ASF Application Security Firewall

ASF-系列中文型錄

應用程式安全防火牆

ASF-系列應用程式安全防火牆提供企業級Web應用程式防火牆(WAF)和分散式拒絕服務(DDoS)緩解解決方案，幫助保護企業資料中心的關鍵服務免於遭受OWASP Top 10 Web攻擊、資訊洩漏、拒絕服務(DoS)攻擊，分散式拒絕服務(DDoS)攻擊和其他安全威脅。

Array Networks ASF-系列採用先進專屬的64位元SpeedCore™多核心處理作業系統(ArrayOS)，可為業務關鍵型應用程式提供全面的偵測，以及防禦攻擊和威脅。Array Networks ASF-系列將正面(Positive)和負面(Negative)的WAF安全防護模型結合在一起，不僅可以偵測和阻止最新的已知攻擊和安全漏洞，還可以有效地防止零日(Zero-Day)攻擊。ASF-系列提供精細度的攻擊防禦控制，支援防禦設定檔的自動學習和動態刷新能力，並通過客戶端來源驗證機制提高攻擊偵測的準確性。

亮點與優勢

- ASF-系列作為下一代Web應用程式防火牆，為關鍵業務伺服器和應用程式提供多層(Multi-Layer)的安全防禦。
- ASF-系列整合了正面(Positive)和負面(Negative)的WAF安全防護模型，不僅可以偵測和阻止最新的已知攻擊和安全漏洞，而且還可以有效地防止零日(Zero-day)攻擊。
- ASF-系列整合了精密的攻擊特徵資料庫，可以防止各種各樣的攻擊，諸如SQL注入(SQL Injection)，PHP注入(PHP Injection)，跨網站指令碼攻擊(XSS)，命令執行(Command Execution)，網路爬蟲(Crawler)/掃描(Scanner)，跨網站請求偽造(CSRF)，盜鏈(Leech)，後門殼層(Webshell)，敏感資料洩漏(Sensitive Data Leakage)，會話劫持(Session Hijacking)和協定違規(Protocol Violation)等攻擊行為。
- ASF-系列針對Web伺服器提供Layer-3~Layer-7防禦功能，包括企業級分散阻斷服務(DDoS)攻擊緩解，進階網路存取控制，白名單和黑名單，HTTP協定符合性檢查，Cookie篡改防禦，暴力防禦(Brute Force)，防盜鏈(anti-Leech)，防爬網(anti-Crawling)/掃描(Scanning)和資料封包異常(Packet Anomaly)檢查等防禦功能。
- ASF-系列支援自定義攻擊特徵，以及靈活的部署模式/防禦模式，滿足各種複雜Web應用程式的要求。
- ASF-系列提供了一個組態精靈(Configuration Wizard)，可幫助您根據應用程式的特性，快速構建防禦設定檔，從而降低了設定複雜性，並提供了準確的防禦功能。
- ASF-系列正面(Positive)的WAF安全防護模型，通過自動學習(Automatically Learn)功能，識別正常流量(Normal Traffic)的特徵，以形成正面白名單(Positive Whitelist)，並可動態刷新WAF設定檔。
- ASF-系列提供了流量基準線學習(Traffic Baseline Learning)功能，可根據學習結果動態刷新並自動設定DDoS設定檔的規則和選項，從而簡化了設定，並提高防禦精確度。
- ASF-系列支援資料洩漏保護(DLP)規則，此規則可以防止洩露用戶的私人訊息或敏感訊息，例如身分訊息，手機號碼，電子郵件地址，信用卡號等。
- ASF-系列支援虛擬修補(Virtual Patching)功能，這個功能可以將第三方的Web漏洞掃描程式，如IBM AppScan的掃描結果轉換為可執行的安全策略，或稱之為虛擬修補程式(Virtual Patch)，從而降低漏洞對客戶所造成的風險。
- ASF-系列支援Web網頁防篡改(WAD)功能，可以即時偵測針對Web頁面的篡改(Defacement)攻擊，並即時恢復為正常未遭篡改時的頁面，以保護客戶的公共形象。
- ASF-系列提供豐富的事件日誌，以幫助重播攻擊(Replay Attacks)並進行審核，並支援導出事件日誌以進行外部分析。
- ASF-系列提供了直觀的圖形化監視功能，可以監視系統狀態，攻擊，流量和封包丟棄。
- ASF-系列提供監視報告，進階服務安全報告，以及符合支付卡產業資料安全標準(PCI DSS)合規性報告，並支援定期產生報告以及客製化報告。
- ASF-系列提供依據角色(Role-Based)的權限管理與控制，並支援外部身分驗證和授權，且提供管理員審核日誌。
- ASF-系列支援軟體和硬體旁路(Bypass)功能，可以幫助避免由於單一ASF設備故障而導致的服務中斷，諸如軟體或硬體故障。
- ASF-系列具備領先業界的橢圓曲線加密演算法(ECC)性能，以及非對稱演算法RSA 2048/4096位元SSL性能。
- ASF-系列提供全面IPv6支援，有助於解決IPv4地址耗盡的問題，並促進邁向全面採用IPv6。
- ASF-系列支援XML-RPC和eCloud™ RESTful API，這使得ASF-系列能夠天衣無縫整合雲管理系統，以及第三方監視和管理平台。
- ASF-系列採用64位元的SpeedCore™多核心處理作業系統，且提供行業領先的性能，並支援與硬體設備和虛擬設備的無縫整合。
- ASF-系列支援N+1群集(Clustering)高可用性方案，最多可群集達32台硬體或虛擬設備，並且可以設定為Active-Active/Active-Standby工作模式，從而提供了業界領先的高可用性和可擴充性。
- ASF-系列使用節省空間的備援電源硬體設備，與其它替代解決方案相比，其功耗相對的降低了10-35%。
- ASF-系列提供易於使用且熟悉的命令行介面(CLI)和直觀的WebUI使用介面，更易於使用和設定。

下一代Web應用程式防火牆

隨著應用程式越來越多地轉移到Web伺服器，承載關鍵業務應用程式的伺服器已成為惡意攻擊，篡改(Tampering)和其他安全事件的目標，這些惡意攻擊事件可能損害知識產權，客戶訊息和其他敏感性業務資料，從而造成巨大的經濟和聲譽損失。

ASF-系列應用程式安全防火牆可防禦最廣泛的攻擊機制，同時提供活躍的事件回報，以阻止駭客的追蹤和攻擊，並通過事後分析和診斷，為加強伺服器防禦未來攻擊提供指導。

ASF-系列採用了將正面(Positive)和負面(Negative)的WAF安全防護模型結合在一起的體系結構，以使它們同時為Web應用程式提供防禦。負面(Negative)的WAF安全防護模型可通過不定期升級Array Networks Signature Library來支援最新攻擊特徵庫，從而抵禦了最新的已知Web攻擊；正面(Positive)的WAF安全防護模型可識別正常流量的特徵，並動態刷新防禦設定檔，從而有效地抵禦各種複雜未知的Web攻擊。

ASF-系列支援虛擬修補程式(Virtual Patching)功能，這個功能可以將第三方Web漏洞掃描程式諸如IBM AppScan的掃描結果轉換為可執行的安全策略，稱之為虛擬修補程式(Virtual Patch)，從而降低了漏洞造成對客戶帶來的風險。

企業級DDoS緩解

ASF-系列可以緩解OSI網路模型中的Layer-3~Layer-7的DDoS攻擊。可以通過學習基準線流量來自動生成適合客戶現有網路的防禦規則，並支援多種來源驗證機制，例如人機驗證(CAPTCHA)和會話跟踪，以準確區分攻擊來源和合法來源，從而實現快速反應和準確防禦機器人程式(BOT)。ASF-系列可以緩解下列的Layer-3~Layer-7的DDoS攻擊，但不僅侷限於下列：

- HTTP GET Flood attack
- HTTP POST Flood attack
- HTTP Slowloris attack
- HTTP Slow POST attack
- HTTP ChallengeCollapsar(CC) attack
- HTTP Packet Anomaly attack
- SSL Handshake attack
- SSL Renegotiation attack
- SSL Packet Anomaly attack
- DNS Query Flood attack
- DNS Reply Flood attack
- DNS NXDomain Flood attack
- DNS Cache Poisoning attack
- DNS Packet Anomaly attack
- TCP SYN Flood attack
- TCP SYN-ACK Flood attack
- TCP ACK Flood attack
- TCP FIN/RST Flood attack
- TCP Connection Exhaustion attack
- TCP Fragment Flood attack
- TCP Slow Connection attack
- TCP Abnormal Connection attack
- UDP Flood attack
- UDP Fragment Flood attack
- ICMP Flood attack
- Smurf、Ping of Death、LAND、IP Spoofing、Teardrop、Fraggle、Winnuke、Tracert 和其他畸形的單資料封包攻擊。

靈活的部署選項

ASF-系列提供了靈活的部署選項，可以滿足各種客戶網路的情況，ASF-系列支援以下部署模式：

- **橋接透明模式(Bridge Transparent Mode)**：ASF在Layer-2網路上透明地建立連接，管理員不需要更改任何網路設定，此模式支援旁路(Bypass)功能，但不支援HTTPS應用程式防禦。
- **橋接代理模式(Bridge Proxy Mode)**：ASF在在Layer-2網路上透明地建立連接，管理員需要修改網路的NAT/路由設定或DNS資源記錄，以將應用程式流量導向到虛擬服務IP(Virtual Service IP)，以確保應用程式流量實際通過ASF設備。
- **路由透明模式(Routing Transparent Mode)**：ASF在Layer-3網路上連接，管理員需要將應用程式流量的請求和回應分別導向到上行鏈路(Uplink)和下行鏈路(Downlink)的連接介面。
- **路由代理模式(Routing Proxy Mode)**：ASF在Layer-3網路上透明地建立連接，管理員需要修改網路的NAT/路由設定或DNS資源記錄，將應用程式流量導向到虛擬服務IP(Virtual Service IP)。
- **路徑外旁接模式(Out-of-path TAP mode)**：ASF設備已部署在流量路徑之外，管理員需要在ASF連接的交換器上設定連接埠鏡像策略，以便將流量複製到ASF設備進行偵測，該模式僅偵測攻擊，不阻止攻擊。此外也不支援HTTPS應用程式防禦。

多階段安全處理

在安全事件發生之前，將使用Web漏洞掃描程式掃描應用程式，並將掃描結果快速轉換為可執行的安全策略，稱之為虛擬修補程式(Virtual Patch)，從而降低了客戶由漏洞引起的風險。

在發生安全事件時，ASF-系列會執行防禦設定檔，以便即時偵測和阻止攻擊，並記錄詳細的稽核日誌，包括可疑請求資料和所有相關的互動資料。

發生安全事件後，管理員可以分析日誌和統計訊息，以便調整防禦設定檔，從而提高防禦的準確性和效率。

精密的特徵資料庫

ASF-系列已整合Array Networks的安全中心(ASC)，安全中心(ASC)會定期發布攻擊特徵庫(ASL)。該特徵庫已包含最新已知Web攻擊預先確定的特徵，包括下列但不僅限於下列攻擊行為：SQL注入(SQL Injection)，PHP注入(PHP Injection)，跨網站指令碼攻擊(XSS)，網路爬蟲(Crawlers)/掃描(Scanners)，跨網站請求偽造(CSRF)，盜鏈(Leech)，後門殼層(Webshell)，敏感性資料洩漏(Sensitive Data Leakage)，會話劫持(session hijacking)和協定違規(Protocol Violations)。 安全中心(ASC)會定期更新和發布特徵庫(ASL)，以添加新攻擊或漏洞的特徵，並更新掃描器/爬網程式類型，惡意URL和後門殼層(Webshell)特徵。ASF-系列支援以手動和自動方式更新特徵庫(ASL)。

ASF-系列讓管理員可以根據應用程式特點，例如應用程式類型，平台類型，資料庫類型和程式語言，來構建最適合其應用程式特徵規則集合，以便提供最高的防禦準確性和性能。

此外，ASF-系列還支援自定義攻擊特徵和第三方商業化攻擊特徵的整合。

SSL卸載(SSL Offload)

ASF-系列提供硬體加速SSL或軟體SSL的卸載(SSL Offload)功能，該功能可將計算密集型的SSL加密和解密工作負載轉移到ASF設備上，從而減少後端伺服器的工作量，並提高伺服器性能。

借助SSL卸載功能，ASF-系列可以對HTTP資料封包進行深度檢查，這使得採用加密方法進行的攻擊無處躲藏。

全面的伺服器保護

ASF-系列為伺服器提供全面的伺服器保護功能

- ASF-系列支援進階ACL，該ACL可以依據Layer-3~Layer-7的流量特性，來對指定的防禦對象進行流量控制。
- ASF-系列支援HTTP過濾器(HTTP Filter)功能，該功能可以根據HTTP協定特點，例如請求方法，標頭，URL，Cookie，來過濾HTTP資料封包，並針對客戶Web應用程式執行深度協定遵從性或安全遵從性檢查。
- ASF-系列提供進階防禦選項，例如HTTP透過標頭屏蔽(HTTP Via Header Masking)，回應標頭移除(Response Header Removal)，Cookie安全性設定，Cookie篡改防禦，會話劫持防禦，客製化錯誤分頁(Error Page)，以及URL偵測和監視。
- ASF-系列支援暴力(Brute Force)防禦功能，可有效防止客戶網站遭受暴力攻擊。

網頁防篡改

ASF-系列提供Web防篡改(WAD)功能，該功能可以即時監視受保護的Web頁面文件並緩衝頁面內容。當偵測到受保護的網頁遭到篡改時，ASF-系列會自動將網站被篡改的網頁恢復為正常頁面，從而保護公眾形象。

自動學習和動態剖析(Dynamic Profiling)

ASF-系列提供正面(Positive)的WAF安全防護功能，可以根據正常流量的特徵生成正面(Positive)的白名單。管理員可以將設備設定為可在指定時間間隔，或增量學習日誌計數的數量達到指定臨界值時，自動生成正面白名單(Positive Whitelist)。

ASF-系列提供流量基準線學習功能，功能啟用後，設備將自動學習防禦對象的流量基準線，並支援根據學習結果自動動態刷新DDoS設定檔。這不僅減少了人工干預，而且提高了防禦精準度。

應用程式安全可視化

- 提供豐富的事件日誌，以便重播和稽核攻擊事件。
- 提供WAF攻擊日誌，WAF稽核日誌，HTTP存取日誌， DDoS警告日誌，DDoS攻擊日誌和HTTP過濾日誌。
- 支援管理員稽核日誌，以便針對管理員進行稽核。
- 支援導出安全事件日誌。
- 提供直觀的圖形監視。
- 顯示系統狀態，例如CPU使用率，RAM使用率，硬碟使用率和流量處理能力(Throughput)。
- 顯示攻擊統計資訊，包括嚴重性分佈，攻擊類型，攻擊來源，攻擊來源區域等。
- 顯示服務流量統計資訊，包括不同協定流量的詳細統計資訊。
- 顯示丟棄封包統計資訊，包括丟棄原因統計資訊。
- 顯示服務存取統計資訊，包括存取的TopN URL，客戶端IP等。
- 通過添加所需的監視圖以支援客製化監視頁面。

- 支援手動導出監視圖並定期生成監視報告。
- 支援產生一次性或定期的進階報告。
- 支援系統狀態報告，應用程式安全狀態報告，符合PCI DSS標準合規性報告等。

高可用性

ASF-系列提供了多種高可用性(High Availability)選項，通過這些選項可以最大程度地延長應用程式的在線時間，並確保應用程式服務的高可用性。

- 群集功能(Clustering)可為在路由模式下部署的兩台或多台ASF設備提供快速故障轉移(Fail-Over)；ASF設備可以在Active-Standby或Active-Active模式下工作。
- 在已部署備援解決方案的網路環境中，管理員可以使用外部HA解決方案，來為以橋接透明或橋接代理模式部署的ASF設備，提供流量的高可用性。
- 軟體和硬體旁路功能(Bypass)可以避免橋透明模式下部署的ASF設備的故障，例如軟體和硬體故障因而導致流量中斷。
- 如果以路徑外旁接模式(Out-of-path TAP mode)部署ASF設備，則設備故障不會導致服務中斷。

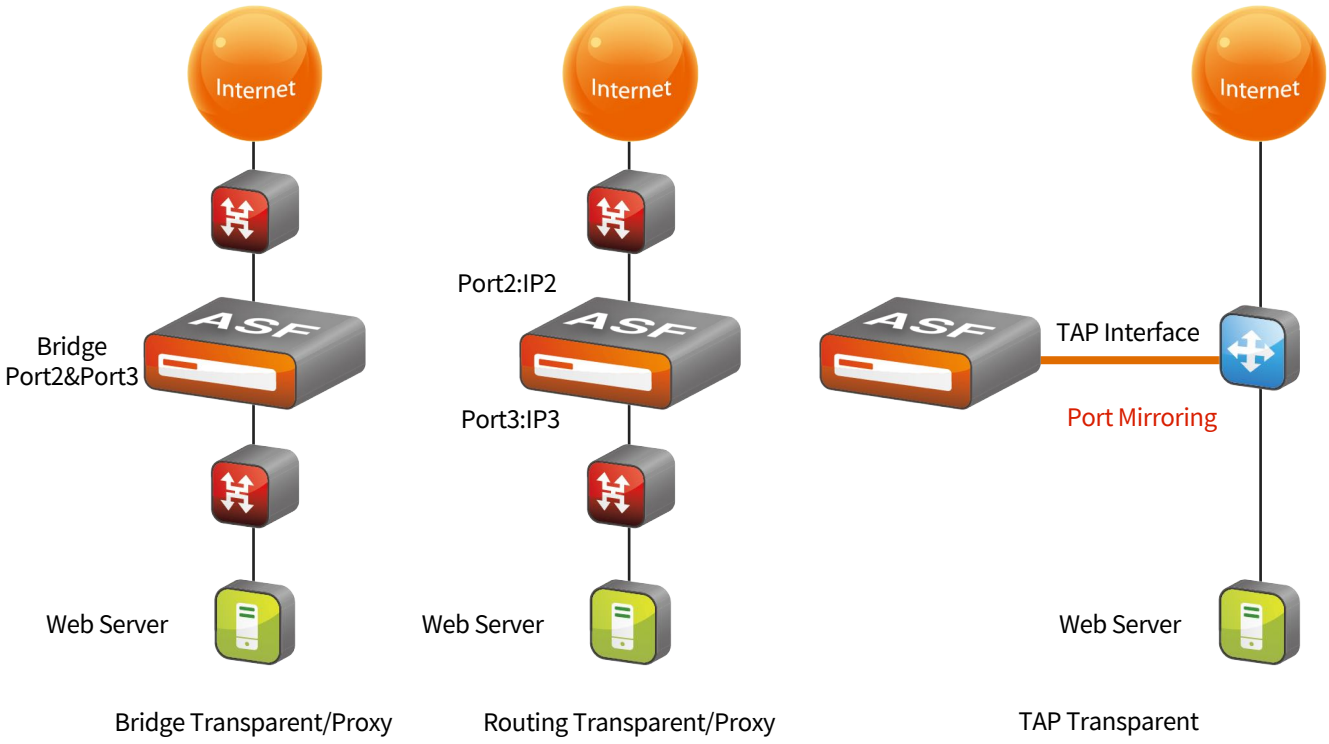
管理和整合

ASF-系列易於部署，為設定管理需求提供直觀的Web用戶介面和易於操作的命令行介面；借助管理工具，網路管理員可以通過使用XML-RPC技術查看系統參數的狀態，啟用服務並實現設定自動化；通過使用可擴充的應用程式開發介面(API)，管理員可以將系統管理與第三方監視和管理系統整合在一起。

為滿足雲端應用程式安全性的部署和管理要求，Array Networks提供eCloud RESTful™ API，為雲管理系統提供了腳本級(script-level)介面，以便管理和監視Array Networks的設備，並協助雲操作系統與運行Array Networks的DDoS緩解方案的虛擬機之間進行互動。

實體和虛擬設備

專用的ASF-系列設備利用多核心體系結構，SSD，軟體或硬體SSL和壓縮，節能組件，以及10GigE或40GigE網路介面來開發，是專門為可擴充的應用程式安全性而設計的解決方案；無論是在Array Networks的AVX-系列網路功能平台上運行，還是在常見的Hypervisor上運行，vASF虛擬設備對於尋求從虛擬環境的靈活性中受益，快速提供基礎架構服務，和新的彈性業務模型，或以最小的風險和前期成本評估的用戶而言，Array Networks應用程式安全防火牆都是理想的選擇。

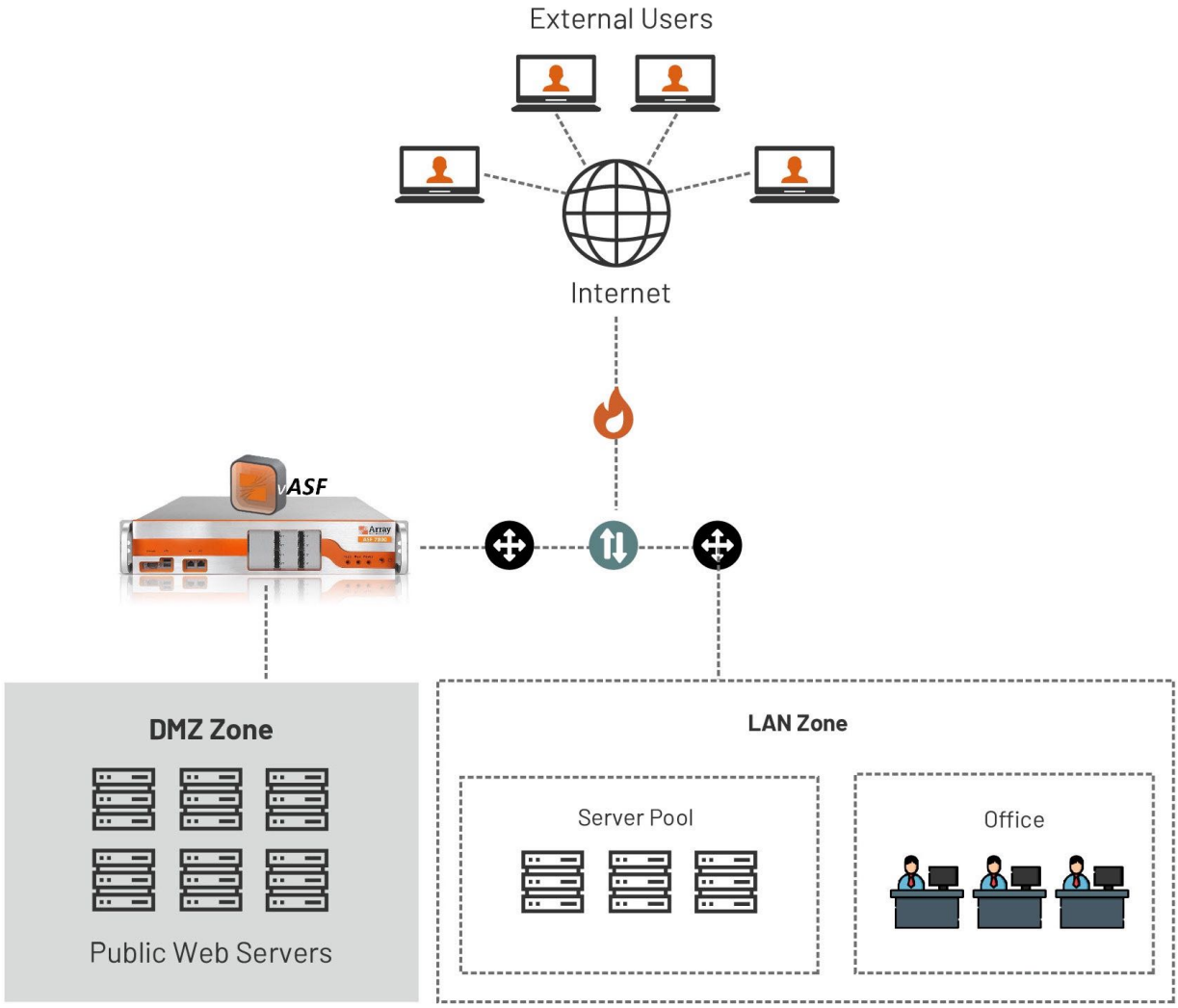


產品功能(Product Features)	
應用程式安全性	
應用程式防火牆(WAF)	· 負面(Negative)的安全防護模型；依據特徵(Signature-based)的防禦，可防止SQL注入(SQL Injection)、跨網站指令碼攻擊(XSS)、網路爬蟲(Crawlers)/掃描(Scanning)攻擊、跨網站請求偽造(CSRF)攻擊、盜鏈(Leech)、後門殼層(Webshell)、本地/遠端文件包含漏洞(File Inclusion)、命令注入(Command Injection)、敏感資料洩漏(Sensitive Data Leakage)等，並支援一鍵(One-Click)特徵排除。 · 身分證資訊、電話號碼、電子郵件地址、銀行卡號的資料洩漏保護(DLP)規則和內容過濾。 · 跨網站請求偽造(CSRF)攻擊防禦、防盜鏈(anti-Leech)、防網路爬行(anti-Crawling)/掃描(Scanning)、以及虛擬修補程式(virtual patching)。 · 正面(Positive)的安全防護模型；自動流量學習，自動生成正面的白名單，防禦零日(Zero-Day)攻擊，學習可信任來源的流量模式。
應用DDoS攻擊緩解	· HTTP GET Flood、HTTP POST Flood、HTTP Slowloris Attack、HTTP Slow POST Attack、HTTP CC Attack、HTTP Packet Anomaly Attacks。 · SSL Handshake Attack、SSL Renegotiation Attack、SSL Packet Anomaly Attacks。 · DNS Query Flood、DNS Reply Flood、DNS NXDomain Flood、DNS Cache Poisoning、DNS Packet Anomaly Attacks。 · 客戶端來源驗證。 · 學習應用流量基準線、動態刷新防禦設定檔。
進階防禦選項	· HTTP過濾器(Filter)、HTTP通過標頭遮罩(HTTP Via Header Masking)、移除包含後端伺服器資訊的HTTP回應標頭。 · Cookie篡改防禦、會話劫持(session hijacking)防禦、暴力攻擊防禦。 · 防網頁置換(Web anti-defacement)。 · 支援將HttpOnly和Source屬性插入HTTP回應cookie。 · URL偵測和URL監視。 · 自定義錯誤頁面和DNS網域統計資訊；真實來源IP偵測。
應用程式 ACL	· HTTP ACL、DNS ACL、URL白名單。 · 靜態黑名單、靜態白名單、動態黑名單、動態白名單、依據GeoIP地理定位的存取控制。
SSL 加速	· 硬體SSL加速。 · RSA/ECC認證，SSLv3/TLSv1/TLSv1.1/TLSv1.2和自定義密碼套件。 · 客戶端憑證認證。 · SSL會話重用(Session Reuse)和超時控制。 · 伺服器名稱指示(SNI)。
網路安全性	
網路DDoS攻擊緩解	· TCP SYN Flood、TCP SYN-ACK Flood、TCP ACK Flood、TCP FIN/RST Flood、TCP Connection Flood、TCP Fragment Flood、TCP Slow Connection、TCP Abnormal Connection。 · UDP Flood、UDP Fragment Flood。 · ICMP Flood。 · 學習流量基準線，動態刷新防禦設定檔。 · 客戶端來源認證。 · IP信譽。

常見的DoS攻擊和格式錯誤的單封包攻擊	· Smurf、LAND、Fraggle、IP Spoofing、Ping of Death、Teardrop、WinNuke、Tracert。 · TCP Packet with Abnormal Flag、Large UDP Packet、ICMP Redirect Packet、ICMP Unreachable Packet、Large ICMP Packet、IP Packet with Routing Record Option、IP Packet with Source Routing Option、IP Packet with Timestamp Option。
網路 ACL	· TCP ACL、UDP ACL、ICMP ACL。 · 靜態黑名單、靜態白名單、動態黑名單、動態白名單、依據GeoIP地理定位的存取控制。
應用程式安全性可視化	
事件日誌	· WAF攻擊日誌，WAF稽核日誌，HTTP存取日誌，HTTP違規日誌，HTTP過濾日誌。 · DDoS警告日誌，DDoS攻擊日誌。 · 日誌整合，通過電子郵件/SNMP發出安全事件警報。
圖形監控	· 廣域攻擊統計，安全群組攻擊統計，安全服務攻擊統計。 · 廣域流量統計，防禦目標流量統計。 · 廣域丟棄封包統計，防禦目標丟棄封包統計。 · CPU使用率，Memory使用率，流量處理能力，硬碟使用率。 · 自定義監視圖。
報告	· 系統狀態監視報告，進階服務安全狀態報告，符合PCI DSS標準合規性報告。 · 客製化報告定，定期報告。
應用程式可用性	
網路和部署	· Link Aggregation，VLAN，MNET。 · 橋接模式，路由模式，旁接模式(TAP)。 · 靜態路由，RIP/OSPF/BGP 動態路由，策略路由。
高可用性	· 可群集(Clustering)達32台，支援Active/Active 或 Active/Standby工作模式。 · 支援設定同步。 · 支援硬體旁路(HW bypass)，虛擬機支援軟體旁路(SW bypass)。
IPv6	· 支援完整的IPv6，支援IPv4和IPv6雙重架構機制。 · 作業系統取得IPv6 Ready Logo Phase-2金質認證。
系統	· 支援集中管理系統。 · 支援安全加密的CLI，WebUI和SSH遠端管理，以及支援XML-RPC遠端管理介面，並可與第三方管理和監視平台整合。 · 支援SNMPv2，SNMPv3和私有MIB檔案。 · 依據TCP和UDP的系統日誌(Syslog)。 · 用戶管理，管理員身分驗證和授權，依據角色的權限管理，管理員稽核日誌。 · 支援通過電子郵件和SNMP發出系統警報。 · 支援多個設定檔，以及節點之間的設定同步。 · 在線故障排除和即時監視。
eCloud RESTful API	· 為雲管理系統提供介面，以便控制和監視硬體ASF設備和虛擬ASF設備，協助CloudOS中的虛擬機等組件之間的協助互動，ASF設備的遠端管理和ASF設備上的事件通知。

ASF應用安全防禦架構

- 應用程式防火牆(WAF)
- 應用層DDoS緩解
- 網路層DDoS緩解
- 防網頁篡改(WAD)
- 進階存取控制
- 自動學習
- 動態刷新設定檔
- 應用程式可視化
- SSL加速
- 支援完整的IPv6
- N+1群集(Clustering)



產品功能(Product Features)					
產品系列型號	ASF 1800-系列	ASF 2800-系列	ASF 5800-系列	ASF 7800-系列	ASF 9800-系列
最大流量處理能力	5 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
最大SSL TPS(RSA 2K)	20K	20K	40K	55K	110K
最大ECC TPS(ECDSA-P256)	14K	14K	28K	38K	76K
10/100/1000Base-T	8	4	4	-	-
1000Base-X SFP	-	-	2(選購)	-	-
10GBase-X SFP+	-	2	4	8	16
40GBase-X QSFP	-	-	-	-	4(選購)
旁路模組(Bypass Card)	標準配備不提供，選購項目				
電源供應器	雙電源供應器： 100-240VAC，8-4A，50-60Hz			雙電源供應器： 100-240VAC，10-5A，50-60Hz	
外觀尺寸	1U-17”W x 19.875”D x 1.75”H			2U-17”W x 22.5”D x 3.5”H	
重量	18.4 lbs.			29.6 lbs.	
標準	10/100/1000Base-TX(GbE)，1000Base-SX/LX/ZX，10 GibE，10 Gig XF SR/LR，IP，SSH，HTTP 1.0/1.1，SSL，SNMP，RS232				
管理	SSH CLI，Direct Console DB9 CLI，SNMP，Single Console per Cluster，XML-RPC，Out of Band Management-RJ-45				
環境	操作溫度：0~45°C，濕度：0~90%，非冷凝				
電磁相容性	ICES-003，EN 55024，CISPR 22，AS/NZS 3548，FCC， 47FR part 15 Class A，VCCI-A				
安規	CSA， C/US， CE，IEC 60950-1，CSA 60950-1，EN 60950-1				
支援	金級、銀級、銅級				
保固	1年硬體，90天軟體				

	支援的 Hypervisor (64-bit only)	虛擬機器需求
vASF 虛擬版本 支援全部的功能	· Array Networks AVX-系列 · VMware ESXi 5.5 或更高 · KVM 1.1-1.8.1 或更高	· 至少需要2顆虛擬CPUs支援 最低需求： · 4GB記憶體，40GB的硬碟空間

1371 McCarthy. Milpitas, CA 95035 | Phone:(408)240-8700 Toll Free:1-886-MY-ARRAY | www.arraynetworks.com

VERSION 2020-10-TW-REV-A

台灣辦事處 | 台北市復興南路二段283號9樓 | 電話：02-2784-6000 傳真：02-2755-3918

© 2020 Array Networks, Inc. All rights reserved. Array Networks, the Array Networks logo, AppVelocity, eCloud, ePolicy, eRoute, SpeedCore and WebWall are all trademarks of Array Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Array Networks assumes no responsibility for any inaccuracies in this document. Array Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice