Utiliser la prise en charge CSC pour la protection DNS Umbrella dans une pile unique IPv6

Table des matières

Introduction

Ce document décrit comment activer Cisco Secure Client (CSC) pour prendre en charge la protection Umbrella DNS dans les réseaux IPv6 à pile unique.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Secure Client dans 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Auparavant, Cisco Secure Client prenait en charge les configurations réseau IPv4 uniquement et

à double pile. Cet article décrit la prise en charge des réseaux IPv6 uniquement à partir de Cisco Secure Client 5.1.4.74 (MR4). La fonctionnalité doit être activée à l'aide d'un fichier d'indicateur.

Fond

Avec la prolifération généralisée de l'IPv6, les FAI du monde entier attribuent de plus en plus des adresses IPv6 uniquement. Cependant, de nombreuses ressources serveur sont toujours sur des réseaux IPv4 uniquement. DNS64, associé à NAT64, sont des fonctionnalités de transition qui permettent une communication transparente entre les clients IPv6 uniquement et les serveurs IPv4 uniquement sans que les clients aient besoin de connaître l'infrastructure IPv4 sous-jacente.

Les enregistrements AAAA sont utilisés exclusivement avec IPv6, tandis que les enregistrements A sont utilisés exclusivement avec IPv4. DNS64 fonctionne en synthétisant les enregistrements AAAA (IPv6) pour les serveurs qui n'ont que des enregistrements A dans leur DNS, permettant aux clients IPv6 uniquement d'accéder aux serveurs IPv4 uniquement. DNS64 crée ces enregistrements AAAA en combinant un préfixe IPv6 configurable avec l'adresse IPv4 à partir d'une recherche d'enregistrement A. L'adresse IPv4 est intégrée dans les 32 derniers bits de l'adresse IPv6.

Cisco Secure Client 5.1.4.74 (MR4) prend désormais en charge la protection Umbrella pour les réseaux IPv6 uniquement. Le module Umbrella détecte le préfixe NAT64 utilisé par la passerelle réseau en interrogeant les résolveurs DNS LAN. Il effectue ensuite la synthèse d'adresse IPv6 DNS64 en utilisant le préfixe NAT64 découvert lorsque le résolveur DNS Umbrella intervient dans la résolution de noms pour l'application de la stratégie.

Activer la fonctionnalité

Fenêtres

Créez un fichier appelé `single_stack_ipv6.flag` et placez-le dans ce répertoire :

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

Une fois le fichier d'indicateur placé dans le répertoire, redémarrez Cisco Secure Client pour que la fonctionnalité prenne effet.

macOS

Créez un fichier appelé `single_stack_ipv6.flag` et placez-le dans ce répertoire :

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

Une fois le fichier d'indicateur placé dans le répertoire, redémarrez Cisco Secure Client pour que la fonctionnalité prenne effet.

Limites

Dans CSC version 5.1.4, DNS64 est pris en charge uniquement pour le trafic DNS chiffré allant vers les résolveurs DNS Umbrella. Il n'est pas pris en charge pour le trafic DNS non chiffré, même si la protection est appliquée.

Forum aux questions

Comment savoir si DNS64/NAT64 est pris en charge sur mon réseau (macOS) ?

Vous pouvez utiliser le test de recherche DNS64/NAT64.

Ces tests sont conçus pour qualifier un réseau dans lequel l'hôte est uniquement configuré avec une adresse IPv6. Pour atteindre les services IPv4 existants sur Internet, l'hôte doit utiliser DNS64 à partir du résolveur configuré pour recevoir l'adresse IPv6 synthétisée de l'adresse IPv4. Une fois qu'Umbrella a l'adresse synthétisée, il s'assure qu'elle est accessible. Elle n'est accessible que si NAT64 est activé sur la passerelle. Umbrella utilise le domaine « api-ipv4.opendns.com » car seules des adresses v4 sont configurées. Ainsi, si Umbrella obtient une adresse v6 dans l'enregistrement de réponse, Umbrella sait qu'elle a été synthétisée. Lorsque vous envoyez une requête `ping6 à` l'adresse retournée par la commande `dig`, vous savez que l'adresse synthétisée est traduite avec succès en une adresse v4 sur Internet et la réponse est retraduite vers l'hôte.

DNS64

La première chose que vous voulez tester :

➜ 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

Vous pouvez maintenant envoyer une requête ping à l'adresse synthétisée :

```
➜ 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
```

Comment savoir si DNS64/NAT64 est pris en charge sur mon réseau (Windows) ?

DNS64

La première chose que vous voulez tester :

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

Réponse ne faisant pas autorité :

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

NAT64

Vous pouvez maintenant envoyer une requête ping à l'adresse synthétisée :

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.