Use CSC Support for Umbrella DNS Protection in Single Stack IPv6

Contents

Introduction

This document describes how to enable Cisco Secure Client (CSC) to support Umbrella DNS protection in single stack IPv6 networks.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Secure Client in Umbrella Roaming Security.

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, ensure that you understand the potential impact of any command.

Overview

In the past, Cisco Secure Client supported IPv4-only and dual stack network configurations. This article describes support for IPv6-only networks starting with Cisco Secure Client 5.1.4.74 (MR4). The feature must be enabled using a flag file.

Background

With the widespread proliferation of IPv6, ISPs around the world are increasingly assigning IPv6 addresses only. However, many server resources are still on IPv4 only networks. DNS64, combined with NAT64, are transitional capabilities that enable seamless communication between IPv6-only clients and IPv4-only servers without requiring the clients to be aware of the underlying IPv4 infrastructure.

AAAA records are used exclusively with IPv6, while A records are used exclusively with IPv4. DNS64 works by synthesizing AAAA (IPv6) records for servers that only have A records in their DNS, allowing IPv6-only clients to reach IPv4-only servers. DNS64 creates these AAAA records by combining a configurable IPv6 prefix with the IPv4 address from an A-record lookup. The IPv4 address is embedded in the last 32 bits of the IPv6 address.

Cisco Secure Client 5.1.4.74 (MR4) now supports Umbrella protection for IPv6-only networks. The Umbrella module discovers the NAT64 prefix that is being employed by the network gateway by querying the LAN DNS resolvers. It then does the DNS64 IPv6 address synthesis using the discovered NAT64 prefix when the Umbrella DNS resolver is involved in name resolution for policy enforcement.

Enable the Feature

Windows

Create a file called `single_stack_ipv6.flag` and place it into this directory:

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

Once the flag file has been placed in the directory, please restart the Cisco Secure Client for the feature to take effect.

macOS

Create a file called `single_stack_ipv6.flag` and place it into this directory:

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

Once the flag file has been placed in the directory, please restart the Cisco Secure Client for the feature to take effect.

Limitations

In CSC release 5.1.4 DNS64 is supported only for encrypted DNS traffic going to Umbrella DNS resolvers. It is not supported for unencrypted DNS traffic, even if protection is applied.

FAQ

How do I know if DNS64/NAT64 is supported on my network (macOS)?

You can use DNS64/NAT64 dig testing.

These tests are designed to qualify a network whereby the host is only configured with an IPv6 address. In order to reach existing IPv4 services on the Internet, the host must use DNS64 from the configured resolver to receive the synthesized IPv6 address of the IPv4 IP address. Once Umbrella has the synthesized address, it ensures that it is reachable. It can only be reachable if NAT64 is enabled on the gateway. Umbrella uses the "api-ipv4.opendns.com" domain because there are only v4 addresses configured. So, if Umbrella gets a v6 address in the answer record, Umbrella knows it has been synthesized. When you `ping6` the returned address from the `dig` command, you know that the synthesized address is successfully translated to a v4 address on the Internet and the reply translated back to the host.

DNS64

The first thing you want to test:

```
➜ 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

Now, you can ping the synthesized address:

```
➜ 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
```

How do I know if DNS64/NAT64 is supported on my network (Windows)?

DNS64

The first thing you want to test:

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

Non-authoritative answer:

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

NAT64

Now, you can ping the synthesized address:

```
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
```