

+ 如何透過 網路 設備 來 防禦 DDoS 攻擊 的 方法



CCTV Botnet in Our Own Back Yard

在 過去 幾年 中，我們 看到 許多 網路 攻擊 事件 發生，其中 最 常見 的 就是 DDoS 攻擊。DDoS 攻擊 的 原理 是 透過 大量的 惡意 IP 地址，向 目標 伺服器 發送 大量的 請求，導致 伺服器 資源 耗盡，無法 正常 運作。在 過去 幾年 中，我們 看到 許多 網路 攻擊 事件 發生，其中 最 常見 的 就是 DDoS 攻擊。DDoS 攻擊 的 原理 是 透過 大量的 惡意 IP 地址，向 目標 伺服器 發送 大量的 請求，導致 伺服器 資源 耗盡，無法 正常 運作。在 過去 幾年 中，我們 看到 許多 網路 攻擊 事件 發生，其中 最 常見 的 就是 DDoS 攻擊。DDoS 攻擊 的 原理 是 透過 大量的 惡意 IP 地址，向 目標 伺服器 發送 大量的 請求，導致 伺服器 資源 耗盡，無法 正常 運作。

如何 防禦 DDoS 攻擊

防禦 DDoS 攻擊 的 方法 有 許多，其中 最 重要 的 就是 網路 設備 的 配置。網路 設備 的 配置 包括 防火牆、路由器和交換機等。防火牆 可以 過濾 掉 惡意 的 請求，防止 惡意 IP 地址 進入 網路。路由器 和 交換機 可以 透過 流量 分析，識別 出 惡意 的 流量，並 將其 丟棄。此外，我們 還 可以 透過 雲 服務 來 防禦 DDoS 攻擊。雲 服務 可以 提供 大量的 資源，用於 吸收 惡意 的 流量，防止 目標 伺服器 受到 攻擊。防禦 DDoS 攻擊 的 方法 有 許多，其中 最 重要 的 就是 網路 設備 的 配置。網路 設備 的 配置 包括 防火牆、路由器和交換機等。防火牆 可以 過濾 掉 惡意 的 請求，防止 惡意 IP 地址 進入 網路。路由器 和 交換機 可以 透過 流量 分析，識別 出 惡意 的 流量，並 將其 丟棄。此外，我們 還 可以 透過 雲 服務 來 防禦 DDoS 攻擊。雲 服務 可以 提供 大量的 資源，用於 吸收 惡意 的 流量，防止 目標 伺服器 受到 攻擊。

□□□□ □□□□□ □□□□ □□□□□□□□ □□□□□ □□□□□□□□□□

[illegible]

:

0000 00000000 00000000 0000 0000 0000 00 00000000 0000 00000000 00000000 0000 0000 00 00000000 0000 00
 HTTP Get 00 000000 (DDoS) 0000 000000 00000000 0000 0000 00 00000000 0000 00000000 .0000 0000 0000 0000000000
 HTTP Flood .000000 00 00000000 00 00 0000000000 0000 20 00000000 00000000 00 00000000 .0000 0000 00000000 Flood
 00 00000000 00000000 0000 00 .00000000 0000 00000000 000000 0000 00 00 000000 000000 00 DDoS 000000 000000 0000 00
 00 00000000 00000000 0000 000000 0000 00000000 00 00000000 00 00000000 00 00000000 0000 00000000 00000000 000000
 000000 000000 00 .00000000 0000 00 00000000 000000 00 00000000 00000000 00 000000 0000 00 000000 0000 .00000000 0000
 malformed 0000000000 00 00 000000 00000000000000 000000 0000 00 0 00000 0000 00000000 0 00000000 00 00000000
 0000000000 0000 0000000000 000000 .000000 000000 00000000 000000 00 0000000000 00000000 spoofing 00 packets
 .000000 000000 000000 000000 0000 0000 00 00000000 00000000 0 000000000000 000000 000000

USB Killer 2.0 :

00000000 0000 0000 00000000 00000000 0000 0000 00 00 IP 00000000 00 00000000 00 00000000 000000 0000 00
 000000000000 0000 00 000000000000 00000000 .0000 00000 000000000000 000000000000 00 IP 00000000 0000 00 00000000
 00 000000 00000 0000 00 00000 00000000 00000000000000000000 000000 00 000000000 0000 000000000000 00000 00 00000
 000000000 BusyBox 00 00000000 00000 0000 0000 00 00 00000000000000 0000000 .0000 000000000000 000000000000
 000000000000 00 000000000 00000 00 0000 00000000 00000000 0 0000 00 000000000000 00000 00 BusyBox .0000000000
 00000000 00 00 0000000 000000 000000 000000 000000000000 .00000000 00000 00000000 00000 000000 00000000 000000 00
 00 ELF Bashlite 000000000 00 00000000 00000000 0000 00000000 000000 0000 00 000000 00000000000000 00000 00 00
 BusyBox 00 00 00000 0000 000000000000 00000 000000000 00 0000 00000 000000 00 00000000 Bashlite .00000 000000
 00000 000000000 00000 0000000000 00000 00000 00 0000 00000 00000000 0000 .00000 00 00000000 00000000
 0000 0000 .0000000 00000 00 0000000 brute force 00000 00 000000000000 0000000 00 TelNet/SSH 0000 0000000000
 000000000000 000000000000 00000 0000 000000 .00000 00 DDos 00000 000000000000 00 00000000 00000 00000 00 0000
 .000000 00000 00 00000000 DDos 00000 000000000000 00000000 000000000000 00 CCTV

