Comprendere il funzionamento del DNS sull'appliance ASA quando vengono utilizzati oggetti FQDN

Sommario

Introduzione

In questo documento viene descritto il funzionamento del DNS (Domain Name System) su ASA (Cisco Adaptive Security Appliance) quando si utilizzano oggetti FDQN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco ASA.

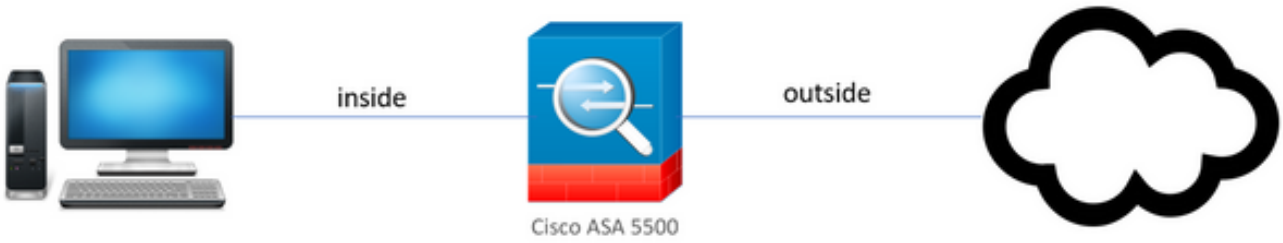
Componenti usati

Per chiarire il funzionamento del DNS quando sull'appliance ASA sono configurati più FQDN in un ambiente di produzione simulato, è stata configurata un'appliance ASAv con un'interfaccia rivolta verso Internet e un'interfaccia connessa a un dispositivo PC ospitato sul server ESXi. Per questa simulazione è stato utilizzato il codice provvisorio ASAv 9.8.4(10).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Di seguito è illustrata l'impostazione della topologia.

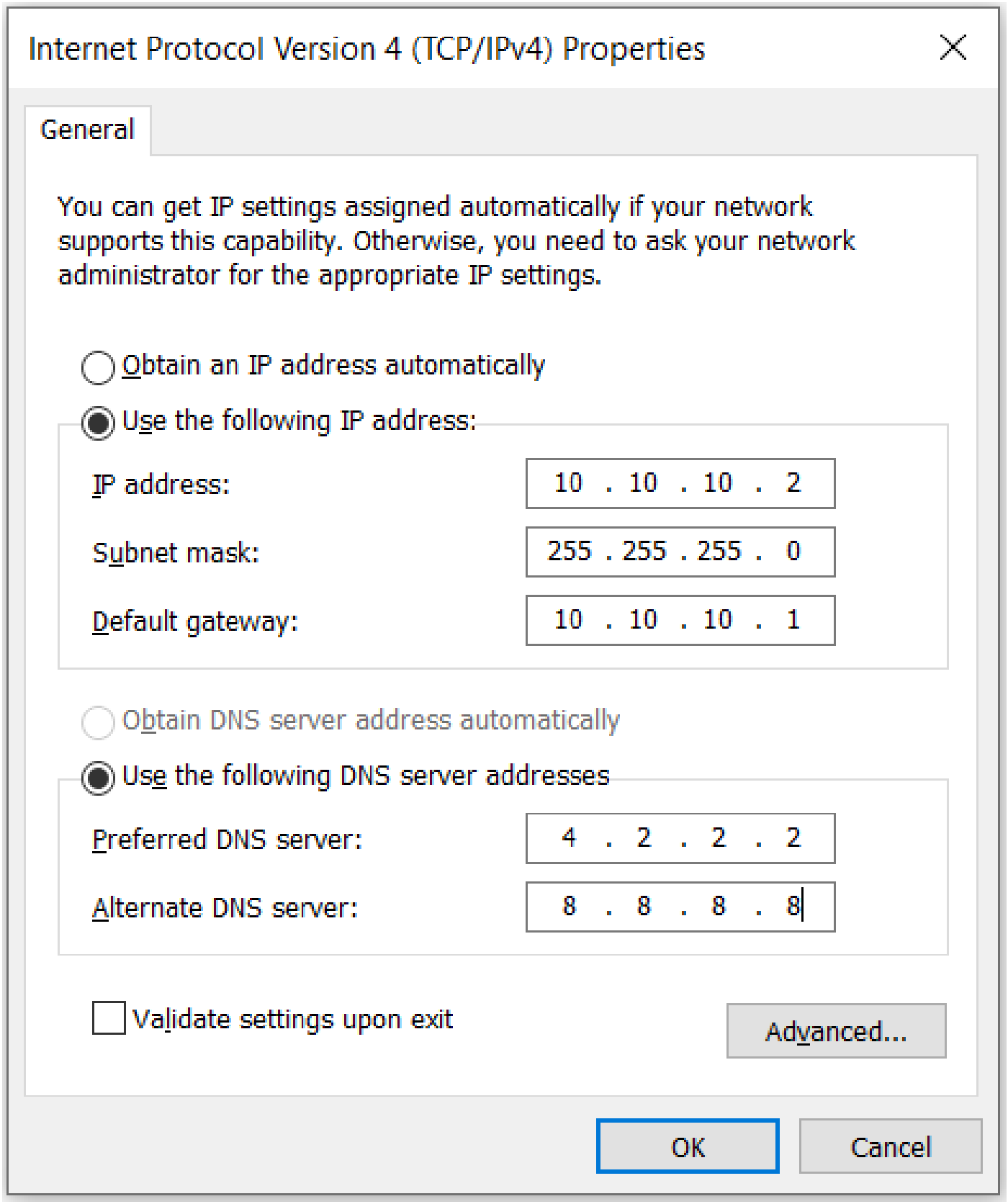


Premesse

Quando si configurano più oggetti FQDN (Fully Qualified Domain Name) su un'ASA, un utente finale che tenti di accedere a uno degli URL definiti negli oggetti FQDN osserverà più query DNS inviate dall'ASA. Il presente documento intende comprendere meglio le ragioni per cui tale comportamento è stato osservato.

Configurazione

Il PC client è stato configurato con questi IP, subnet mask e server dei nomi per la risoluzione DNS.



Sull'appliance ASA, sono state configurate due interfacce, una interna con un livello di sicurezza di 100 a cui era connesso il PC e l'altra esterna con connettività a Internet.

```
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)#
```

Qui l'interfaccia Gig0/1 è l'interfaccia esterna con un'interfaccia IP di 10.197.223.9 e l'interfaccia Gig0/3 è l'interfaccia interna con un'interfaccia IP di 10.10.10.1 e collegata al PC sull'altra estremità.

```
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
```

Configurare la configurazione DNS sull'appliance ASA come mostrato di seguito:

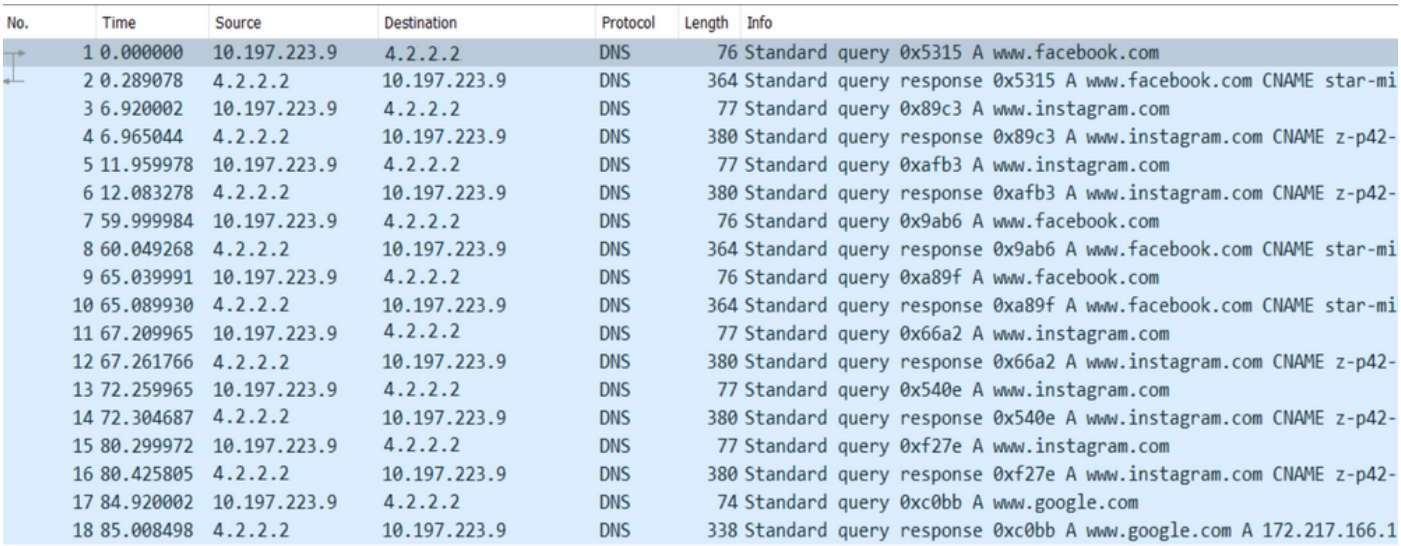
```
ciscoasa(config)# sh run dns
dns domain-lookup outside
DNS server-group DefaultDNS
    name-server 4.2.2.2
ciscoasa(config)#
```

Configurare 4 oggetti FQDN per www.facebook.com, www.google.com, www.instagram.com e 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
```

Configurare un'acquisizione sull'interfaccia esterna ASA per acquisire il traffico DNS. Quindi, dal PC client, provare ad accedere a www.google.com da un browser.

Cosa osservate? Osservate l'acquisizione dei pacchetti.



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

In questo esempio si rileva che, anche se si è tentato di risolvere solo www.google.com, sono state inviate query DNS per tutti gli oggetti FQDN.

Ora guardate come la memorizzazione nella cache DNS funziona per gli IP sull'appliance ASA per capire perché succede.

- Quando si digita www.google.com nel browser Web dei PC client, il PC invia una query DNS per risolvere l'URL in un indirizzo IP.

- Il server DNS risolve quindi la richiesta dei PC e restituisce un indirizzo IP in cui è indicato che google.com risiede nella posizione specificata.
- Il PC avvia quindi una connessione TCP all'indirizzo IP risolto di google.com. Tuttavia, quando il pacchetto raggiunge l'ASA, non ha una regola ACL che dice che l'IP specificato è autorizzato o rifiutato.
- L'ASA, tuttavia, sa di avere 4 oggetti FQDN e che qualsiasi oggetto FQDN potrebbe essere risolto nell'IP in questione.
- L'ASA invia quindi query DNS per tutti gli oggetti FQDN in quanto non sa quale oggetto FQDN può essere risolto nell'IP interessato. (Ecco perché sono state osservate più query DNS).
- Il server DNS risolve gli oggetti FQDN con gli indirizzi IP corrispondenti. L'oggetto FQDN può essere risolto nello stesso indirizzo IP pubblico risolto dal client. In caso contrario, l'ASA crea una voce dell'elenco degli accessi dinamico per un indirizzo IP diverso da quello che il client cerca di raggiungere, quindi l'ASA rifiuta il pacchetto. Ad esempio, se l'utente ha risolto google.com nella versione 203.0.113.1 e l'ASA la risolve nella versione 203.0.113.2, l'ASA crea una nuova voce dell'elenco degli accessi dinamico per la versione 203.0.113.2 e l'utente non è in grado di accedere al sito Web.
- Al successivo arrivo di una richiesta, che richiede la risoluzione di un determinato IP, se tale IP è archiviato sull'ASA, non viene più eseguita una query su tutti gli oggetti FQDN, poiché ora sarebbe presente una voce ACL dinamica.
- Se un client è preoccupato per il numero elevato di query DNS inviate dall'ASA, aumentare la scadenza del timer DNS e gli host finali forniti tentano di accedere agli indirizzi IP di destinazione presenti nella cache DNS. Se il PC richiede un indirizzo IP, non archiviato nella cache DNS dell'ASA, le query DNS vengono inviate per risolvere tutti gli oggetti FQDN.
- Per risolvere questo problema, se si desidera ridurre ancora il numero di query DNS, è possibile ridurre il numero di oggetti FQDN o definire l'intero intervallo di IP pubblici in cui risolvere l'FQDN, compromettendo tuttavia in primo luogo lo scopo di un oggetto FQDN. Cisco Firepower Threat Defense (FTD) è una soluzione migliore per gestire questo scenario.

Verifica

Per verificare quali IP sono presenti nella cache DNS delle appliance ASA e a quali oggetti FQDN vengono risolti, è possibile utilizzare il comando 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
```

Informazioni correlate

[Supporto tecnico e download Cisco]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).