DNS Doctoring on ASA Configuration Example

Contents

Introduction

This document shows how DNS Doctoring is used on the Adaptive Security Appliance (ASA) to change the embedded IP addresses in Domain Name System (DNS) responses so that clients can connect to the correct IP address of servers.

Prerequisites

Requirements

DNS Doctoring requires configuration of Network Address Translation (NAT) on the ASA, as well as enablement of the DNS inspection.

Components Used

The information in this document is based on the Adaptive Security Appliance.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

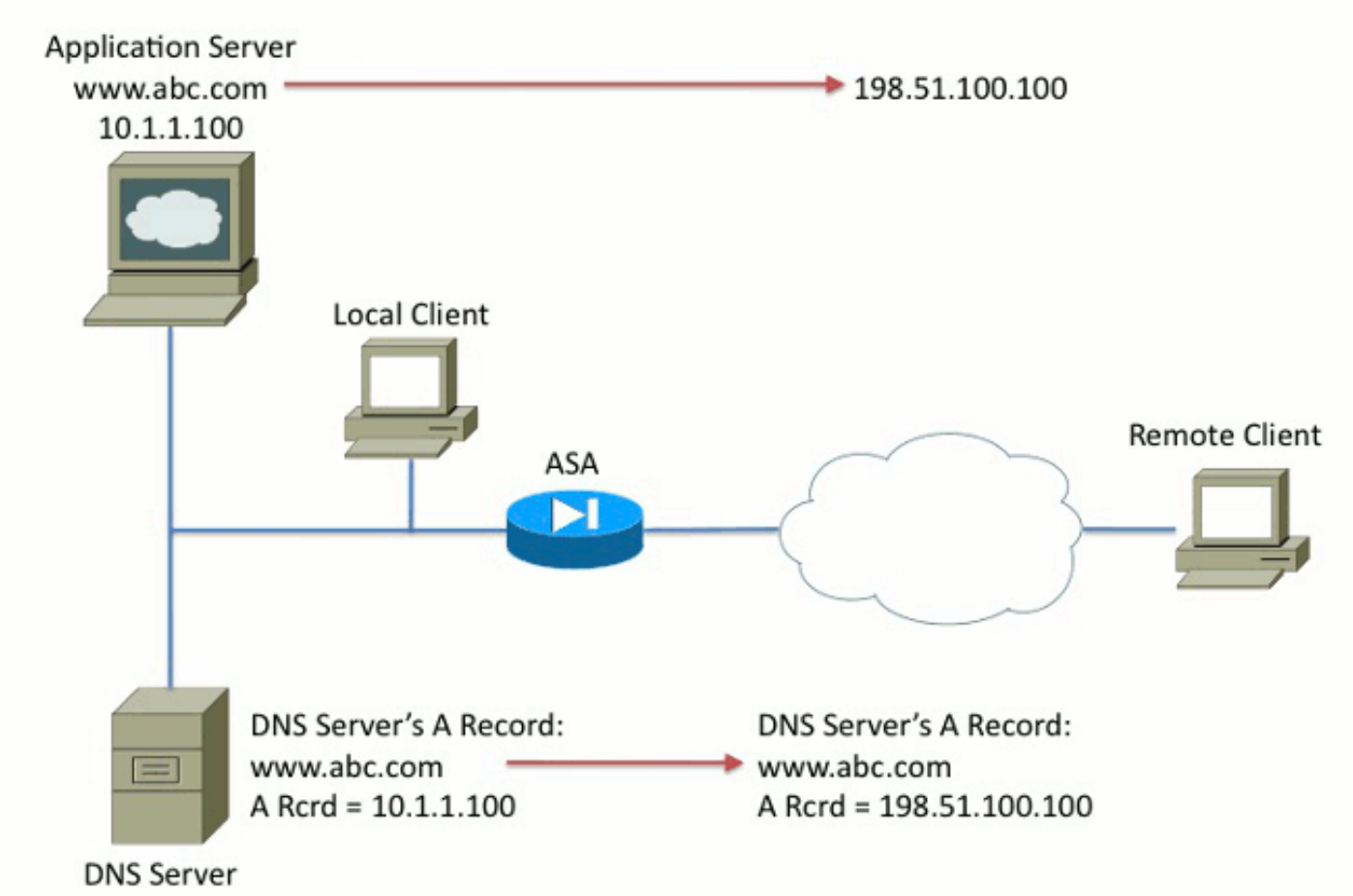
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

DNS Doctoring Examples

DNS Server on the Inside of ASA

Figure 1



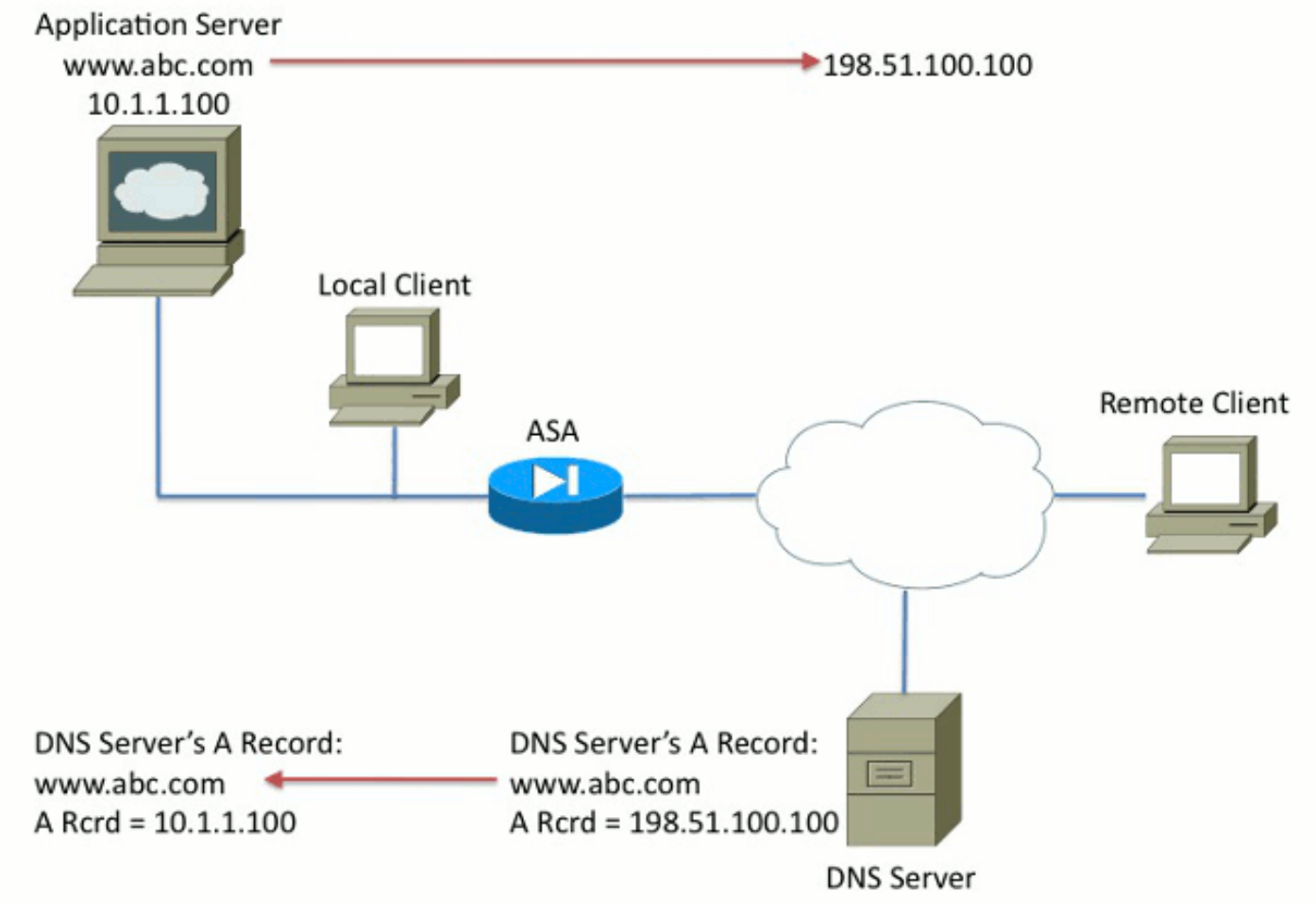

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In Figure 1, the DNS server is controlled by the local administrator. The DNS server should hand out a private IP address, which is the *real* IP address assigned to the application server. This allows the local client to connect directly to the application server.

Unfortunately, the remote client cannot access the application server with the private address. As a result, DNS Doctoring is configured on the ASA to change the embedded IP address within the DNS response packet. This ensures that when the remote client makes a DNS request for www.abc.com, the response they get is for the translated address of the application server. Without the DNS keyword on the NAT statement, the remote client tries to connect to 10.1.1.100, which does not work because that address cannot be routed on the internet.

DNS Server on the Outside of the ASA

Figure 2



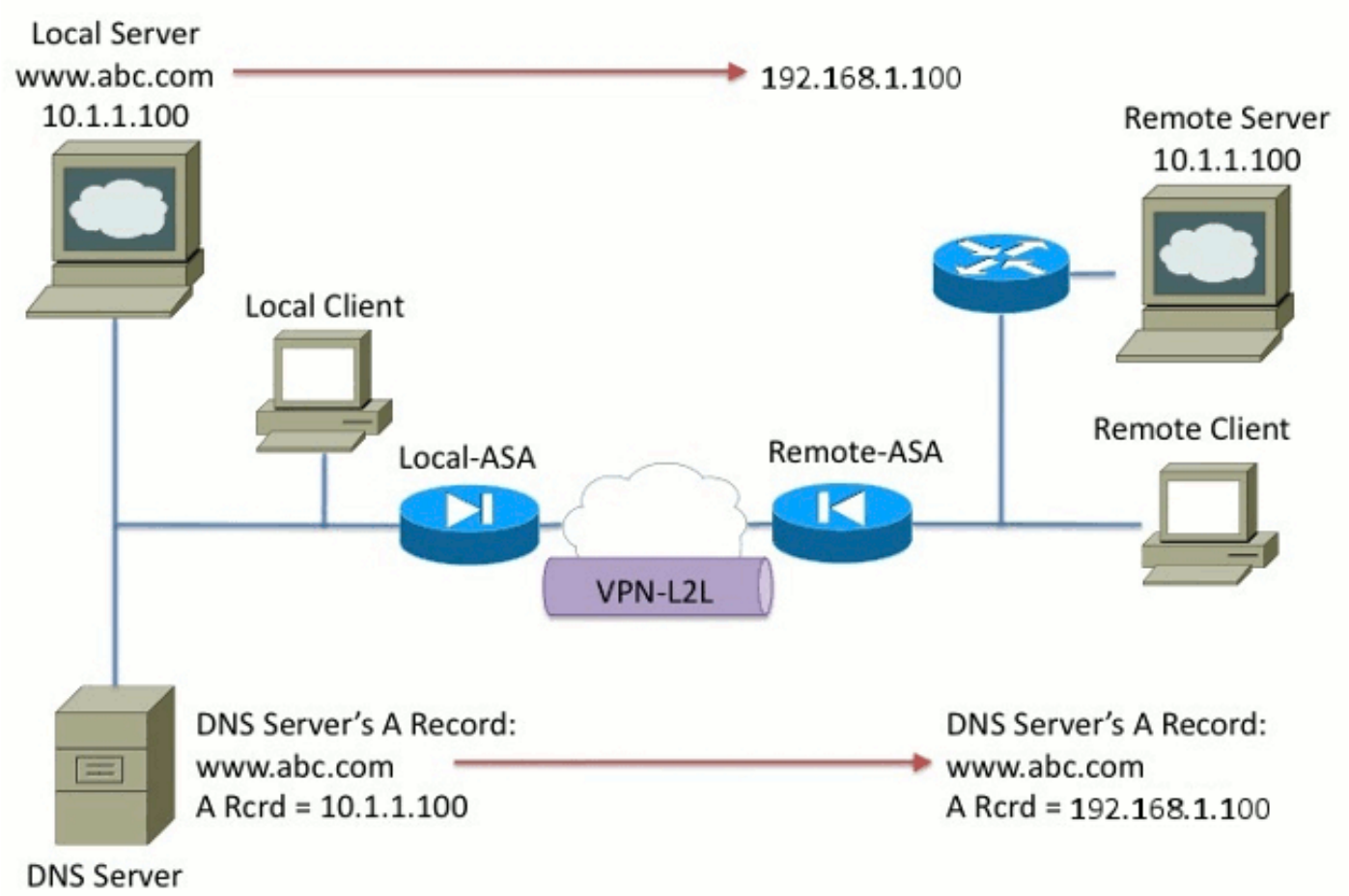

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

In Figure 2, the DNS server is controlled by the ISP or similar service provider. The DNS server should hand out the public IP address, that is, the *translated* IP address of the application server. This allows all internet users to access the application server via the internet.

Unfortunately, the local client cannot access the application server with the public address. As a result, DNS Doctoring is configured on the ASA to change the embedded IP address within the DNS response packet. This ensures that when the local client makes a DNS request for www.abc.com, the response received is the real address of the application server. Without the DNS keyword on the NAT statement, the local client tries to connect to 198.51.100.100. This does not work because this packet is sent to the ASA, which drops the packet.

VPN NAT and DNS Doctoring

Figure 3



Consider a situation where there are networks that overlap. In this condition, the address 10.1.1.100 lives on both the remote side and the local side. As a result, you need to perform NAT on the local server so that the remote client can still access it with the IP address 192.1.1.100. In order to get this to work properly, DNS Doctoring is required.

DNS Doctoring cannot be performed in this function. The DNS keyword can only be added to the end of an object NAT or source NAT. The twice NAT does not support the DNS keyword. There are two possible configurations and both fail.

Failed Configuration 1: If you configure the bottom line, it translates 10.1.1.1 to 192.1.1.1, not only for the remote client, but for everyone on the internet. Since 192.1.1.1 is not internet routable, no one on the internet can access the local 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
```

Failed Configuration 2: If you configure the DNS Doctoring NAT line after the necessary twice NAT line, this causes a situation where the DNS Doctoring never works. As a result, the remote client tries to access www.abc.com with the IP address 10.1.1.100, which does not work.

```
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
```

Related Information

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances > Software Downloads
- Technical Support & Documentation - Cisco Systems