



FORTINET

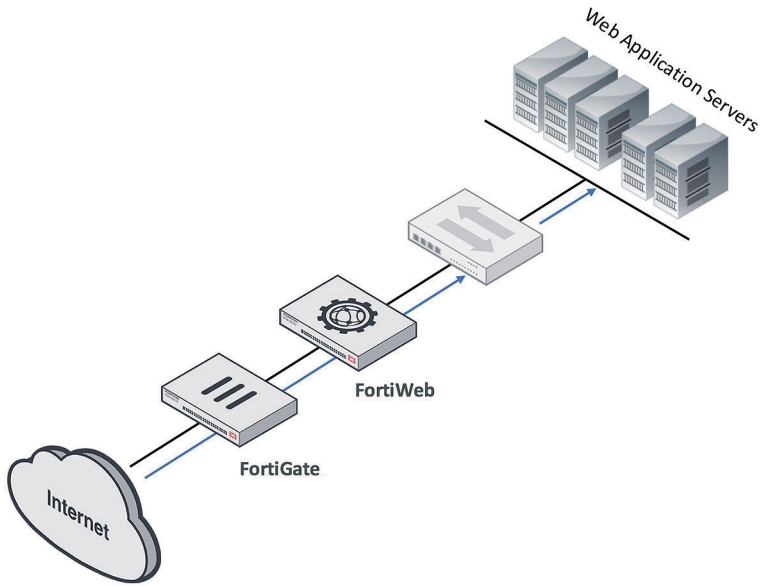
FortiWeb - 與“時”同行的 極致防護 -

與時間賽跑，鞏固品牌價值之利器

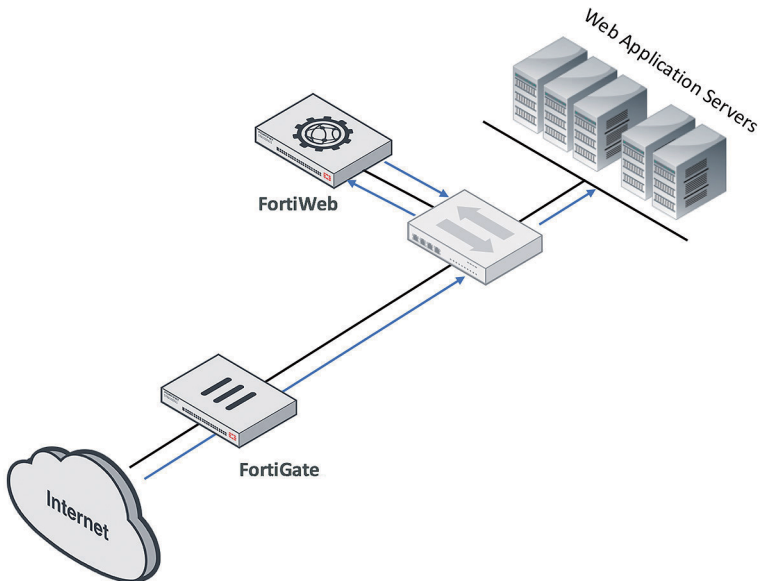
FortiWeb 網頁應用程式防火牆解決方案 - 1

<p>應用說明</p>	<p>隨著網路資訊蓬勃發展便利性成為新世代不可缺少的環節之一，但往往因為網站設計不當、應用程式漏洞與低強度密碼的問題而導致資料外洩、網頁遭置換與惡意程式的散播...事件發生，在 2015 年駭客們發現 HTTP 明文傳輸不僅會導致數據外洩，同時也容易遭受到注入攻擊，Gartner 也預測：截至 2019 年有超過 80% 的企業 WEB 流量皆做加密，HTTPS 流量加密的普及化意味著敏感數據暴露給未授權方的可能性降低，但駭客也不斷的在找尋新的攻擊方法，在面對多元化的威脅下，資訊管理人員可以尋求提供有效且即時的防護並爭取漏洞修補所需的時間。</p> <p>FortiWeb 支援 SSL 加密流量檢測，同時支援多元化的部署模式下並依照客戶需求快速部署至客戶環境中，提供網頁應用程式完善的防護。同時當偵測網頁遭到惡意人士進行竄改時提供告警與復原服務。此外 FortiWeb 內建 By Pass 模組當硬體或是軟體故障時，能夠快速恢復服務。</p>
<p>解決方案</p>	<ol style="list-style-type: none"> 1. 依據客戶的需求提供不同的部署模式並部署至客戶環境中。 2. 檢測 SSL 加密流量。 3. 透過政策提供防護機制，如：OWASP TOP 10 威脅、Brute Force、DDOS...etc。
<p>銷售重點</p>	<ol style="list-style-type: none"> 1. 直覺式管理介面。 2. 完整的日誌與深入的分析。 3. 不需繁瑣且複雜的設定。 4. 不需購買額外 License，即具備病毒特徵庫、WAF 特徵庫、IP 信譽評比等更新。 5. 內建 By pass 模組。 6. 可整合 FortiWeb Central Manager 集中化管理與日誌收容。
<p>產業別</p>	<p>各行業皆可適用。</p>

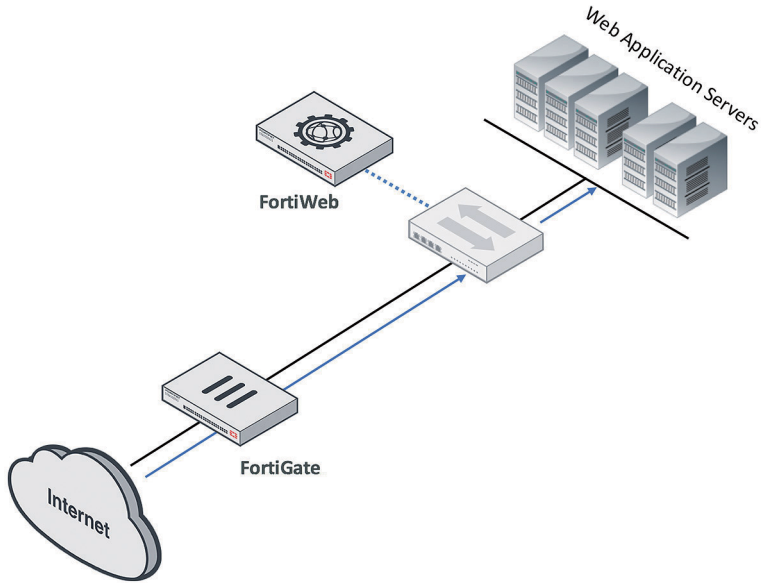
■ FortiWeb - 部署方式 - True Transparent Proxy



■ FortiWeb - 部署方式 - Reverse Proxy



■ FortiWeb - 部署方式 - Offline Protection



FortiWeb 網頁防置換解決方案 - 2

應用說明	FortiWeb 本身具備網站防護之功能，但若客戶環境中已具有其他的 WAF 解決方案時，此時 FortiWeb 仍可以透過內建網頁防置換之功能強化他牌 WAF 所不足的功能，進而執行策略聯防同時支援 Email 告警當偵測網頁遭到惡意人士進行竄改時提供告警與復原服務。
解決方案	<ol style="list-style-type: none"> 1. 內建網頁防竄改與告警功能。 2. 透過 FTP, SSH, Windows Share 方式備份。
銷售重點	<ol style="list-style-type: none"> 1. 直覺式管理介面。 2. 完整的事件日誌。 3. 不需繁瑣且複雜的設定。 4. 不需購買額外的 License。 5. 可整合 FortiWeb Central Manager 集中化管理與日誌收容。
產業別	各行業皆可適用。

■ FortiWeb - 部署方式 - Reverse Proxy

