ASA上的DNS修正配置示例

目录

简介

本文档介绍如何在自适应安全设备(ASA)上使用DNS修正来更改域名系统(DNS)响应中的嵌入式IP地址，以便客户端可以连接到服务器的正确IP地址。

先决条件

要求

DNS修正需要在ASA上配置网络地址转换(NAT)并启用DNS检查。

使用的组件

本文档中的信息基于自适应安全设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

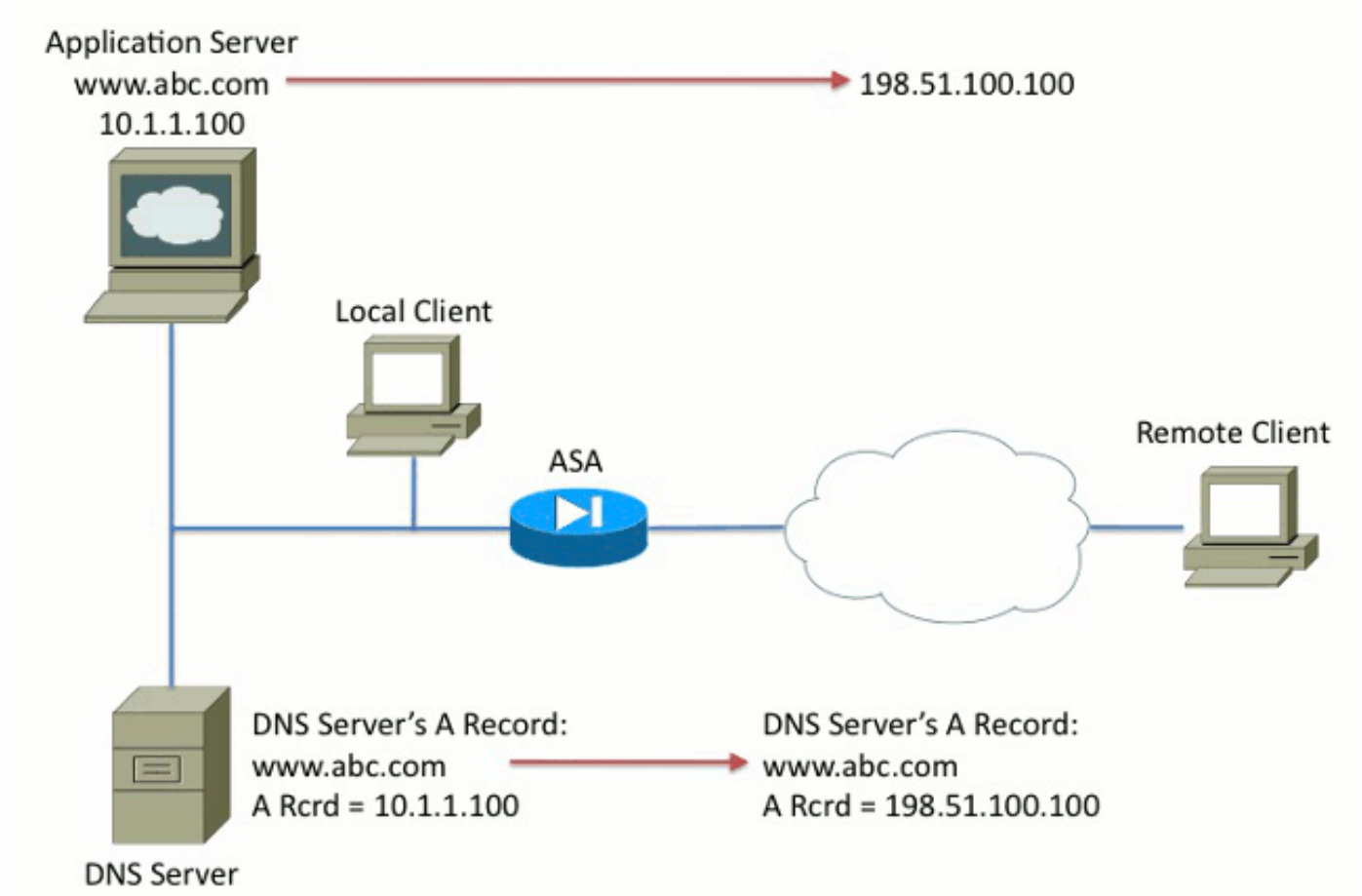
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

DNS修正示例

ASA内部的DNS服务器

图 1



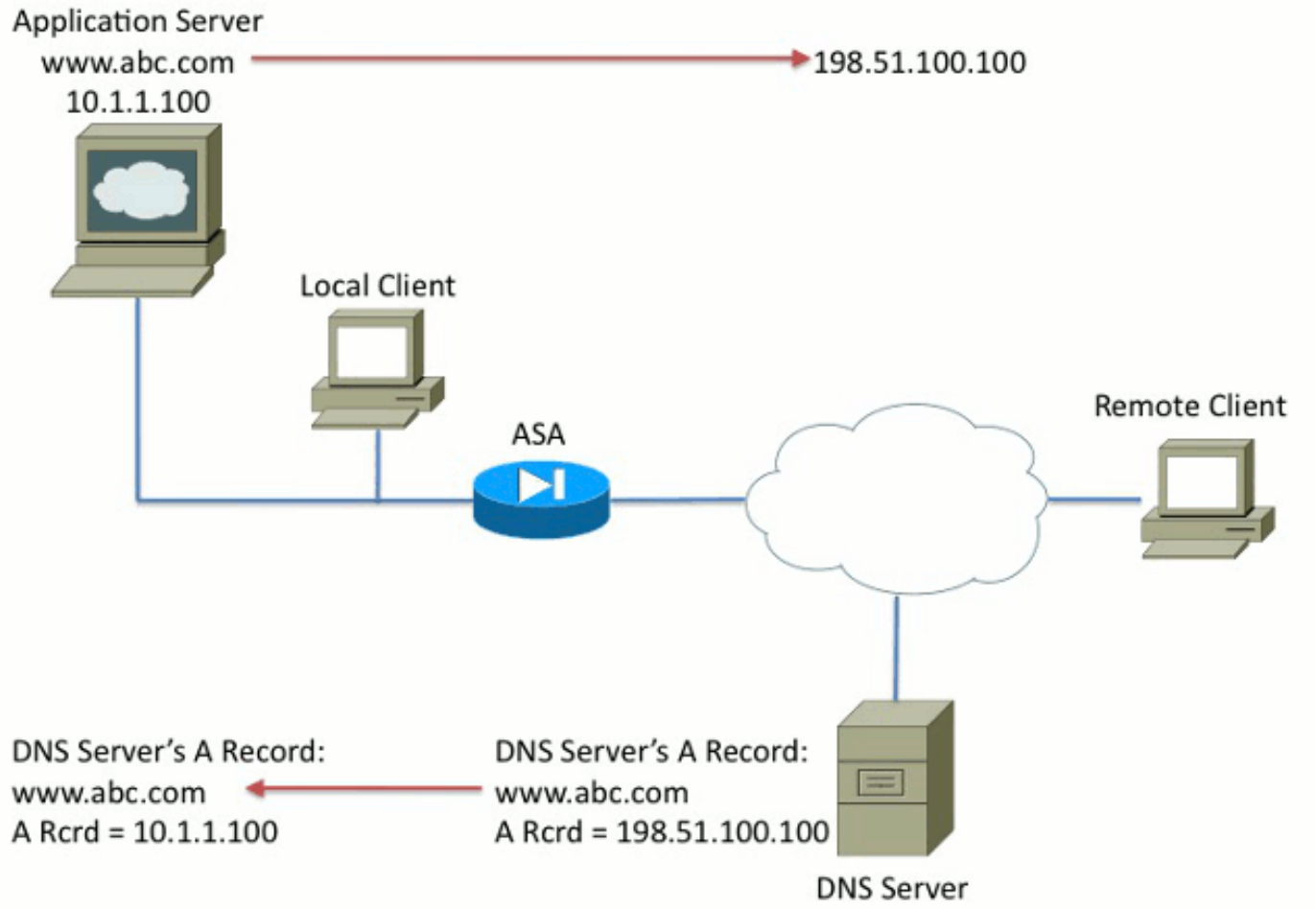

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

在图1中，DNS服务器由本地管理员控制。DNS服务器应分发私有IP地址，即分配给应用服务器的实际IP地址。这允许本地客户端直接连接到应用服务器。

很遗憾，远程客户端无法使用私有地址访问应用服务器。因此，ASA上配置了DNS修正以更改DNS响应数据包中的嵌入式IP地址。这可确保当远程客户端向www.abc.com发出DNS请求时，它们获得的响应针对的是应用服务器的转换地址。如果NAT语句中没有DNS关键字，远程客户端将尝试连接到10.1.1.100，该连接不起作用，因为该地址无法在Internet上路由。

ASA外部的DNS服务器

图 2



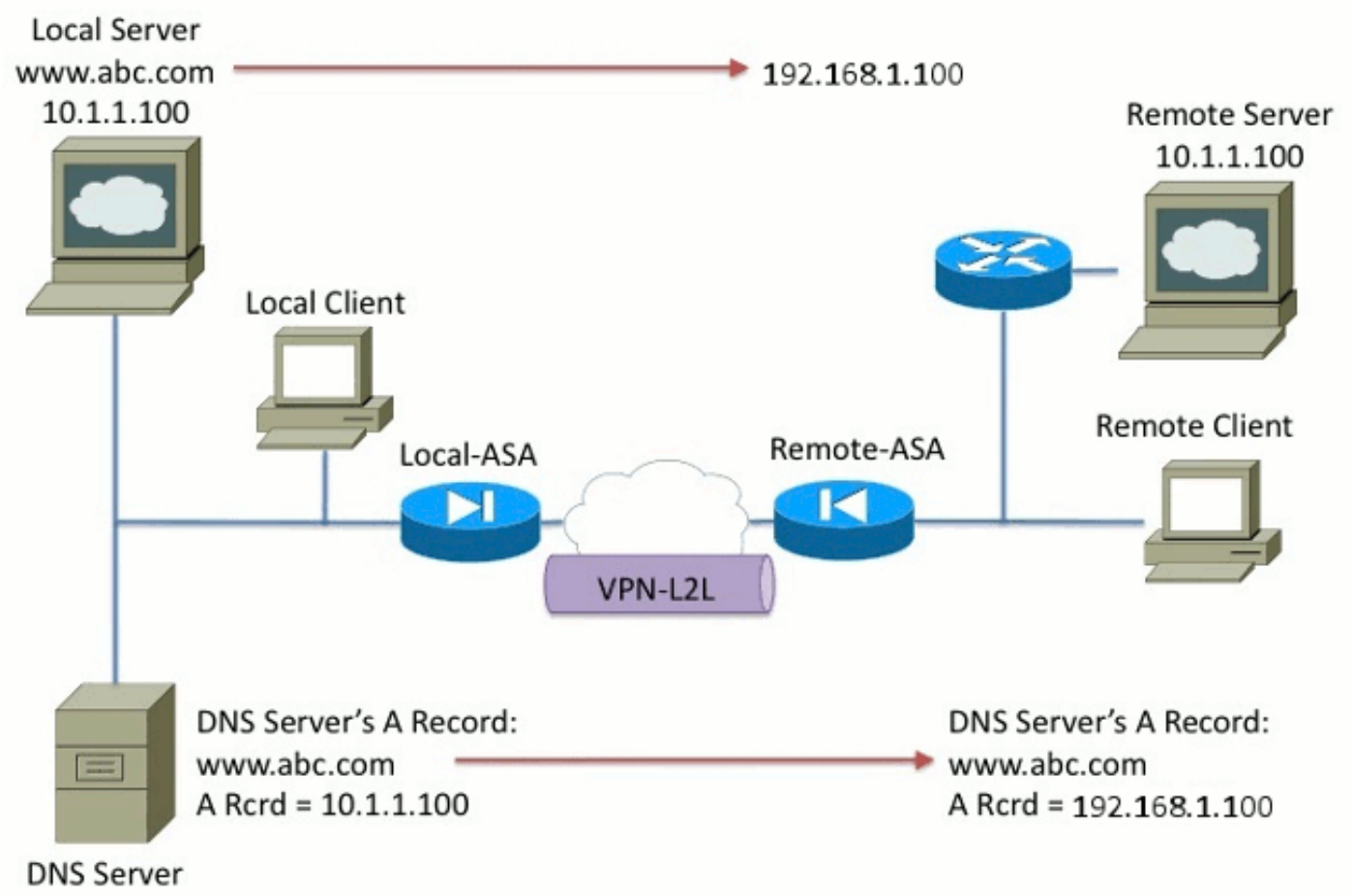

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

在图2中，DNS服务器由ISP或类似服务提供商控制。DNS服务器应分发公有IP地址，即应用服务器的转换 IP地址。这样，所有Internet用户都可以通过Internet访问应用服务器。

很遗憾，本地客户端无法使用公共地址访问应用服务器。因此，ASA上配置了DNS修正以更改DNS响应数据包中的嵌入式IP地址。这可确保当本地客户端对www.abc.com发出DNS请求时，收到的响应是应用服务器的实际地址。如果NAT语句中没有DNS关键字，本地客户端将尝试连接到198.51.100.100。这不起作用，因为此数据包被发送到ASA，ASA会丢弃该数据包。

VPN NAT和DNS修正

图 3



考虑网络重叠的情况。在这种情况下，地址10.1.1.100同时位于远程端和本地端。因此，您需要在本地服务器上执行NAT，以便远程客户端仍然可以使用IP地址192.1.1.100访问它。为了使其正常工作，需要DNS修正。

无法在此功能中执行DNS修正。DNS关键字只能添加到对象NAT或源NAT的末尾。两次NAT不支持DNS关键字。有两种可能的配置，两种配置都失败。

失败的配置1：如果配置底线，它将10.1.1.1转换为192.1.1.1，不仅对于远程客户端，而且对于Internet上的每个人。由于192.1.1.1不可路由到Internet，因此Internet上的任何人都无法访问本地服务器。

```
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
```

失败配置2:如果在必要的两次NAT线路之后配置DNS修正NAT线路，则会导致DNS修正永远无法正常运行的情况。因此，远程客户端尝试访问IP地址为10.1.1.100的www.abc.com，但该地址不起作用。

```
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
```

相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco ASA 5500系列自适应安全设备>软件下载
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。