CSC-Unterstützung für Umbrella DNS Protection in Single Stack IPv6

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Cisco Secure Client (CSC) aktivieren, um Umbrella DNS Protection in IPv6-Netzwerken mit einem Stack zu unterstützen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Client in Umbrella Roaming Security.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

In der Vergangenheit unterstützte Cisco Secure Client nur IPv4- und Dual-Stack-Netzwerkkonfigurationen. In diesem Artikel wird die Unterstützung für IPv6-Netzwerke beschrieben, die mit Cisco Secure Client 5.1.4.74 (MR4) beginnen. Die Funktion muss mithilfe einer Flagdatei aktiviert werden.

Hintergrund

Mit der weit verbreiteten Verbreitung von IPv6 weisen ISPs weltweit zunehmend nur IPv6-Adressen zu. Viele Serverressourcen befinden sich jedoch nach wie vor in reinen IPv4-Netzwerken. DNS64 in Kombination mit NAT64 sind Übergangsfunktionen, die eine nahtlose Kommunikation zwischen Nur-IPv6-Clients und Nur-IPv4-Servern ermöglichen, ohne dass die Clients die zugrunde liegende IPv4-Infrastruktur kennen müssen.

AAAA-Einträge werden ausschließlich mit IPv6 verwendet, während A-Einträge ausschließlich mit IPv4 verwendet werden. DNS64 verwendet AAAA-Einträge (IPv6) für Server, die nur über A-Einträge in ihrem DNS verfügen, wodurch nur IPv6-Clients IPv4-Server erreichen können. DNS64 erstellt diese AAAA-Einträge, indem ein konfigurierbares IPv6-Präfix mit der IPv4-Adresse aus einer A-Datensatz-Suche kombiniert wird. Die IPv4-Adresse ist in die letzten 32 Bit der IPv6-Adresse eingebettet.

Cisco Secure Client 5.1.4.74 (MR4) unterstützt jetzt Umbrella Protection für IPv6-Netzwerke. Das Umbrella-Modul erkennt das NAT64-Präfix, das vom Netzwerk-Gateway verwendet wird, indem es die LAN-DNS-Resolver abfragt. Anschließend wird die DNS64-IPv6-Adresssynthese mithilfe des erkannten NAT64-Präfix durchgeführt, wenn der Umbrella DNS-Resolver an der Namensauflösung für die Richtliniendurchsetzung beteiligt ist.

Aktivieren der Funktion

Windows

Erstellen Sie eine Datei mit dem Namen `single_stack_ipv6.flag`, und legen Sie sie in diesem Verzeichnis ab:

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

Sobald die Kennzeichnungsdatei im Verzeichnis abgelegt wurde, starten Sie den Cisco Secure Client neu, damit die Funktion wirksam wird.

MacOS

Erstellen Sie eine Datei mit dem Namen `single_stack_ipv6.flag`, und legen Sie sie in diesem Verzeichnis ab:

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

Sobald die Kennzeichnungsdatei im Verzeichnis abgelegt wurde, starten Sie den Cisco Secure Client neu, damit die Funktion wirksam wird.

Einschränkungen

In der CSC-Version 5.1.4 wird DNS64 nur für verschlüsselten DNS-Datenverkehr an Umbrella DNS Resolver unterstützt. Es wird nicht für unverschlüsselten DNS-Datenverkehr unterstützt, selbst wenn der Schutz angewendet wird.

Häufig gestellte Fragen

Woher weiß ich, ob DNS64/NAT64 in meinem Netzwerk (macOS) unterstützt wird?

Sie können DNS64/NAT64-Grabungstests verwenden.

Diese Tests sollen ein Netzwerk qualifizieren, bei dem der Host nur mit einer IPv6-Adresse konfiguriert ist. Um bestehende IPv4-Dienste im Internet zu erreichen, muss der Host DNS64 vom konfigurierten Resolver verwenden, um die synthetisierte IPv6-Adresse der IPv4-IP-Adresse zu erhalten. Sobald Umbrella die synthetisierte Adresse hat, stellt es sicher, dass sie erreichbar ist. Er ist nur erreichbar, wenn NAT64 auf dem Gateway aktiviert ist. Umbrella verwendet die Domäne "api-ipv4.opendns.com", da nur v4-Adressen konfiguriert sind. Wenn Umbrella also eine v6-Adresse im Antwortdatensatz erhält, weiß Umbrella, dass sie synthetisiert wurde. Wenn Sie die vom `Befehl dig` zurückgegebene Adresse `pingen6`, wissen Sie, dass die synthetisierte Adresse erfolgreich in eine v4-Adresse im Internet übersetzt wurde und die Antwort zurück an den Host übersetzt wurde.

DNS 64

Das Erste, was Sie testen möchten:

➜ 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

Jetzt können Sie einen Ping an die synthetisierte Adresse senden:

```
➜ 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
```

Woher weiß ich, ob DNS64/NAT64 in meinem Netzwerk (Windows) unterstützt wird?

DNS 64

Das Erste, was Sie testen möchten:

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

Nicht-autoritative Antwort:

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

NAT64

Jetzt können Sie einen Ping an die synthetisierte Adresse senden:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.