corero [NETWORK SECURITY]

SMARTWALL ONE™

產品規格表_

突破平凡，盡在 SmartWall ONE

SmartWall ONE 以高度延展性的架構為核心，採全自動化設計，直覺性操作且易於管理，能有效因應高強度 DDoS 攻擊。其不僅是一項防護機制，更是為企業打造的關鍵防禦基礎，確保網路安全並維持營運穩定。

多地備援能力

DDoS 防護應具備與企業網路同等的韌性與可靠性。SmartWall ONE 提供可彈性調整的多站點韌性防禦，能於各地即時執行防禦策略。即使發生光纖中斷、斷電或站點故障，防禦機制仍可自動持續運作，無需人工介入。

具前瞻性的擴充與靈活性

SmartWall ONE 採用模組化設計，提供高度靈活的擴充能力，企業可依業務需求調整吞吐量授權，或靈活配置 400GE/100GE 實體模組。此設計使防禦能力可隨業務成長無縫擴展，無需重新部署，即可持續保障網路安全。

高解析度流量的可視性

SmartWall ONE 透過深入駭客行為分析，掌握攻擊與網路全貌。Corero 領先業界的分析能力將攻擊模式具象化，提供可行的資訊，協助企業精準強化防禦策略。

全方位防護

SmartWall ONE 可有效防護多種 DDoS 攻擊型態，包括大流量攻擊、狀態耗盡攻擊、高頻短時攻擊、IoT 殭屍網路、地毯式攻擊、DNS 洪水攻擊及脈衝式攻擊。同時，透過成熟的混合雲防禦架構，系統可在面對高強度與複合式攻擊時形成穩定且可靠的防護層，確保網路服務在攻擊期間仍能維持連續運作與高可用性。

DDoS 專用防禦裝置

SmartWall ONE，讓你始終領先威脅一步

DDoS 攻擊手法正逐年演進，不僅攻擊規模持續擴大，策略亦趨於多樣且更具隱蔽性。攻擊者透過不斷變換攻擊模式，並鎖定各類通訊協定發動攻擊，使防禦環境日益複雜。此類攻擊往往來得迅速、結束也快，卻對既有的 DDoS 即時偵測與立即防禦設備造成極大壓力。面對這類快速且高變化的攻擊型態，單純依賴傳統防禦設備已難以因應，企業需部署能即時感知威脅，並迅速採取行動的 DDoS 防禦系統。

這就是為什麼企業應部署 SmartWall ONE 以強化網路防護能力。

SmartWall ONE 是一套快速、極致靈敏且全自動化的 DDoS 防禦解決方案，提供實體設備與虛擬機版本，滿足不同部署的需求。其彈性化、軟體導向的架構設計，能無縫整合至現有網路與基礎設施中。不論網路架構如何轉變，SmartWall ONE 都能為您帶來高度防護的安心體驗，讓您專注於核心業務發展，無須擔心服務中斷的風險。

強大擴充能力，助你從容應變

SmartWall ONE 採用 Speed-Agnostic 架構設計，支援多種速率，並不受單一設備固定吞吐量授權限制，可隨企業規模彈性擴充，真正實現高延展性。全新一代 400G Network Threat Defense（NTD）設備，大幅提升系統效能與部署靈活性。這些先進設備可支援 SmartWall ONE 在本地部署，無論實體硬體或虛擬化軟體形式，皆可完美整合至現有網路架構，與高速網路發展無縫接軌。此設計不僅滿足頻寬需求，更以卓越敏捷性，超越當前與未來的流量挑戰。

支援軟體與虛擬環境部署

SmartWall ONE 適用於雲端與資料中心環境，DDoS 防護可透過軟體形式部署於虛擬機或雲端實例，提供高度延展性與彈性的防禦能力。此部署方式不僅能快速導入與輕鬆擴充，亦可有效降低營運成本，免去專用硬體需求，節省機櫃空間並減少能源消耗。更重要的是，系統可依保護需求快速調整，無需修改實體基礎架構，為追求資源效率且維持高防護水準的企業提供最佳解決方案。

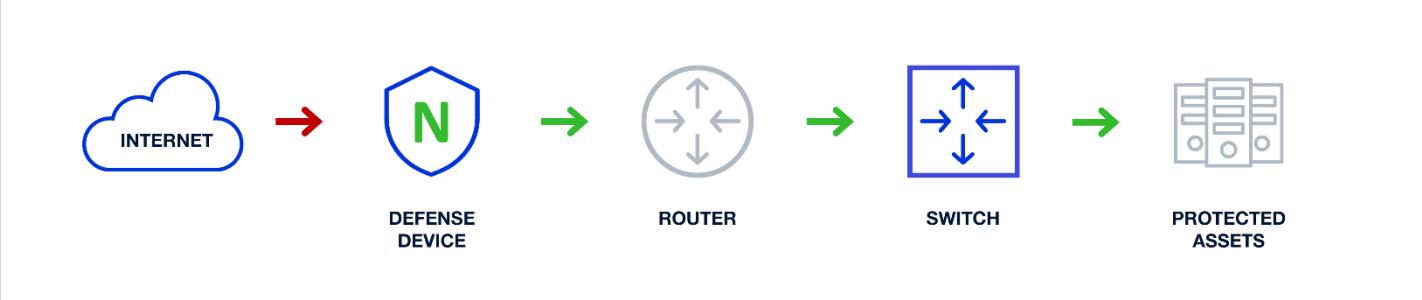
硬體實作

無論採用全新硬體設備，或沿用既有網路架構，SmartWall ONE 均可部署於企業實體網路基礎設施中，提供對 DDoS 防護措施的完整掌控。最新一代 Corero 防護設備採用高度模組化設計，支援雙網路模組配置，使服務提供者能依需求靈活切換介面組合，例如：2 組 400G、2 組 100G 與 1 組 400G，或 4 組 100G 接口。此高彈性模組化架構可根據不同網路需求與容量變化快速調整，無需重新建置整套系統，顯著提升部署效率與投資效益。

SmartWall ONE 支援多元彈性的部署方式，可依防護環境靈活配置，並採用 Always-On 架構，以最快速有效的防護方式，部署於所有網路入口點（Ingress Point）。無論是直接串接網際網路連線（Inline）、部署於資料路徑（Data Path）中，或是與邊界路由器相連，所有進入網路的流量皆透過 SmartWall ONE 進行即時防護。

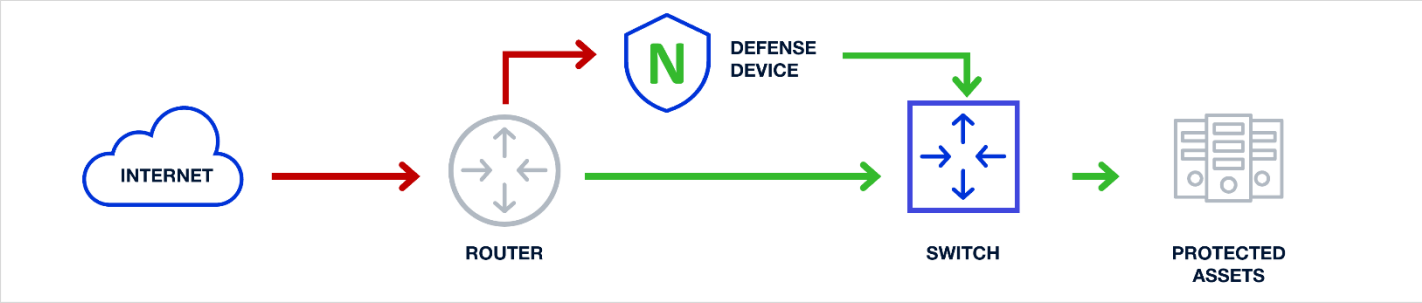
此外，Corero SmartWall ONE 亦支援傳統 DDoS 清洗（DDoS Scrubbing）模式，可依需求透過封包取樣或基於 Flow（Netflow/sFlow）的偵測與流量重導功能，引導異常流量至防禦設備進行清洗與處理，確保網路服務持續可用且穩定。

Inline 部署



N Network Defense Device

Data Path & Scrubbing 部署



N Network Defense Device

真正有感的產品效益

一覽無遺，精準防禦
透過先進的資料分析技術，Corero 呈現清晰透明的攻擊全貌，讓您輕鬆掌握並理解 DDoS 攻擊模式。您可以快速取得所有關鍵細節，不必再為複雜數據煩惱。

對抗 DDoS，快人一步
時時戒備，不僅能阻擋規模龐大、引發關注的攻擊，連那些隱匿且容易被其他系統忽略的小型攻擊也逃不過 Corero 防線。

精準、自動分辨合法與惡意流量
即時攔截惡意 DDoS 流量，讓攻擊在造成影響前就被完全阻擋。整個防禦過程讓使用者完全無感，服務穩定不中斷，運作順暢如常。

削減開銷，防護不打折
SmartWall ONE 防護效能穩定流暢，自動化防禦讓您不必再為 DDoS 頭痛費神，省時又省錢。

輕鬆部署，持續守護
DDoS 攻擊交給 Corero 自動處理，無需手動干預，網路依然穩定暢通、不中斷。

支援 On-Prem 與 Hybrid 架構
結合 Corero 高精準、即時反應的本地部署防護能力，有效強化您的純雲端防護架構 。混合式防護無縫整合，無感部署，效能強勁，提供始終在線的持續守護。

靈活對應各種使用情境
無論採用哪種部署模式，SmartWall ONE 都能靈活配合您的環境。不論是實體、虛擬、Inline 防護或旁線監控，Corero 都能全面守護，在攻擊造成任何損害前即時攔截，將風險降到最低。

強化服務，同步提升營收表現
如果您是服務提供商，SmartWall ONE 將是您提供高階即時 DDoS 防護服務的黃金利器。不僅能強化營收來源，還能有效保障客戶的營運不中斷及不影響正常流量。

穩定無縫的服務連續性
自動化在各分散式據點執行 DDoS 緩解防禦，無延遲、無需重新設定，且沒有單點故障風險。

你的 DDoS 中控中心，狀況全都掌握

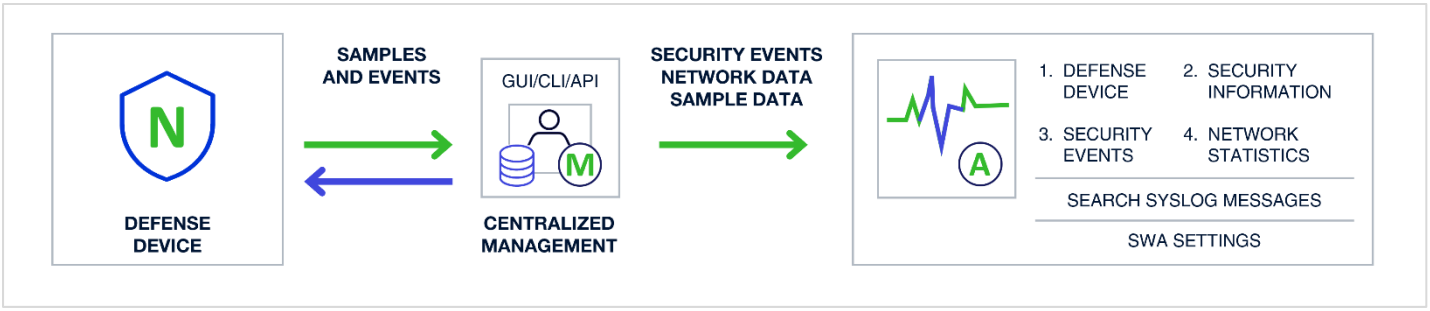
SmartWall ONE 的 SecureWatch Analytics 是您面對 DDoS 攻擊時的全方位監控之眼。它不只是監控儀表板，更能從混亂中理出頭緒，精準指出該如何應對，用最簡單明瞭的方式讓重要資訊一目了然，不用再辛苦過濾雜訊。

全時監看不中斷
資訊可透過即時或歷史圖表與儀表板呈現，讓您全面掌握流量與攻擊趨勢。

精準調校防護策略
轉化數據為行動依據，全面提升資安策略效能。

深入剖析攻擊模式
深入鑽研攻擊期間的詳細流量資訊，掌握被封鎖與允許的流量細節。

升級版威脅情資分析
所有事件都會被安全儲存與索引，並可透過 API 與 syslog 提供給其他資安工具進行外部分析，強化整體整合能力與事件可視性。



N Network Defense Device | **M** Provider Service Management | **W** DDoS Traffic Analysis

設備安全防護範圍

靈活的資安防護功能

- 可防禦針對單一或多個 IP 與子網段的攻擊
- Smart-Rules：專利的高效能啟發式引擎，可自動偵測並封鎖
- 大流量 DDoS 攻擊，包含零時差（Zero-Day）威脅
- Flex-Rules：可客制化過濾規則，採用 Berkeley Packet Filter（BPF）語法，並加入 Corero 強化功能
  - 應對各類型大流量攻擊向量，從反射型（Reflective）攻擊到特定應用負載（如 TeamSpeak、RIPv1、NetBIOS）
- DDoS Intelligence 主動式防禦情報饋送
- 殭屍網路與來源泛洪（Source Flood）偵測與封鎖機制
- 智慧型自動封鎖異常封包片段（Fragment）
- 基於 TCP/UDP 埠號的精準防護
- 支援頻率限制（Rate Limiting）策略設定
- 支援雲端緩解及 BGP RTBH / FlowSpec 訊號回傳整合

資源耗盡型攻擊（Resource Exhaustion）

- 異常格式與截斷封包（例如：UDP 炸彈攻擊 / UDP bombs）
- IP 封包分段／重組規避技術（AETs）
- 無效的 TCP 封包段識別碼（Segment ID）
- TCP/UDP 封框中的錯誤檢查碼與非法旗標（Flags）
- 無效的 TCP / UDP 埠號
- 針對 DNS 基礎架構的 NXDOMAINwater torture

頻寬及資源耗盡型 DDoS 攻擊

- TCP flood（TCP 洪水攻擊）
- UDP flood（UDP 洪水攻擊）
- UDP fragmentation（UDP 封包碎片攻擊）
- SYN flood（SYN 洪水攻擊
- ICMP floods（ICMP 洪水攻擊）
- Carpet bombing（地毯式攻擊）

反射放大式 DDoS 攻擊（Reflective Amplification DDoS）

- NTP monlist 回應放大攻擊
- DNS query 查詢放大攻擊
- 無連線式 LDAP（CLDAP）反射攻擊
- SSDP/UPnP 回應放大攻擊
- SNMP 封包反射攻擊
- CHARGEN 回應放大攻擊

產品技術規格

SmartWall ONE NTD 硬體設備	NTD 280	NTD 1100	NTD 3400
網路介面	16 x 1/10G SFP/SFP+ or 2 / 4 x 10G LR zero-power bypass	2 x 100G QSFP28 or 2 x 100G LR4 zero-power bypass	1 or 2 x 400G OSFP DR4 or 2 / 4 x 100G with QSFP28 / LR4 zero-power bypass
設備管理介面	1 x 10/100/100 RJ45		
Console Port（序列埠）	1 x RJ45 Serial		
Performance （效能）			
Maximum Throughput (Gigabits per second)	80 Gbps	100 Gbps	800 Gbps
Maximum Throughput (Packets per second)	100 Million	150 Million	400 Million
Typical Latency(平均延遲時間)[1]	<0.5 Microseconds		
Inspected Latency(檢測延遲)[1]	< 60 Microseconds		
SYN Flood 攻擊最高處理能力 (Packets per second)	100 Million	100 Million	400 Million
攻擊緩解反應時間	Sub-Second (秒內反應)		
Management（管理介面）			
管理系統	透過獨立的實體或虛擬設備（VMware/KVM），實現集中式物件導向管理		
網路介面	1 x 10/100/1000 RJ45/Virtual Ethernet		
Web 圖形化操作介面	透過管理站台進行 HTTP(S) 存取		
CLI（命令列介面）	透過管理站台進行 SSH 存取		
Programmatic API	JSON-Based REST 透過管理站台存取		
Remote Monitoring（遠端監控）	SNMP v2/v3* Standard MIB GETs, SYSLOG		
Software Upgrade（軟體升級）	遠端升級的映像檔與組態儲存於內建 SSD		
Security Dashboards（安全儀表板）	Link Utilization (Gbps/PPS), Attack Targets, Attack Vectors, Alerts, Detailed Drill Downs, Top IPs/Ports/TTLs/Packet Sizes, Export to PCAP		
報表功能與第三方整合	SYSLOG for Traffic & Security Events with REST API for SIEM Integration. Corero Analysis Application for Splunk Integration.		

User Authentication（使用者驗證）	Role-Based Access Control (LDAP/Active Directory & RADIUS		
硬體 / 環境規格			
Size（尺寸）	1-RU / 44 mm (H) x 438 mm (W) x 630 mm (D)		1-RU / 44mm (H) x 438 mm (W) x 650 mm (D)
Operating Temperature（操作溫度）	0°C to 40°C (32°C to 104°C)		
Storage Temperature（儲存溫度）	-20°C to 70°C (-4°C to 158°C)		
Humidity（濕度）	5% to 95% Non-Condensing		
MTBF Rating	>100,000 Hours (25°CAmbient)		
Operating Altitude	0-10,000 Feet		
Tamper Protection（防篡改保護）	Tamper-Evident Seal（防拆封條）		
電源 / 散熱			
電源輸入路徑 / 供電路徑	雙電源冗餘、可熱插拔，支援 AC 或 DC 電源供應器		
AC Input（交流電輸入）	90 to 264 VAC Auto-Ranging, 47-63Hz		
DC Input（直流電輸入）	43 to 53 VDC		
最大功耗	330W	340W	580W
Cooling（散熱）	4 組獨立 N+1 冗餘、可熱插拔風扇模組，具備智慧風扇控制功能		
法規遵循 / 認證通過			
Compliance to EMC Emissions	FCC Part 15-7.10.2008, EN55022:2006+A1: 2007,CISPRR 22:2005+A1+A2:2005, VCCI-3 2009.04, AS/NZS CISPR22:2006, EN 61000-3-2:2006, EN61000-3-3:1995 +A1:2001+A2:2005, EN61000-3-11:2000, EN 61000-3-12:2005		
Compliance to EMC Immunity	EN55024: 1998 Including Amendment 1:2001 & Amendment 2:2003 (CIS PRE24:1997+A1:2001 + A2:2002), EN 61000-4-2:1995 +A1:1998 +A2:2001, EN 61000-4-3:2006, EN 61000-4-4:2004, EN 61000-4-5:2006, EN 6100-4-6:1996 +A1:2001, EN 61000-4-8:1993 +A1:2001, EN 61000-4-11:2004		
Compliance to Safety	UL 60950-1, 2nd Ed., CSA C22.2 No. 60950-1, 2nd Ed., EN 60950-1, 2nd Ed., IEC 60950-1, 2nd Ed.		
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A		

NTD 虛擬化版本

網路介面 4 x 10/100/400G Virtual Ethernet	**設備管理介面** 1 x 10/100/1000 Virtual Ethernet

Performance（效能）

最大可防禦通訊吞吐量 (Gigabits per second) 400Gbps (on 32 x CPU cores running KVM)	**Maximum Throughput (Packets per second)** 80 Million (deployed on KVM)	**最大可分析流量 (Packet/s- Flow samples or NetFlow records)** 0.5 Million per second
Typical Latency(平均延遲時間)[1] < 0.5 Microsecond	**Inspected Latency(檢測延遲)[1]** < 60 Microseconds	**攻擊緩解反應時間** < 60 Microseconds
SYN Flood 攻擊最高處理能力 (Packets/Second) 80 Million (Line-Rate)	**Jumbo Frames** Yes (9,216 bytes)	

硬體及虛擬設備需求

Hypervisors （虛擬機） KVM running on Red Hat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+ VMware ESXi 6.5+	**最低系統需求** 16GB Memory, 20GB Disk	**網路介面** 10G - XL710 NIC 100G - E810 / ConnectX-5/6 NIC 400G - ConnectX-7 NIC

[1] Typical Latency(平均延遲時間)針對封包大小最大至 1518 bytes所量測之數值

台灣區代理商 CipherTech 亞利安科技