

医治在ASA配置示例的DNS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[篡改示例的DNS](#)

[在ASA的里面的DNS服务器](#)

[在ASA的外部的DNS服务器](#)

[VPN NAT和DNS医治](#)

[相关信息](#)

简介

本文显示DNS医治如何在可适应安全工具(ASA)用于更改在域名系统(DNS)答复的嵌入式IP地址，以便客户端能连接到服务器的正确IP地址。

先决条件

要求

DNS医治要求网络地址转换(NAT)的DNS检查的配置在ASA的，以及启动。

使用的组件

本文档中的信息根据可适应安全工具。

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](#)。

篡改示例的DNS

在ASA的里面的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，DNS服务器是由本地管理员控制的。DNS服务器应该实施专用IP地址，是实际IP地址分配到应用服务器。这允许本地客户端连接直接地到应用服务器。

不幸地，远程客户端不能访问有专用地址的应用服务器。结果，DNS医治在ASA配置更改在DNS响应数据包内的嵌入式IP地址。这保证，当远程客户端做www.abc.com的时—DNS请求，他们得到的答复是为应用服务器的转换地址。没有在NAT语句的DNS关键字，远程客户端设法连接到10.1.1.100，不工作，因为该地址在互联网不可能路由。

[在ASA的外部的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

在表2，DNS服务器是由ISP或相似的服务提供商控制的。DNS服务器应该实施公网IP地址，即，应用服务器的转换后的IP地址。这允许所有互联网用户通过互联网访问应用服务器。

不幸地，本地客户端不能访问有公共地址的应用服务器。结果，DNS医治在ASA配置更改在DNS响应数据包内的嵌入式IP地址。这保证，当本地客户端做www.abc.com的时—DNS请求，接收的答复是应用服务器的实际地址。没有在NAT语句的DNS关键字，本地客户端设法连接到198.51.100.100。这不工作，因为此数据包发送对ASA，丢弃数据包。

[VPN NAT和DNS医治](#)

图 3

考虑有网络交迭的一个情况。在此情况下，地址10.1.1.100在远端和本地端居住。结果，您需要执行在当地服务器的NAT，以便远程客户端能仍然访问它与IP地址192.1.1.100。为了获得此适当地运作，DNS医治要求。

DNS医治在此功能不可能执行。DNS关键字可能只被添加到对象NAT或来源NAT的结尾。NAT不两次支持DNS关键字。有两可能的配置，并且两个发生故障。

失败的配置1：如果配置最后一行，翻译10.1.1.1对192.1.1.1，不仅远程客户端的，但是大家的互联网的。因为192.1.1.1不是可路由的互联网，没人在互联网能访问当地服务器。

```
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
```

失败的配置2：如果配置DNS两次篡改NAT线路的在必要的NAT线路以后，这导致医治的DNS从未运转的一个情况。结果，远程客户端设法访问与IP地址10.1.1.100的www.abc.com，不工作。

```
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](#)