DNS-doctoring op ASA Configuration Voorbeeld

Inhoud

Inleiding

Dit document laat zien hoe DNS-doctoring wordt gebruikt op de adaptieve security applicatie (ASA) om de ingesloten IP-adressen in DNS-antwoorden (Domain Name System) te wijzigen, zodat clients verbinding kunnen maken met het juiste IP-adres van servers.

Voorwaarden

Vereisten

DNS-doctoring vereist configuratie van Network Address Translation (NAT) op de ASA en inschakeling van de DNS-inspectie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de adaptieve security applicatie.

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 de potentiële impact van elke opdracht begrijpen.

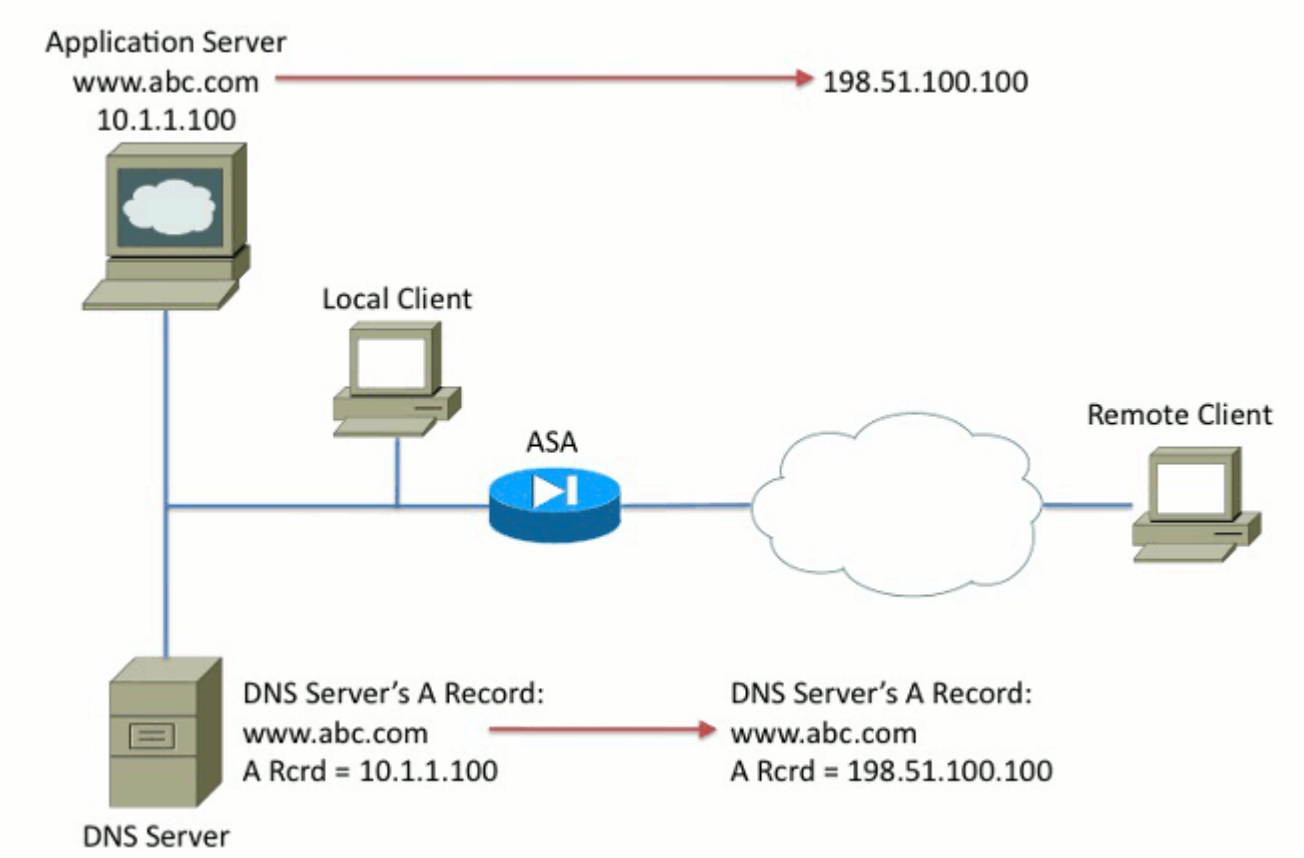
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

DNS-doctoringvoorbeelden

DNS-server binnen de ASA

Afbeelding 1



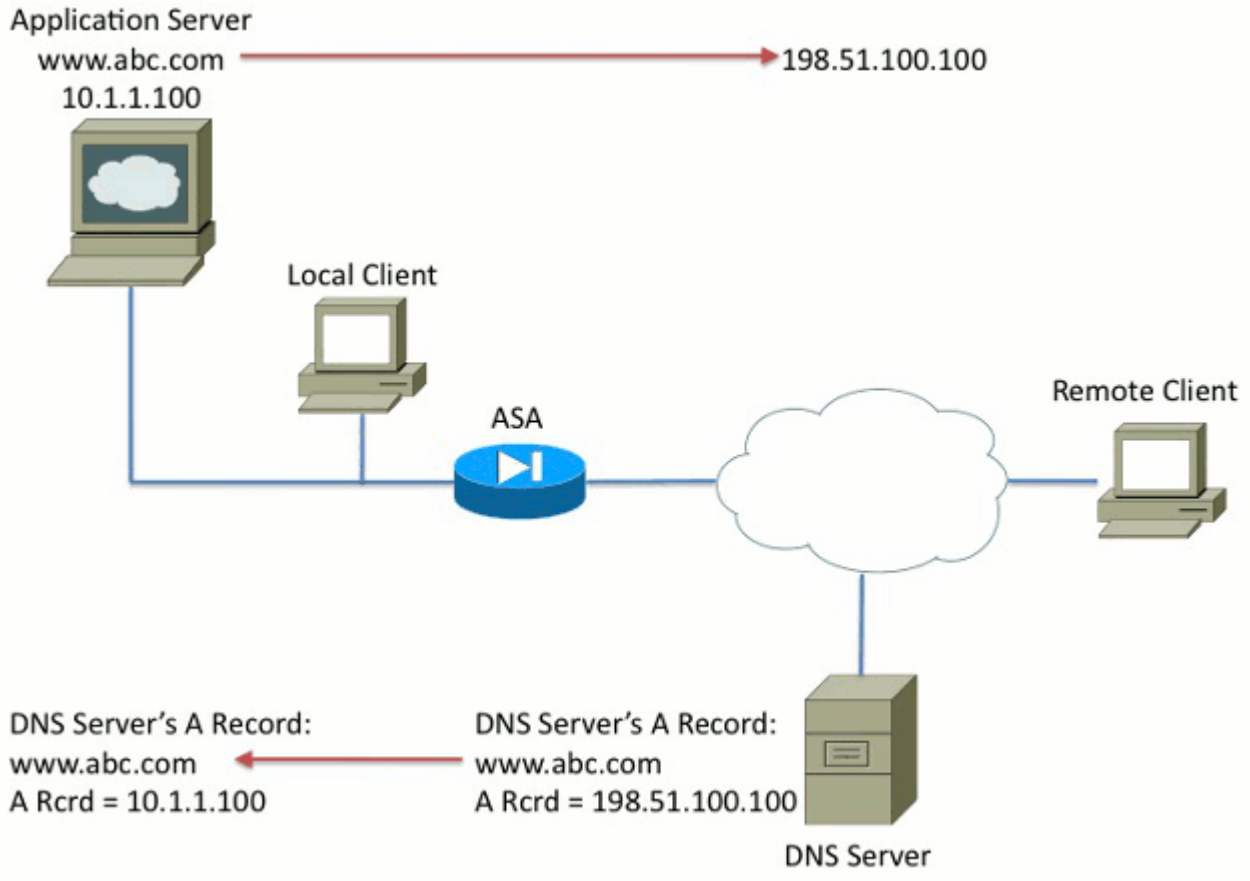

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In afbeelding 1 wordt de DNS-server bestuurd door de lokale beheerder. De DNS-server moet een privaat IP-adres opgeven, dat het *echte* IP-adres is dat aan de toepassingsserver is toegewezen. Hierdoor kan de lokale client rechtstreeks verbinding maken met de toepassingsserver.

Helaas kan de externe client geen toegang krijgen tot de toepassingsserver met het privé-adres. Als gevolg hiervan is DNS Doctoring ingesteld op de ASA om het ingesloten IP-adres in het DNS-reactiepakket te wijzigen. Dit zorgt ervoor dat wanneer de externe client een DNS-verzoek doet voor www.abc.com, de respons die ze krijgen is voor het vertaalde adres van de toepassingsserver. Zonder het DNS sleutelwoord op de NAT verklaring, probeert de verre cliënt om met 10.1.1.100 te verbinden, die niet werkt omdat dat adres niet op internet kan worden gerouteerd.

DNS-server buiten de ASA

Afbeelding 2



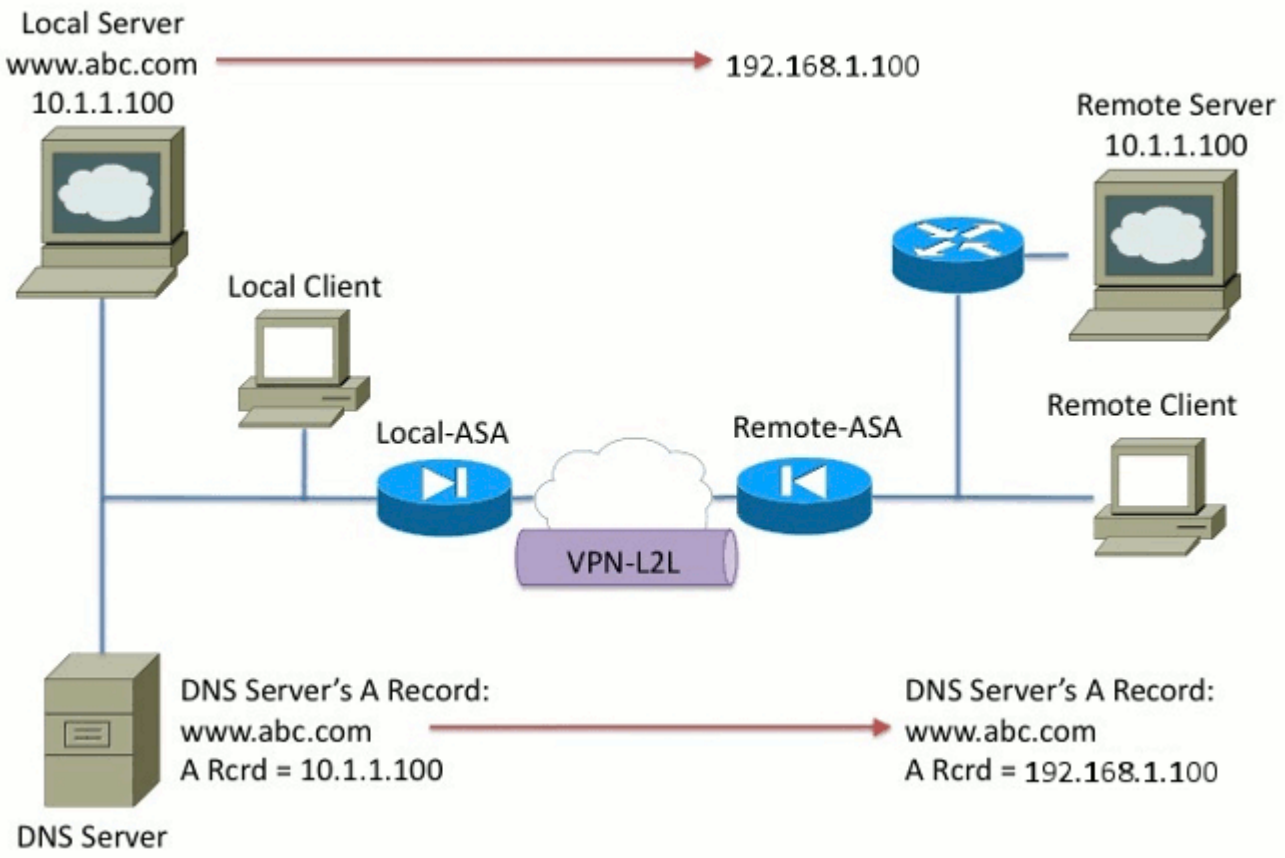

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In afbeelding 2 wordt de DNS-server bestuurd door de ISP of soortgelijke serviceprovider. De DNS-server moet het openbare IP-adres, dat wil zeggen het *vertaalde* IP-adres van de toepassingsserver, uitdelen. Hierdoor hebben alle internetgebruikers toegang tot de applicatieserver via het internet.

Helaas heeft de lokale client geen toegang tot de applicatieserver met het openbare adres. Als gevolg hiervan is DNS Doctoring ingesteld op de ASA om het ingesloten IP-adres in het DNS-reactiepakket te wijzigen. Dit zorgt ervoor dat wanneer de lokale client een DNS-verzoek doet voor www.abc.com, de ontvangen reactie het echte adres van de toepassingsserver is. Zonder het DNS sleutelwoord op de NAT verklaring, probeert de lokale cliënt om met 198.51.100.100 te verbinden. Dit werkt niet omdat dit pakket wordt verzonden naar de ASA, die het pakket laat vallen.

VPN NAT en DNS-doctoring

Afbeelding 3



Overweeg een situatie waar er netwerken zijn die overlappen. In deze situatie, het adres 10.1.1.100 leeft aan zowel de verre kant als de lokale kant. Dientengevolge, moet u NAT op de lokale server uitvoeren zodat de verre cliënt tot het met het IP adres 192.1.1.100 kan nog toegang hebben. Om dit goed te laten werken is DNS Doctoring vereist.

DNS-doctoring kan in deze functie niet worden uitgevoerd. Het DNS sleutelwoord kan alleen worden toegevoegd aan het einde van een object NAT of bron NAT. Tweemaal NAT ondersteunt het DNS-sleutelwoord niet. Er zijn twee mogelijke configuraties en beide mislukken.

Mislukte configuratie 1: Als u de onderste regel instelt, vertaalt deze 10.1.1.1 naar 192.1.1.1, niet alleen voor de externe client, maar voor iedereen op het internet. Aangezien 192.1.1.1 niet routeerbaar is op het internet, kan niemand op het internet toegang krijgen tot de lokale server.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Mislukte configuratie 2: Als u de DNS Doctoring NAT-lijn na de noodzakelijke dubbele NAT-lijn vormt, veroorzaakt dit een situatie waarin de DNS Doctoring nooit werkt. Hierdoor probeert de externe client toegang te krijgen tot www.abc.com met het IP-adres 10.1.1.100, dat niet werkt.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Gerelateerde informatie

- **Adaptieve security applicaties van Cisco ASA 5500 Series**
- **Cisco ASA 5500 Series adaptieve security applicaties > Software downloads**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

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.