# Usa supporto CSC per protezione DNS Umbrella in IPv6 stack singolo

## Sommario



## Introduzione

In questo documento viene descritto come abilitare Cisco Secure Client (CSC) al supporto della protezione DNS Umbrella nelle reti IPv6 a stack singolo.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni di questo documento si basano su Cisco Secure Client in Umbrella Roaming Security.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica

In passato, Cisco Secure Client supportava configurazioni di rete solo IPv4 e a doppio stack. In questo articolo viene descritto il supporto per le reti solo IPv6 a partire da Cisco Secure Client 5.1.4.74 (MR4). La funzionalità deve essere attivata utilizzando un file di flag.

# Introduzione

Con la proliferazione diffusa di IPv6, gli ISP di tutto il mondo stanno assegnando sempre più solo indirizzi IPv6. Tuttavia, molte risorse server si trovano ancora su reti solo IPv4. Il DNS64, combinato con NAT64, è una funzionalità di transizione che consente una comunicazione senza interruzioni tra client solo IPv6 e server solo IPv4 senza richiedere ai client di essere a conoscenza dell'infrastruttura IPv4 sottostante.

I record AAAA vengono utilizzati esclusivamente con IPv6, mentre i record A vengono utilizzati esclusivamente con IPv4. DNS64 funziona tramite la sintesi dei record AAAA (IPv6) per i server che dispongono solo di record A nel DNS, consentendo ai client solo IPv6 di raggiungere i server solo IPv4. DNS64 crea questi record AAAA combinando un prefisso IPv6 configurabile con l'indirizzo IPv4 da una ricerca di record A. L'indirizzo IPv4 è incorporato negli ultimi 32 bit dell'indirizzo IPv6.

Cisco Secure Client 5.1.4.74 (MR4) supporta ora la protezione Umbrella per le reti solo IPv6. Il modulo Umbrella individua il prefisso NAT64 utilizzato dal gateway di rete interrogando i resolver DNS LAN. Esegue quindi la sintesi degli indirizzi IPv6 DNS64 utilizzando il prefisso NAT64 individuato quando il resolver DNS Umbrella è coinvolto nella risoluzione dei nomi per l'applicazione dei criteri.

# Attivare la funzionalità

## Windows

Creare un file denominato `single_stack_ipv6.flag` e inserirlo nella directory seguente:

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

Dopo aver inserito il file di flag nella directory, riavviare Cisco Secure Client per rendere effettiva la funzione.

## macOS

Creare un file denominato `single_stack_ipv6.flag` e inserirlo nella directory seguente:

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

Dopo aver inserito il file di flag nella directory, riavviare Cisco Secure Client per rendere effettiva la funzione.

### Limitazioni

In CSC release 5.1.4 DNS64 è supportato solo per il traffico DNS crittografato diretto ai resolver DNS Umbrella. Non è supportata per il traffico DNS non crittografato, anche se è applicata la protezione.

## Domande frequenti

### Come è possibile stabilire se DNS64/NAT64 è supportato nella rete (macOS)?

È possibile utilizzare il test di analisi DNS64/NAT64.

Questi test sono progettati per qualificare una rete in cui l'host è configurato solo con un indirizzo IPv6. Per raggiungere i servizi IPv4 esistenti su Internet, l'host deve utilizzare DNS64 dal resolver configurato per ricevere l'indirizzo IPv6 sintetizzato dell'indirizzo IPv4. Una volta che Umbrella ha l'indirizzo sintetizzato, si assicura che sia raggiungibile. Può essere raggiunto solo se NAT64 è abilitato sul gateway. Umbrella utilizza il dominio "api-ipv4.opendns.com" perché sono configurati solo indirizzi v4. Quindi, se Umbrella ottiene un indirizzo v6 nel record di risposta, Umbrella sa che è stato sintetizzato. Quando si esegue il `ping6` dell'indirizzo restituito dal comando `dig`, si è certi che l'indirizzo sintetizzato viene convertito correttamente in un indirizzo v4 su Internet e che la risposta viene tradotta nuovamente nell'host.

DNS64

La prima cosa da testare:

➜ 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

A questo punto, è possibile eseguire il ping dell'indirizzo sintetizzato:

```
➜ 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
```

## Come verificare se DNS64/NAT64 è supportato nella rete (Windows)?

### DNS64

La prima cosa da testare:

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

Risposta non autorevole:

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

### NAT64

A questo punto, è possibile eseguire il ping dell'indirizzo sintetizzato:

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).