**1. 水平擴展（Horizontal Scaling）是什麼？**

水平擴展，也稱為**平行擴展**，指的是通過增加更多的伺服器或節點來擴大系統的處理能力。這與垂直擴展（Vertical Scaling）不同，垂直擴展是指通過升級單個伺服器的硬體（例如增大 CPU、內存、硬碟空間等）來提高性能。

水平擴展通常會部署多台伺服器或節點來共享負載，並且這些伺服器之間可以並行處理請求。這樣，即使某一台伺服器遭到攻擊或負載過高，其他伺服器仍能繼續運行，從而保障整體服務的穩定性。

**2. 如何通過水平擴展防止 DDoS 攻擊？**

在 DDoS 攻擊中，攻擊者會從多個分佈的機器發送大量的請求來淹沒目標伺服器，這會讓目標伺服器無法處理合法的用戶請求，最終導致服務中斷。採用水平擴展可以有效分散這些流量，防止單個伺服器被過多的流量擊垮。

**具體的運作方式如下：**

* **增加伺服器數量：** 當 DDoS 攻擊發生時，水平擴展可以讓系統根據需求動態擴展更多的伺服器來承擔請求。這些伺服器之間會協同工作，共同處理來自用戶的請求。
* **負載均衡：** 通常，水平擴展需要搭配 **負載均衡器**（Load Balancer）來將流量均勻分配到所有伺服器上。負載均衡器根據伺服器的負載情況動態選擇最合適的伺服器來處理請求，這樣即使某些伺服器遭受攻擊，流量也能快速轉移到其他健康的伺服器上。

例如，你可以使用 AWS、Azure 或 Google Cloud 等雲服務提供的 **Elastic Load Balancing** 服務來實現自動化的流量分發。

* **自動擴展（Auto-scaling）：** 在雲端環境中，許多服務提供商（如 AWS、Azure、Google Cloud）提供自動擴展功能，根據流量負載自動增加或減少伺服器數量。當流量激增（如遇到 DDoS 攻擊時），系統會自動增加伺服器的數量來分散流量，反之，當流量減少時，系統會減少不必要的伺服器。
* **動態防禦：** 通過不斷擴展和收縮伺服器群集，可以有效應對流量波動。即便是 DDoS 攻擊，也能通過自動擴展將流量分攤到更多伺服器上，保持服務的可用性。

**3. 水平擴展的優點**

* **可擴展性：** 水平擴展可以根據流量需求動態擴展。當流量增大或遇到攻擊時，系統能夠快速增加更多的伺服器來應對，而不會受到單個伺服器的性能瓶頸限制。
* **高可用性：** 由於服務分佈在多個伺服器上，即使部分伺服器因為攻擊或故障而失效，系統仍然可以繼續運行，從而提高服務的穩定性和可用性。
* **降低單點故障風險：** 當 DDoS 攻擊集中於某一伺服器時，單個伺服器可能會崩潰或停擺，但水平擴展通過將流量分散到多個伺服器，能有效避免單點故障。

**4. 與其他防禦策略結合**

水平擴展不僅是單獨應對 DDoS 攻擊的一種策略，通常它會與其他防禦技術結合使用，以達到最佳效果：

* **DDoS 防禦服務：** 許多雲平台（如 AWS Shield、Azure DDoS Protection 等）提供專門的 DDoS 防護服務，這些服務能夠自動識別並過濾大部分攻擊流量，從而減少不必要的流量進入你的系統。
* **IP 黑名單與流量過濾：** 你可以配合使用流量過濾技術，將來自惡意 IP 的流量屏蔽或丟棄。這可以在攻擊早期階段篩選掉大量攻擊流量，減少伺服器的負擔。
* **Web 應用防火牆（WAF）：** 使用 WAF 可以對 HTTP 請求進行深度檢查，過濾掉不符合規範的請求，例如 SQL 注入、XSS 攻擊等，這可以減少來自攻擊者的無效請求，從而減少伺服器負擔。

**5. 示範架構**

假設你使用雲端服務來部署一個網站，並希望使用水平擴展來應對 DDoS 攻擊，架構可以是這樣的：

* 用戶請求首先進入 **負載均衡器**，負載均衡器將流量分發到多台伺服器。
* 這些伺服器實際處理請求，並且可以通過自動擴展來動態增加或減少。
* 若攻擊流量過大，可以將流量導向 DDoS 防禦服務來過濾攻擊流量。
* 最終，若伺服器群集仍然面對較大的流量，可以進行流量調節、IP 過濾，並結合 WAF 進行進一步的保護。