Use o suporte do CSC para a proteção Umbrella DNS no IPv6 de pilha única

Contents

Introdução

Este documento descreve como habilitar o Cisco Secure Client (CSC) para suportar a proteção Umbrella DNS em redes IPv6 de pilha única.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Client no Umbrella Roaming Security.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

No passado, o Cisco Secure Client oferecia suporte a configurações de rede somente IPv4 e de pilha dupla. Este artigo descreve o suporte para redes somente IPv6 iniciando com o Cisco Secure Client 5.1.4.74 (MR4). O recurso deve ser habilitado usando um arquivo de sinalizador.

Background

Com a proliferação generalizada do IPv6, os ISPs em todo o mundo estão atribuindo cada vez mais endereços IPv6 apenas. No entanto, muitos recursos de servidor ainda estão em redes somente IPv4. O DNS64, combinado com o NAT64, são recursos de transição que permitem uma comunicação transparente entre clientes somente IPv6 e servidores somente IPv4 sem exigir que os clientes estejam cientes da infraestrutura subjacente IPv4.

Os registros AAAA são usados exclusivamente com o IPv6, enquanto os registros A são usados exclusivamente com o IPv4. O DNS64 funciona sintetizando registros AAAA (IPv6) para servidores que têm apenas registros A em seu DNS, permitindo que clientes somente IPv6 acessem servidores somente IPv4. O DNS64 cria esses registros AAAA combinando um prefixo IPv6 configurável com o endereço IPv4 de uma pesquisa de registro A. O endereço IPv4 está incorporado nos últimos 32 bits do endereço IPv6.

O Cisco Secure Client 5.1.4.74 (MR4) agora oferece suporte à proteção Umbrella para redes somente IPv6. O módulo Umbrella descobre o prefixo NAT64 que está sendo empregado pelo gateway de rede consultando os resolvedores de DNS da LAN. Em seguida, ele faz a síntese de endereços IPv6 DNS64 usando o prefixo NAT64 descoberto quando o resolvedor DNS Umbrella está envolvido na resolução de nomes para aplicação de política.

Ativar o recurso

Windows

Crie um arquivo chamado `single_stack_ipv6.flag` e coloque-o neste diretório:

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

Depois que o arquivo de flag for colocado no diretório, reinicie o Cisco Secure Client para que o recurso entre em vigor.

MacOS

Crie um arquivo chamado `single_stack_ipv6.flag` e coloque-o neste diretório:

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

Depois que o arquivo de flag for colocado no diretório, reinicie o Cisco Secure Client para que o recurso entre em vigor.

Limitações

No CSC versão 5.1.4, o DNS64 é suportado apenas para tráfego DNS criptografado que vai para os resolvedores de DNS Umbrella. Ele não é suportado para tráfego DNS não criptografado, mesmo se a proteção for aplicada.

FAQ

Como posso saber se o DNS64/NAT64 é suportado em minha rede (macOS)?

Você pode usar o teste dig DNS64/NAT64.

Esses testes são projetados para qualificar uma rede na qual o host é configurado apenas com um endereço IPv6. Para acessar os serviços IPv4 existentes na Internet, o host deve usar DNS64 do resolvedor configurado para receber o endereço IPv6 sintetizado do endereço IPv4. Quando o Umbrella tiver o endereço sintetizado, ele garantirá que seja alcançável. Ele só poderá ser alcançado se o NAT64 estiver habilitado no gateway. O Umbrella usa o domínio "api-ipv4.opendns.com" porque há apenas endereços v4 configurados. Então, se a Umbrella obtém um endereço v6 no registro de resposta, a Umbrella sabe que ele foi sintetizado. Quando você `efetua ping6` no endereço retornado do comando `dig`, você sabe que o endereço sintetizado é convertido com êxito em um endereço v4 na Internet e a resposta é convertida de volta para o host.

DNS64

A primeira coisa que você quer testar:

➜ 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

Agora, você pode fazer ping no endereço sintetizado:

```
➜ 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
```

Como posso saber se o DNS64/NAT64 é suportado em minha rede (Windows)?

DNS64

A primeira coisa que você quer testar:

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

Resposta não autoritativa:

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

NAT64

Agora, você pode fazer ping no endereço sintetizado:

```
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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.