

단일 스택 IPv6에서 Umbrella DNS 보호를 위해 CSC 지원 사용

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[배경](#)

[기능 활성화](#)

[참](#)

[맥OS](#)

[제한 사항](#)

[FAQ](#)

[DNS64/NAT64가 내 네트워크\(macOS\)에서 지원되는지 어떻게 알 수 있습니까?](#)

[DNS64/NAT64가 내 네트워크\(Windows\)에서 지원되는지 어떻게 알 수 있습니까?](#)

소개

이 문서에서는 CSC(Cisco Secure Client)가 단일 스택 IPv6 네트워크에서 Umbrella DNS 보호를 지원하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella Roaming Security의 Cisco Secure Client를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

과거에는 Cisco Secure Client가 IPv4 전용 및 듀얼 스택 네트워크 컨피그레이션을 지원했습니다. 이 문서에서는 Cisco MR4(Secure Client 5.1.4.74)로 시작하는 IPv6 전용 네트워크에 대한 지원에

대해 설명합니다. 이 기능은 플래그 파일을 사용하여 활성화해야 합니다.

배경

IPv6가 널리 확산되면서 전 세계 ISP에서 IPv6 주소만 할당하는 경우가 늘고 있습니다. 그러나 여전히 많은 서버 리소스가 IPv4 전용 네트워크에 있습니다. NAT64와 결합된 DNS64는 클라이언트가 기본 IPv4 인프라를 인식하지 않고도 IPv6 전용 클라이언트와 IPv4 전용 서버 간의 원활한 통신을 지원하는 전환 기능입니다.

AAAA 레코드는 IPv6에서만 사용되고 A 레코드는 IPv4에서만 사용됩니다. DNS64는 DNS에 A 레코드만 있는 서버에 대한 AAAA(IPv6) 레코드를 합성하여 IPv6 전용 클라이언트가 IPv4 전용 서버에 도달할 수 있도록 합니다. DNS64는 구성 가능한 IPv6 접두사를 A 레코드 조회의 IPv4 주소와 결합하여 이러한 AAAA 레코드를 생성합니다. IPv4 주소는 IPv6 주소의 마지막 32비트에 포함됩니다.

Cisco MR4(Secure Client 5.1.4.74)는 이제 IPv6 전용 네트워크에 Umbrella 보호를 지원합니다. Umbrella 모듈은 LAN DNS 리졸버를 쿼리하여 네트워크 게이트웨이에서 사용 중인 NAT64 접두사를 검색합니다. 그런 다음 Umbrella DNS 확인자가 정책 시행을 위한 이름 확인에 관여할 때 검색된 NAT64 접두사를 사용하여 DNS64 IPv6 주소 합성을 수행합니다.

기능 활성화

창

single_stack_ipv6.flag라는 파일을 생성하여 이 디렉토리에 배치합니다.

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

플래그 파일이 디렉토리에 배치되면 Cisco Secure Client를 재시작하여 이 기능을 적용하십시오.

맥OS

single_stack_ipv6.flag라는 파일을 생성하여 이 디렉토리에 배치합니다.

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

플래그 파일이 디렉토리에 배치되면 Cisco Secure Client를 재시작하여 이 기능을 적용하십시오.

제한 사항

CSC 릴리스 5.1.4에서는 Umbrella DNS 확인기로 이동하는 암호화된 DNS 트래픽에 대해서만

DNS64가 지원됩니다. 보호가 적용된 경우에도 암호화되지 않은 DNS 트래픽에 대해서는 지원되지 않습니다.

FAQ

DNS64/NAT64가 내 네트워크(macOS)에서 지원되는지 어떻게 알 수 있습니까?

DNS64/NAT64 dig 테스트를 사용할 수 있습니다.

이 테스트는 호스트가 IPv6 주소로만 구성된 네트워크를 검증하도록 설계되었습니다. 인터넷에서 기존 IPv4 서비스에 도달하려면 호스트가 구성된 확인자의 DNS64를 사용하여 IPv4 IP 주소의 합성 IPv6 주소를 받아야 합니다. Umbrella에 종합 주소가 있으면 해당 주소에 연결할 수 있는지 확인합니다. 게이트웨이에서 NAT64가 활성화된 경우에만 연결할 수 있습니다. 구성된 v4 주소만 있으므로 Umbrella는 "api-ipv4.opendns.com" 도메인을 사용합니다. 따라서 Umbrella가 응답 레코드에서 v6 주소를 가져오면 Umbrella는 해당 주소가 합성되었음을 알게 됩니다. dig 명령에서 반환된 주소를 ping6할 때, 합성된 주소가 인터넷의 v4 주소로 성공적으로 변환되고 응답이 다시 호스트로 변환된다는 것을 알 수 있습니다.

DNS64

가장 먼저 테스트해야 할 사항은 다음과 같습니다.

```
→ 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

이제 합성된 주소를 ping할 수 있습니다.

```
→ 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
```

DNS64/NAT64가 내 네트워크(Windows)에서 지원되는지 어떻게 알 수 있습니까?

DNS64

가장 먼저 테스트해야 할 사항은 다음과 같습니다.

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

신뢰할 수 없는 대답:

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

NAT64

이제 합성된 주소를 ping할 수 있습니다.

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.