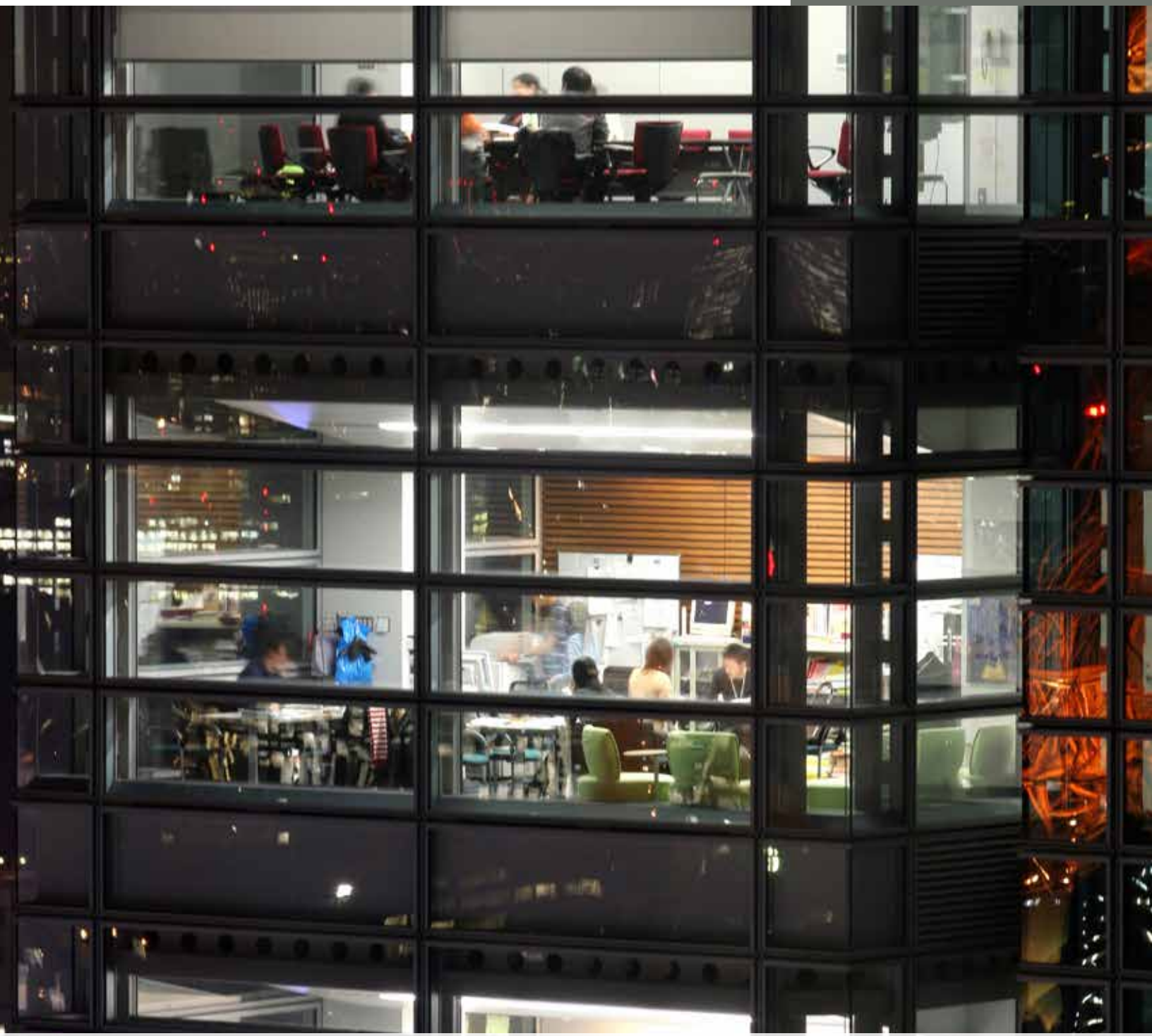

內網安全防火牆解決方案指南

簡介

網路攻擊活動正與日俱增。資安事件會引起不必要的公眾關注，聲譽及客戶信心的損失，企業還可能為此付出龐大的復原成本。此外，現今企業採用的最新技術（自帶設備、雲端應用程式、物聯網），也使傳統的網路邊界變得越來越難控制及防衛。

為了防止威脅進入內部基礎架構，公司不斷投資在分支機構、園區及資料中心等不同的企業網路層級上建立周邊安全防護系統。在過去十年裡，這已證明是個高價值且有效的策略。除了網路周邊防火牆之外，特定功能專用的安全解決方案可以提供應用級的多層式進階持續性威脅防護。然而，現今日益複雜的攻擊在很多情況下仍然能夠滲透企業網路。一旦滲入之後，漏洞利用程式（如惡意軟體）可能會在網路中隱藏及潛伏很長時間，然後再伺機發動攻擊。

企業應接受某些威脅能突破周邊防線的事實，因此需要在內網中增設一個可隔離不同關鍵資源的存取權、提供新一代安全防護、提供更大的可見度並控制潛在的威脅以緩解資安事件損害的額外安全層。

威脅的可見度及隔離

Fortinet 的內網安全防火牆可提供涵蓋整個內部網路的更強大可見度，與現有的次世代防火牆邊緣部署相輔相成。當駭客從網路內部一個被入侵的主機擴散至其它主機，試圖尋找有價值的資產及資料時，Fortinet 的內網安全防火牆解決方案可將內部網路區隔分段，以限制駭客與惡意程式碼的側向移動及散播。這種交互運作的方式可為整個攻擊面帶來無懈可擊的全面安全性，抵禦端對端跨越全網路的一致威脅態勢。

挑戰：為什麼僅依賴周邊防線的時代已經過去

事實一：威脅的次數、複雜性及衝擊度與日俱增。在今天的環境中，企業網路的存取點持續成倍增加。行動力技術、智慧型裝置和雲端都意味著不斷擴大的攻擊面，也表示能夠進入網路的複雜威脅將會越來越多。

事實二：內部網路是個扁平、開放式的結構。為了提升靈活性及應變力，網路已趨向扁平化及更開放的結構發展。大多數內部網路中採用的是基本的安全配置，並只限於虛擬局域網路和第 4 層存取清單。因此，一旦越過安全防線之後，駭客便能輕易擴散，並對憑證、資源及數據資料予取予求。內部網路如缺乏安全基礎設施，也會大大限制企業對可疑的流量行為與資料流的可見度，進而減低其偵測出安全漏洞的能力。

事實三：單憑虛擬局域網路（VLAN）分隔策略是不夠的。以往，內部網路分隔策略利用部署 VLAN 的方式進行，其中 VLAN 的內部通信透過路由功能執行。VLAN 分隔可將一個簡單威脅的擴散範圍局限於同一 VLAN 內的成員。但是，較複雜的威脅仍能輕易在 VLAN 之間散佈，因為路由器並不是安全設備，也沒有能有效識別及阻擋威脅所需的安全服務及認知。

VLAN 分隔模式的擴充能力也極有限，最高只能支援至 4K VLAN，而這將會限縮現今可能包含數千部伺服器及虛擬機器的企業環境所需要的微分隔層級。

解決方案：內網安全防火牆

為了幫助克服上述挑戰，企業可以在內網中的重要位置點部署一種新型態的防火牆。Fortinet 的內網安全防火牆解決方案便可提供一個擁有多項獨特優點的額外安全層，用於輔助現有的邊界防護機制。

優點一：透過政策主導的隔離方式將關鍵資源 / 資產的存取控制在盡可能接近用戶的位置

優點二：建立安全屏障，透過具備進階安全機制的實體隔離方式，遏阻及限制內部網路中不受控制的威脅擴散與駭客活動

優點三：將威脅的潛在損害限縮在周邊以內

優點四：提高威脅的可見度，並提升發現及修補安全漏洞的能力

優點五：強化企業的整體安全態勢

為了實現最大化的威脅控制及潛在損害限制，內網安全防火牆的部署依據兩項基本原則進行：

- 政策主導的防火牆隔離
- 實體與虛擬的防火牆隔離

政策主導的防火牆隔離

政策主導安全隔離的目的，在於透過自動將每個用戶的身份與限制該用戶可能攜帶的攻擊向量及威脅的安全政策建立關聯，以控制其對網路、應用程式和資源的存取。

用戶的身份可以定義為一組屬性，例如實體位置、登入網路使用的裝置類型、或使用的應用程式等。因此，執行的安全政策必須自動跟隨用戶的身份，因為此身份會隨著使用情境而動態變化。例如，一位用戶可能根據登入網路使用的裝置類型，執行不同的政策。

為了達到所需的用戶識別以及建立和執行粒狀安全政策所需的整體參數，內網隔離防火牆必須能夠：

1. 允許用戶、裝置和應用程式識別
2. 提供與企業的目錄服務解決方案（如 Microsoft Active Directory）整合的功能，以便能動態地識別用戶
3. 將每位用戶的身份動態地映射至特定的安全政策及執行

一個用戶設定檔在與特定的安全政策建立關聯時，應盡可能在接近來源或存取點的位置執行。因此，部署在組織中各個層級 – 從分公司至園區 / 總部 – 的所有防火牆都必須能夠動態地識別用戶，並在整個組織中執行適當的政策。事實上，整個防火牆基礎架構將會變成一個智慧型的政策主導分隔結構。

實體與虛擬的防火牆隔離

政策主導的安全隔離也可定義防火牆所採用的安全服務，例如 AV、IPS 及應用控制等。不過，無論這些措施的效率多高，不知名的威脅仍有可能進入網路。為了達到最大化的偵測及防護能力，必須採用實體安全隔離限縮威脅在內部網路中的散播範圍。安全漏洞可能帶來的潛在嚴重損害及「零信任」概念的日益普及化，使實體安全隔離更形重要。

實體及/或虛擬的內網安全防火牆透過部署一個適配的基礎架構對企業網路中的資產、用戶及資源進行安全隔離及微分隔有效且安全地將伺服器、數據儲存庫和應用程式與潛在的漏洞利用程式隔離。

內網安全防火牆涵蓋整個企業的功能運作

用於軟體定義資料中心（SDDC）的虛擬內網安全防火牆 - 基於虛擬化及軟體定義運算已成為全球各地企業資料中心的主流趨勢，企業早已透過先進的虛擬防火牆設備對每個虛擬機器實行微分隔策略。FortiGate-VM 及 FortiGate-VMX 等虛擬內網安全防火牆所提供的安全服務，可滿足虛擬機器之間流量（亦稱為「東西向流量」流量）的可見度、分析與防護需求。

實體內網安全防火牆 - 實體內網安全防火牆用於進出網路外圍及資料中心的流量（即「南北向流 量」流量），可提供一個高成本效益並且可擴充的方式，將安全隔離及可見度延伸至整個企業 – 從最終用戶至網路與運算資源、應用程式及數據資料。

不同於虛擬內網安全防火牆由單一的虛擬 FortiGate 內網安全防火牆隔離及保護所有虛擬機器或一個伺服器內的區段，實體防火牆的安全隔壟粒度（伺服器 / 網路區段 / 工作群組 / 部門等）取決於防火牆的實際位置、網路結構、企業的信任架構、以及資料中心資產的重要性與位置等多項因素。

安全防護

Fortinet 的內網安全防火牆可提供由內至外的智慧型、自適應威脅防禦，以縮短漏洞空窗期及降低損害。Fortinet 的內網安全防火牆可利用網路隔離、可操作的安全及完整的登記與審核措施來緩解威脅並保護重要的資產及資料。 從 FortiView 之類的可見度組件到應用控制（Application Control）之類的安全控制，以及 FortiGuard 經驗證的威脅情報，企業可以隨時提高對整個網路中任何動態的感知度。

作為內網安全防火牆的 **FortiGate 防火牆** 可提供簡易的虛擬線路模式，有利於迅速部署。在此模式下，防火牆將以「線路插件」（bump in the wire）的形式運作，而不是在連接的裝置間穿越的路由器，因此並不需要修改 IP 位址。

主要考量 - 無論選擇哪一種部署模式，都應該評估下列條件：

- 結合虛擬與實體的內網安全防火牆可提供一個完整的端對端解決方案
- 與目錄服務整合
- 提升現有安全政策以容許政策主導隔離
- 內網安全防火牆的效能必須滿足傳輸速率與延遲率的條件，同時能在一個高度區隔化的環境中提供次世代的安全性

Fortinet 內網安全防火牆解決方案的優點

Fortinet 開創出內網安全防火牆的概念並納入其進階威脅防護（ATP）的部署框架中，為組織防禦當前最複雜的威脅。

Fortinet FortiGate 防火牆是動態、可管理並可擴充的內網安全防火牆解決方案，具備下列多項優點：

1. 為政策主導的隔離方式提供用戶 / 裝置 / 應用程式感知的防火牆政策
2. 可支援與 RADIUS、LDAP 及 Active Directory 的整合，提供用戶驗證及管理功能
3. 可支援包括AV、IPS 和應用控制等豐富多樣的安全服務，提供最大的內部網路保護
4. 提供一個可在高度區隔化環境中發揮所需性能、速度與低延遲率的 ASIC 技術實體設備
5. 包含虛擬防火牆選項，用於 SDDC 及公共雲中提供 ISFW 功能
6. 包含種類廣泛的實體與虛擬設備，可滿足在整個網路達到最佳隔離效果所需的性能及擴充能力
7. 可結合 FortiManager、FortiAnalyzer/FortiView 及 FortiAuthenticator 構成一個可擴充、可管理且自動化的端對端解決方案

輕鬆部署

利用預設的虛擬線路模式，能夠將 Fortinet 內網安全防火牆迅速部署至現有的環境，同時不會造成過多的干擾。這意味著 IT 人員可以在最小的設定要求下輕鬆完成部署，而無需重新設計現有的網路。

線速級性能

Fortinet 內網安全防火牆擁有高達數千兆位的運作速度，可提供深度的封包/連線檢測而不會拖慢內網速度。我們的內網安全防火牆可發揮極高的性能，以滿足內部東西向流量的需求。

適用於內網安全防火牆的管理工具

內網安全防火牆是 Fortinet 端對端安全平台內的一個元件，從安全無線存取至實體和虛擬的資料中心防火牆及應用級安全設備，皆可透過 FortiManager 及 FortiAnalyzer 在單一的虛擬管理平台上管理。

在部署內網安全防火牆的環境中，定義的政策數量預期會隨著政策主導的內網隔離策略而增加。此外，企業網路中的任何防火牆應能夠動態執行政策主導式隔離，因此每一個防火牆都必須知道所定義的所有各項政策。這樣的要求很可能成為管理上的噩夢，並會影響防火牆資源。

Fortinet 的 FortiManager、FortiAnalyzer 及 FortiAuthenticator 可採用以下方式克服這些問題：

1. 透過 FortiManager 一次界定政策
2. FortiManager 可自動將政策分配至參與內網安全防火牆功能性隔離的防火牆
3. 透過與 FortiAuthenticator 整合，可提供 FortiGate 防火牆及目錄服務的整合及自動化，實現用戶認知及政策主導隔離的可擴充性
4. FortiAnalyzer 及 FortiView 可提供涵蓋整個企業的粒狀、聚集流量可見度（用戶、裝置、應用程式、威脅等）

即時的安全防護

Fortinet 的內網安全防火牆可提供全方位的進階安全服務（IPS、應用可見度、防病毒、防垃圾郵件、整合沙箱功能以提供進階威脅防護），促進內部網路內的政策執行。即時的可見度與安全防護是限制惡意程式在網路內部散佈的關鍵條件。

總結

隨著威脅的數量、複雜性及影響程度持續增加，將所有安全措施集中於網路周邊防護的做法顯然已不合時宜，留在內部網路的機密資料反而未受到保護而可能遭受入侵外洩。

內網安全防火牆可在組織的網路周邊之內提供多一層的保護，同時提高其偵測漏洞及縮短緩解延遲時間的能力。

Fortinet 創先推出一個精密、高成本效益且高效能的端對端內網安全防火牆解決方案，並容許高性能的虛擬及實體內網安全防火牆從單一的虛擬管理平台管控，滿足最嚴苛的組織及環境需求。

全球總部
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
電話：+1.408.235.7700
www.fortinet.com/sales

歐洲、中東和非洲銷售辦事處
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
電話：+33.4.8987.0500

亞太銷售辦事處
300 Beach Road 20-01
The Concourse
Singapore 199555
電話：+65.6513.3730

拉丁美洲銷售辦事處
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P.06600
México D.F.
電話：011-52-(55) 5524-8428

2016年2月5日