De werking van DNS op ASA begrijpen wanneer FQDN-objecten worden gebruikt

Inhoud

Inleiding

Dit document beschrijft de werking van Domain Name System (DNS) op Cisco adaptieve security applicatie (ASA) wanneer FDQN-objecten worden gebruikt.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco ASA.

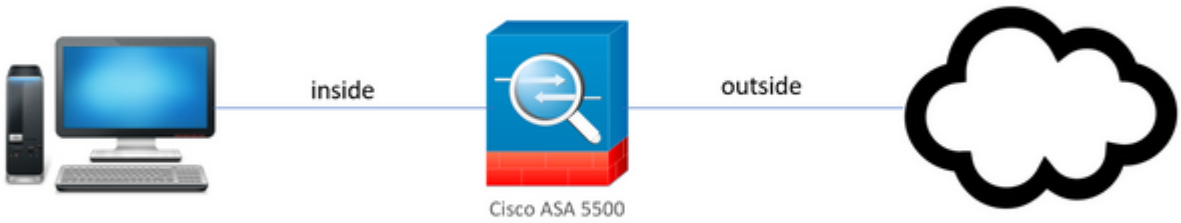
Gebruikte componenten

Om de werking van de DNS te verduidelijken wanneer in een gesimuleerde productieomgeving meerdere FQDNâ€™s op de ASA zijn geconfigureerd, is een ASAv ingesteld met één interface met het internet en één interface die is aangesloten op een pc-apparaat dat op de ESXi-server wordt gehost. Voor deze simulatie werd de ASAv interim code 9.8.4(10) gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram

De topologieopstelling wordt hier getoond.

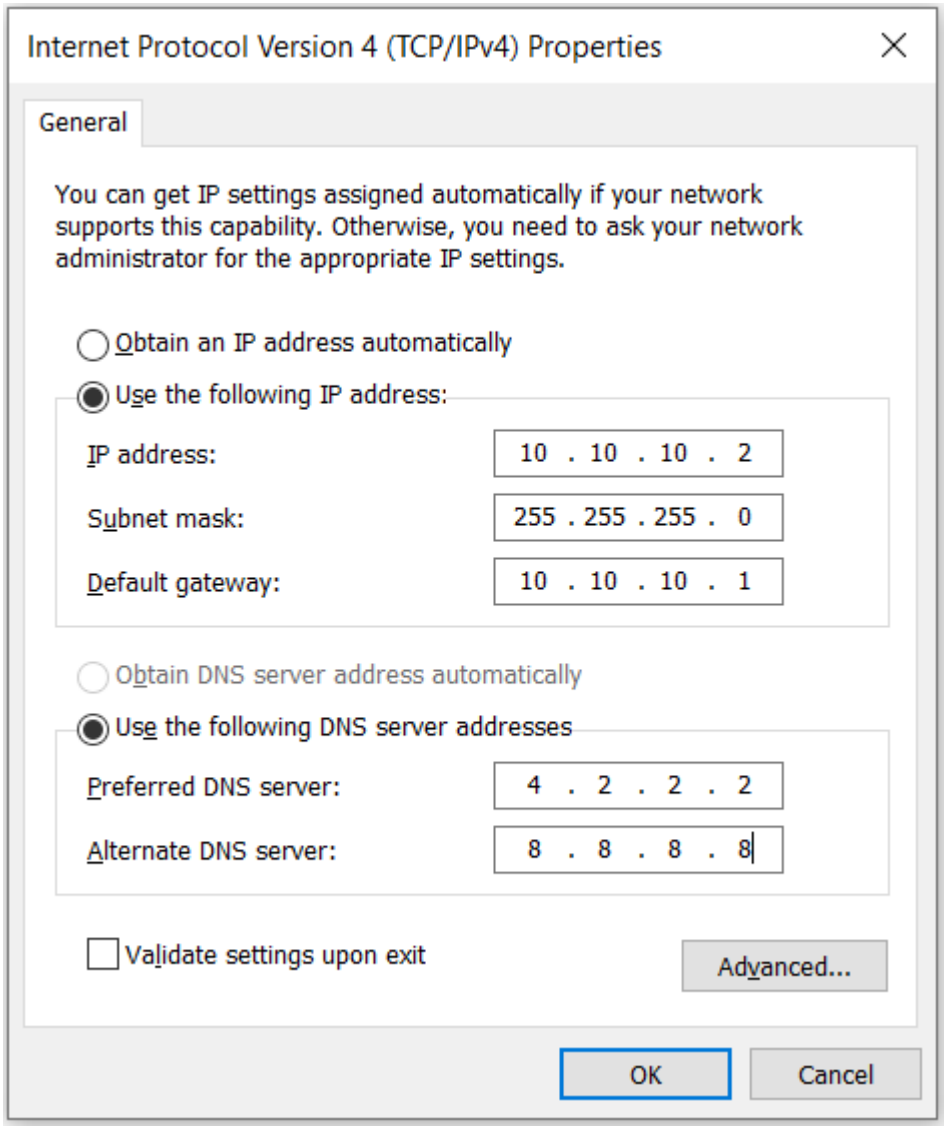


Achtergrondinformatie

Wanneer meerdere FQDN-objecten (Fully Qualified Domain Name) op een ASA zijn geconfigureerd, zou een eindgebruiker die probeert toegang te krijgen tot een van de URLâ€™s die in de FQDN-objecten zijn gedefinieerd, meerdere DNS-vragen waarnemen die door de ASA zijn verzonden. Dit document is bedoeld om beter te begrijpen waarom dit soort gedrag wordt waargenomen.

Configureren

De client-pc is geconfigureerd met deze IP-, subnetmasker- en naamservers voor DNS-resolutie.



Op de ASA waren twee interfaces geconfigureerd, 1 binneninterface met een beveiligingsniveau van 100 waarmee de PC was verbonden en 1 buiteninterface die verbinding met het internet heeft.

```
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 is de Gig0/1 interface de buiteninterface met een interface IP van 10.197.223.9 en de Gig0/3 interface is de binneninterface met een interface IP van 10.10.10.1 en verbonden met PC op het andere eind.

```
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
```

Configureer de DNS-instelling op de ASA zoals hier wordt getoond:

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

Configureer 4 FQDN-objecten voor www.facebook.com, www.google.com, www.instagram.com en 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
```

Stel een opname in op de ASA buiteninterface om DNS-verkeer op te nemen. Probeer vervolgens vanaf de client-pc www.google.com te openen vanuit een browser.

Wat observeer je? Neem een kijkje bij de pakketopname.

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 zien we dat hoewel we alleen www.google.com probeerden op te lossen, er DNS-vragen werden verzonden voor alle FQDN-objecten.

Kijk nu hoe DNS-caching werkt voor IP's op de ASA om te begrijpen waarom dit gebeurt.

- Wanneer www.google.com wordt getypt in de webbrowser van de client-pc's, stuurt de pc een DNS-query om de URL opgelost te krijgen naar een IP-adres.
- De DNS-server lost vervolgens het PC-verzoek op en geeft een IP-adres terug dat aangeeft dat google.com zich op de opgegeven locatie bevindt.
- De PC initieert vervolgens een TCP verbinding met het opgeloste IP-adres van google.com. Wanneer het pakket echter de ASA bereikt, heeft het geen ACL-regel die aangeeft dat het opgegeven IP is toegestaan of geweigerd.
- De ASA weet echter dat het 4 FQDN-objecten heeft en dat elk van de FQDN-objecten mogelijk kan worden opgelost aan de betreffende IP.
- Vandaar stuurt de ASA DNS-vragen voor alle FQDN-objecten omdat het niet weet welk FQDN-object kan worden opgelost voor het betreffende IP. (Daarom zijn er meerdere DNS-vragen waargenomen).
- De DNS-server lost de FQDN-objecten op met de bijbehorende IP-adressen. Het FQDN-object kan worden opgelost op hetzelfde openbare IP-adres als door de client is opgelost. Anders maakt de ASA een dynamische toegangslijst voor een ander IP-adres dan het adres dat de client probeert te bereiken, waardoor de ASA het pakket laat vallen. Als de gebruiker bijvoorbeeld google.com tot 203.0.113.1 heeft opgelost en de ASA het tot 203.0.113.2 heeft opgelost, creëert de ASA een nieuwe dynamische toegangslijst voor 203.0.113.2 en heeft de gebruiker geen toegang tot de website.
- De volgende keer wanneer een verzoek aankomt, dat om resolutie van een bepaalde IP verzoekt, als dat bepaalde IP op ASA wordt opgeslagen, vraagt het niet alle FQDN voorwerpen opnieuw aangezien

een dynamische ACL ingang nu aanwezig zou zijn.

- Als een client bezorgd is over het grote aantal DNS-vragen verzonden door ASA, verhoog de DNS-timer verlopen, en opgegeven eindhosts probeert toegang te krijgen tot de IP-adressen van de bestemming die zich in het DNS-cache bevinden. Als de PC vraagt om een IP, niet opgeslagen op de ASA DNS-cache, worden DNS-vragen verzonden om alle FQDN-objecten op te lossen.

- Een mogelijke oplossing hiervoor, als u nog steeds het aantal DNS-vragen wilt verminderen, zou zijn om het aantal FQDN-objecten te verminderen of om het hele bereik van openbare IP's te definiëren die u zou oplossen van de FQDN-objecten, die echter het doel van een FQDN-object in de eerste plaats verslaat. Cisco Firepower Threat Defence (FTD) is een betere oplossing voor deze use case.

Verifiëren

Om te verifiëren welke IP's aanwezig zijn in de ASA DNS cache waaraan elk van de FQDN-objecten wordt opgelost, kan de opdracht **ASA# sh dns** worden gebruikt.

```
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
```

Gerelateerde informatie

Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.