DNS Doctoring en el ejemplo de configuración ASA

Contenido

Introducción

Este documento muestra cómo el DNS Doctoring se utiliza en el dispositivo de seguridad adaptante (ASA) para cambiar los IP Address incluidos en las respuestas del Domain Name System (DNS) de modo que los clientes puedan conectar con la dirección IP correcta de los servidores.

prerrequisitos

Requisitos

El DNS Doctoring requiere la configuración del Network Address Translation (NAT) en el ASA, así como la habilitación del examen DNS.

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

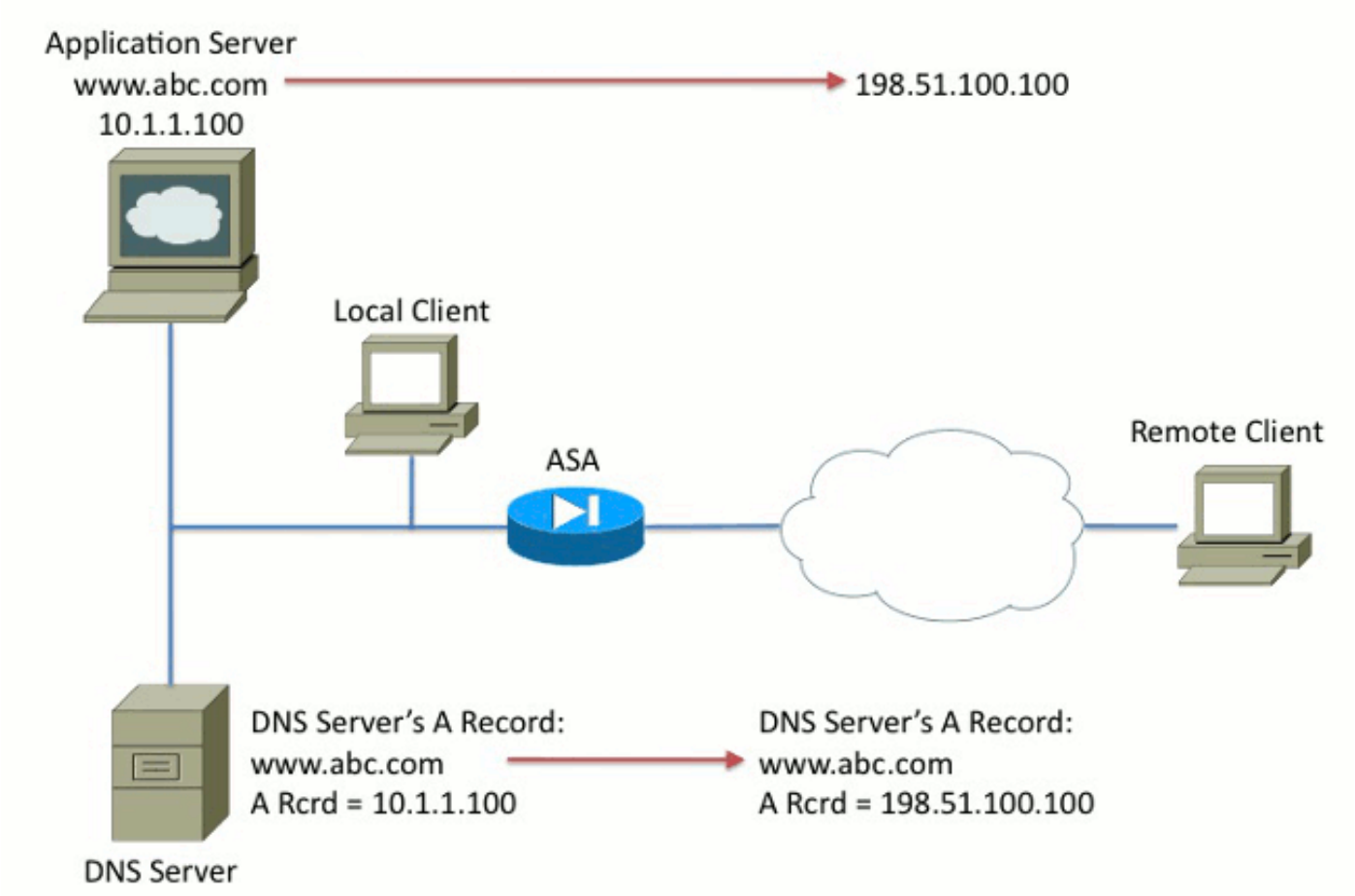
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las

convenciones del documento.

Ejemplos del DNS Doctoring

Servidor DNS en el interior del ASA

Figura 1



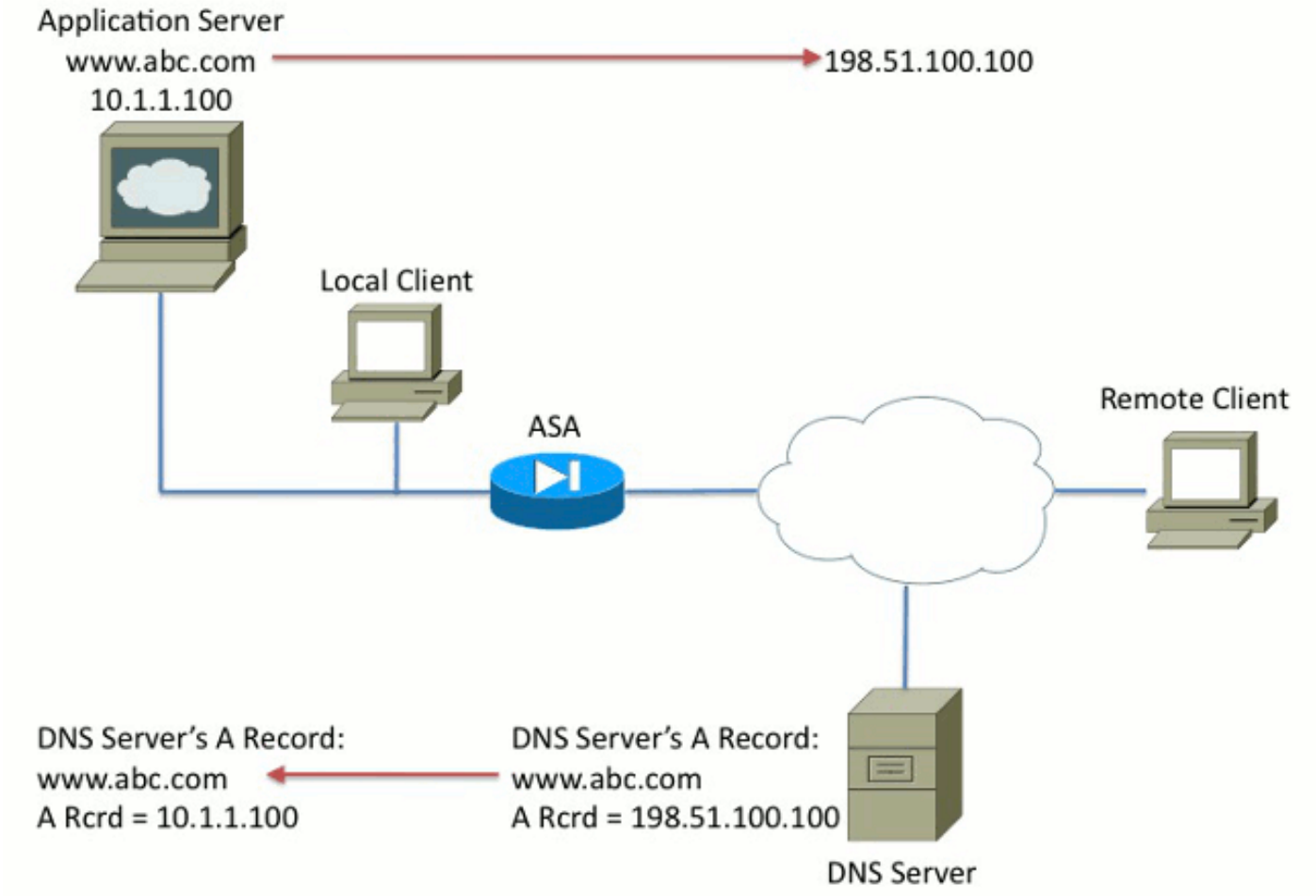

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

En el cuadro 1, al administrador local controla al servidor DNS. El servidor DNS debe distribuir un IP Address privado, que es el *IP Address real* asignado al servidor de aplicaciones. Esto permite que el cliente local conecte directamente con el servidor de aplicaciones.

Desafortunadamente, el cliente remoto no puede acceder al servidor de aplicaciones con la dirección privada. Como consecuencia, el DNS Doctoring se configura en el ASA para cambiar el IP Address incluido dentro del paquete de la respuesta de DNS. Esto se asegura de que cuando el cliente remoto hace una petición DNS para www.abc.com, la respuesta que consiguen esté para la dirección traducida del servidor de aplicaciones. Sin la palabra clave DNS en la sentencia NAT, el cliente remoto intenta conectar con 10.1.1.100, que no trabaja porque ese direccionamiento no se puede rutear en Internet.

Servidor DNS en el exterior del ASA

Figura 2



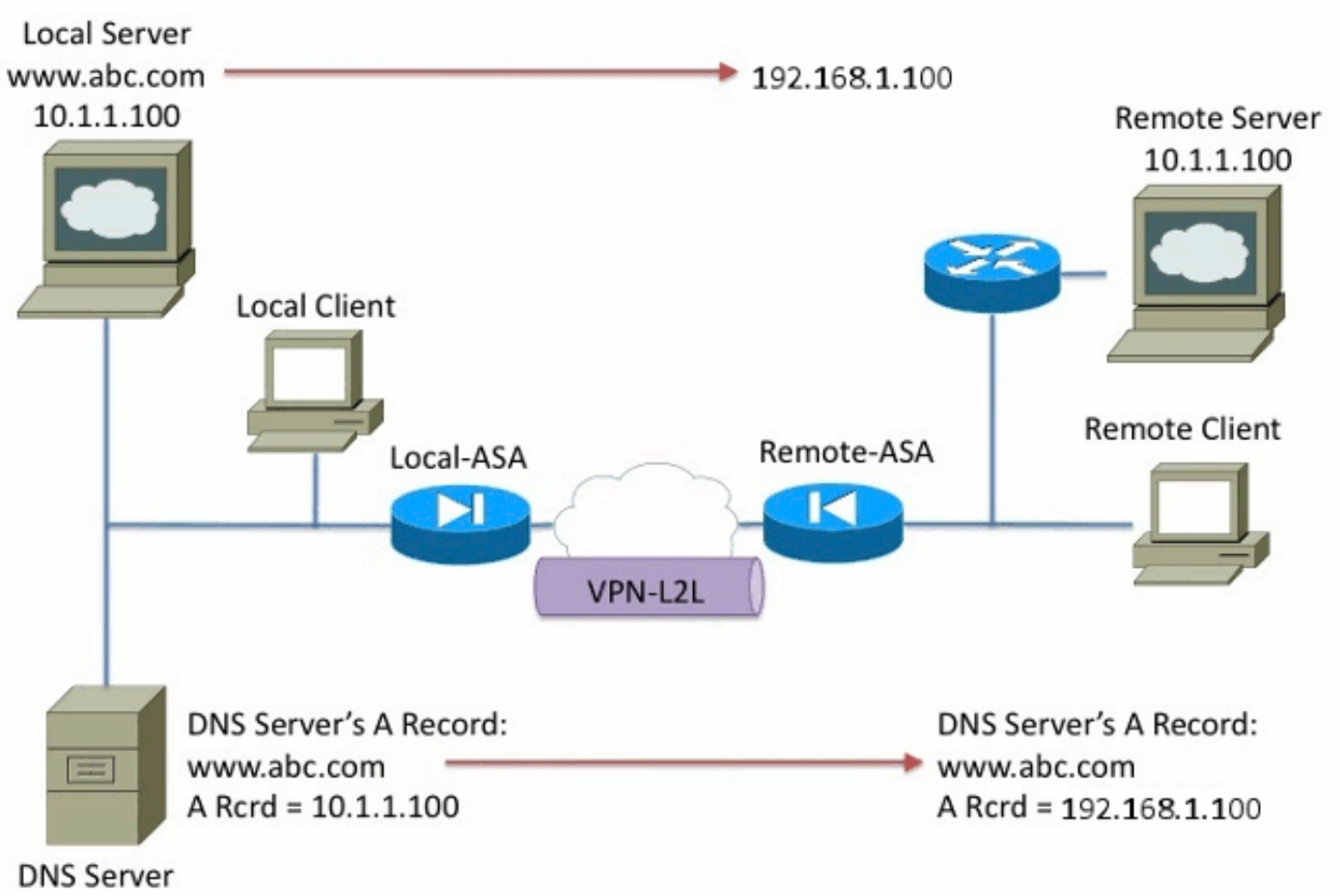

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

En el cuadro 2, el proveedor de servicio similar controla al servidor DNS el ISP o. El servidor DNS debe distribuir el IP Address público, es decir, la dirección IP *traducida del* servidor de aplicaciones. Esto permite que todos los usuarios de Internet accedan al servidor de aplicaciones vía Internet.

Desafortunadamente, el cliente local no puede acceder al servidor de aplicaciones con la dirección pública. Como consecuencia, el DNS Doctoring se configura en el ASA para cambiar el IP Address incluido dentro del paquete de la respuesta de DNS. Esto se asegura de que cuando el cliente local hace una petición DNS para www.abc.com, la respuesta recibida sea la dirección real del servidor de aplicaciones. Sin la palabra clave DNS en la sentencia NAT, el cliente local intenta conectar con 198.51.100.100. Esto no trabaja porque este paquete se envía al ASA, que cae el paquete.

VPN NAT y DNS Doctoring

Figura 3



Considere una situación donde hay las redes que solapan. En esta condición, el direccionamiento 10.1.1.100 vive en el lado remoto y el lado local. Como consecuencia, usted necesita realizar el NAT en el servidor local de modo que el cliente remoto pueda todavía accederlo con la dirección IP 192.1.1.100. Para conseguir esto para trabajar correctamente, se requiere el DNS Doctoring.

El DNS Doctoring no se puede realizar en esta función. La palabra clave DNS se puede agregar solamente al final de un objeto NAT o de la fuente NAT. El NAT no soporta dos veces la palabra clave DNS. Hay dos configuraciones posibles y ambas fall.

Configuración fallada 1: Si usted configura lo importante, traduce 10.1.1.1 a 192.1.1.1, no sólo para el cliente remoto, pero para todo el mundo en Internet. Puesto que 192.1.1.1 no es enrutable por Internet, nadie en Internet puede acceder al servidor local.

```
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
```

Configuración fallada 2: Si usted configura la línea del DNS Doctoring NAT después dos veces de la línea necesaria NAT, ésta causa una situación donde el DNS Doctoring nunca trabaja. Como consecuencia, el cliente remoto intenta acceder www.abc.com con la dirección IP 10.1.1.100, que no trabaja.

```
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
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 > descargas del software
- Soporte Técnico y Documentación - Cisco Systems