



DDos 攻擊是指攻擊者利用大量的 IP 地址向目標系統發送大量的請求，導致目標系統資源耗盡，無法正常服務。DDos 攻擊的種類很多，常見的有 SYN Flood、UDP Flood、ICMP Flood 等。攻擊者通常會利用僵尸網絡（Botnet）進行攻擊，這些僵尸機是由攻擊者通過惡意軟件感染普通電腦、手機等設備而形成的。DDos 攻擊的代價很高，據統計，全球每年因 DDos 攻擊造成的損失高達數十億美元。為了防止 DDos 攻擊，企業和個人需要採取有效的防禦措施，如使用防火牆、入侵檢測系統、DDos 防禦服務等。

ISP (Internet Service Provider) 是提供互聯網接入服務的企業。ISP 的職責是為用戶提供穩定、高速的網絡連接。ISP 通常會與多個上游網絡運營商合作，以確保網絡的穩定性和覆蓋範圍。ISP 還負責管理用戶的賬戶、提供技術支持和故障排除服務。在 DDos 攻擊發生時，ISP 可以通過封鎖攻擊源 IP 地址、限制流量等方式來減輕攻擊的影響。然而，ISP 的防禦能力有限，企業和個人需要採取更全面的防禦措施。

DDos 攻擊的防禦措施包括：1. 使用 DDos 防禦服務：專業的 DDos 防禦服務可以實時監測網絡流量，識別並阻斷惡意流量。2. 配置防火牆和入侵檢測系統：防火牆可以過濾掉可疑流量，入侵檢測系統可以發現異常活動。3. 分散服務器：將服務器部署在多個地理位置，可以分散攻擊的影響。4. 定期更新軟件：確保系統和服務器軟件是最新的，可以防止已知漏洞被利用。5. 備用網絡：建立備用網絡連接，可以在主網絡受到攻擊時切換使用。6. 與 ISP 合作：與 ISP 建立緊密的合作關係，可以獲得更及時的支持和建議。

:□□□□ □□□□

□□□□□□

:□□□□□□ □□□□□□

11:02 - 06/05/1395

:□□□□□□

[DDoS](#) - [□□□□□□□□](#) - [□□□□□□□□□□](#) - [□□□□](#)

---

<https://www.shabakeh-mag.com/security/3945>:□□□□ □□□□□□