シングルスタックIPv6での包括DNS保護にCSCサポートを使用する

内容

はじめに

このドキュメントでは、Cisco Secure Client(CSC)を有効にして、シングルスタックIPv6ネットワークでUmbrella DNS保護をサポートする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrellaローミングセキュリティ のCisco Secure Clientに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

これまで、Cisco Secure ClientはIPv4のみのデュアルスタックネットワーク構成をサポートしていました。この記事では、Cisco Secure Client 5.1.4.74(MR4)以降のIPv6専用ネットワークのサポートについて説明します。 この機能は、フラグファイルを使用して有効にする必要があります。

背景

IPv6の普及に伴い、世界中のISPではIPv6アドレスのみを割り当てるケースが増加しています。ただし、多くのサーバリソースは依然としてIPv4のみのネットワーク上にあります。DNS64とNAT64の組み合わせは、IPv6専用クライアントとIPv4専用サーバの間で、基盤となるIPv4インフラストラクチャをクライアントが認識しなくてもシームレスな通信を可能にする移行機能です。

AAAAレコードはIPv6でのみ使用され、AレコードはIPv4でのみ使用されます。DNS64は、DNSにAレコードだけを持つサーバのAAAA(IPv6)レコードを合成することで機能し、IPv6専用クライアントがIPv4専用サーバに到達できるようにします。DNS64は、設定可能なIPv6プレフィクスとAレコードのルックアップで取得したIPv4アドレスを組み合わせて、これらのAAAAレコードを作成します。IPv4アドレスは、IPv6アドレスの最後の32ビットに埋め込まれます。

Cisco Secure Client 5.1.4.74(MR4)では、IPv6のみのネットワークに対するUmbrella保護をサポートするようになりました。Umbrellaモジュールは、LAN DNSリゾルバに照会することで、ネットワークゲートウェイに採用されているNAT64プレフィックスを検出します。次に、Umbrella DNSリゾルバがポリシー適用のための名前解決に関与している場合は、検出されたNAT64プレフィクスを使用してDNS64 IPv6アドレス合成が行われます。

機能の有効化

Windows

`single_stack_ipv6.flag`というファイルを作成し、次のディレクトリに配置します。

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

ディレクトリにフラグファイルを配置したら、Cisco Secure Clientを再起動して機能を有効にしてください。

MacOS

`single_stack_ipv6.flag`というファイルを作成し、次のディレクトリに配置します。

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

ディレクトリにフラグファイルを配置したら、Cisco Secure Clientを再起動して機能を有効にしてください。

制限事項

CSCリリース5.1.4では、DNS64はUmbrella DNSリゾルバに向かう暗号化されたDNSトラフィックに対してのみサポートされています。保護が適用されている場合でも、暗号化されていないDNSトラフィックに対してはサポートされません。

FAQ

ネットワーク(macOS)でDNS64/NAT64がサポートされているかどうかは、どのように確認できますか。

DNS64/NAT64 digテストを使用できます。

これらのテストは、ホストにIPv6アドレスのみが設定されているネットワークを特定するように設計されています。インターネット上の既存のIPv4サービスに到達するためには、ホストは設定されたリゾルバからDNS64を使用して、IPv4 IPアドレスの合成されたIPv6アドレスを受信する必要があります。Umbrellaは、合成されたアドレスを取得すると、到達可能であることを確認します。到達可能なのは、ゲートウェイでNAT64が有効になっている場合だけです。v4アドレスのみが設定されているため、Umbrellaは「api-ipv4.opendns.com」ドメインを使用します。そのため、Umbrellaが応答レコードでv6アドレスを取得すると、Umbrellaはそれを合成したことを認識します。`dig`コマンドから返されたアドレスに対して`ping6`を実行すると、合成されたアドレスがインターネット上でv4アドレスに正常に変換され、応答がホストに戻されます。

DNS64

最初にテストする項目は次のとおりです。

```
➜ 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

次に、合成されたアドレスにpingを実行できます。

```
➜ 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
```

ネットワーク(Windows)でDNS64/NAT64がサポートされているかどうかはどうすればわかりますか。

DNS64

最初にテストする項目は次のとおりです。

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

信頼できない回答：

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

NAT64

次に、合成されたアドレスにpingを実行できます。

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。