1. 服務主機防護設定

本文件內容提供業者常見之服務主機(如網站、NTP及DNS)相關防護設定，以維持服務主機的可用性，同時避免遭利用主動或間接參與DDoS攻擊，而造成網路頻寬損耗。

## 網站服務主機調校步驟

### Linux事前防護設定(以ubuntu上安裝iptables與Apache為例)

針對網頁伺服器調校設定進行調校，例如系統參數、IP、Port及封包FLAG等加以辨別與限制，可於事前防禦DDoS攻擊。本文件係以下列環境進行設定說明，如業者網頁伺服器非以下環境，可由伺服器服務廠商協助設定。

#### 系統設定

* 啟用SYN Cookie

|  |
| --- |
| sysctl –w net.ipv4.tcp\_syncookie=1 |

* 縮短SYN Timeout時間

|  |
| --- |
| sysctl –w net.netfilter.nf\_conntrack\_tcp\_loose=0sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_established=1800sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_close=10sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait=10sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait=20sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_last\_ack=20sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_syn\_recv=20sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_syn\_sent=20sysctl –w net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait=10 |

#### iptables

iptables是一個運行在Linux被廣泛使用的應用軟體，通過控制Linux內核netfilter模組，來管理網路封包的流動與轉送。

* 限制對PORT的連線頻率

|  |
| --- |
| iptables -A INPUT -p tcp --dport (port-here) -m state --state NEW -m recent --set --name DDOS –rsourceiptables -A INPUT -p tcp --dport (port-here) -m state --state NEW -m recent --update --seconds 5 --hitcount 5 --name DDOS --rsource -j DROP |

* 限制單一PORT所接受之IP連線數

|  |
| --- |
| iptables -A INPUT -p tcp --syn --dport (port-here) -m connlimit --connlimit-above (limit-here) --connlimit-mask 32 -j REJECT --reject-with tcp-rese |

* 阻擋特定IP

|  |
| --- |
| iptables -A INPUT -s (ip-here) -j DROP |

* 阻擋進行PORT掃描之IP一天

|  |
| --- |
| iptables -A INPUT -m recent --name portscan --rcheck --seconds 86400 -j DROPiptables -A FORWARD -m recent --name portscan --rcheck --seconds 86400 -j DROP |

#### Apache模組

* qos模組
* 【步驟1】安裝mod\_qos

|  |
| --- |
| apt-get install libapache2-mod-qos |

* 【步驟2】至/etc/apache2/mods-availables/目錄下依需求修改qos.conf後儲存

|  |
| --- |
| QS\_ClientEntries 100000 #最多同時容許多少不同IP連線QS\_SrvMaxConnPerIP 50 #單一IP最多容許幾個連線MaxClients 256 #最大TCP連線數QS\_SrvMaxConnClose 180 #當TCP連線數達到此數時，取消keep-alive選項 |

* 【步驟3】啟用該模組並重 啟apache伺服器
* Reqtimeout模組
* 【步驟1】至/etc/apache2/mods-availables/目錄依需求修改reqtimeout.conf後儲存

|  |
| --- |
| #予header10至20秒的等待時間，最小傳送速率為500bytes/秒RequestReadTimeout header=10-20,minrate=500#予body最多10秒的等待時間，最小傳送速率為500bytes/秒RequestReadTimeout body=10,minrate=500 |

* 【步驟2】啟用該模組並重啟apache伺服器
* evasive模組
* 【步驟1】安裝mod\_evasive

|  |
| --- |
| apt-get install libapache2-mod-evasive |

* 【步驟2】至/etc/apache2/mods-availables/目錄下依需求修改evasive.conf後儲存

|  |
| --- |
| DOSHashTableSize 3097 #用來儲存黑名單的檔案大小，所以當網站流量越大，此值就需要越大。DOSPageInterval 2 #DOSPageCount的時間區段，單位為秒DOSSiteInterval 2 #DOSSiteCount的時間區段，單位為秒DOSPageCount 5 #DOSPageInterval所設定的時間區段中，同一個來源 IP 存取同一個頁面的最大存取次數DOSSiteCount 100 #DOSSiteInterval所設定的時間區段中，同一個來源 IP 可同時發出 HTTP 存取的最大次數DOSBlockingPeriod 600 #超過上述所設定的最大次數時，暫時停止對方存取的時間，單位為秒 |

* 【步驟3】啟用該模組並重啟apache伺服器

### Windows事前防護設定(以Windows Server上安裝IIS為例)

#### 啟用並設定Dynamic IP Restrictions

* 請至http://www.iis.net/downloads/microsoft/dynamic-ip-restrictions，下載並安裝「Dynamic IP Restrictions」元件(Windows 10已內建此元件)，詳見圖1。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. Dynamic IP Restrictions元件下載
 |

* 開啟IIS管理員
* 選擇特定站台或全域進行設定
* 開啟Dynamic IP Restrictions(詳見圖2)，依需求進行防護設定，相關欄位說明詳見表1。

|  |
| --- |
|  |
| 行政院國家資通安全會報技術服務中心整理 |
| 1. Dynamic IP Restrictions設定
 |

1. Dynamic IP Restrictions欄位說明

| **欄位** | **說明** |
| --- | --- |
| **Deny IP address based on the number of concurrent requests** |
| Maximum number of concurrent requests | 設定用戶端的最大並行要求，若超出時執行Action Type所指定的動作。 |
| **Deny IP addresses based on number of requests over a period of time** |
| Maximum number of requests | 設定要求允許進入IIS的最大數量。 |
| Time period (in seconds) | 設定要求最大數量的監測週期時間。 |
| Deny for time period (in seconds) | 設定超出要求最大數量時，封鎖要求的時間週期。 |
| **Deny Action** |
| Action type | 當發生必須封鎖的動作時，要執行的動作。 |
| 行政院國家資通安全會報技術服務中心整理 |

#### 設定參考資訊

業者可參考以下網站資訊，依需求進行設定：

* https://www.microsoft.com/taiwan/technet/iis/expand/DynamicIPRestrictions.aspx
* http://www.iis.net/learn/manage/configuring-security/using-dynamic-ip-restrictions

## NTP服務主機調校步驟

為避免NTP服務主機遭利用進行反射式放大攻擊，造成額外頻寬耗損，建議業者採取以下其一動作執行以關閉monliste功能，以下以ubuntu上安裝NTP為例：

* 將NTP軟體版本升級至4.2.7p26之後的版本，以將monlist功能完全移除。
* 若無法進行升級，則在ntp.conf配置文件中新增Disable Monitor選項後重啟NTP服務以關閉monlist功能。
* 【步驟1】修改/etc/ntp.conf後儲存

disable monitor

* 【步驟2】重啟NTP服務

sudo service ntp restart

* 【步驟3】輸入指令確認是否有收到回應，若無則代表設定完成

ntpdc -n -c monlist 192.0.2.1

ntpq -c rv 192.0.2.1

## DNS服務主機調校步驟

為避免DNS服務主機遭利用進行反射式放大攻擊，造成額外頻寬耗損，建議業者採取以下動作，防止主機主動或間接參與DDoS攻擊，而造成網路頻寬損耗。以下以ubuntu上安裝BIND9為例：

* 限制可使用DNS遞迴功能之IP範圍

DNS遞迴是一種名稱解析技術，DNS伺服器可以代替提出要求的用戶端查詢其他伺服器，用以完整解析名稱後將查詢結果傳回該用戶端，如非必要應該限制服務存取對象，避免攻擊者濫用查詢服務造成伺服器本身直接或間接參與攻擊。

* 【步驟1】修改/etc/bind/named.conf後儲存

//設定能存取 DNS 服務的 IP 範圍

acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };

* 【步驟2】修改/etc/bind/named.conf.options後儲存

//僅允許符合上述 設定的網段進行遞迴解析請求

options {

 ………

 allow-recursion { corpnets; };

 ………

 };

* 【步驟3】重啟DNS服務

sudo service bind9 restart

* 設定DNS Response Rate Limiting(DNS RRL)

若所建置的DNS伺服器必須提供外部服務的轉址功能，可透過限制攻擊者對DNS服務主機產生的密集查詢之方式防止成為DRDoS的執行跳板或者攻擊目標。

* 【步驟1】修改/etc/bind/named.conf.options後儲存

options {

 ………

 rate-limit {

 responses-per-second 5;

 window 5;

 };

………

};

* 【步驟2】重啟DNS服務

sudo service bind9 restart