CSC-ondersteuning gebruiken voor overkoepelende DNS-bescherming in IPv6 met één stapel

Inhoud

Inleiding

In dit document wordt beschreven hoe Cisco Secure Client (CSC) Umbrella DNS-beveiliging kan ondersteunen in IPv6-netwerken met één stapel.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Client in Umbrella Roaming Security.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

In het verleden ondersteunde Cisco Secure Client netwerkconfiguraties met alleen IPv4 en dubbele stapels. In dit artikel wordt ondersteuning beschreven voor netwerken die alleen IPv6 ondersteunen, te beginnen met Cisco Secure Client 5.1.4.74 (MR4). De functie moet zijn ingeschakeld met behulp van een vlagbestand.

Achtergrond

Met de wijdverspreide verspreiding van IPv6 wijzen ISP's over de hele wereld steeds meer alleen IPv6-adressen toe. Veel serverbronnen bevinden zich echter nog steeds op alleen IPv4-netwerken. DNS64, in combinatie met NAT64, zijn overgangsmogelijkheden die naadloze communicatie mogelijk maken tussen clients met alleen IPv6 en servers met alleen IPv4 zonder dat de clients zich bewust moeten zijn van de onderliggende IPv4-infrastructuur.

AAAA-records worden uitsluitend gebruikt met IPv6, terwijl A-records uitsluitend worden gebruikt met IPv4. DNS64 werkt door AAAA (IPv6)-records te synthetiseren voor servers die alleen A-records in hun DNS hebben, waardoor alleen IPv6-clients IPv4-servers kunnen bereiken. DNS64 maakt deze AAAA-records door een configureerbaar IPv6-voorvoegsel te combineren met het IPv4-adres uit een A-record-zoekopdracht. Het IPv4-adres is ingebed in de laatste 32 bits van het IPv6-adres.

Cisco Secure Client 5.1.4.74 (MR4) ondersteunt nu overkoepelende bescherming voor IPv6-netwerken. De Umbrella-module ontdekt het NAT64-voorvoegsel dat wordt gebruikt door de netwerkgateway door de LAN DNS-resolvers te bevragen. Vervolgens wordt de DNS64 IPv6-adressynthese uitgevoerd met behulp van het ontdekte NAT64-voorvoegsel wanneer de Umbrella DNS-resolver betrokken is bij de naamoplossing voor beleidshandhaving.

Schakel de functie in

Windows

Maak een bestand met de naam `single_stack_ipv6.flag` en plaats het in deze directory:

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

Zodra het vlaggenbestand in de directory is geplaatst, start u de Cisco Secure Client opnieuw op om de functie in werking te laten treden.

macOS

Maak een bestand met de naam `single_stack_ipv6.flag` en plaats het in deze directory:

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

Zodra het vlaggenbestand in de directory is geplaatst, start u de Cisco Secure Client opnieuw op om de functie in werking te laten treden.

Beperkingen

In CSC versie 5.1.4 wordt DNS64 alleen ondersteund voor gecodeerd DNS-verkeer dat naar Umbrella DNS-resolvers gaat. Het wordt niet ondersteund voor niet-gecodeerd DNS-verkeer, zelfs als er bescherming wordt toegepast.

FAQ

Hoe weet ik of DNS64/NAT64 wordt ondersteund op mijn netwerk (macOS)?

U kunt DNS64/NAT64 dig testen gebruiken.

Deze tests zijn ontworpen om een netwerk te kwalificeren waarbij de host alleen is geconfigureerd met een IPv6-adres. Om bestaande IPv4-services op internet te bereiken, moet de host DNS64 van de geconfigureerde resolver gebruiken om het gesynthetiseerde IPv6-adres van het IPv4-IP-adres te ontvangen. Zodra Umbrella het gesynthetiseerde adres heeft, zorgt het ervoor dat het bereikbaar is. Het kan alleen worden bereikt als NAT64 is ingeschakeld op de gateway. Umbrella gebruikt het domein "api-ipv4.opendns.com" omdat er alleen v4-adressen zijn geconfigureerd. Dus als Umbrella een v6-adres krijgt in het antwoordrecord, weet Umbrella dat het is gesynthetiseerd. Wanneer u `ping6` het geretourneerde adres van de `dig`-opdracht, weet u dat het gesynthetiseerde adres met succes wordt vertaald naar een v4-adres op het internet en het antwoord terug naar de host wordt vertaald.

DNS64

Het eerste wat je wilt testen:

```
➜ 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

Nu kunt u het gesynthetiseerde adres pingen:

```
➜ 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
```

Hoe weet ik of DNS64/NAT64 wordt ondersteund op mijn netwerk (Windows)?

DNS64

Het eerste wat je wilt testen:

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

Niet-gezaghebbend antwoord:

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

NAT64

Nu kunt u het gesynthetiseerde adres pingen:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.