資訊處
Office of Information Technology

# 資安宣導

## 分散式阻斷服務攻擊

### －以DNS反射放大攻擊為例

中華民國110年11月

編號：018

# 大綱

一、什麼是分散式阻斷服務攻擊?

二、什麼是DNS反射放大攻擊

三、如何防範DNS反射放大攻擊?

四、如何正確設定本校DNS伺服器(很重要)

五、政令宣導-汰換大陸廠牌資通訊產品

六、參考資料

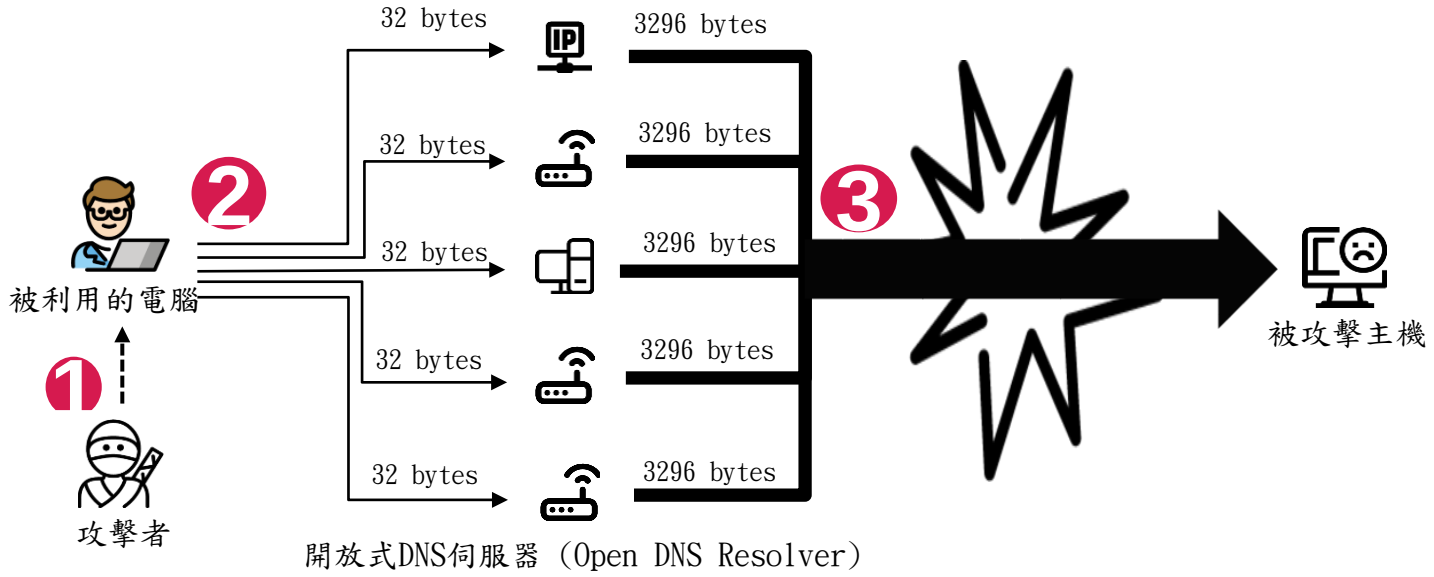
# 什麼是分散式阻斷服務攻擊?

- 阻斷服務攻擊 (Denial of Service, DoS)
  - ✓對被攻擊的目標主機(victim)傳送大量封包，使其網路或系統資源耗盡而無法提供正常服務的一種攻擊方式。
  - ✓攻擊成敗取決於封包瞬間流量的大小。
- **分散式**阻斷服務攻擊 (Distributed Denial of Service, **DDoS**)
  - ✓攻擊者利用**多部**受其控制或利用的電腦，針對攻擊對象**同時**發動阻斷服務攻擊，透過更大的封包流量來達成攻擊目的。
  - ✓駭客常利用開放式主機做為攻擊工具，並以反射攻擊將流量導向攻擊目標，再利用放大攻擊手法加大攻擊強度。

# 什麼是DNS反射放大攻擊（1/2）

- DNS反射放大攻擊

攻擊者假冒被害主機的IP，同時向多部分散在網路上的開放式DNSn四服器發送DNS遞迴查詢的請求，讓回應流量送往被害主機端，使其網路頻寬滿載或主機資源耗盡，造成服務中斷。




<DNS 反射放大攻擊示意圖>

# 什麼是DNS反射放大攻擊（2/2）

- 說明：

（1）攻擊者會先入侵安全防護不良的電腦做為跳板，以避免自己的真實位置被追查到。

（2）攻擊者利用跳板電腦同時對多部開放式DNS伺服器不斷地發送竄改來源IP的DNS遞迴查詢請求封包，使回覆封包反射(導向)到受害者主機端。

（3）DNS請求封包大約是32個字元，而經處理後的回覆封包可以達到3296個字元，攻擊者可以輕易將流量放大100倍左右。

✓ 假設攻擊者透過10部開放式DNS伺服器同時對被害主機發動攻擊，攻擊者只需對每部DNS伺服器送出10M的請求封包，就可以輕易將擊流量放大到10G左右，攻擊效益相當高。

# 如何防範DNS反射放大攻擊？(1/6)

- 在DNS的運作上，反射放大攻擊是難以避免的問題，唯有杜絕開放式DNS伺服器，才能有效防範DNS反射放大攻擊。
  - ✓關閉沒有必要存在的DNS伺服器，尤其是IP分享器內建的DNS。
  - ✓必要的DNS伺服器必須做好管理，嚴格限制服務範圍，避免成為開放式DNS伺服器。
  - ✓本校提供的DNS伺服器為140.123.5.100及140.123.1.100，僅供校內電腦使用。
  - ✓各單位自行架設的DNS伺服器必須做好管理，只提供給單位內部使用。

# 如何防範DNS反射放大攻擊？(2/6)

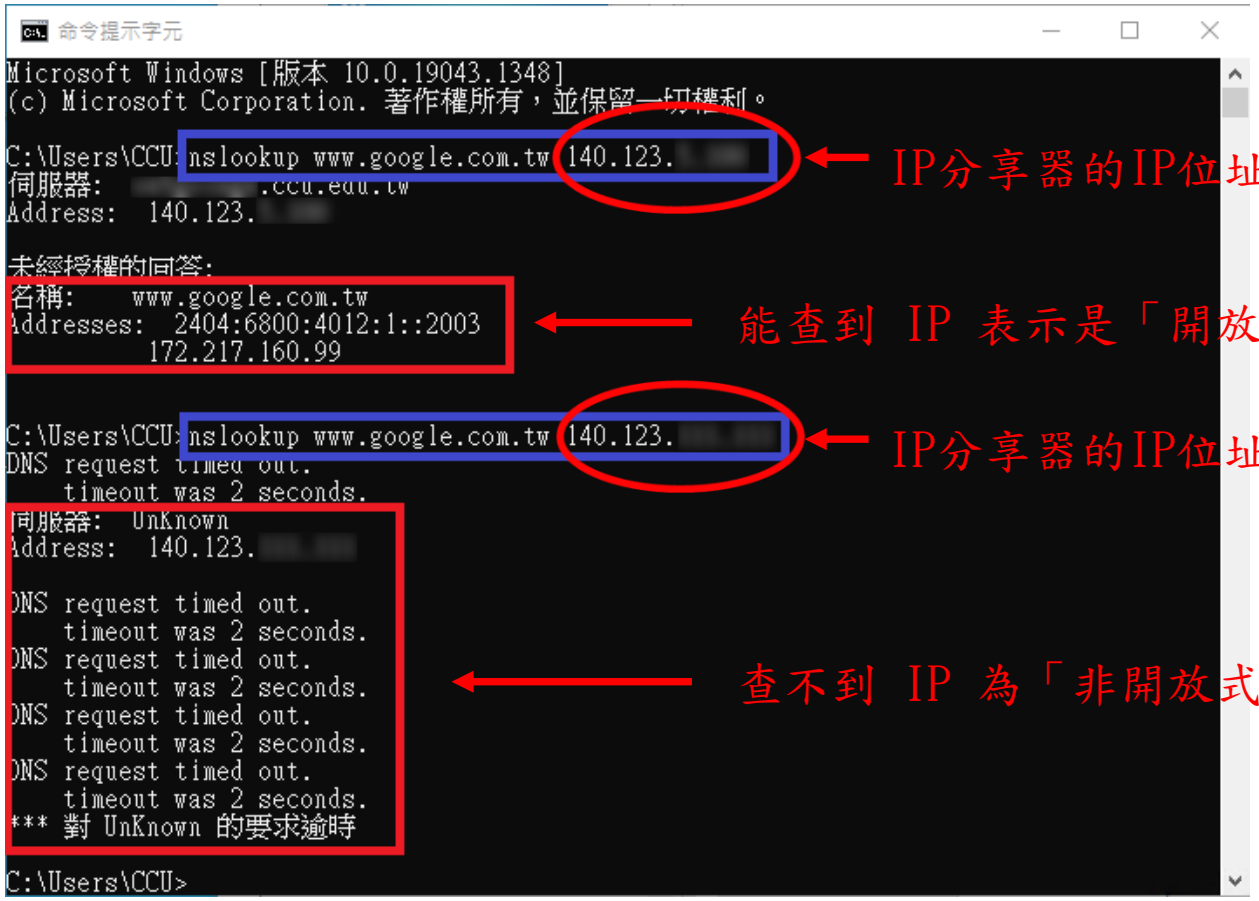
- 各單位常在辦公室自行安裝小型的有線或無線IP分享器，讓電腦及行動裝置可以方便的共用網路，而這些IP分享器經常成為開放式DNS伺服器的問題來源。

| | | | |
|---|---|---|---|
| 原發布編號 | NISAC-EWA-202111-41338 | 原發布時間 | 2021-11-16 16:40:37 |
| 事件類型 | 系統疑存在弱點 | 原發現時間 | 2021-11-16 08:16:30 |
| 事件主旨 | A-ISAC 140.123. . 用戶資訊設備疑似存在DNS Open Resolver弱點 | | |
| 事件描述 | 技服中心接獲外部情資，發現 A-ISAC 140.123. . 用戶資訊設備疑似存在DNS Open Resolver弱點，可供外部人士查詢任意網址，由於DNS遞迴查詢功能可被有心人士用做DDoS用途，此外，曝露網域內使用之DNS查詢伺服器，亦會增加被DNS快取污染攻擊的機率，為降低網路攻擊風險，建議評估服務開放外部存取之必要性，適時調整為內部網路存取或存取控管。 | | |
| 建議措施 | 1. 檢視系統上有無不明帳號。 2. 可以用終端機中nslookup指令確認附件IP的DNS服務是否開啟DNS Open Resolver。 範例: 欲確認168.x.x.x是否開啟DNS Open Resolver，可用指令 nslookup www.google.com.tw 168.x.x.x，如果查詢有回答網路位址，表示有開啟。 3. 系統上DNS服務若非必要，建議關閉，或是調整服務設定，限制遞迴查詢功能僅提供本地網域使用者。 | | |
| 參考資料 | 請參考上傳附件 | | |
| 如果此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業 | | | |
| 如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。 | | | |

# 如何防範DNS反射放大攻擊？(3/6)

- 如何測試IP分享器是否為開放式DNS伺服器？

  方法一：在Windows的命令提示字元視窗，使用nslookup指令測試



# 如何防範DNS反射放大攻擊？(4/6)

方法二：使用 Open recursive DNS resolver test 線上服務


輸入IP分享器位址，然後按「Test this IP」鈕即可

測試結果：

- ✓ Open recursive resolver detected on 140.123.xxx.xxx （開放式）
- ✓ Recursive resolver is not detected on 140.123.xxx.xxx（非開放式）

# 如何防範DNS反射放大攻擊？(5/6)

- IP分享器廠牌型號繁多，設定方式各異難以詳列，有開放式DNS 問題的設備，請自行參考使用手冊或洽廠商協助處理，以下僅就設定原則提供參考：
  - ✓外部網路（或稱為：WAN / 網際網路 ...）

# 如何防範DNS反射放大攻擊？（6/6）

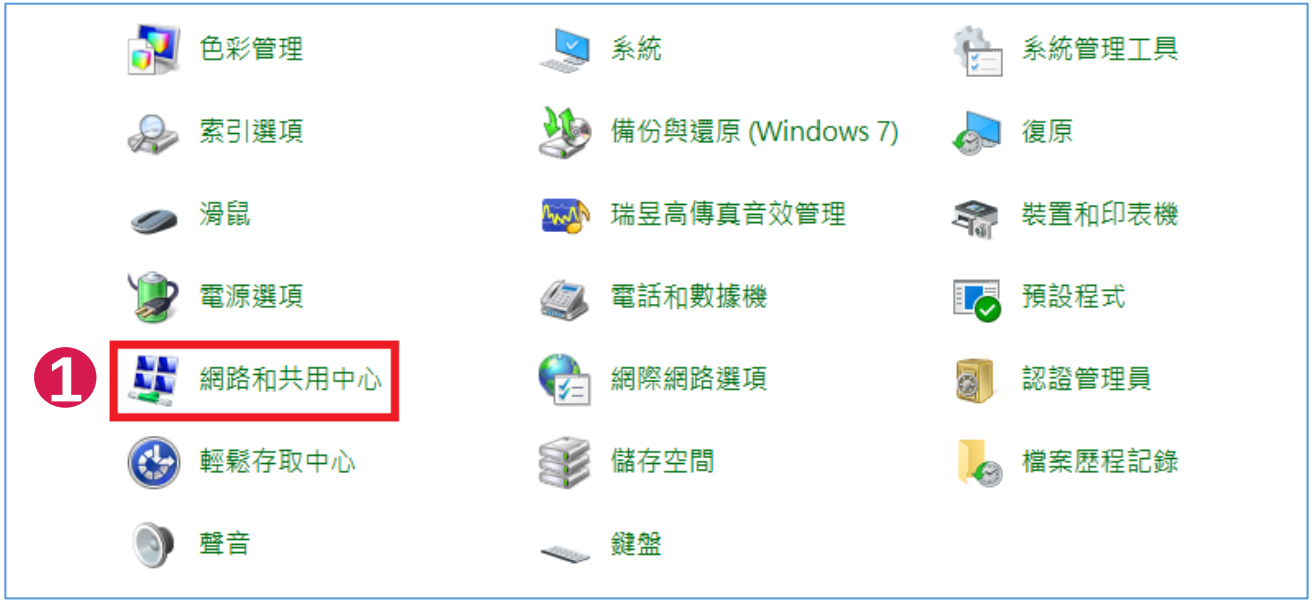
✓內部網路（或稱為：LAN / 區域網路 ...）


※設定畫面若出現 DNS Relay 或 DNS Proxy，請取消勾選

# 如何正確設定本校DNS伺服器（1/3）

- 本校提供的DNS伺服器為140.123.5.100和140.123.1.100，僅供校內網路(140.123.*.*)使用。
- Win10 可以從控制台進行設定：

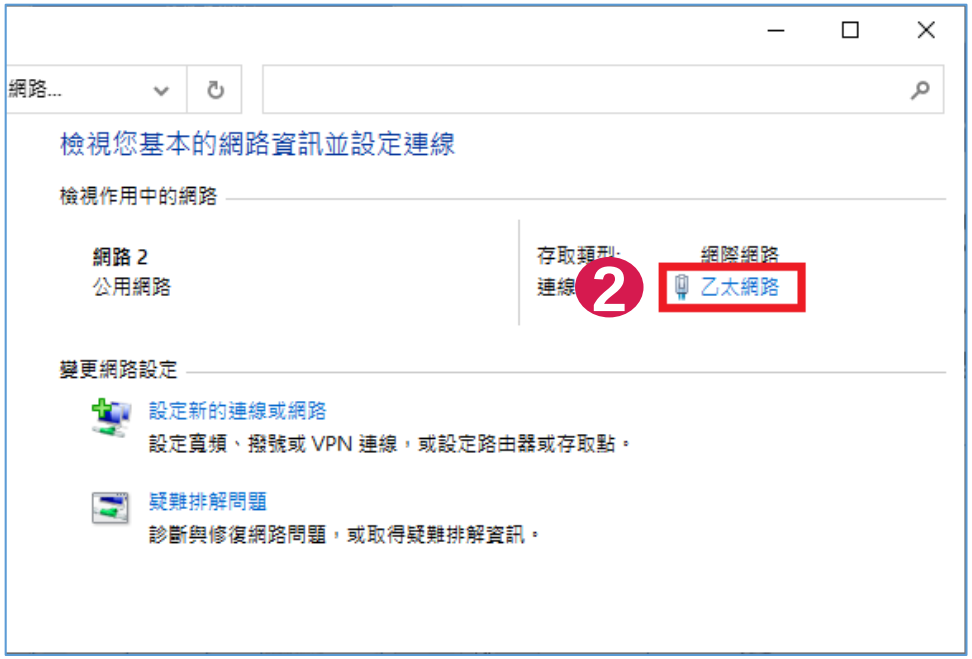
  (1) 開啟「網路和共用中心」

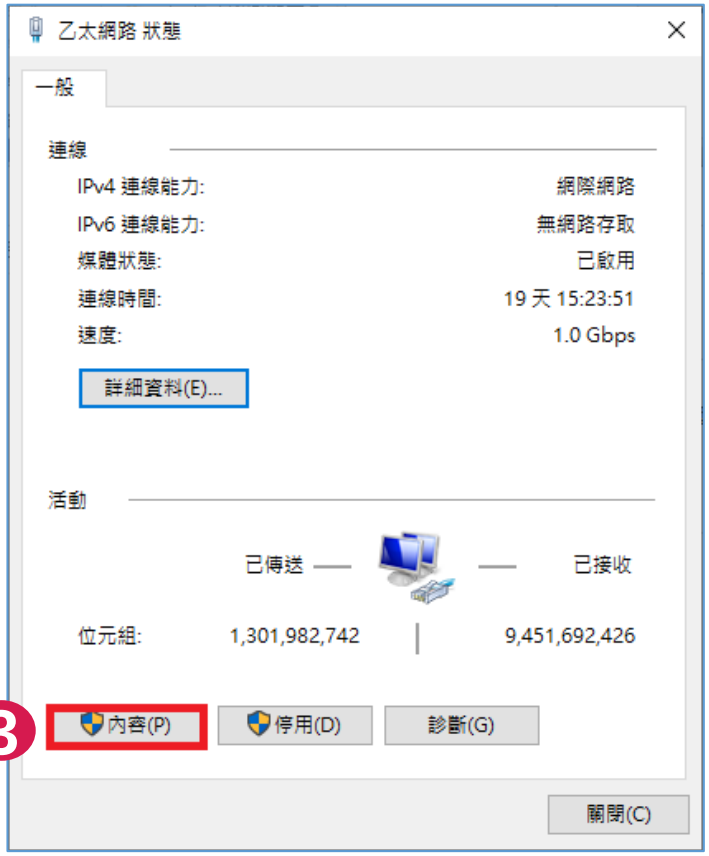


# 如何正確設定本校DNS伺服器（2/3）

(2) 在網路和共用中心視窗中，點選「乙太網路」 。

(3) 在乙太網路狀態視窗中，點擊「內容」鈕。

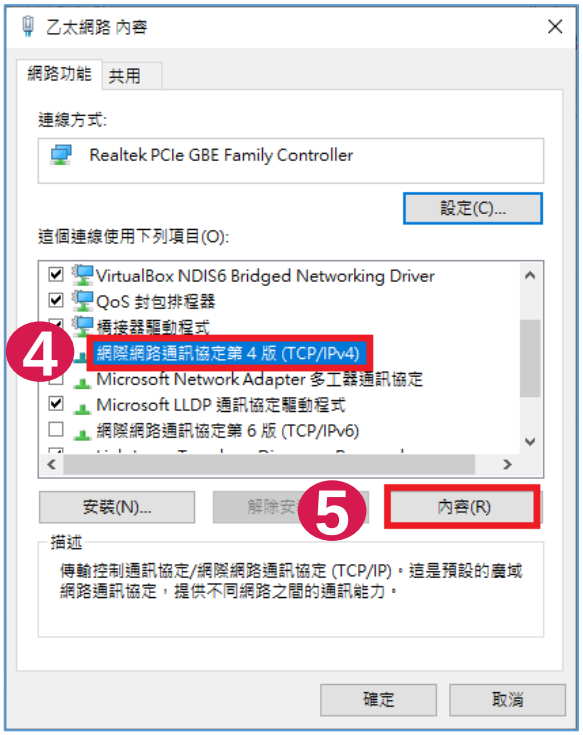


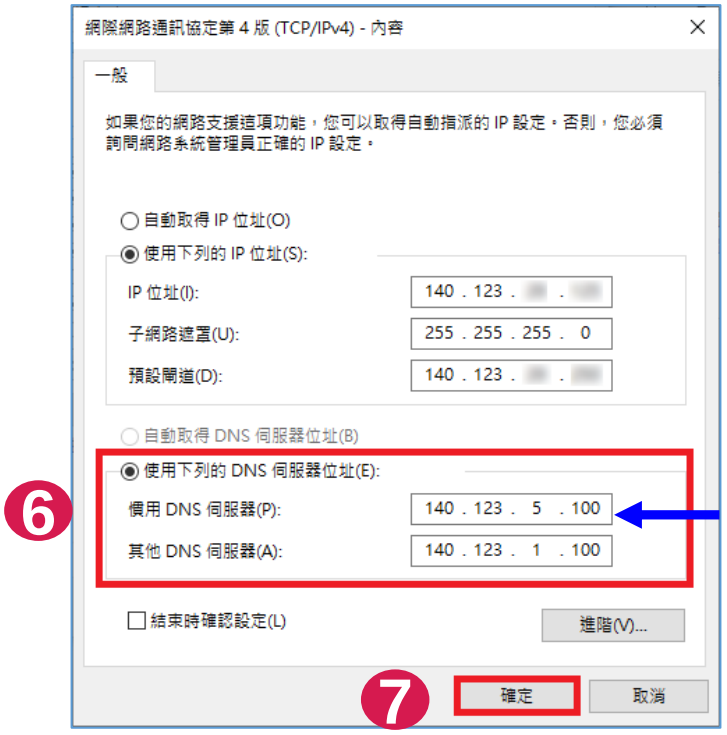



# 如何正確設定本校DNS伺服器（3/3）

（4）點選「網際網路通訊協定第4版(TCP/IPv4)」後按「內容」鈕。

（5）點選「使用以下的DNS伺服器位址」，設定本校DNS伺服器位址後按「確定」鈕即可完成設定。




本校的DNS伺服器：
140.123.5.100(優先)
140.123.1.100

# 政令宣導-汰換大陸廠牌資通訊產品

- 請各單位於110年底前完成汰換所使用或採購大陸廠牌資通訊產品（含軟體、硬體及服務）。
- 公務機關使用資通訊產品（含軟體、硬體及服務）相關原則：
  - ✓ 公務或線上教學用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
  - ✓ 個人資通訊設備不得處理公務事務，亦不得與公務環境介接。
  - ✓ 各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

受文者：如正副本行文單位
發文日期：中華民國110年1月25日
發文字號：中正資訊字第1100000266號
速別：普通件
密等及解密條件或保密期限：
附件：「教育部及所屬公務機關擴大盤點及汰換具資安疑慮產品討論會議」紀錄

主旨：檢送教育部109年12月29日「教育部及所屬公務機關擴大盤點及汰換具資安疑慮產品討論會議」紀錄，請查照並配合辦理。

說明：

一、依據教育部110年1月11日臺教資(四)字第1090190896號函辦理。

二、前已以110年01月07日中正資訊字第1100000018號函，請各單位於110年底前完成汰換所使用或採購大陸廠牌資通訊產品（含軟體、硬體及服務），並配合擴大盤點（盤點範圍為全機關，包含委外廠商及其分包廠商）。

三、為保障線上教學資通安全，維護師生權益，採購或使用線上教學平台時做好審慎評估，不得使用大陸廠牌產品（從嚴認定），已採購或使用者，應依大陸廠牌資通訊產品擴大盤點及汰換作業方式辦理。

四、請依旨揭會議討論事項案由二決議，落實辦理及依限完成。

# 參考資料

- DNS 服務，你對於 DNS 懂多少？
- 如何避免DNS主機被當成攻擊跳板
- Open DNS resolver 的問題
- IP分享器可能成為放大攻擊的幫兇
- 行政院國家資通安全會報（資通安全網路月報-109年12月）
- DDoS 攻擊簡介與案例分享（行政院國家資通安全會報 技術服務中心）

資訊處
Office of Information Technology

# 感謝閱讀