實做於 P4 的 DDoS 防禦

DDoS Defense Implemented on P4

指導教授 張燕光
專題成員 楊逸婷、龍帆軒、楊舒翔
開發工具 P4、Mininet、Scapy、Python
測試環境 Linux Ubuntu 20.04

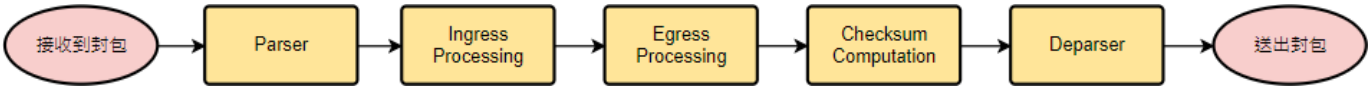
一、簡介：

DDoS 全名為 Distributed Denial of Service，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。

近年來因為 IoT 產品的增加，攻擊者可以輕鬆地建立龐大的殭屍網路來產生巨量的 DDoS 攻擊，研究指出每個月有總共 400,000 起 DDoS 攻擊發生。但是 DDoS 防禦卻沒有跟上 DDoS 攻擊的快速發展。現今最被常使用的防禦機制為流量清洗中心，但是架起流量清洗服務中心的設備卻不便宜且不易維護。雖然這些硬體設備在處理封包上非常有效率，但是相對地也在容量、功能性、設置地點非常不彈性。當有新的攻擊出現時，也要去更新這些硬體設備，所以也會產生一筆不菲的經濟支出。

最近熱門的網路題目——Software Defined Network (SDN) 就可以解決一些上述的問題。SDN 是一種網路設計理念，處於 datalink layer 與 network layer 上。SDN 主要有三大架構：Application Layer、Control Layer、Infrastructure Layer，將 router 的 control plane (routing、ARP、DHCP) 與 data plane (IPv4、IPv6) 分開，交給 controller 負責。其目的就是為了簡化過多的網路結構，通過軟體統一地進行調整與控制。SDN 有三大優勢，分別為降地成本、提高效率、安全穩定。相同的功能下， 透過 SDN 運行的伺服器所承擔的成本遠低於硬體設備。SDN 網路架構在進行升級的時候，網路配置的時間也低於傳統網路。

現今 SDN 透過 programmable swtich 與 domain-specific language 來達成將 data plane 程式化。而在 domain-specific language 裡最被大家使用的語言就是 P4。P4 全名為 Programming Protocol-Independent Packet Processors，P4 讓我們可以透過程式定義好對每個封包的行為，使得對封包的存取與運作變得更有效率。

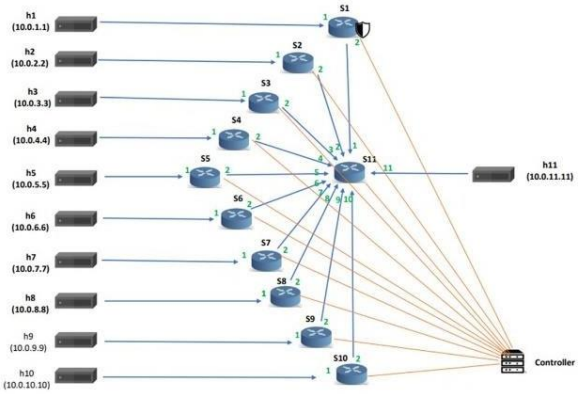


（圖一）P4 程式架構圖

二、方法：

首先選定好要實做的防禦種類，之後再將 topology 定義好。使用 scapy 跟python 分開測試完成的防禦機制，因為現今 Openflow 很常被使用，所以 switch 自己並不知道 topology，所以我們再加上了 LLDP 讓 controller 可以得知各個節點的連接狀況。最後再將所有的機制整合起來，統一測試。

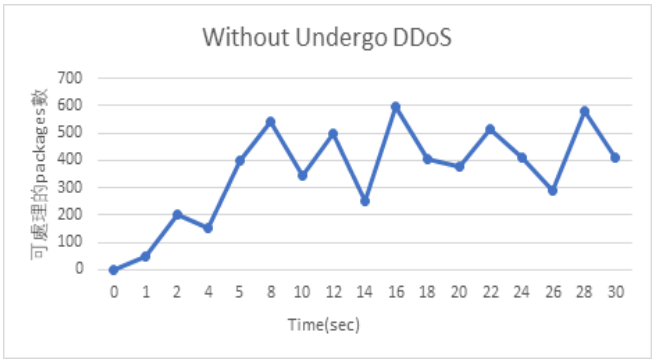
我們選定的 DDoS 攻擊分別是：SYN Flood、SYN-ACK Flood、DNS Amplification、ICMP Flood。



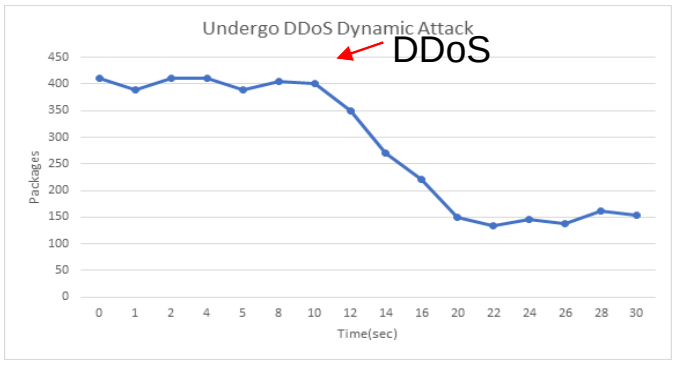
（圖二） Topology 架構圖

三、測試結果：

在沒有 DDoS 攻擊發生的時候，可以看到封包最大的流量大概是在 400 到 500 這個區間裡（圖四）震盪。

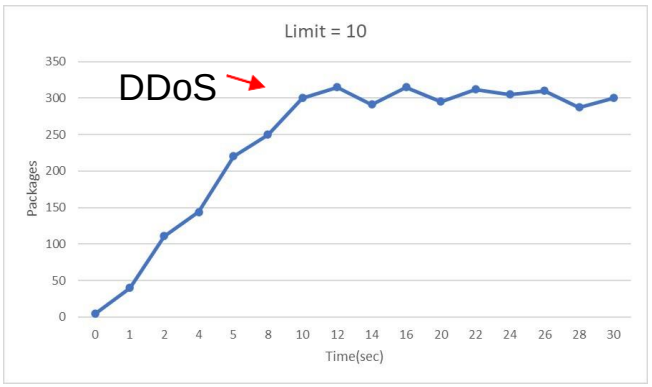


（圖三）沒有 DDoS 發生時封包流量圖

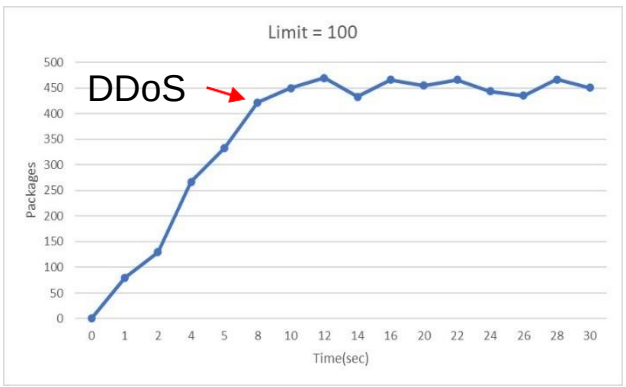


（圖四）DDoS 發生但是防禦並沒有開啟

看到 DDoS 防禦開啟後，從原本被攻擊時，正常封包只有 150 個左右，到現在因為限制了異常的 IP 流量，所以正常封包的流量又變回正常。最後我們調整 P4 程式裡 limit 的值來比較不同 limit 的封包流量狀況。



（圖五） 將 limit 設定成 10



（圖六）將 limit 設定成 100

防禦開啟的時候，switch 會判斷這個 IP 傳送的封包數量有沒有超過一個值 (limit) ，因為DDoS 都是以大量的封包來塞滿 host ，佔據資源，所以將流量不正常的 IP 限制住，讓真正不是攻擊的封包通過，是我們防禦機制的核心概念。

如果將 limit 的值調整到太大，會導致通過 switch 防禦的封包增加，會無法攔截到攻擊的封包。如果將 limit 設定的太小，會導致通過的封包太少，限制到不是攻擊的封包。所以將 limit 的設定成一個最佳的值是很重要的。

四、結論：

透過 P4 語言的幫助，我們可以撰寫 switch 間的處理邏輯，讓新的 Protocal 與功能開發能夠更加容易。同時，P4 在數據平面上的靈活性，使測試的工作能夠更為順利的進行，也能夠利用 switch 間的溝通達到更好的效果。P4 具備的 Protocal Independence、Target Independence 和 In-Field Re-Configurability 三種特性，使其能夠更靈活的與其他主題配合。相信除了本次的 DDoS 防禦，在各個領域上，P4 都能夠貢獻出自身的一份力量吧。