FORTINET

分布式混合資料中心需要更多防火牆防護

概述

現代資料中心的發展導致許多應用程式和數據越來越多地分布在混合基礎架構中。雖然這有助於提高靈活性，但它同時也擴大了組織受攻擊面，並且模糊了可視性並讓管理受到侷限。網路工程師和營運高層需要的是安全與進階功能的整合，以保護到來的混合 IT 資料中心的環境。

具體來說，他們需要的是包含具有關鍵風險管理功能的新世代防火牆，能將資料中心的保護延伸到組織的各個層面、並且能將管理自動化，確保業務的持續運作、減輕工作人員的負擔，同時加快威脅來臨時的反應時間。

根據統計，包括對客戶信任和公司聲譽的損失，平均每家公司兩年因為資安問題所造成的損失高達 6,720 萬美元。[1]

分布式資料中心擴大了受攻擊面

越來越多的企業從分布式資料中心中存取資料，這些工作和資料分別儲存在企業的內部、各地託管主機、私有雲和公有雲環境，延伸在整個混合 IT 架構中，而這種廣泛分布與多樣的環境，非常易受入侵，讓企業曝露在不斷擴大的攻擊面中。

為了彌補這些不斷增加的風險，許多網路工程師和營運高層都嘗試在原有設備中另外再加上獨立的安全設備，以覆蓋疊加的方式來解決不斷變化的環境與修補所遇到的漏洞。不幸的是，這種零碎的方法不僅無法解決當前和未來的問題，因此方式遭受惡意入侵的機率更是增加，而對企業來說，總體擁有成本 (TCO) 和管理的複雜性也會跟著增加。

確保混合IT環境的安全

為了應對這種不斷擴大的資料中心攻擊面，網路工程師和營運高層應先進行橫跨所有混合 IT 環境的資安整合，同時需要新世代防火牆防護，導入策略控管與 IPS 入侵防禦、確保各端點的可視性等統一威脅管理，更需要以下的進階能力:

高效能

風險管理最需要的是與高效能的網路同步，以及有效幫助減少攻擊面的強大功能。

混合資料防護最需注重的地方分別是資料安全的法規遵從性（71%），高效能（62%）和易管理性（53%）。[2]

靈活與擴充性

隨著混合 IT 環境的擴大和多樣化，為確保業務連續不中斷，資料中心安全性必須提供可擴充性、靈活與可用性。整個網路和安全架構還需能夠在網路中斷和自然災害中斷後的擁有最快速的復原能力。

自動化與協同運作 (Orchestration)

安全架構的整合為混合 IT 架構的智慧自動化打開了大門，自動化安全響應與加速的管理功能縮小了風險的暴露，同時減少了工作人員負擔、人為錯誤，並有效讓營運成本（OpEx）降低。

風險管理的能力

資料中心防火牆通常會部署在網路中最快的地方，因此，防火牆必須能夠在對網路效能影響最小的情況下應用高階 L7 層的安全性。為了實現這一點，防火牆解決方案需要專用的安全處理器，使防火牆能夠可靠執行安全功能而不會造成網路流量流通的阻礙，而保護現代分布式資料中心的資安還需要橫跨所有不同環境，如：內部網站、外部託管、雲端環境等等，讓所有已部署的資安元素，如：用戶、應用程式和設備擁有完整的可見性。

有 77% 的企業目前在內部一定程度上仍處於未經過整合的資安解決方案。[4]

現在，有超過三分之一的漏洞來自內部。[3] 因此，對內部網路的存取控制變得非常重要。網路工程師和營運高層可以透過網路分段來實現資安防護，網路分段需具有足夠的擴充性和靈活性，以處理各種需求狀況（包括用戶、設備和應用程式等等的動態信任）。

但是網路的分段本身不能為今天的進階威脅提供關鍵性的安全功能。因此，資料中心的防火牆必須能夠適應各種分段技術，能夠與協力廠商安全解決方案共享威脅情報，並且還可提供內容檢查與自動威脅響應等進階防護。

為了跟上當今網路威脅的數量和速度的不斷增加，需要在整合的資安架構中導入即時共享情報的安全機制。同時，資安部門應該應用人工智慧（AI）來識別未知的威脅，最重要的是，這種由 AI 來驅動的威脅檢測和預防必須能夠用在所有數位設備與裝置上。

靈活與擴充性

數位創新不斷擴大的特性直接影響了安全性。隨著資料中心的工作越來越分散在各項混合 IT 環境中，安全性需要更高的靈活性，以隨著新的應用程式和不斷擴大的工作範圍得到擴充，除了傳統設備之外，還要包括雲端與虛擬機(VM)。隨著新的應用程式和不斷成長的工作負載，資安防護需要更高的彈性，以應付越來越多的雲端和虛擬機（VM）的運算需求。

資料中心安全還必須適應不斷擴大的未加密與加密資料流量需求。以目前來說，已有超過 72% 的網路流量為加密流量，比上一年增加了近 20%。[5] 分布式資料中心特別容易受到加密流量中以加密方式存取的威脅。為了緩解這種態勢，應該要為用戶與系統之間以及跨系統的大量流量提供 SSL/TLS 的加密檢查，利用沙箱和誘捕系統（Honey Pot）進行包括最新的 TLS 1.3 檢查的資安檢測，並且同時不影響網路傳輸效能。[6]

在恢復能力和可用性方面，解決方案必須確保在發生系統故障時能夠進行即時切換，內建的 N+1 架構可消除任何單點故障，並且由獨立業界專家進行的第三方驗證測試也助於確保解決方案網路的可靠性。

自動化與協同運作

資安人才的短缺使許多人手不足的安全組織面臨沉重的工作負擔。降低操作的複雜性是讓營運成本降低的關鍵，開放資安技術，讓企業從而更專注於業務面與效率優化，而不是耗費時間在冗沉的任務上。

在這方面，有效的資料中心防火牆應該包括工作流程優化，簡化部署和管理。高度整合的資安架構為情報共享和自動響應提供了基礎，協調整個混合基礎架構的安全，支持開放 API 的防火牆解決方案，實現工作流程自動化，針對未修補的應用程式和不斷變化的 DevOps 環境，提供同步安全響應的關鍵優勢。

該解決方案還應該能夠應用業務羅輯，建立用戶、設備和應用程式的持續信任，幫助自動化管理（如管理和資源調配）。這減少員工工作量和營運成本，同時提高了營運效率和安全效率。新世代防火牆還要能夠進行自動化合規報告和稽核流程，幫助網路工程師和營運高層減少大量的工作，同時更需跟上不斷變化的政府公佈與相關業界的法規，如美國國家標準暨技術研究院（NIST）及和網路安全中心（CIS）等安全標準規章。

超過半數的 IT 決策者（54%）表示，如何留住人才是企業採用混合 IT 模式的關鍵課題。[7]

選擇最佳的新世代防火牆

隨著資料中心變得越來越分散並發展成為混合 IT，企業所受的攻擊面也會擴大。人們對資料中心效能的要求越來越高。面對不斷擴大的風險、不斷增加的網路中斷機率和不斷上升的成本，企業必須重新審視現代資料中心的資安問題。為了讓高安全性和高效能並存，網路工程師和營運高層需要的是一個新世代防火牆解決方案，為企業提供整合安全架構，高效能、高靈活、可擴充性，擁有自動化能力的解決方案。

[1] Filip Truta, "Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation," Security Boulevard, February 21, 2019.

[2] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, November 15, 2018.

[3] "2019 Data Breach Investigations Report," Verizon, April 2019.

[4] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[5] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

[6] Alex Samonte, "TLS 1.3: What This Means For You," Fortinet, March 15, 2019.

[7] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, November 15, 2018.

www.fortinet.com/tw

725546-0-0-TW

February 23, 2021 11:08 AM

ebook-convert-distributed-hybrid