

思科 ACE 網路應用程式防火牆

(Cisco® ACE Web Application Firewall) 中文規格

產品綜覽

思科 ACE 網路應用程式防火牆 (Cisco® ACE Web Application Firewall) (圖1) 是 Cisco Application Control Engine (ACE) 應用控制引擎系列產品的最新成員。

近年來，越來越多組織希望透過 Web 基礎應用、Web 2.0 及 SOA 的建置，來增加營運效率及商業獲利。這些新的 Web 網路服務提供顧客、員工和夥伴之間一個高彈性以及高覆蓋率的互動平台，讓企業與機關行號擁有一個整合性的資料傳輸架構。然而，新型態的網路攻擊行為，如財務詐欺、身分資料盜取、間諜軟體等，同時也因為 Web 的存取便利性以及缺乏保護而產生。

根據 [privacyrights.org](http://www.privacyrights.org) 統計顯示，單就美國而言，自 2005 年起已有近 2.5 億筆資料外洩。有鑑於此，包括 Sarbanes-Oxley、Graham-Leach-Bliley、HIPAA、PCI、Basel II、EU Data Privacy Regulation、J-SOX 及 PIPEDA 等組織，特別就資料及個人情資的儲存及傳送等提出加強保護要求之相關規範。

Cisco ACE Web Application Firewall 是專門針對 Application 層的防火牆，可以滿足 Payment Card Industry (PCI) Data Security Standard (DSS) 要求，協助企業組織儲存、處理與傳送信用卡資料。針對 HTML 及 XML 安全要求的獨特性，Cisco ACE 網路應用程式防火牆 Section 6.5 和 6.6，是完全符合 PCI DSS 1.1 版本要求的解決方案。其中 Section 6.6 更要求凡是處理、傳送或儲存信用卡資訊的企業組織，都必須於 2008 年 6 月 30 日前，對於 OWASP 所列前十大惡意攻擊 (http://www.owasp.org/index.php/Top_10_2007) 加以防範。

Cisco ACE Web Application Firewall 透過 Web 應用層的分析及高效能 XML 分析管理技術來保護 Web 應用服務。常見的攻擊包括跨站腳本攻擊 (Cross-Site Scripting)、注入弱點 (Injection Flaw)、惡意程式執行 (Malicious File Execution)、不安全的物件參考 (Insecure Direct Object Reference)、跨站冒名請求 (Cross-Site Request Forgery)、程式碼錯誤訊息外漏 (Information Leakage and Improper Error Handling)、身分驗證功能缺失 (Broken Authentication and Session Management)、未加密的儲存設備 (Insecure Cryptographic Storage)、未加密的網路連線 (Insecure Communication)、無權限的控制 (Failure to Restrict URL Access)，其中 Cross-Site Scripting 與 SQL Injection 已連續兩年列為全球頭號的嚴重資安弱點。

Cisco ACE Web Application Firewall 具備整合 Extensible Markup Language (XML) 防火牆能力，將有效防護從傳統 HTML-based Web 應用延伸到新型態 XML-enabled Web 服務運用。其中 XML 防火牆功能包含檢查 XML 內容以防止違法內容影響 Web 服務正常運作。

Cisco ACE Web Application Firewall 支援全代理模式，可處理包含需求 (request) 和回應 (response) 雙向服務。不僅可對攻擊行為進行阻斷 (Block)，也可過濾非必要的網站資訊。透過網路的回應 (response) 訊息，封鎖駭客取得資訊的同時也擔任資料庫的守門員，防止包含信用卡帳號、身份證字號或其他重要資料的外洩。



圖1：思科 ACE 網路應用程式防火牆 (Cisco® ACE Web Application Firewall)

- 新一代應用防火牆
- 含完整特徵碼 (signatures) 可針對已知攻擊型態進行防堵
- 針對 Web 應用話務進行過濾
- 容易使用

主要特性與效益

- 大幅降低針對關鍵任務應用網路 (Web) 攻擊的機率
- 以具成本競爭力的解決方案，在短時間內部署安全性網路 (Web) 專案。
- 藉由整合 SOAP 與 XML 相關應用，簡化當前網路 (Web) 安全性管理。

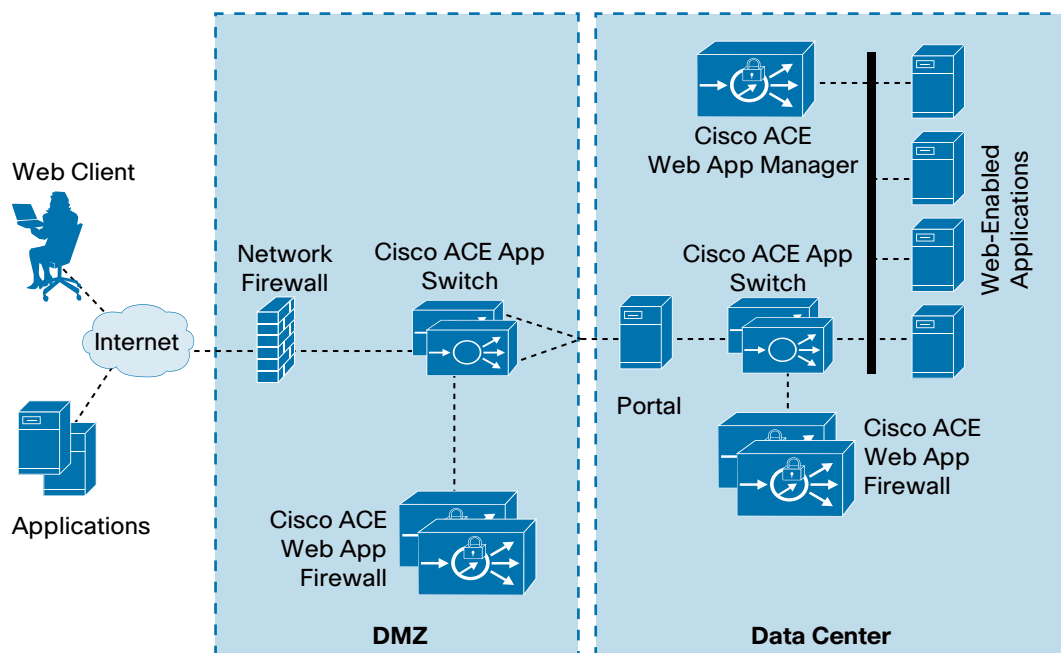


圖2：思科 ACE 網路應用程式防火牆 (Cisco® ACE Web Application Firewall) 網路架構

產品規格

1. 網路應用程式安全

- 支援 Reverse Proxy 模式
- 支援 Monitor Mode 部署方式，並可藉由人工輔助學習方式 (Human-Assisted Learning) 部署
- 可防護 Web-based 的 HTML 及 XML 威脅
- 可保護應用程式免於 XML DoS 的攻擊
- 可支援使用者自行客製化過濾規則 (Rules) 及特徵碼 (Signatures)
- 系統可提供預設的符合 PCI DSS 1.1 之 Section 6.5 及 6.6 裏有關 OWASP TOP 10 的規範的規則
- 具備網站 (Web Site) 攻擊與網頁 (Web Page) 參數竄改攻擊之防禦與偵測
- 可針對以下特性對後端網路系統進行保護
 - 緩衝區溢位 (Buffer Overflow) 攻擊
 - 異常 HTTP 協定偵測，HTTP 參數非法修改
 - Null Byte 阻斷
 - 輸入參數編碼攻擊及參數正規化 (Canonicalization)
 - HTTP 回應 (HTTP Response) 的重寫 (Rewrite) 及過濾
 - 可防範 Cookie 及 Session 的篡改
 - 可防範跨站攻擊 (Cross-Site Scripting)
 - 可防範 SQL 注入 (SQL Injection) 及命令注入 (Command Injection) 攻擊
 - 可保護有關個人隱私資料 (Privacy) 免於外洩
 - 可對後端伺服器及應用程式錯誤訊息進行客製化及遮蓋 (Cloaking)
 - 可對 Referrer 標頭進行檢查，保護網路使用者免於跨站偽冒攻擊 (CSRF, Cross-Site Request Forgery) 的危險
 - Web application attacks (支援 HTTP、HTTPS 及 XML 應用攻擊)
 - Session Hijacking (連線截奪)
 - Cookie Poisoning (資訊塊中毒)
- 可提供正面表列 (Positive) 與負面表列 (Negative) 的過濾方式
- 內建可符合 PCI 規範中有關 OWASP 網路應用程式攻擊的 Profile 供管理者快速套用

2. 傳輸安全

- 支援 SSL v2/3，並可自行設定 Cipher Suite
- 支援 FIPS 140-2 Level 3 平台 (可選)

3. 加密及簽章

- 可防禦 Cookie 篡改 (Cookie Tampering) 並維持 Cookie 在瀏覽器中儲存的機密性
- 可支持 FIPS 規範，並可藉由將 SSL 密鑰儲存在本硬體設備中以防止遭受 SSL 密鑰挾持 (SSL Key Hijacking) 攻擊
- 可支援以下加密演算法：
 - Advanced Encryption Standard (AES)
 - Data Encryption Standard (DES)
 - Triple DES (3DES)
 - Blowfish
 - RSA
 - Diffie-Helman
 - Digital Signature Algorithm (DSA)
 - Secure Hash Algorithm 1 (SHA-1) and Message-Digest 5 (MD5)

4. 管理

- 支援 Web-based 的管理界面
- 支援 Command-line 界面
- 支援 SSH
- 支援 Simple Network Management Protocol (SNMP)
- 支援 Roles-based Access Control (RBAC) 存取控制模式
- 設定檔與記錄可以匯入及匯出

5. 稽核與記錄

- 系統需可產生 Syslog、Message 及 Event Logs
- 流量的監控與報告
- 警示的監控與統計
- 可記錄管理者有系統設定的稽核軌跡 (Audit Trail)

6. 硬體規格

- 為標準 1U 設備
- 可提供硬體加速：1 FIPS 140-2 Level 3-Compliant 4,000 SSL TPS 或 1 Non-FIPS complaint (14,000 SSL TPS)
- 可提供 4 埠 Gigabit Ethernet 及獨立的 Light-out management Ethernet port
- 可提供 4GB 的 RAM
- 可提供 Dual hot-swappable SAS HDD with RAID (20 GB usable)
- 支援 HA 架構

更多資訊

欲知更多思科 ACE 網路應用程式防火牆的詳細資訊請參考 <http://www.cisco.com/en/US/products/ps9586/index.html> 網站，或洽詢當地的 Cisco 專員



台北總公司
台北市信義路四段 460 號 12 樓
www.cisco.com.tw
Tel: 02 - 8758 - 7100
Fax: 02 - 8758 - 7199

台中辦事處
台中市公益路二段 51 號 20 樓 A2
www.cisco.com.tw
Tel: 04 - 2327 - 1372

高雄辦事處
高雄市希雅區三多四路 110 號 19 樓之 2
www.cisco.com.tw
Tel: 07 - 338 - 1092
Fax: 07 - 338 - 1094

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco System Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609F)