在單堆疊IPv6中使用CSC支援保護Umbrella DNS

目錄

簡介

本檔案介紹如何在單一堆疊IPv6網路中啟用Cisco安全使用者端(CSC)以支援Umbrella DNS保護。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Umbrella漫遊安全中的思科安全使用者端。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

過去，思科安全客戶端支援僅IPv4和雙堆疊網路配置。本文描述從Cisco Secure Client 5.1.4.74(MR4)開始的對IPv6專用網路的支援。 必須使用標誌檔案啟用該功能。

背景

隨著IPv6的廣泛普及，世界各地的ISP越來越多地只分配IPv6地址。但是，許多伺服器資源仍然位於僅IPv4網路上。DNS64與NAT64是過渡功能，可在僅支援IPv6的客戶端和僅支援IPv4的伺服器之間實現無縫通訊，而無需客戶端瞭解底層IPv4基礎架構。

AAAA記錄僅用於IPv6，而A記錄僅用於IPv4。DNS64通過合成伺服器的AAAA(IPv6)記錄來工作，這些伺服器在其DNS中僅具有A記錄，從而允許僅使用IPv6的客戶端訪問僅使用IPv4的伺服器。DNS64通過將可配置的IPv6字首與A記錄查詢中的IPv4地址組合來建立這些AAAA記錄。IPv4地址嵌入在IPv6地址的最後32位中。

Cisco Secure Client 5.1.4.74(MR4)現在支援對僅IPv6網路的Umbrella保護。Umbrella模組通過查詢LAN DNS解析器來發現網路網關使用的NAT64字首。當Umbrella DNS解析程式參與策略實施的名稱解析時，它會使用發現的NAT64字首執行DNS64 IPv6地址合成。

啟用功能

Windows

建立名為`single_stack_ipv6.flag`的檔案，然後將其放入此目錄中：

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

標籤檔案放入目錄後，請重新啟動Cisco Secure Client以使功能生效。

macOS

建立名為`single_stack_ipv6.flag`的檔案，然後將其放入此目錄中：

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

標籤檔案放入目錄後，請重新啟動Cisco Secure Client以使功能生效。

限制

在CSC 5.1.4版中，只有進入Umbrella DNS解析器的加密DNS流量才支援DNS64。即使應用了保護，未加密的DNS流量也不支援此功能。

常見問題

如何知道我的網路(macOS)是否支援DNS64/NAT64?

您可以使用DNS64/NAT64挖掘測試。

這些測試旨在檢驗網路是否有效，以便主機僅配置有IPv6地址。為了到達Internet上的現有IPv4服務，主機必須使用配置的解析器中的DNS64來接收IPv4 IP地址的合成IPv6地址。一旦Umbrella擁有了合成地址，它將確保該地址可訪問。只有在網關上啟用了NAT64後，才能訪問該埠。Umbrella使用「api-ipv4.opendns.com」域，因為只配置了v4地址。因此，如果Umbrella在應答記錄中獲得v6地址，則Umbrella知道它已被合成。從dig命令返回的地址發出ping6命令時，您知道合成地址已成功轉換為Internet上的v4地址，並將回覆轉換回主機。

DNS64

您首先要測試的是：

```
➜ 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

現在，您可以對合成的位址執行Ping:

```
➜ 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
```

如何知道我的網路(Windows)上是否支援DNS64/NAT64?

DNS64

您首先要測試的是：

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

非授權答案：

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

NAT64

現在，您可以對合成的位址執行Ping:

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。