在单堆栈IPv6中使用CSC支持Umbrella DNS保护

目录

简介

本文档介绍如何在单堆栈IPv6网络中启用思科安全客户端(CSC)以支持Umbrella DNS保护。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella漫游安全中的Cisco安全客户端。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

过去，思科安全客户端支持仅IPv4和双堆栈网络配置。本文描述从Cisco安全客户端 5.1.4.74(MR4)开始的仅支持IPv6的网络。 必须使用标志文件启用该功能。

背景

随着IPv6的广泛普及，世界各地的ISP越来越多地只分配IPv6地址。但是，许多服务器资源仍然位于仅IPv4网络上。DNS64与NAT64是过渡功能，可在纯IPv6客户端和纯IPv4服务器之间实现无缝通信，而无需客户端了解底层IPv4基础设施。

AAAA记录专门用于IPv6，而A记录则专门用于IPv4。DNS64的工作原理是合成服务器的AAAA(IPv6)记录，这些服务器在其DNS中只有A记录，从而允许仅IPv6客户端访问仅使用IPv4的服务器。DNS64通过将可配置的IPv6前缀与A记录查找中的IPv4地址组合来创建这些AAAA记录。IPv4地址嵌入在IPv6地址的最后32位中。

思科安全客户端5.1.4.74(MR4)现在支持对仅IPv6网络的Umbrella保护。Umbrella模块通过查询LAN DNS解析器来发现网络网关使用的NAT64前缀。当Umbrella DNS解析器参与策略实施的名称解析时，它会使用发现的NAT64前缀进行DNS64 IPv6地址合成。

启用功能

Windows 窗口版本

创建一个名为`single_stack_ipv6.flag`的文件，并将其放入此目录中：

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data
```

将标志文件放入目录后，请重新启动Cisco安全客户端，使功能生效。

macOS

创建一个名为`single_stack_ipv6.flag`的文件，并将其放入此目录中：

```
/opt/cisco/secureclient/umbrella/data
```

将标志文件放入目录后，请重新启动Cisco安全客户端，使功能生效。

限制

在CSC版本5.1.4中，DNS64仅支持发往Umbrella DNS解析器的加密DNS流量。未加密的DNS流量不支持此功能，即使应用了保护也是如此。

常见问题

如何知道我的网络(macOS)是否支持DNS64/NAT64?

您可以使用DNS64/NAT64挖掘测试。

这些测试旨在检验网络是否符合要求，从而主机只配置了IPv6地址。为了访问Internet上的现有IPv4服务，主机必须使用已配置的解析器中的DNS64来接收IPv4 IP地址的合成IPv6地址。一旦Umbrella拥有了综合地址，它将确保可以访问它。只有在网关上启用了NAT64时，该地址才能到达。Umbrella使用“api-ipv4.opendns.com”域，因为只配置了v4地址。因此，如果Umbrella在应答记录中获得v6地址，则Umbrella知道它已被合成。当您对dig命令返回的地址执行ping6时，您知道合成地址已成功转换为Internet上的v4地址，并且回复已转换回主机。

DNS64

您要测试的第一件事是：

```
➜ osx dig AAAA api-ipv4.opendns.com

; <<>> DiG 9.10.6 <<>> AAAA api-ipv4.opendns.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31228
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;api-ipv4.opendns.com. IN AAAA

;; ANSWER SECTION:
api-ipv4.opendns.com. 60 IN AAAA 64:ff9b::9270:ff9b <—synthesized address

;; Query time: 921 msec
;; SERVER: 2001:4860:4860::6464#53(2001:4860:4860::6464)
;; WHEN: Thu Jun 20 17:28:12 PDT 2024
;; MSG SIZE rcvd: 77
```

NAT64

现在，您可以ping合成地址：

```
➜ osx ping6 64:ff9b::9270:ff9b
PING6(56=40+8+8 bytes) 2001:db8:1:0:785e:e00f:f8fe:9f7b --> 64:ff9b::9270:ff9b
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=0 hlim=54 time=103.653 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=1 hlim=54 time=51.491 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=2 hlim=54 time=54.278 ms
16 bytes from 64:ff9b::9270:ff9b, icmp_seq=3 hlim=54 time=78.153 ms
```

如何知道我的网络(Windows)是否支持DNS64/NAT64?

DNS64

您要测试的第一件事是：

```
C:\>nslookup -type=AAAA api-ipv4.opendns.com.
Server: UnKnown
Address: 2600:1f14:1799:7000:d2b9:d714:e957:6d4
```

非授权应答：

```
Name: api-ipv4.opendns.com
Address: 64:ff9b::9270:ff9b <-synthesized address
```

NAT64

现在，您可以ping合成地址：

```
C:\>ping 64:ff9b::9270:ff9b

Pinging 64:ff9b::9270:ff9b with 32 bytes of data:
Reply from 64:ff9b::9270:ff9b: time=18ms
Reply from 64:ff9b::9270:ff9b: time=22ms
Reply from 64:ff9b::9270:ff9b: time=21ms
Reply from 64:ff9b::9270:ff9b: time=19ms

Ping statistics for 64:ff9b::9270:ff9b:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 18ms, Maximum = 22ms, Average = 20ms
```

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）。