史特林有限公司
STIRLINGNET.COM

SKUDONET WAAP

Advanced Load Balancer/Web Application and API Protection
進階負載平衡器/Web 應用程式和 API 保護

萬物聯網的內網及外網環境中，保護您的 Web 應用程式和 API 免受安全威脅

SKUDONET

顧問總監 鄭迦聲
SkudoNet & StirlingNet

簡報大綱

甫卸任的美國國安局長暨網戰司令部司令Paul Nakasone，直言：「Cybersecurity is National Security.」

一. 前言

二. 什麼是 Skudonet WAAP

三. 技術架構簡述

四. 系統實例演示

五. 總結與回饋

圖文來源：https://www.ithome.com.tw/article/163001

一、前言

1. GDPR（General Data Protection Regulation, 參照 GDPR）

GDPR 是歐盟的一項數據保護法規，要求企業採取技術和組織措施來保護個人數據的安全性，包括防止數據洩漏和未經授權的訪問，雖然 GDPR 沒有明確要求使用 WAAP 或負載平衡器，但這些技術可以幫助企業達到數據保護的要求。

2. ISO/IEC 27001 (參照 ISO)

ISO/IEC 27001 是一個資訊安全管理系統（ISMS）的國際標準，該標準要求企業識別和管理資訊安全風險，並實施適當的控制措施，雖然 ISO/IEC 27001 沒有具體要求使用 WAAP 或負載平衡器，但這些技術可以作為控制措施的一部分來保護企業的網路和應用程式。

3. NIST SP 800-53 (參照 NIST)

NIST SP 800-53 是美國國家標準與技術研究院（NIST）發布的一套資訊安全控制標準，該標準為聯邦資訊系統提供安全和隱私控制，適用於各種組織， NIST SP 800-53 包括多層次的安全控制，這可能包括使用 WAAP 解決方案來保護 Web 應用程式和 API。

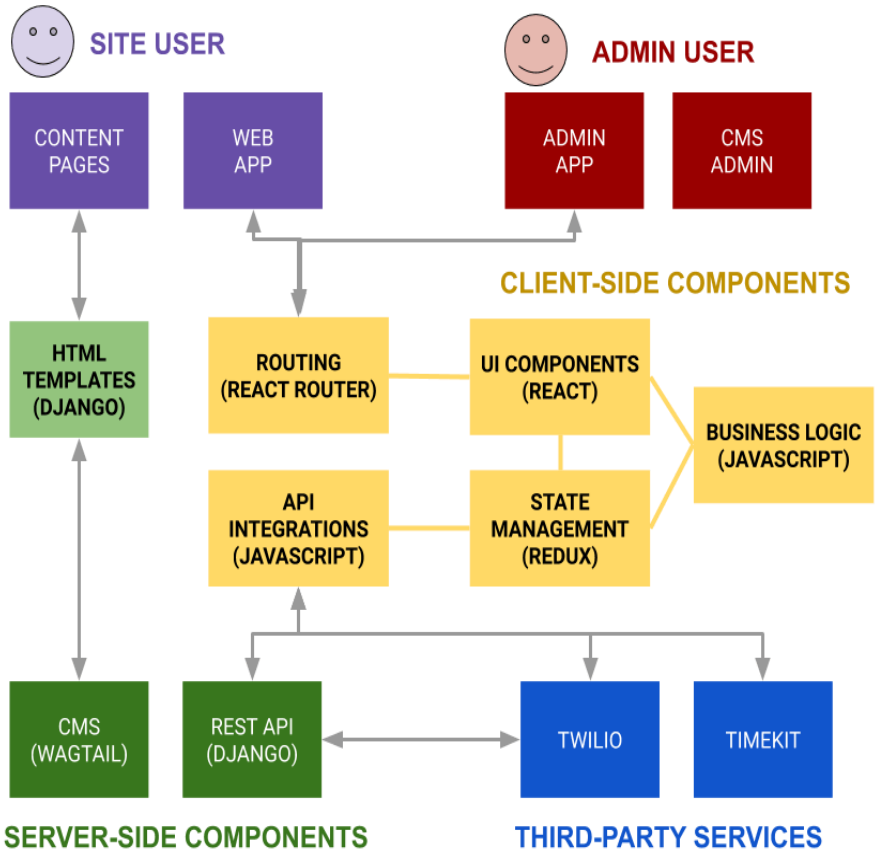
4. CIS Controls (參照 CIS)

CIS Controls 是一套資安框架，由國際資訊安全專家組成的共識指南，幫助企業保護其系統和數據免受已知的網路威脅，這些控制措施包括多層次的防護，這可能涉及到使用 WAAP 和負載平衡器來提升網絡安全。

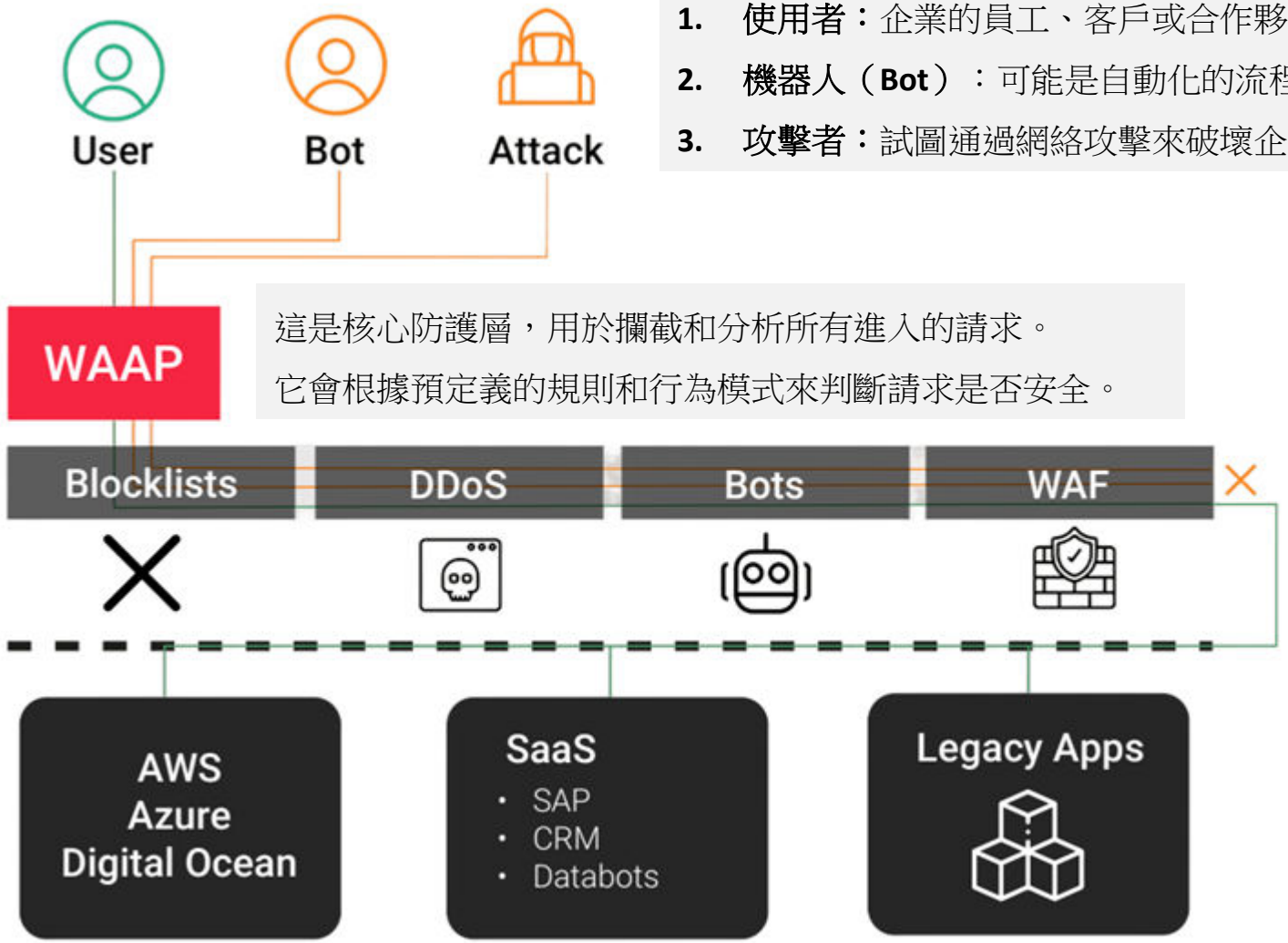
二、什麼是 Skudonet WAAP？

由於人們可以在網路上輕鬆存取 API 和 Web 應用程序，安全性是一個大問題，因為敏感資料會被揭露，攻擊者可能會造成安全漏洞以獲取私人資訊。因此，WAAP 技術能處理傳統 Web 無法處理的安全性措施：

1. Web 應用程式和 API 保護 (WAAP) 是一組在保護網路應用程式的安全性措施和技術，應用程式介面 (API) 免受各種威脅和漏洞的影響。
2. WAAP 是 SKUDONET 安全產品 Web 應用程式防火牆 (WAF) 的逐步演進，除了提供與傳統 WAF 相同的功能，也保護 Web 應用程式以外的 API。
3. 隨著雲端服務和 SaaS（軟體即服務）的發展，整合各種環境的需求推動了 API 的使用，為所有這些服務提供了最佳解決方案。
4. 這項功能使 WAAP 比 傳統 WAF 更先進，因為人們可以在包含公共服務的網路邊緣部署 WAAP，或將其配置在與 ADC 相同的環境中。
5. HTTP(S) 流量是目前使用最多的流量，可能會導致分析變得複雜，Web 流量主要發生在使用 HTTP(S) 的 OSI 第 7 層，現代安全必須超越傳統的 IPS/IDS，才能有效保護第 7 層協定。



三、Skudonet 技術架構簡述：WAAP 工作模式



1. **使用者**：企業的員工、客戶或合作夥伴，他們合法地訪問應用程式。
2. **機器人（Bot）**：可能是自動化的流程（如數據抓取）或潛在的威脅。
3. **攻擊者**：試圖通過網絡攻擊來破壞企業系統或竊取數據。

這是核心防護層，用於攔截和分析所有進入的請求。
它會根據預定義的規則和行為模式來判斷請求是否安全。

1. **黑名單（Blocklists）**：阻擋來自已知惡意IP地址或域名的請求。
2. **DDoS 防護**：防止分散式拒絕服務攻擊，確保系統穩定運行。
3. **機器人防護（Bots）**：檢測和防止惡意機器人活動。
4. **Web應用防火牆（WAF）**：監控和過濾HTTP請求，防止常見的Web應用攻擊（如SQL注入、XSS等）。

1. **雲端服務**：企業使用的雲端平台，如AWS、Azure、Digital Ocean，這些平台承載了大量的業務應用和數據。
2. **SaaS應用程式**：如SAP、CRM、Databots等，這些都是企業運營中不可或缺的應用程式。
3. **傳統應用程式**：企業內部的傳統軟體系統，這些系統可能包含關鍵業務數據和流程。

三、Skudonet 技術架構簡述： IPDS(入侵防禦和偵測系統)如何工作

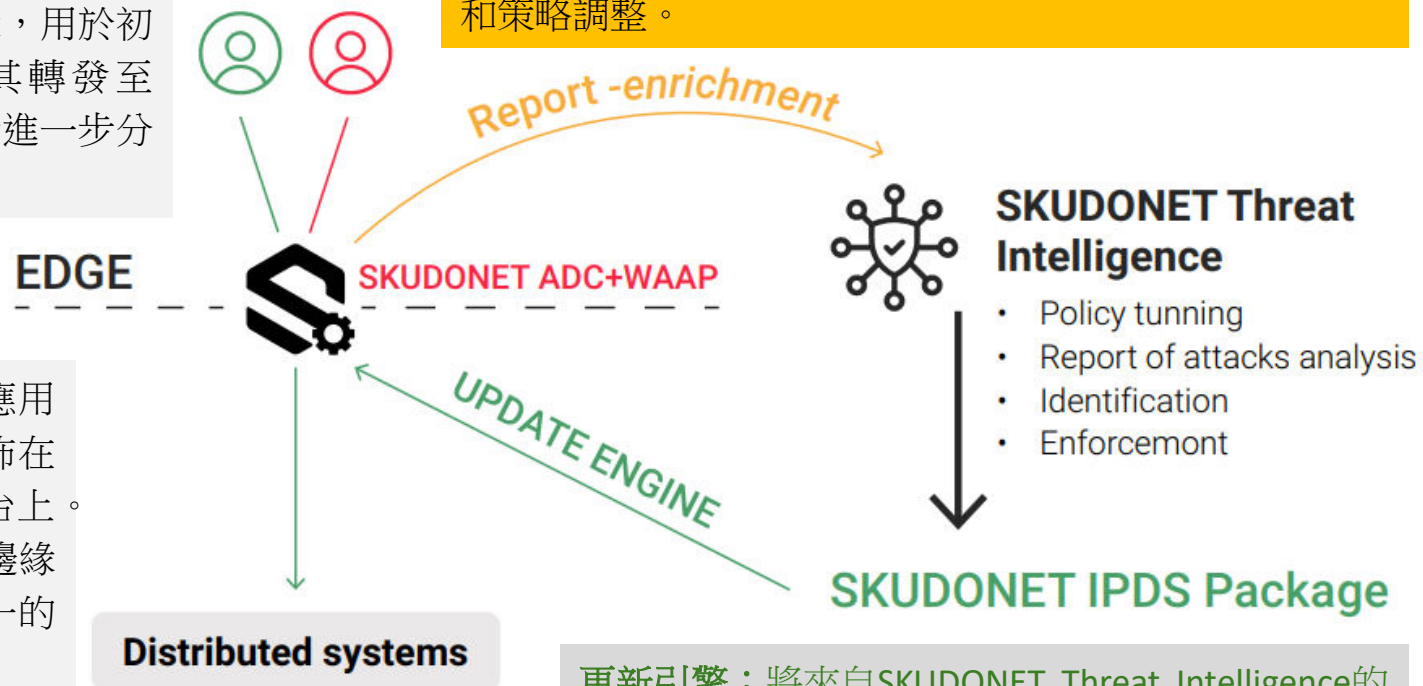
ADC（Application Delivery Controller）：應用交付控制器，主要負責流量管理和應用程序性能優化。
WAAP（Web Application and API Protection）：Web應用和API保護，主要用於防止網絡攻擊和保護應用程序安全。

使用者和攻擊者：來自合法使用者和潛在攻擊者的請求都會首先經過邊緣設備。

邊緣設備：部署在網絡邊緣，用於初步過濾和處理請求，將其轉發至SKUDONET ADC+WAAP進行進一步分析和處理。

分散式系統：企業的各種應用程序和服務，這些系統分佈在不同的地理位置或雲端平台上。SKUDONET ADC+WAAP通過邊緣設備和更新引擎，提供統一的安全防護。

報告強化：將來自SKUDONET ADC+WAAP 的攻擊報告進行豐富化處理，增加更多的上下文信息和威脅分析結果，然後返回至SKUDONET Threat Intelligence進行進一步處理和策略調整。

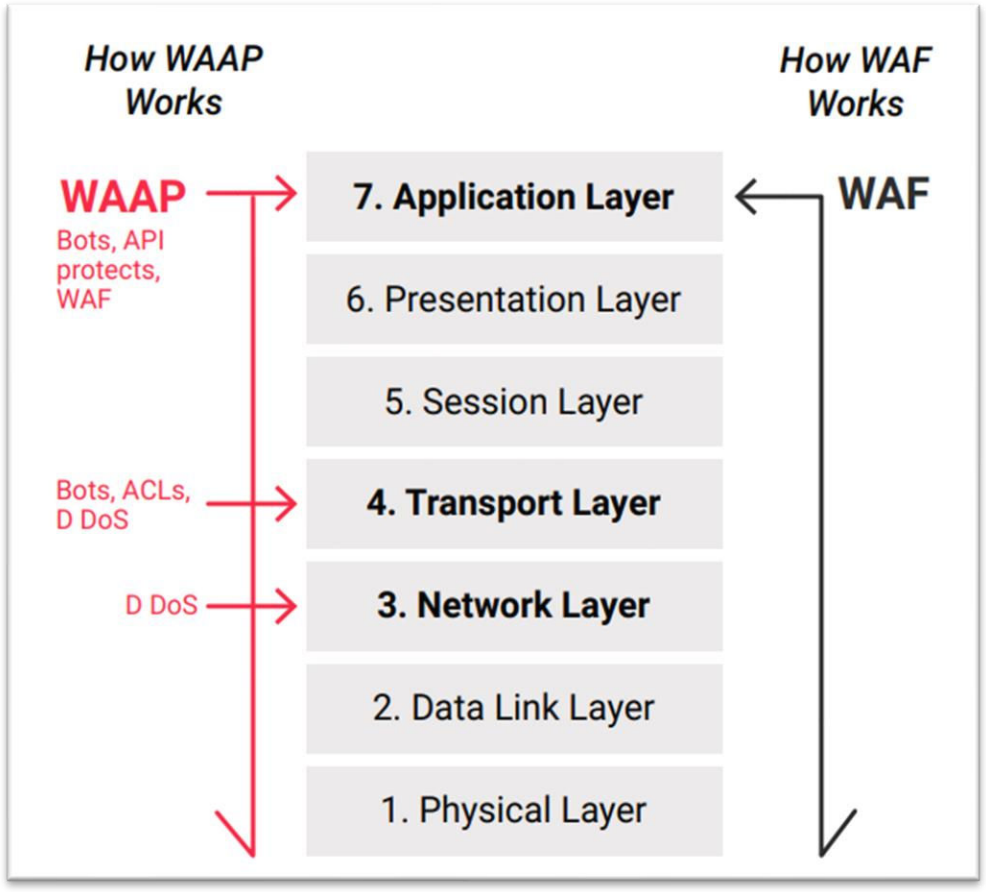


更新引擎：將來自SKUDONET Threat Intelligence的最新策略和威脅情報更新至SKUDONET ADC+WAAP，以確保防護措施始終處於最新狀態。

1. **策略調整（Policy tuning）**：根據最新的威脅情報和攻擊模式，調整安全策略以提高防護效果。
2. **攻擊分析報告（Report of attacks analysis）**：生成攻擊分析報告，提供詳細的攻擊行為和來源信息。
3. **識別（Identification）**：識別並標記新的威脅和攻擊模式。
4. **執行（Enforcement）**：實施新的安全策略和規則，以應對已識別的威脅。

三、Skudonet 技術架構簡述： WAAP 提供傳統 WAF 無法提供的功能

1. **多層負載平衡**：支持第2層、第3層、第4層和第7層的負載平衡，適用於 WAN 上行鏈路、服務、應用和數據中心。
2. **多種協議支持**：支持 TCP、UDP、SCTP、SIP、FTP、TFTP、HTTP、HTTPS、RDP、SSH、POP3、IMAP、SMTP、DNS、NTP、LDAP、LDAPS、RADIUS、WebSocket 等協議，以及 MS Exchange、Lynx、ICA 等應用。
3. **進階 HTTP 應用特性**：如會話保持、重定向、虛擬主機、即時解密/加密、SSL 證書(SNI 和通配符)、Cookie 插入、反向代理等。



4. **進階的網絡管理**：包括 VLAN、虛擬 IP、鏈路聚合、自動和自定義路由配置、自定義靜態路由和 IPv6。
5. **開放 SD-WAN 邊緣**：建立高可用性和加權負載平衡的 WAN 上行鏈路，確保雲端或分支機構之間的連接，並配置 WAN 的有限訪問。

6. **基於角色的訪問控制**：允許多租戶和 LDAP/AD 連接器。
7. **集中管理控制台**：提升在可擴展和靈活的多虛擬服務環境中的管理。
8. **完整的 JSON REST API**：輕鬆整合自動化和數據中心的擴展服務。

9. **多層次的防護**：包括入侵防禦和檢測系統（IPS/IDS），白名單/黑名單、DoS 防護、實時黑洞列表（RBL）和 Web 應用防火牆（WAF）。
10. **多達 200 多個預載自動保護列表**：按區域或地理位置劃分，包括私人網絡、惡意節點、僵屍網絡、垃圾郵件列表、網頁抓取器、匿名代理、暴力破解主機、網頁漏洞利用等。
11. **可配置的 DoS 和 DDoS 防護規則**：每個服務包括每秒連接限制、每源 IP 的總連接數限制、偽造 TCP 保護、每秒重置請求限制等。

三、Skudonet 技術架構簡述： SKUDONET 透過 WAAP 保護什麼？

1. 超過 200 個按國家/地區劃分的 IP 位址和範圍清單

• SKUDONET WAAP 能夠根據 IP 位址和範圍清單來過濾和阻止來自特定國家或地區的惡意流量，有助於：

1. 地理封鎖：防止來自高風險地區的攻擊。

2. 流量管理：根據地理位置優化流量分配，提升性能。

2. 按應用程式（電子郵件、網路、垃圾郵件...）排序的攻擊者列表

• SKUDONET WAAP 可以根據攻擊者針對的應用程式類型來排序和管理攻擊者列表：

1. 電子郵件安全：阻止針對電子郵件伺服器的釣魚攻擊和垃圾郵件。

2. 網路攻擊防護：識別並阻止針對Web應用程式的攻擊。

3. **垃圾郵件防護**：過濾和阻止垃圾郵件來源。

3. 攻擊者被認定為間諜軟體、爬蟲、機器人、DDoS 攻擊、暴力破解等

• SKUDONET WAAP 能夠識別並阻止各類自動化攻擊工具：

1. 間諜軟體：檢測並阻止試圖竊取數據的惡意軟體。

2. 爬蟲和機器人：管理和限制爬蟲訪問，防止數據爬取和資源濫用。

3. DDoS 攻擊：即時監控和分析流量模式，識別和阻止異常的高流量攻擊。

4. 暴力破解：監控和分析登錄嘗試，識別和阻止異常的多次失敗登錄，防止暴力破解。

三、Skudonet 技術架構簡述： SKUDONET 透過 WAAP 保護什麼？

4. 透過 HTTPS 協定識別保護 API

- SKUDONET WAAP 使用 HTTPS 來保護 API 通訊，確保數據傳輸的機密性和完整性：

1. **加密通訊**：防止中間人攻擊和數據竊取。
2. **API 安全**：識別和阻止未經授權的 API 請求。

5. 防範 SQLI、XSS、LFI、RCE、RFI等常見的網路攻擊

- SKUDONET WAAP 提供全面的應用程序安全防護，防止常見的網絡攻擊：

1. **SQL Injection（SQLI）**：防止惡意 SQL 查詢注入應用程序，從而操控資料庫執行未經授權的操作。
2. **Cross-Site Scripting（XSS）**：在受信任的網站中注入惡意腳本，而竊取敏感信息或執行未經授權的操作。
3. **Local File Inclusion（LFI）**：將本地文件包含到應用程序中，從而讀取敏感息或執行未經授權的操作。
4. **Remote Code Execution（RCE）**：利用應用程序的漏洞，在目標系統上執行惡意程式碼，獲得完全控制權。
5. **Remote File Inclusion（RFI）**：將遠端文件包含到應用程序中，從而執行惡意程式碼或竊取敏感訊息。

6. 防範 PHP、Node.js、Java 等的程式碼漏洞

- SKUDONET WAAP 能夠識別和防止針對不同程式語言的漏洞攻擊：

1. **PHP 漏洞防護**：防止 PHP 應用程序中的常見漏洞利用。
2. **Node.js 安全**：識別和阻止針對 Node.js 應用的攻擊。
3. **Java 安全**：防止針對 Java 應用程序的漏洞利用。

三、Skudonet 技術架構簡述： SKUDONET 透過 WAAP 保護什麼？

7. 防禦 DDoS 攻擊，例如 RESET FLOOD 和 IP ORIGIN

- SKUDONET WAAP 提供強大的 DDoS 防護功能：

1. **RESET FLOOD 防護**：識別並阻止大量的TCP RST（重置）封包，試圖中斷現有的連接並耗盡伺服器資源。
2. **IP ORIGIN 防護**：管理和限制來自特定 IP 的過多請求，防止大量偽造的 IP 位址發起攻擊，試圖通過分散攻擊源來繞過傳統的 IP 黑名單防護來耗盡系統資源。

8. 每日內容更新

- SKUDONET WAAP 提供每日安全內容更新，確保防護措施始終最新：

1. **威脅情報更新**：持續更新最新的威脅情報和攻擊模式。
2. **安全策略調整**：根據最新的威脅情報自動調整安全策略。

9. 與第三方無縫整合的可能性

- SKUDONET WAAP 支持與各種第三方工具和服務無縫整合：

1. **SIEM 整合**：與安全訊息和事件管理（SIEM）系統整合，提供全面的安全監控。
2. **API 整合**：通過 API 與其他安全工具和服務整合，增強整體安全防護能力。
3. **SSO 整合**：與單一登入系統（如 Okta、Microsoft Azure AD）整合，提供統一的身份驗證和授權管理，減少重複登錄和提高使用者的體驗。
4. **MFA 整合**：支持多因素驗證（如 Google/Microsoft Authenticator、Duo Security），增強安全性，防止未經授權的訪問。

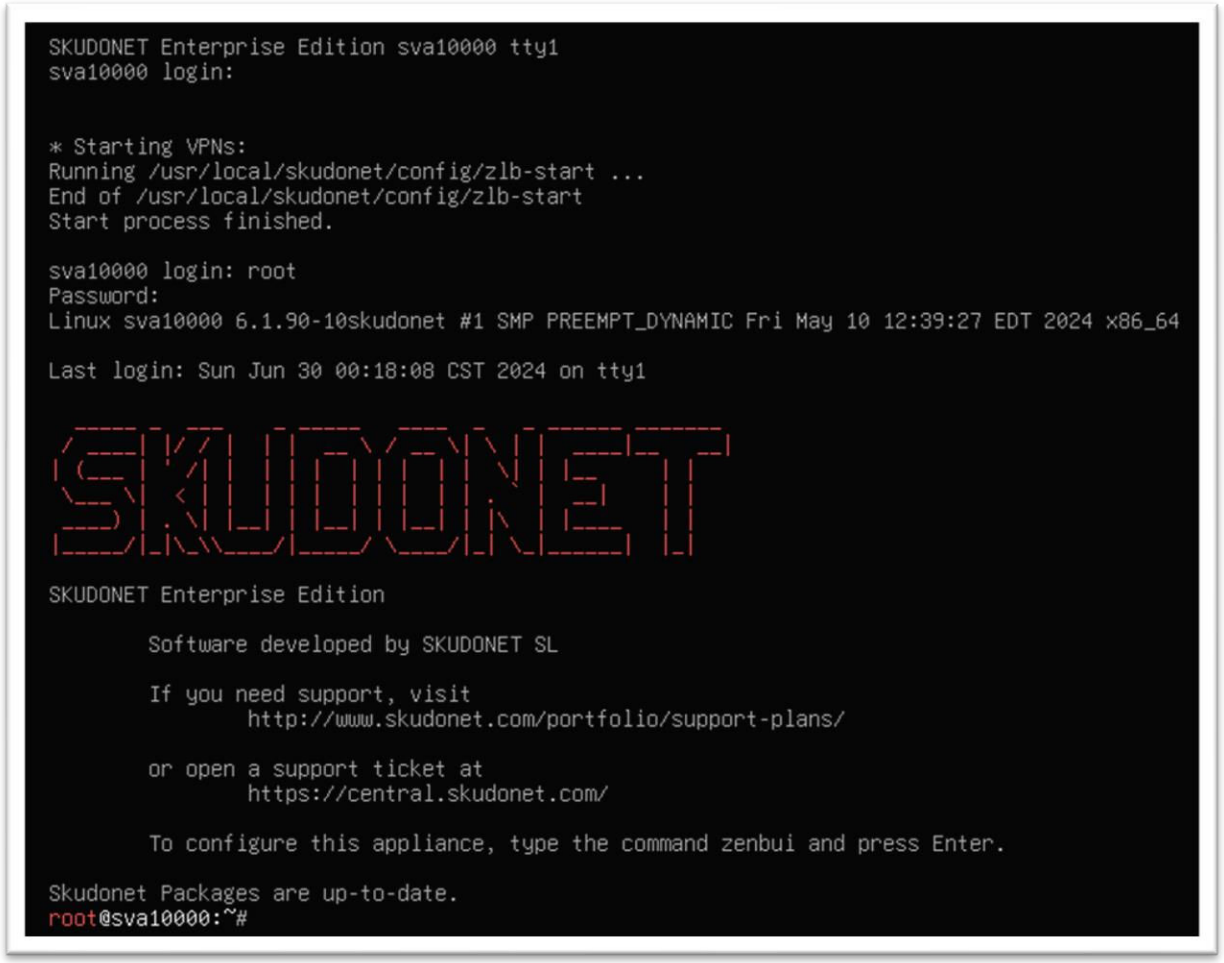
三、Skudonet 技術架構簡述：揭開社群版和企業版的差異

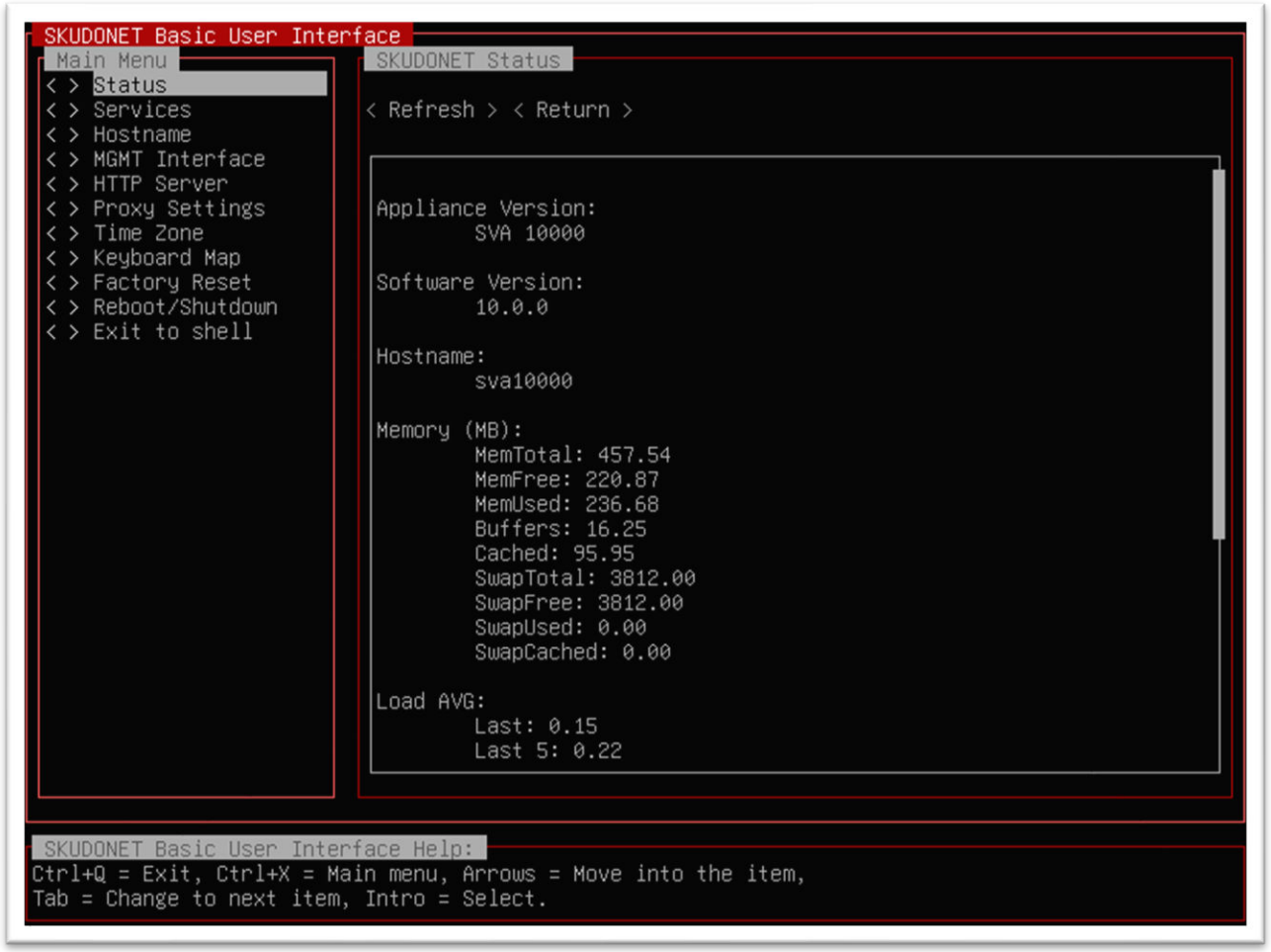
Community Edition 社群版	Enterprise Edition 企業版
Open Source with Linux 核心 6 使用者友善的 Web GUI	Open Source with Linux 核心 6 使用者友善的 Web GUI
基本負載平衡能力	進階負載平衡功能（Concurrency, Requests per second）
本機服務負載平衡模組 (LSLB)	**Local** Service Load Balancing Module 本機服務負載平衡模組 (LSLB)
Basic Clustering 基本聚類	**Global** Service Load Balancing Module 全域服務負載平衡模組 (GSLB)
Basic Networking configuration	**Datalink** Load Balancing Module 資料鏈路負載平衡模組 (DSLB)
Support from Community 社群的支持	**Advanced** Networking configuration 進階網路配置 • Bonding 黏合、VLAN 虛擬區域網、VPN
AMAZON and **Azure** Support	**Intrusion Prevention and Detection System** (IPDS)入侵防禦和偵測系統 1. **Blocklist protection** (ACLs) 阻止清單保護 2. **Denial of Service Protection** (DoS) 拒絕服務保障 3. **Web Application Firewall** (WAF) Web 應用程式防火牆 4. **Real-time BlockList protection** (RBL) 即時阻止清單保護
Complete API for management	Stateful Clustering 狀態集群
	SKUDONET 工程師的支持
	OEM模組，升級圖形使用者介面

四、系統實例演示(一)

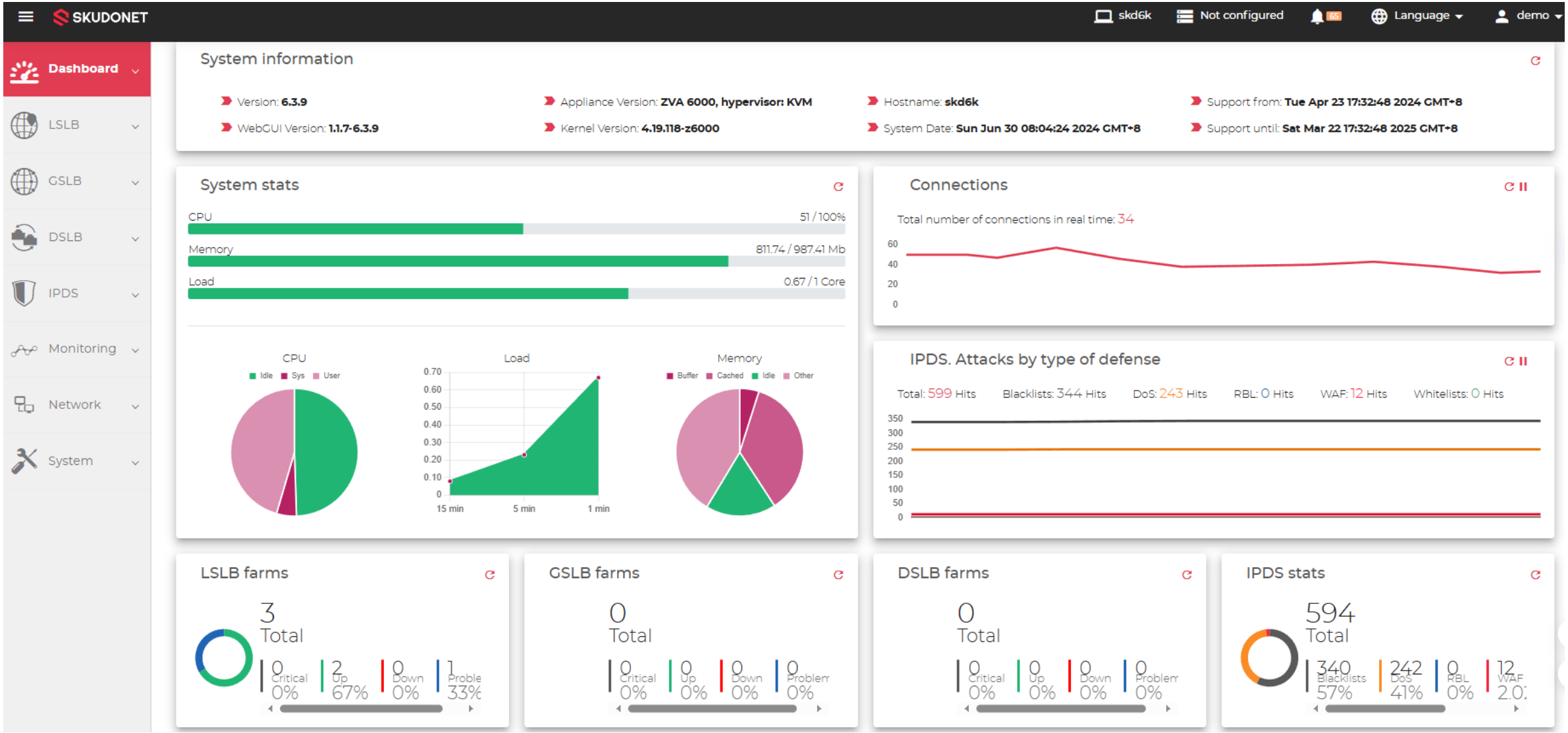
SKUDONET 企業版系統登入

基本設定工具：系統管理配置





四、系統實例演示(一)：在 L4XNAT 模式中配置



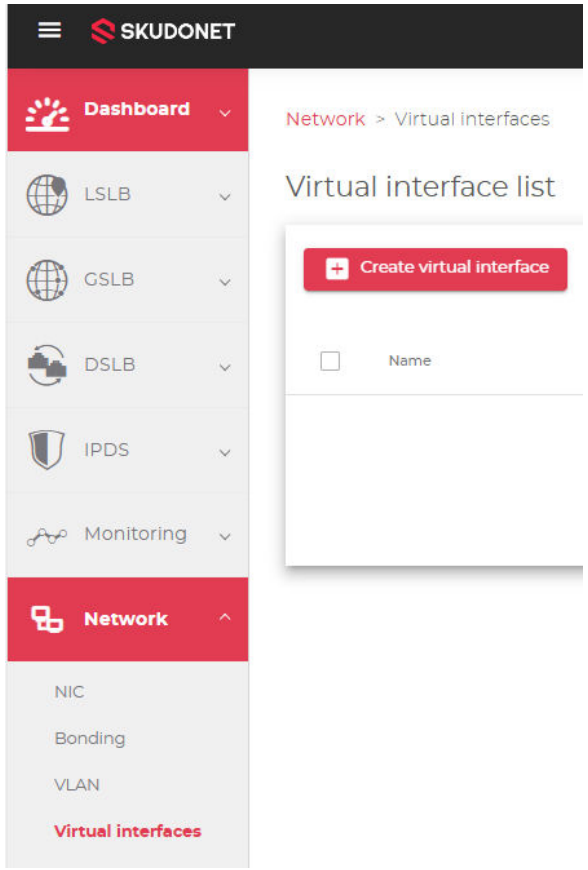
Reference：Enterprise - Web GUI (skudonet.cloud)

四、系統實例演示(一)：在 L4XNAT 模式中配置

為了配置 JD Edwards 的高可用性以獲得高效能和可擴展性，需要在本地或雲端部署 SKUDONET 應用程式交付控制器設備。

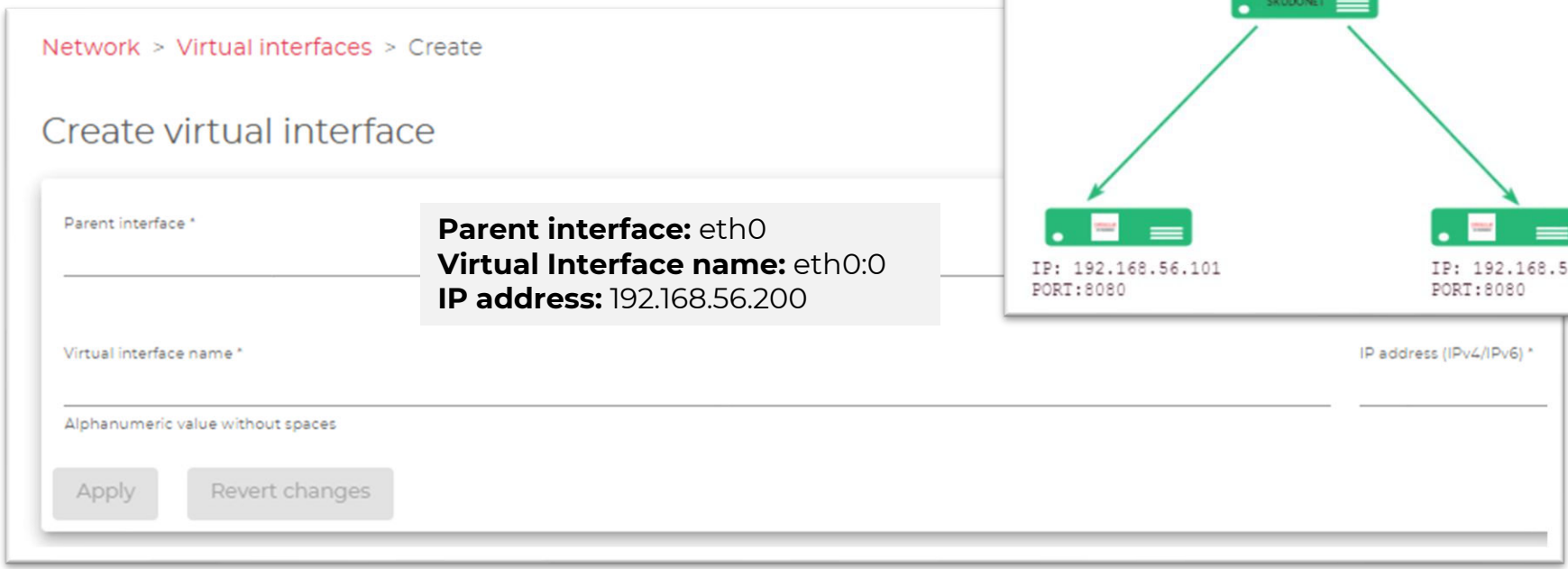
1. SKUDONET ADC 將配置 L4XNAT 設定檔（模式 1），TCP 流量將通過負載平衡器。
2. SKUDONET ADC 將使用 HTTP(S) 設定檔進行配置，轉送應用程式資料並根據 HTTP 標頭做出決策。

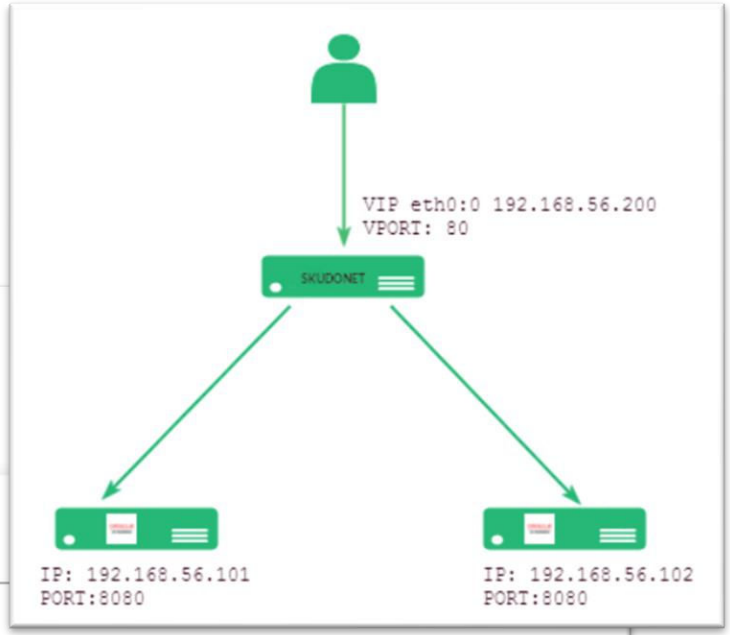
描述的環境如下



步驟 1：虛擬IP配置 (Virtual IP configuration)

IP是用於負載平衡目的的IP，相同的虛擬IP可以在多個場中配置，但無法在多個場中配置相同的虛擬連接埠。



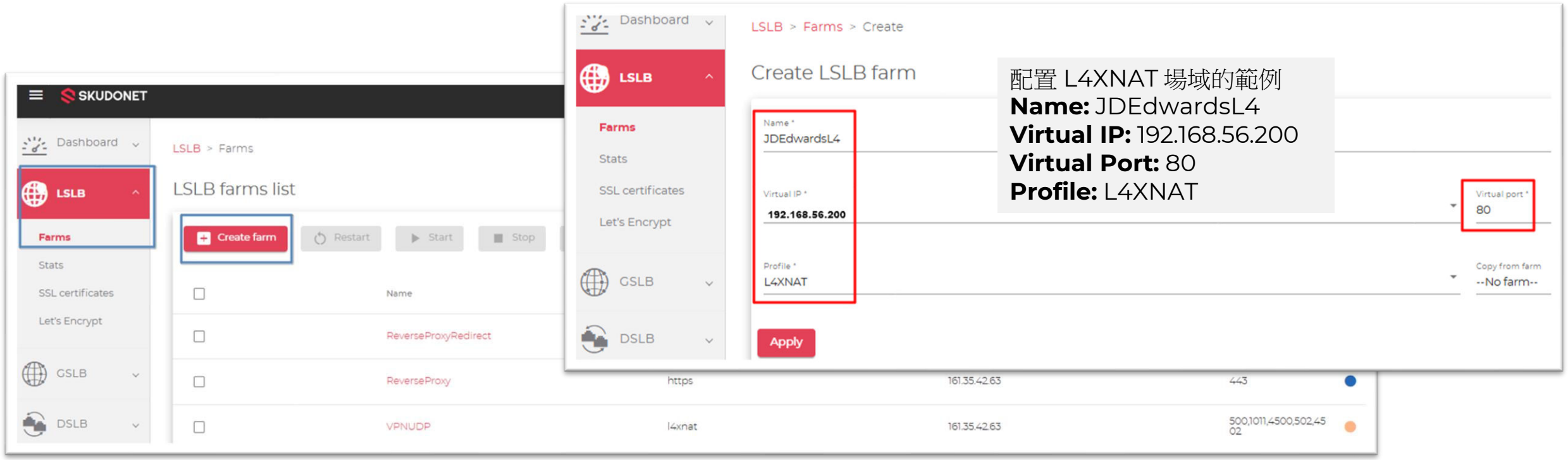


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(一)：在 L4XNAT 模式中配置

步驟 2：配置 JD Edwards 場以實現 TCP 負載平衡 (Configure the JD Edwards farm for TCP load balancing)

1. Farm 是 SKUDONET 應用程式交付控制器中的虛擬概念，透過 Farm，SKUDONET 捕獲客戶端流量並將請求轉發到建置應用程式叢集以實現高可用性的不同伺服器。
2. 前往 LSLB >>Farms >> Create Farm，在新表單中選擇一個描述性名稱，此設定檔在傳輸層 4 提供高效能負載平衡系統，並結合了多種負載平衡方法，例如來源 NAT 和目標 NAT。

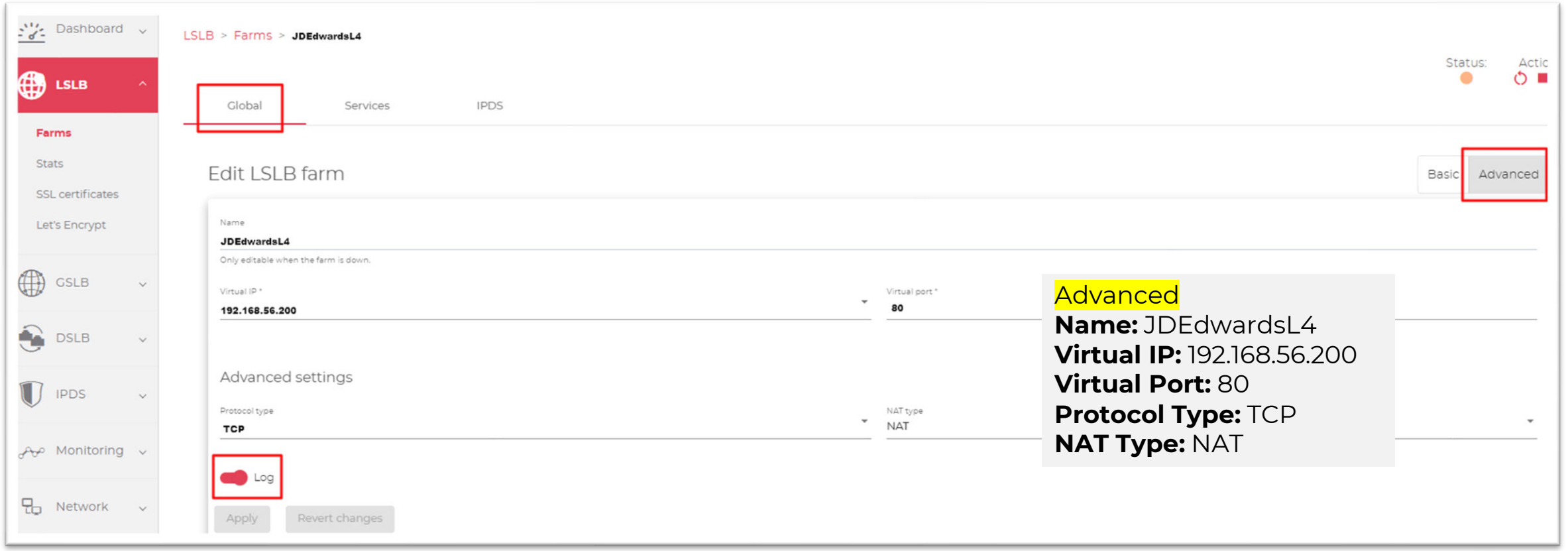


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(一)：在 L4XNAT 模式中配置

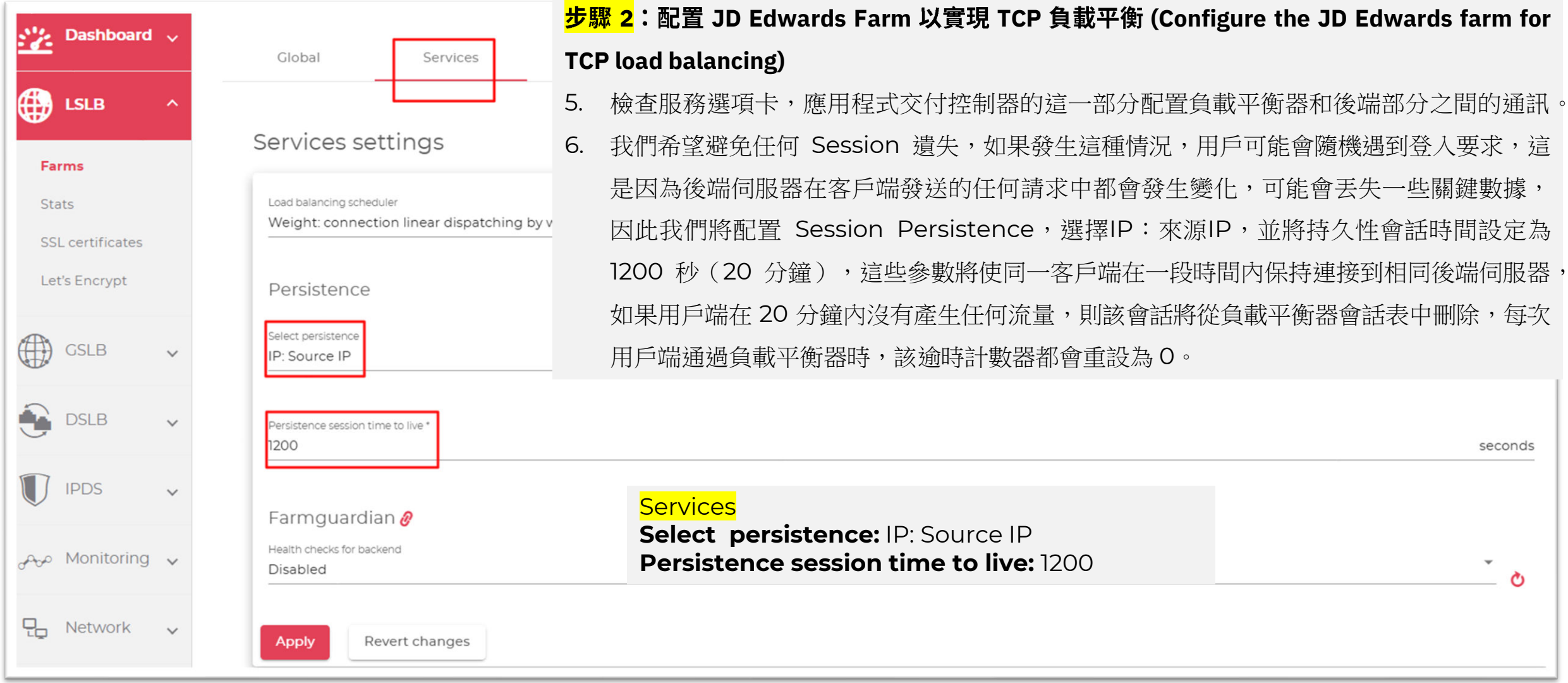
步驟 2：配置 JD Edwards 場以實現 TCP 負載平衡 (Configure the JD Edwards farm for TCP load balancing)

3. 建立 Farm 後，按下編輯，會載入「Global」選項卡，按一下右上的「Advanced」，顯示新參數，最後按下「 Apply」按鈕儲存變更。
4. 如果想檢查通過此 Farm 的流量，請啟用日誌，但考慮到所有流量將保存在日誌檔案 /var/log/syslog 中，因此需要額外的磁碟可用空間，我們僅建議在故障排除時啟用日誌。



Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(一)：在 L4XNAT 模式中配置



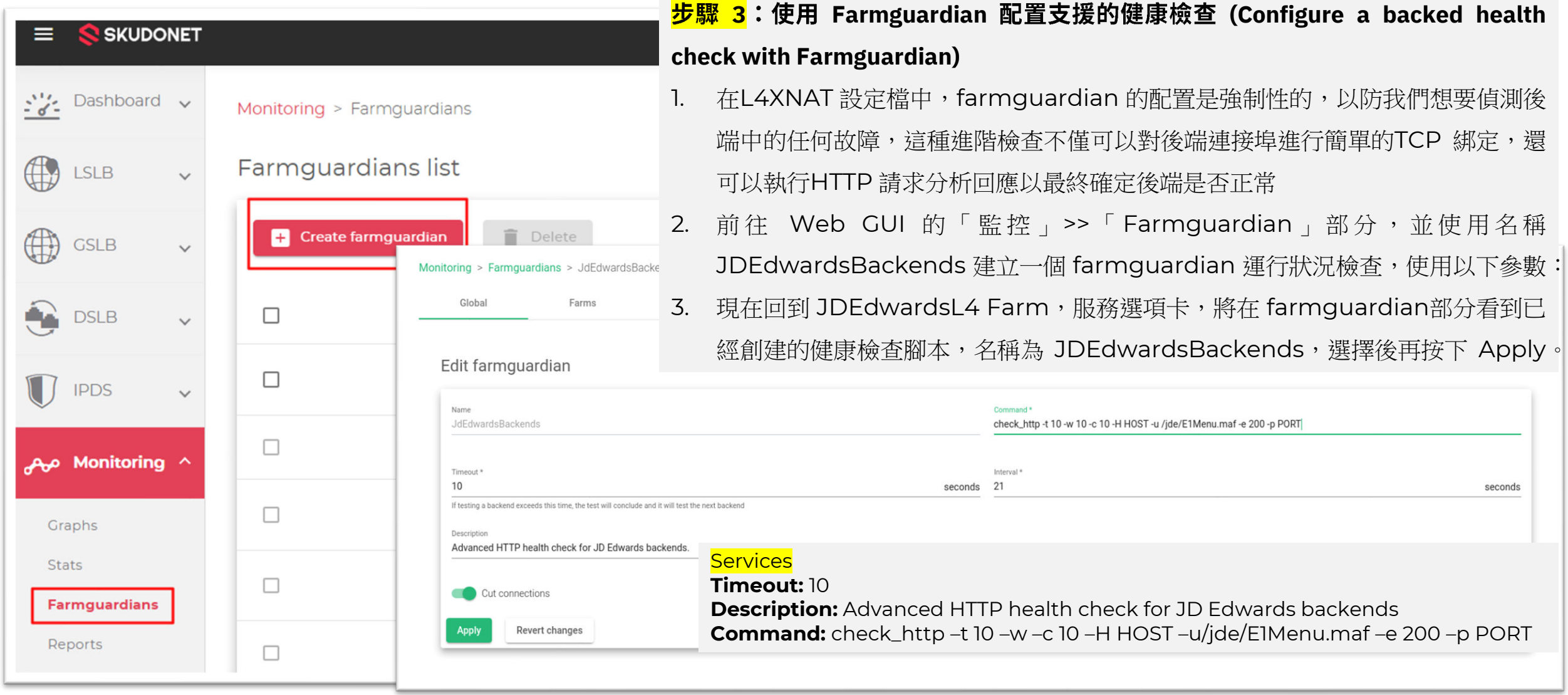
步驟 2：配置 JD Edwards Farm 以實現 TCP 負載平衡 (Configure the JD Edwards farm for TCP load balancing)

5. 檢查服務選項卡，應用程式交付控制器的這一部分配置負載平衡器和後端部分之間的通訊。
6. 我們希望避免任何 Session 遺失，如果發生這種情況，用戶可能會隨機遇到登入要求，這是因為後端伺服器在客戶端發送的任何請求中都會發生變化，可能會丟失一些關鍵數據，因此我們將配置 Session Persistence，選擇IP：來源IP，並將持久性會話時間設定為 1200 秒（20 分鐘），這些參數將使同一客戶端在一段時間內保持連接到相同後端伺服器，如果用戶端在 20 分鐘內沒有產生任何流量，則該會話將從負載平衡器會話表中刪除，每次用戶端通過負載平衡器時，該逾時計數器都會重設為 0。

Services
Select persistence: IP: Source IP
Persistence session time to live: 1200

Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(一)：在 L4XNAT 模式中配置



步驟 3：使用 Farmguardian 配置支援的健康檢查 (Configure a backed health check with Farmguardian)

1. 在L4XNAT 設定檔中，farmguardian 的配置是強制性的，以防我們想要偵測後端中的任何故障，這種進階檢查不僅可以對後端連接埠進行簡單的TCP 綁定，還可以執行HTTP 請求分析回應以最終確定後端是否正常
2. 前往 Web GUI 的「監控」>>「Farmguardian」部分，並使用名稱 JDEdwardsBackends 建立一個 farmguardian 運行狀況檢查，使用以下參數：
3. 現在回到 JDEdwardsL4 Farm，服務選項卡，將在 farmguardian部分看到已經創建的健康檢查腳本，名稱為 JDEdwardsBackends，選擇後再按下 Apply。

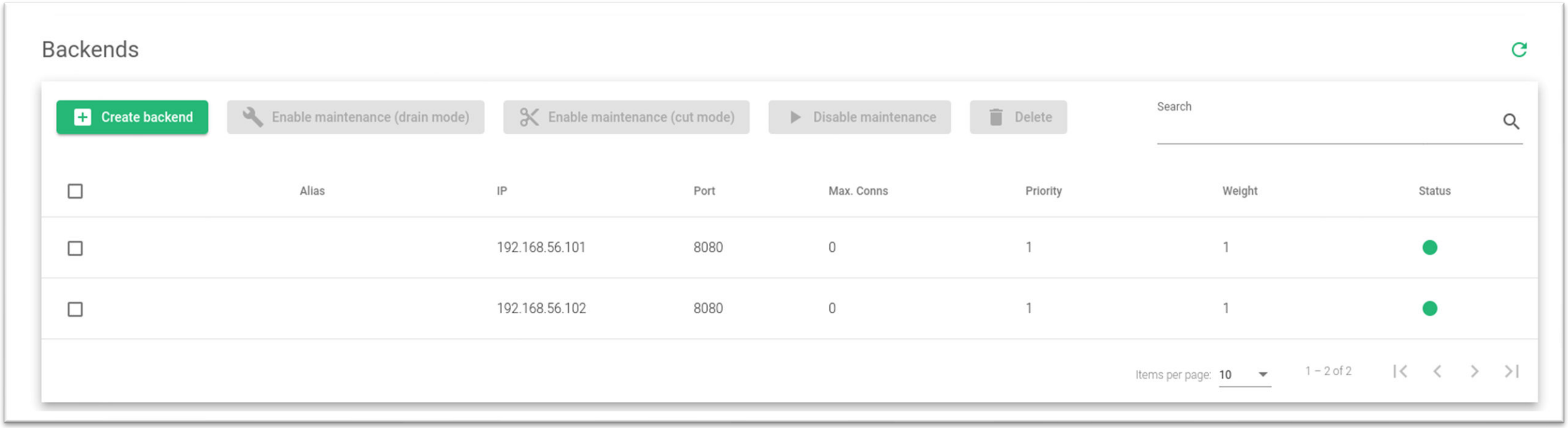
Services
Timeout: 10
Description: Advanced HTTP health check for JD Edwards backends
Command: check_http –t 10 –w –c 10 –H HOST –u/jde/E1Menu.maf –e 200 –p PORT

Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(一)：在 L4XNAT 模式中配置

步驟 4：增 JD Edwards EnterpriseOne 後端伺服器 (Adding the JD Edwards EnterpriseOne backend servers)

1. 在負載平衡服務中指示配置並運行 JD Edwards 的真實伺服器，在我們的範例中，後端 192.168.56.101 和 192.168.56.102 是使用 JD Edwards 配置的監聽 WebLogic 8080 端口，請參考以下畫面。
2. 現在，系統已準備好在虛擬IP 192.168.56.200 連接埠 80 中使用 SKUDONET L4XNAT 場對 JD Edward EnterpriseOne 進行負載平衡，使用後端連接埠 80 將流量以NAT 模式轉送到後端 192.168.56.101 和 196.1962.102，也會檢查每個後端每 21 秒使用自訂運行狀況檢查確認給定 URL HTTP 請求的 200 OK 回應。

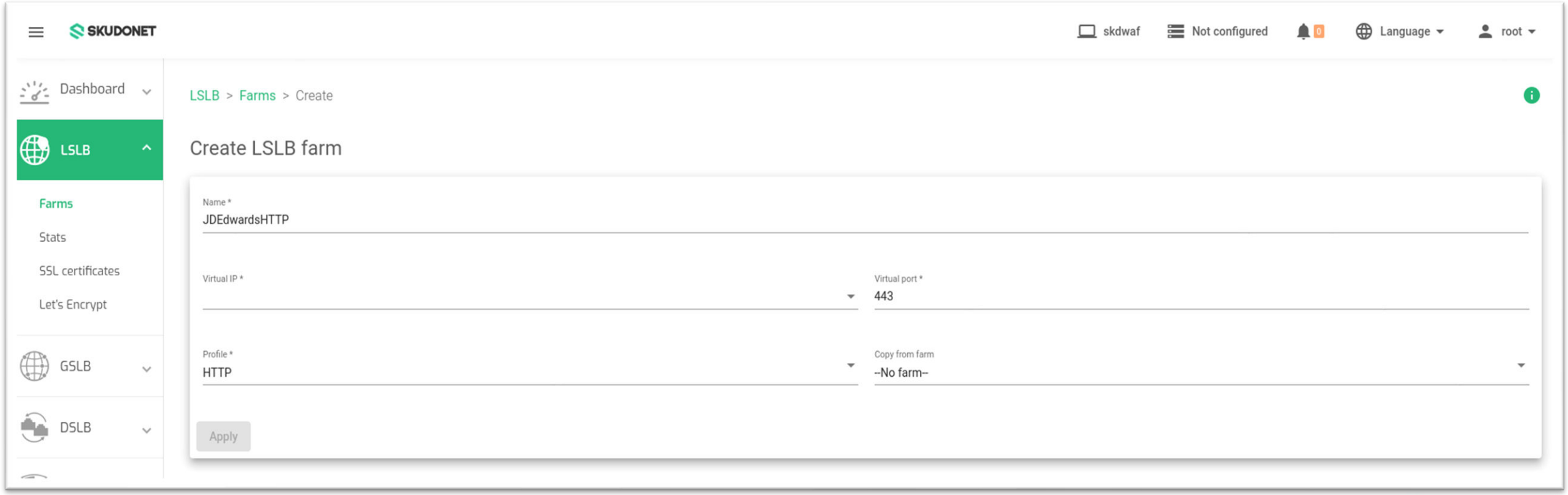


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(二)：在 HTTPS 模式中配置

步驟1：建立 HTTP(S) 場 (Create an HTTP(S) farm)

1. 我們將介紹一種不同的配置方法，負載平衡器現在將像用戶空間中的反向代理一樣工作，分析 HTTP 標頭並在應用程式層級（HTTP 協定）而不是 TCP 層級移動流量。
2. 前往 Web GUI 的橫向選單，LSLB >> 農場，在 LSLB 部分建立一個新場，現在選擇 HTTP 作為設定文件，連接埠 443，配置 JDEdwardsHTTP 的描述性名稱，然後選擇虛擬 IP 192.168.56.200（先前已配置為虛擬介面）

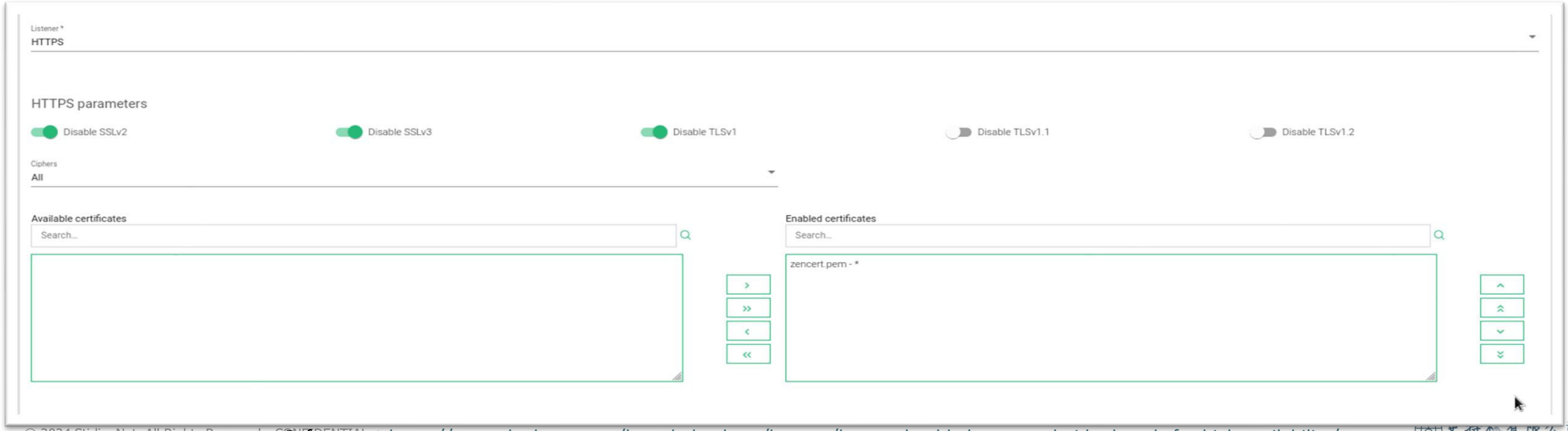


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(二)：在 HTTPS 模式中配置

步驟1：建立 HTTP(S) 場 (Create an HTTP(S) farm)

3. 建立場後，對其進行編輯並按一下「Global」選項卡，請將 Listener 變更為 HTTPS 模式，此變更將顯示與 HTTPS 協定配置相關的新參數，請依下所示配置參數：HTTPS 參數，應僅啟用 TLSv1.1 和 TLSv1.2。預設啟用 TLSv1.3，密碼在「All」模式下配置，但如果您不想允許不同的密碼，請在 Ciphers 下拉選擇適合的 Security 選項。
4. Available certificates 顯示系統中可用的 certificates，目前為測試，預設現有 certificates 即可，一旦系統上線，我們建議配置新的 certificates，您可以從第三方認證機構的 CN(Common Name) 部署 certificate 或使用我們的憑證 Lets Encrypt 連接器，在左側的選單 LSLB > Let's Encrypt

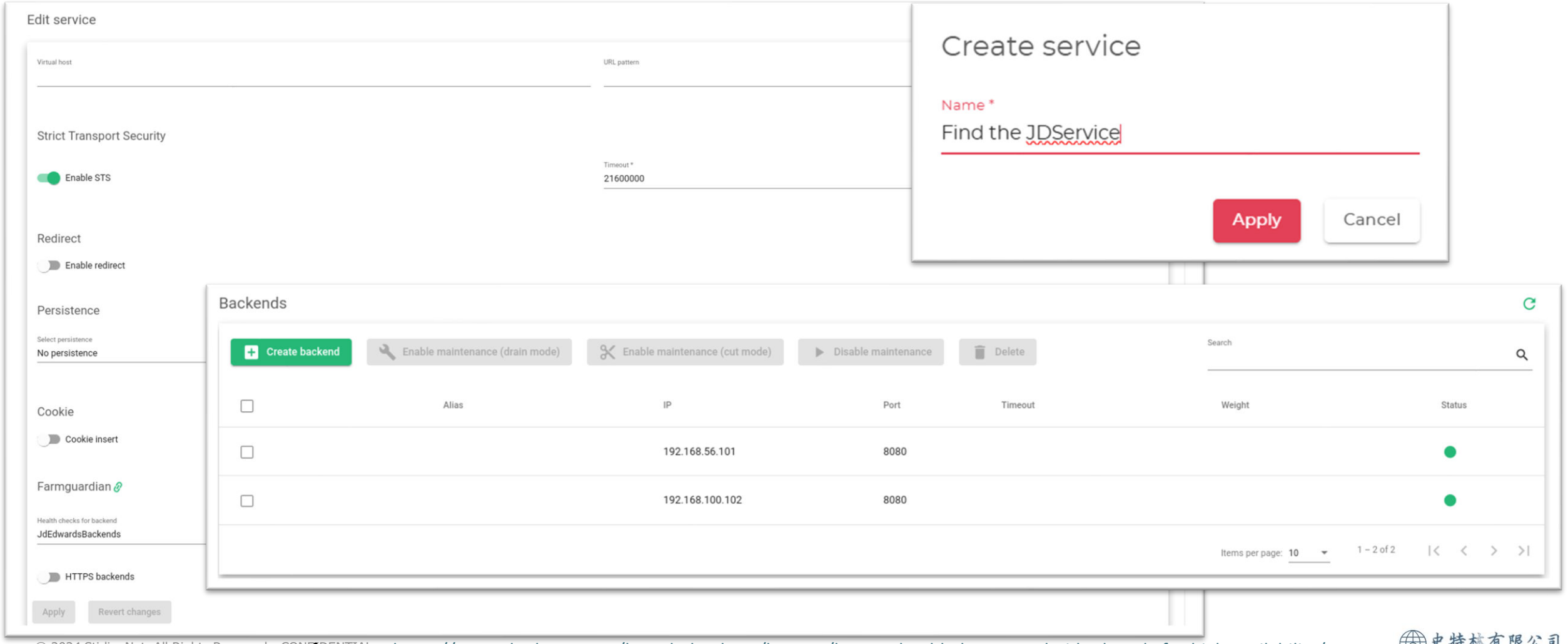


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(二)：在 HTTPS 模式中配置

步驟2：建立服務和後端 (Create a service and the backends)

1. 到配置的 HTTPS Farm 中的「Service」選項，並新增一個名為 Find the JDService 的 New Service

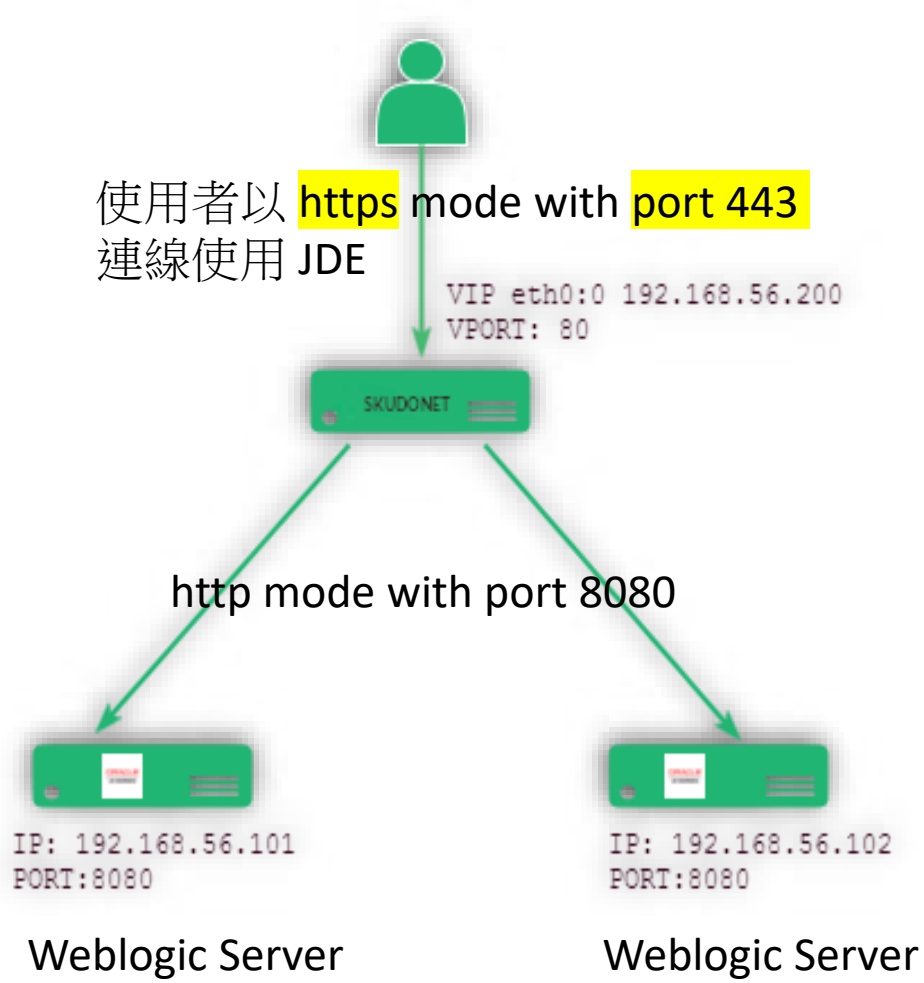


Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

四、系統實例演示(二)：在 HTTPS 模式中配置

步驟3：進階檢查 (Advanced Checking)

1. 我們將按照與 L4xNAT Farm 完全相同的方式進行操作，使用已建立 L4XNAT Farm 來檢查它的運行狀況，與 L4XNAT 設定檔不同，在 HTTP(S) 場中使用 farmguardian 不是強制性的，因為此設定檔在每個 HTTP 後端連線中需執行固有的 TCP 檢查，L4XNAT 設定檔不執行任何檢查，因此如果我們想要偵測在此配置中，是否有設定檔後端中故障的情形，則需要進行「farmguardian health check」。
2. 系統已準備好在 LSLB 模組中使用 SKUDONET HTTPS 設定檔在 TCP 連接埠 443 中使用相同的虛擬 IP 192.168.56.200 在 SSL 模式下偵聽，對 JD Edward EnterpriseOne 進行負載平衡。
3. 此請求以 HTTP 模式透過 Port 8080 傳送至 WebLogic 伺服器 IP 192.16.56.101 和 192.168.56.102 中的 JD Edwards 後端。此配置稱為「SSL Offloading」，客戶端和負載平衡器之間的通訊以 HTTPS 安全模式完成，但負載平衡器和後端之間的通訊以 HTTP 模式（無 SSL）完成。

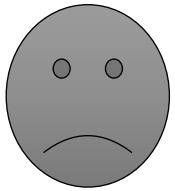


最後的考慮因素 (Final Considerations)

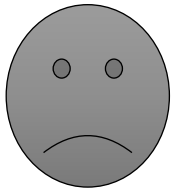
SKUDONET 完全支援高可用性，並且具備有資訊安全的 JD Edwards 進階性負載平衡。

Reference：https://www.skudonet.com/knowledge-base/howtos/how-to-load-balance-oracle-jd-edwards-for-high-availability/

五、總結：傳統防火牆 (Firewall) 與 Skudonet WAAP 比較

	1. 靜態規則設置	2. 缺乏應用層防護	3. 無法處理加密流量	4. 有限的威脅情報整合
問題 	傳統防火牆依賴靜態規則，無法動態適應新的威脅。	許多防火牆僅能檢查數據包的標頭，無法深入應用層進行檢查。	對於 HTTPS 等加密流量，傳統防火牆無法有效檢查其內容。	缺乏實時更新的威脅情報，無法及時防護新出現的攻擊。
Skudonet 解決方案 	**動態威脅檢測與防禦：** Skudonet 提供即時黑名單（Real-time Block Lists, RBL）系統，能夠動態更新並阻止新出現的攻擊源。 內建 DDOS 引擎，能夠有效防禦分散式拒絕服務攻擊。	**應用層防護：** Skudonet 的 Web 應用防火牆（WAF）能夠防護 SQL 注入（SQLi）、跨站腳本攻擊（XSS）等應用層攻擊。 支援多達 400 條規則，涵蓋各種應用層攻擊防護需求。	**處理加密流量：** 支援 SSL 加解密，能夠檢查 HTTPS 流量，確保加密數據的安全性。	**威脅情報整合：** Skudonet 的威脅情報系統能夠每日更新，確保防護策略始終處於最新狀態。

五、總結：傳統負載均衡器 (Load Balancer) 與 Skudonet WAAP 比較

	1. 性能瓶頸	2. 缺乏多層次負載均衡	3. 有限的協議支持	4. 缺乏高可用性支持
問題 	傳統負載均衡器在高流量環境下容易成為瓶頸，影響整體性能。	許多負載均衡器僅支持基本的 L4 負載均衡，無法進行更高層次的 L7 負載均衡。	不支持多種協議，限制了其使用場景。	無法提供有效的高可用性方案，容易在故障時導致服務中斷。
Skudonet 解決方案 	**高性能負載均衡：** Skudonet 提供每核心 450,000 個 TCP 請求/秒的處理能力，顯著提升性能。 支持每核心 11,000 個 HTTP 請求/秒和 9,000 個 HTTPS 請求/秒，適應高流量需求。	**多層次負載均衡：** 支持 L2、L3、L4 和 L7 層的負載均衡，涵蓋從網絡層到應用層的全面負載均衡需求。 提供 DNS 服務負載均衡（GSLB），實現跨數據中心的流量分配。	**支持廣泛的通訊協議：** 支持多種通訊協議，包括 TCP、UDP、SCTP、HTTP、HTTPS 等，適應多樣化的應用場景。	**高可用性支持：** 支持無狀態和有狀態的故障切換，保證服務的高可用性。 提供主動-被動集群高可用性方案，確保服務不中斷。

史特林有限公司
STIRLINGNET.COM

Thank You

鄭迦聲 alton@stirlingnet.com

史特林有限公司 2024/6/30

SKUDONET