```
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
```

Konfigurieren Sie das DNS-Setup auf der ASA wie folgt:

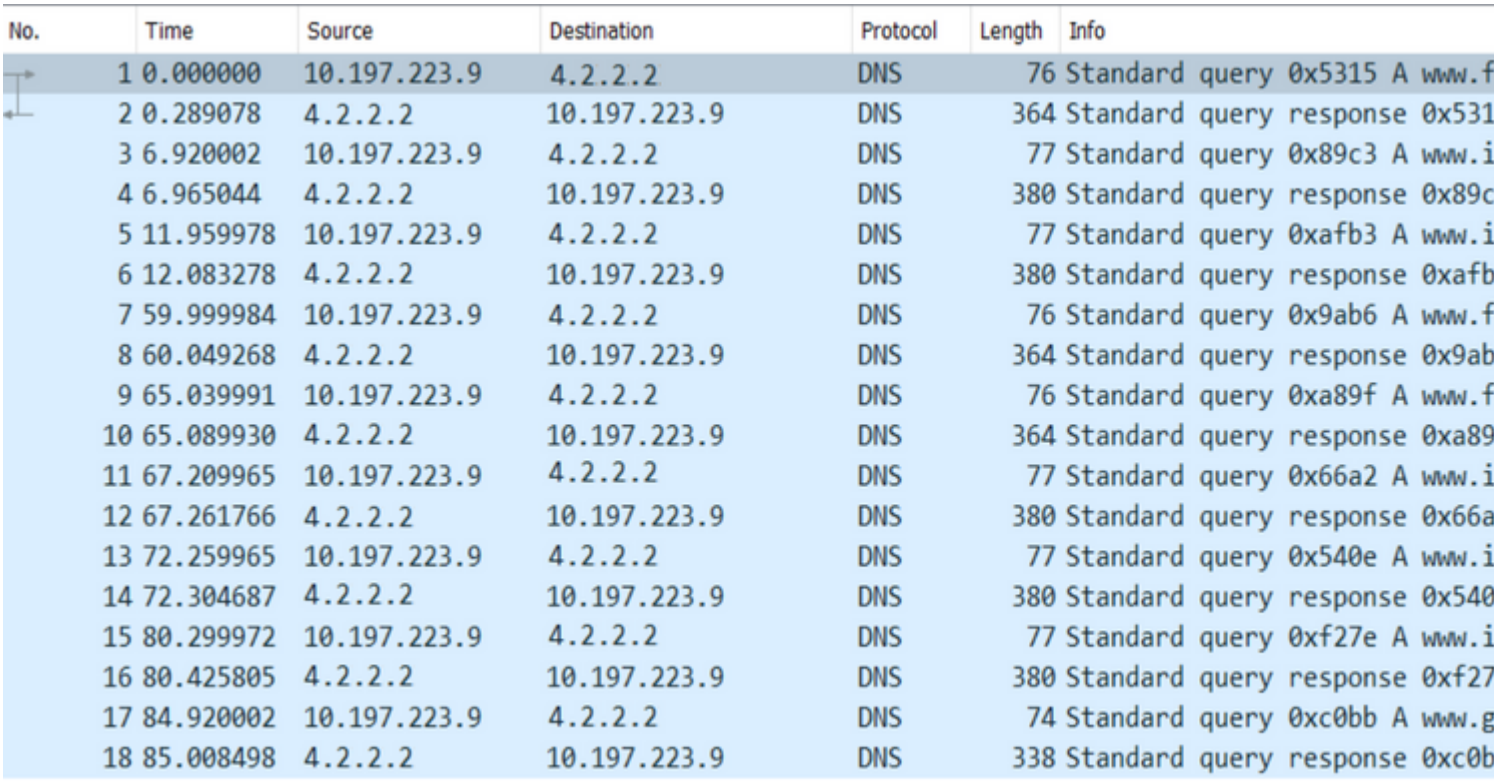
```
ciscoasa(config)# sh run dns
dns domain-lookup outside
DNS server-group DefaultDNS
    name-server 4.2.2.2
ciscoasa(config)#
```

Konfigurieren Sie vier FQDN-Objekte für www.facebook.com, www.google.com, www.instagram.com und 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
```

Richten Sie auf der externen ASA-Schnittstelle eine Erfassung ein, um den DNS-Verkehr zu erfassen. Versuchen Sie dann, vom Client-PC aus über einen Browser auf www.google.com zuzugreifen.

Was beobachten Sie? Sehen Sie sich die Paketerfassung an.



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

Hier sehen wir, dass, obwohl wir nur versucht haben, www.google.com aufzulösen, für alle FQDN-Objekte DNS-Abfragen gesendet wurden.

Sehen Sie sich nun an, wie DNS-Caching für IPs auf der ASA funktioniert, um zu verstehen, warum dies geschieht.

- Wenn www.google.com in den Webbrowser des Client-PCs eingegeben wird, sendet der PC eine DNS-Abfrage, um die URL in eine IP-Adresse aufzulösen.
- Der DNS-Server löst dann die PC-Anforderung auf und gibt eine IP-Adresse zurück, die google.com angibt und sich am angegebenen Speicherort befindet.
- Der PC initiiert dann eine TCP-Verbindung zur aufgelösten IP-Adresse von google.com. Wenn das

Paket jedoch die ASA erreicht, verfügt es nicht über eine ACL-Regel, die besagt, dass die angegebene IP zulässig ist oder abgelehnt wird.

- Die ASA weiß jedoch, dass sie über 4 FQDN-Objekte verfügt und dass eines der FQDN-Objekte möglicherweise in die betreffende IP aufgelöst werden kann.
- Daher sendet die ASA DNS-Abfragen für alle FQDN-Objekte, da sie nicht weiß, welches FQDN-Objekt an die betreffende IP aufgelöst werden kann. (Aus diesem Grund wurden mehrere DNS-Abfragen beobachtet.)
- Der DNS-Server löst die FQDN-Objekte mit den entsprechenden IP-Adressen auf. Das FQDN-Objekt kann mit derselben öffentlichen IP-Adresse aufgelöst werden, die auch vom Client aufgelöst wurde. Andernfalls erstellt die ASA einen dynamischen Zugriffslisteneintrag für eine andere IP-Adresse als die, die der Client zu erreichen versucht. Daher verwirft die ASA das Paket. Wenn der Benutzer beispielsweise google.com in 203.0.113.1 aufgelöst hat und die ASA dies in 203.0.113.2 auflöst, erstellt die ASA einen neuen dynamischen Zugriffslisteneintrag für 203.0.113.2, und der Benutzer kann nicht auf die Website zugreifen.
- Wenn das nächste Mal eine Anforderung eingeht, die die Auflösung einer bestimmten IP anfordert, fragt diese, wenn diese bestimmte IP auf der ASA gespeichert ist, nicht mehr alle FQDN-Objekte ab, da nun ein dynamischer ACL-Eintrag vorhanden wäre.
- Wenn ein Client Bedenken hinsichtlich der großen Anzahl von DNS-Abfragen hat, die von der ASA gesendet werden, erhöhen Sie das Ablaufdatum des DNS-Timers, und der bereitgestellte End-Host versucht, auf die Ziel-IP-Adressen zuzugreifen, die sich im DNS-Cache befinden. Wenn der PC eine IP anfordert, die nicht im DNS-Cache der ASA gespeichert ist, werden DNS-Abfragen gesendet, um alle FQDN-Objekte aufzulösen.
- Wenn Sie die Anzahl der DNS-Abfragen dennoch reduzieren möchten, wäre eine mögliche Problemumgehung, entweder die Anzahl der FQDN-Objekte zu reduzieren oder den gesamten Bereich der öffentlichen IPs zu definieren, zu denen Sie den FQDN auflösen würden, was jedoch den Zweck eines FQDN-Objekts von vornherein umgeht. Cisco FirePOWER Threat Defense (FTD) ist die bessere Lösung für diesen Anwendungsfall.

Überprüfung

Um zu überprüfen, welche IPs im DNS-Cache der ASAs vorhanden sind, in den jedes der FQDN-Objekte aufgelöst wird, kann der Befehl **ASA# sh dns** verwendet werden.

```
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
```

Zugehörige Informationen

Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.