CISCO
SECURE

白皮書
思科公開資訊

防火牆的未來

以更強而有力的措施，守護您的當下，同時建立滿足未來業務和資安需求的橋樑

cisco The bridge to possible

目錄

摘要

此白皮書的目的是討論網路資安的發展，以及為保護組織的未來環境而需採取的措施。

隨著網路變得越來越異質，組織越來越難以實現一致的原則管理和實施，並維持統一的能見度。這些互連網路的複雜性通常會導致錯誤或設定錯誤，使它們容易受到持續演進的複雜威脅攻擊。

組織可以做些什麼來重新獲取控制權並實現一致性？可以從資安的整合方式開始，將防火牆放在重要的位置。

防火牆仍然是組織網路資安策略的基石，但是正如網路的演進一樣，我們的防火牆也必須不斷發展。過去，防火牆位於入口/出口「邊界」的單一設備，做為原則導向的控制點，以允許或拒絕網路流量。為了在當今的數位世界中獲取成功，組織需要考慮超越單一防火牆，採用「防火牆設定」，這是一種原則導向的方法，跨異質網路的邏輯控制點，戰略性地協調進階安全防護。

「防火牆設定」將會是組織讓資安更能因應不斷變化的業務和網路需求的重要步驟。思科不斷致力於建構一個以防火牆為基礎的整合式資安平台，讓企業能夠進行轉換作業。

> 「防火牆仍然是組織網路安全策略的基石，但是正如網路的演進一樣，我們的防火牆也必須不斷發展。」

透過防火牆設定，進行數位轉換的組織可以使用更強而有力的安全措施，守護您的當下，同時建立滿足未來業務和資安需求的橋樑。

第 1 節：防火牆的歷史

網路資安的演進

傳統上，防火牆在網路邊際上是做為閘道管理員。它做為全方位的控制點，可以檢查網路流量在此邊界的傳輸情況。防火牆位於網路的入口/出口點，負責驗證通訊：內部網路流量本質上是可信任的，而外部流量本質上是不可信任的。在此單一控制點上建立並執行規則集和原則，以確保允許所需的流量進出網路，並防止不必要的流量。

將網路邊界比作城堡周圍的護城河，防火牆就像一座吊橋，控制進出堡壘的所有流量。

傳統網路資安

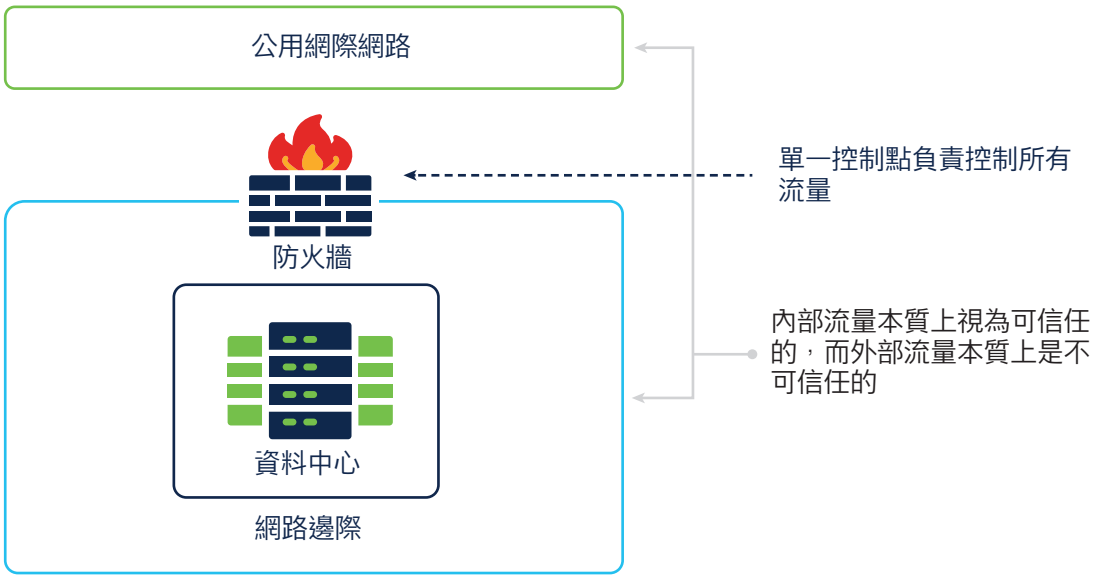


圖 1. 傳統網路防火牆方法

隨之而來的是雲端，以及應用程式。

不久之後，這種透過單一控制點強制執行安全性的做法面臨了挑戰。首先，是遠端存取和企業行動化的興起。但是，隨著雲端計算的出現，真正帶動了轉型。當業務轉移到雲端時，裝置和使用者開始大規模移轉到受控內部網路之外，這使得單一控制點模型失效。很快地，出現多個邊界。他們都需要受到保護。沒有有效的方法可以在網路邊界設置護城河。

如今，分公司地點、遠端員工，以及越來越頻繁使用雲端服務，正在促使更多資料遠離傳統的「邊界」，完全繞過傳統的安全控制點。此外，許多企業皆採用自帶設備 (BYOD) 模型，讓員工可透過其私人電腦或行動裝置存取敏感的企業應用程式。實際上，超過 67% 的員工會在工作中使用自己的裝置 – 上升趨勢一發不可收拾。透過可公開存取的 Wi-Fi 網路連線的行動裝置和筆記型電腦非常普遍，甚至對於日常業務營運也至關重要。

此外，絕大多數企業地點和使用者也需要直接存取網際網路，而現在越來越多雲端關鍵應用程式和資料都儲存在網際網路中。企業持續跨多個雲端服務、作業系統、硬體設備、資料庫等部署工作負載。應用程式和資料變得更加分散，網路也隨之變得更多樣化。

全新事實

事實證明，這種「一體適用」的方法在目前環境中是無效的。

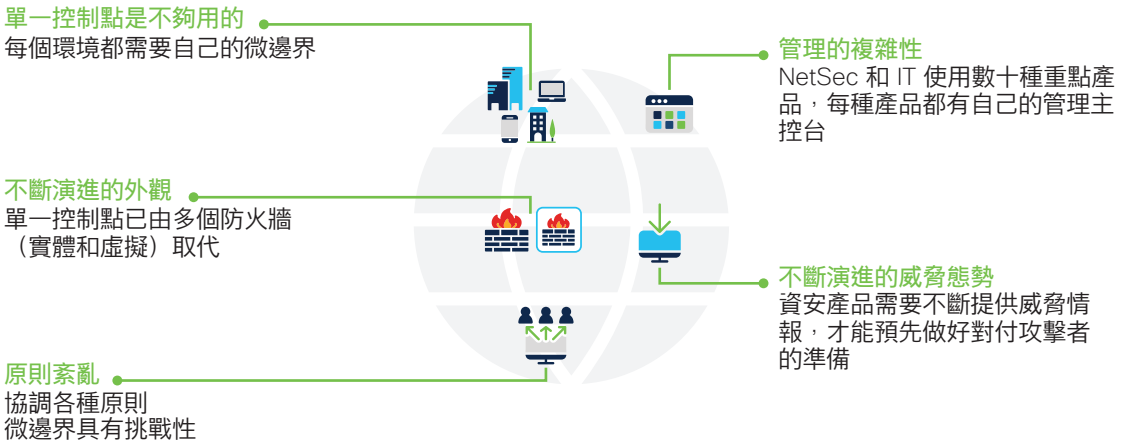


圖 2. 網路複雜性和不斷演進的威脅正在挑戰傳統的防火牆模型

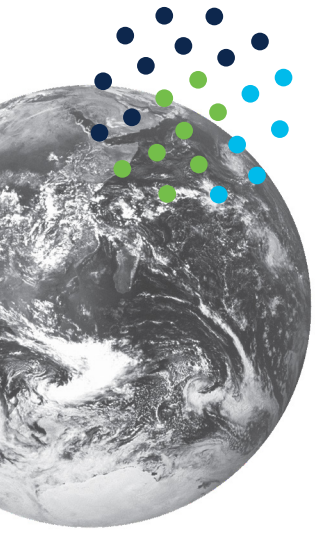
全新、更複雜的現實

儘管這些創新為人們提供了更加緊密且更具生產力的工作環境，但它們已改變我們經營方式的本質。控制應用程式和授權使用者進行內部部署的時代已經演變成動態的多雲端生態系統，可在企業之間提供服務和應用程式。不僅如此，我們也管理關鍵業務的第三方關係。大量的擴張和外包服務提供規模經濟和效率，但並非沒有折衷方案。此網路架構的演進大幅增加了我們的攻擊面，使得保護商業網路、資料和使用者的工作變得更加複雜。

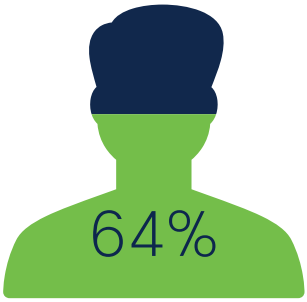
用單點產品進行反擊

一般而言，組織已嘗試藉由新增「最佳」點資安解決方案來應對這些挑戰，以解決每個出現的新問題。由於這種方法，我們看到了大型裝置「蔓生」，平均每個企業使用多達 75 種資安工具 [1]。跨不同供應商的多種資安產品可能為網路資安團隊帶來嚴重的管理問題。在大多數情況下，安全裝置和功能的激增會導致遭受攻擊的風險增加。當問及時，有 94% 的 IT 和資安專業人員擔心網路複雜性的增加使他們更容易受到攻擊，而 88% 的人希望讓網路安全性原則的改變更具彈性 [2]。

在 2019 年 1 月至 7 月之間，共揭露了 3800 起資料外洩事件 – 與 2018 年上半年相比，增加了 54%[3]。這種急遽攀升證明了惡意人士使用越來越複雜的方法來破壞網路。入侵成功率越來越高，這也表示傳統的網路資安方法已無法抵禦新式威脅。



1《Defense in depth: Stop spending, start consolidating》CSO，2016 年 3 月 4 日。
2《Navigating Network Security Complexity》ESG 研究深入分析報告，2019 年 6 月。
3《Navigating Network Security Complexity》ESG 研究深入分析報告，2019 年 6 月。



人為錯誤是設定錯誤的主要原因

更多威脅、更多干擾，甚至更大的風險

隨著惡意方攻擊新媒介 – 從電子郵件到 BYOD 原則下未經審查的端點，再到 Web 入口網站和 IoT 裝置，組織也被迫嘗試各種其他方法來保護自己。

如上所述，新增單點產品的趨勢無法改善組織的整體安全狀況。恰好相反！它為資安團隊製造更多「干擾」，需要管理。當他們竭盡全力留意無法避免的新攻擊和試圖利用任何漏洞（已知或未知）的惡意軟體時，這種增加的複雜性使得建立、管理和實施安全性原則的工作變得更加困難。

對此，網路資安團隊的任務是個別設定大量雲端資源，進一步提高可能導致資料外洩之資安設定錯誤的機會。未實施或已實施但發生錯誤的資安控制可能是最大的罪魁禍首：64% 的組織表示人為錯誤是設定錯誤的主要原因[4]。無論這樣的錯誤導致違反法律規範、造成中斷，還是為惡意人士敞開大門，都是您承受不起的風險。

是時候重新思考防火牆了

網路資安已成為一項艱鉅的任務。今天的人員無法繼續嘗試管理各種端點資安解決方案、雲端資源和設備。是時候採用其他方法了。

現在應該讓防火牆取代彈性和整合式網路資安平台的基礎，它將為當今和未來的企業帶來便利。

第 2 節：從防火牆到防火牆設定

為何選擇防火牆設定？

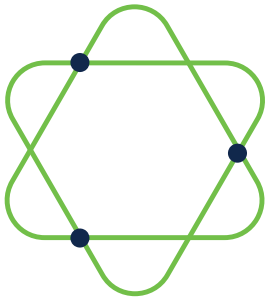
隨著我們的網路不斷發展，以適應新的經營方式，我們的網路資安也必須如此。在當今的分散式 IT 資產世界中，防火牆對於穩健的資安狀態仍然至關重要。

但是，防火牆要求已大幅提升，以保護各種網路基礎架構、連線的裝置和作業系統免於遭受進階威脅的侵害。因此，透過實體和虛擬裝置的組合，藉此增強我們的「傳統」防火牆裝置，其中一些內嵌到網路中，而另一些隨服務交付，有的是主機式或包含在公用雲端環境中。有些甚至採用新的外觀，例如可擴充到大流量需求的叢集設備、在個人裝置上執行的軟體、SD-WAN 路由器，和安全的網際網路閘道。在所有這些不同的防火牆裝置之間共享威脅情報（無論位於何處），對於統一的威脅能見度和強大的資安狀態至關重要。

為了全面轉型，並更加保護現今的網路，企業必須擺脫傳統的「邊界」方法。他們必須在整個網路光纖中建立策略強制執行點，使其更接近需要保護的資訊或應用程式。具體而言，在實體和邏輯控制點上建立微邊界已成為必要事實。

我們需要減少考慮將防火牆做為獨立的實體網路裝置，而應該多加考慮*防火牆*設定的功能。

4《Cloud Security Breaches and Human Errors》Fugue，2019 年 2 月 7 日



什麼是防火牆設定？

請不要誤會：防火牆比以往任何時候都更重要。事實上，為了保護當今的網路，我們**隨時隨地都需要**更多的**防火牆**。區別在於防火牆設定著重在**如何**在任何地方建立原則型控制：

防火牆設定可以針對在日益複雜的異質網路中，進行集中式原則、進階安全功能以及一致的實施，提供一種彈性且整合的方法。它應該提供全面的保護、能見度，原則協調性，以及更強大的使用者和裝置驗證。防火牆設定應該也受益於所有控制點之間共享威脅情報，以建立統一的威脅能見度和控制，大幅減少偵測、調查和修補威脅所需的時間和心力。

藉由這種方式，防火牆設定已成為當今保護複雜網路安全的關鍵策略。隨著您的業務和威脅態勢的不斷發展，它提供了通往未來的橋樑。

它是什麼樣子？

無論是在雲端、內部部署，或遠端位置保護資產和資料，防火牆設定都需要持續提供進階威脅防護、原則強制執行和共享威脅情報。挑戰是在部署和利用不同裝置的不同環境中提供一致性。

無論是在公司總部、資料中心、遠端位置、公用雲端，或在員工進行遠端工作的任何位置，安全漏洞可以源自可存取網際網路的任何裝置。這就是為什麼在更多邏輯位置加入強大的安全控制點，以減少暴露並降低風險，比以往任何時候都更重要。安全控制適用於需要在私有環境（實體或虛擬設備和網路裝置，例如路由器），以及非私有環境（安全即服務[SECaaS]）、原生控制和工作負載上使用的地方。

什麼是防火牆設定？

在現今的異質網路中，強制執行點無處不在。

防火牆設定可提供一致的威脅防禦功能，以及一致的原則和威脅能見度，因此您可以在隨時隨地更快、更準確地預防、偵測和阻止攻擊。

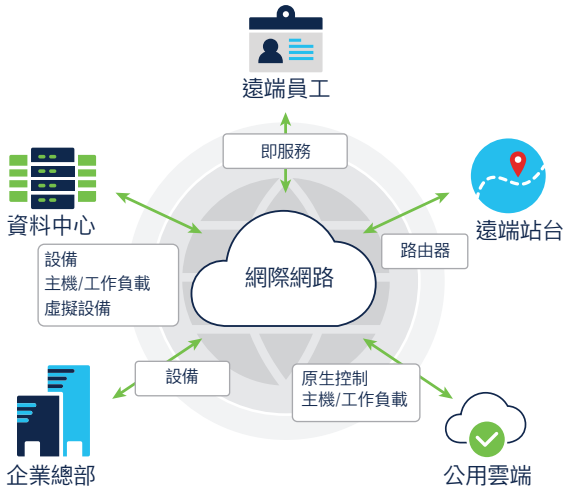


圖 3. 防火牆設定的核心租用戶是應對現代網路安全挑戰的一種手段

擴充資安控制

在傳統防火牆的前提下，由於所有內部流量和授權使用者本質上都是可信任的（外部流量則不可信任），因此在網路邊界保護整個組織是可行的。此網路邊界成為保護整個組織的邏輯資安控制點。無論是來自總部、資料中心還是遠端員工，所有網路流量都會透過此單一控制點進行分配。

當然，此模型不適用於當今複雜的環境，在該環境中，組織的 IT 基礎架構跨越了多種外觀和交付模式，包括實體和虛擬設備、網路內嵌式路由器或交換機、交付即服務、主機式，或包含在公有雲端中。

透過防火牆設定方法，可以部署一致的安全性控制以提供完整的能見度、整合原則和全面的威脅能見度。這些資安控制可在越來越多的異質環境中啟用更強大的使用者和裝置驗證。它們收集、共用和回應有關使用者、位置、裝置等的環境，以確保裝置符合定義的資安要求。在每個微邊界使用一致的安全性控制，資安團隊可以開始自動執行任務（例如自動隔離不符合規定的使用者和裝置、在所有資安控制中阻止可疑的網域，並支援有效的微分段）。在防火牆中，完整的能見度可讓我們全面瞭解所有資安警示和入侵指標，共享威脅情報可為任何連線的裝置提供最新的威脅偵測。

雲端管理

這不僅僅是單點產品。網路邊界和雲端資源的爆炸式增長也提高了漏洞暴露的風險。在管理各種資安產品的同時，在複雜的雲端環境中保護企業最有價值的資產絕非易事。資安團隊需要即時能見度和簡化的管理，以幫助減少設定錯誤。

防火牆設定藉由支援集中的雲端管理來幫助資安團隊克服複雜性，使原則符合整個組織，進而增強安全性。範本可以藉由寫入一次原則，並在整個網路成千上萬的資安控制中擴充其強制實施範圍，以改善原則設計和一致性。使用標準原則範本快速部署新裝置，有助於減少組態錯誤。隨著組織的發展，新的部署會自動繼承最新的原則。可擴充的原則管理系統會將多個安全性功能整合至單一存取原則中，並最佳化各資安裝置的原則，以識別不一致，並快速加以更正。

此外，集中的雲端管理解決方案可將團隊的能力提升至新境界。他們可以快速識別所有裝置的風險，使其達到更加一致和安全的狀態。使用單一管理主控台，可以在所有裝置之間比較物件，以發現不一致之處並最佳化目前的資安狀態。人員可以簡化原則管理、提高效率，並獲得更一致的安全性，同時降低複雜性。

借助威脅情報進行反擊

隨著網路邊界的擴大以及直接連線到網際網路的裝置數量激增，我們的攻擊面也隨之擴大。網路安全威脅涉及惡意軟體、加密貨幣、網路釣魚，以及殭屍網路活動不斷升級，網路罪犯正在轉向機器學習和 AI，以利用現有軟體漏洞並加速惡意攻擊。很少有組織有足夠的資源可完整測試和鑑定所有軟體供應商的漏洞修補程式 – 大多數都面臨著抵禦新興威脅和不斷發展的威脅的挑戰。

防火牆設定另一個引人注目的方面可以在這裡提供幫助。利用業界領先的威脅情報和最新的威脅研究（有些幾乎是最新的），可以存取防護更新，有助於緩解持續不斷的威脅。威脅研究人員可以快速識別入侵指標，並迅速確認和共享威脅情報。利用規模經濟，目標是在保護組織免於遭受發展中威脅的入侵。在互連的網路、端點、工作負載和雲端環境之間共享威脅情報，可以幫助資安團隊將看似無關的事件建立關聯、消除雜音，並更快地阻止威脅。

不進行防火牆設定的風險是什麼？

隨著網路的發展，組織已進行調整，部署各種單點產以支援業務需求和營運。隨著新攻擊途徑的公開，他們也做了相同的事，逐一新增產品，以抵禦最新的 XYZ 威脅。那些依靠傳統防火牆以保護跨多個邊界的每台已連線裝置的人，可能會將其最有價值的資料和資產暴露在資安漏洞之下。根據 2019 年的《Cybersecurity Almanac》指出，到 2021 年，網路犯罪造成的損失每年將使全球損失 6 兆美元[5]。

這些威脅可能會迅速滲透到網路中，並危及缺乏全面網路安全性和端點能見度的企業運營。

也就是說，無論在何處保護組織的網路、雲端環境、裝置和資料，對於資安團隊都是巨大的負擔。

防火牆設定的開始和結束都以防火牆做為禁得起時間考驗的網路資安基石

在思科，我們一直在努力實現此願景。我們與全球各種規模的公司和企業合作，他們都需要網路資安更敏捷、整合性更高 – 融入網路本身。這就是為什麼我們提供有史以來最安全的架構，即以防火牆做為基礎的強大而全面的平台。

透過此概念提供前所未有的防護層級是我們資安策略的重要組成部分。思科資安產品組合和思科的防火牆系列可在您所需要的任何地方提供世界一流的安全性控制、一致的原則和能見度，以及可改善安全營運的革新，讓您對於不斷發展的威脅早一步做好準備。

在當今威脅情勢比以往更加不斷變化的時代，思科將網路領導力和尖端技術結合在一起，因此您可以擁有當今和未來可用的最強大安全性狀態。

5《2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics》網路犯罪雜誌，2019 年 2 月 6 日

傳統防火牆只能提供有限的檢視資料；IT 需要透過共享威脅情報提高整個網路的能見度，以更早、更快地偵測和阻止威脅。藉由根據整合管理和全方位的安全性功能（例如入侵防護、URL 篩選和利用自動化和機器學習來提高效率的進階惡意軟體防護）提供全面的資安狀態，讓防火牆設定更加強大。

如果沒有適當的防火牆設定原則，網路複雜性可能會導致設定錯誤，提高資安漏洞的風險。根據 Gartner 報告指出「到 2022 年，至少 95 % 的雲端安全失敗將是客戶的過錯。」[6] 藉由採用跨多個控制點協調資安政策的防火牆設定策略，組織可以改善其整體安全性狀態。

第 3 節：設定防火牆設定策略的四個步驟

步驟 1：使用現代的新一代防火牆為成功的防火牆設定策略奠定基礎。正確的 Cisco Secure Firewall 將為您的整合資安解決方案提供一致的安全性原則、能見度和改善的威脅回應。

步驟 2：選擇 Cisco Secure Firewall 之後，下一步就是標準化管理解決方案。在確定哪種解決方案適合您的組織時，請考慮以下因素：

- 確定偏好的管理位置（內部部署或雲端）以及哪一個群組將負責管理資安（SecOps 或 NetOps）。
- 最重要的是，確保管理解決方案符合 IT 目前和未來的目標。如果要將工作負載轉移到雲端、啟動供應商入口網站，或處理數位化轉型專案或SaaS 應用程式，您可能需要採用雲端管理。如果您的組織依賴整合型舊版應用程式，則內部部署應用程式可能符合您的需求。一般而言，舊版應用程式需要進行一些重組才能在雲端上正常運作，如果沒有立即計畫升級這些應用程式，通常最好使用內部部署管理系統。
- 雲端管理解決方案可幫助網路營運團隊對整個組織套用一致的原則、降低複雜性，並從中央儀表板管理所有資安控制點。這樣簡化了從一個地方協調和管理原則一致性的過程，以抵禦最新的威脅。使用集中管理的雲端應用程式，您可以簡化資安管理，使用範本更快地部署新裝置，以及追蹤整個環境隨時間發生的所有變化。

步驟 3：利用整合增強您的資安狀態。您的防火牆策略應提供所有微邊界的全面保障，並為所有已連線裝置和資安解決方案提供保護和控制。在異質網路中、跨雲端應用程式和服務、公司電子郵件，以及所有連線的端點之間整合安全性，可以保護您的企業免於遭受不斷擴大的威脅。

此步驟可讓您的資安團隊阻止更多威脅，對進階威脅做出更快的回應，並在整個網路、雲端應用程式以及端點中提供自動化。

步驟 4：最後，確保您的防火牆設定策略結合了持續進行的進階威脅分析，以保護您的企業資產並為您提供幫助事先預防新興威脅。最簡單的方法之一，就是選擇一種解決方案以透過防火牆向您的網路自動提供最新的威脅資訊。最新的情報和充分掌握，讓資安團隊能夠瞭解最新的漏洞。而且，如果威脅進入內部，即可確定威脅的發生地點和發生方式。內建的新一代 IPS 功能可自動進行風險排名和影響旗標，以識別優先順序，以便確定最重要的資產和資訊，並確定其優先順序。資安團隊可以立即採取修正措施並修補威脅，專注於最重要的資產，而不會淹沒在「干擾」中，讓 SOC 營運更加安全。

6《Is the Cloud Secure?》Gartner，2018 年 3 月 27 日。

首先，要有正確的防火牆做為基礎

現今的資安團隊需要：

以業界領先的威脅情報做為後盾，提供了更好的安全性，可保護您的複雜網路，及早偵測到威脅，盡快行動。

在整個網路中**有效設定、擴充和協調安全性原則**的方法。

使用整合管理和自動化來提高能見度並降低複雜性，以加速安全營運，並改善他們的體驗。

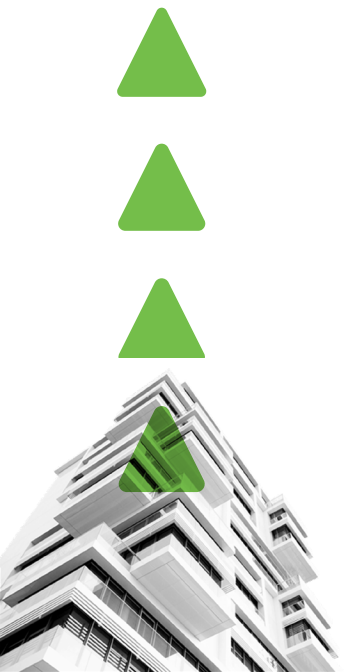
網路和資安一起協同合作，讓現有的投資發揮最大效用。正確的解決方案將為全面的安全性提供一套深入的整合，隨時隨地提供防護。

使用 Cisco Secure Firewall 之防火牆設定策略的好處

將資安架構延伸到整個網路：藉由使用 Cisco Secure Firewall 共享通用原則、入侵防禦功能，以及其他核心功能，交換器和路由器可以執行資安強制執行，將網路基礎架構綁定到全面的資安產品組合中。快速在整個架構中共享威脅情報，將看似無關的事件建立關聯、消除干擾，並更快地阻止威脅。

世界一流的資安控制：Cisco Secure Firewall 提供出色的威脅效能，可以保護您的複雜網路免於遭受現今日益複雜的攻擊。業界領先的進階威脅情報可幫助您的組織發現新的惡意軟體網域和惡意 URL，以及未知或未揭露的漏洞，及早偵測到威脅，盡快行動。內建的新一代 IPS 可讓您使用自動風險排名及影響旗標全面掌握狀態，為您的資安團隊識別優先順序，將噪音降至最低。追溯性安全可讓您瞭解情況，並在首次偵測到威脅後繼續對其進行分析，以深入有效識別最初可能無法偵測到的複雜惡意軟體。

整合式原則和威脅能見度：資安團隊可以藉由標準化和推動跨所有裝置（從網路設備到主機以及跨雲端）的資安控制，來實現原則的一致性和協調性 。思科靈活而集中的管理，可讓您的團隊快速輕鬆地將可擴充控制項套用至許多裝置，以維持一致的原則。透過緊密整合的資安功能（包括應用程式防火牆設定、NGIPS 和 AMP），使用整合管理和自動化威脅關聯性，以降低複雜性。簡化擴充網路中的安全性原則和裝置管理，並加速關鍵安全操作，例如偵測、調查和修復。



第 4 節：針對未來設計的資安解決方案

我們的工作方式已有所轉變。我們的業務和網路已經轉型，改變了網路資安規則。這些發展要求我們重新思考防火牆，並採用防火牆設定。

思科正在透過資安平台來推動創新，以因應這些趨勢，此平台可隨時隨地提供世界級的資安控制，並以業界領先的威脅情報為後盾，提供一致的安全性原則和能見度。最新一代的 Cisco Secure Firewall 構成了我們緊密整合產品組合的基礎。

思科的旗艦級雲端管理解決方案 – **Cisco Defense Orchestrator** – 在各種思科資安產品之間提供原則協調性。

每個思科資安產品都包括**安全威脅回應**，這是一種自動化威脅回應解決方案，可透過在整個安全架構中自動共享和部署因應措施，對新的網路攻擊做出反應。

安全端點提供全球威脅情報、進階沙箱和即時惡意軟體封鎖功能。AMP 持續分析擴充網路間的檔案活動，以快速偵測、遏制和移除進階惡意軟體。

Talos 威脅情報是由全職威脅研究人員、資料科學家和工程師組成的世界知名團隊，負責收集現有和發展中威脅的相關資訊。Talos 是整個思科資安生態系統的基礎，針對攻擊和惡意軟體提供保護。Talos 可讓您掌握最新的全球威脅、有關防禦和緩解措施的可行情報，以及集體回應，以積極保護所有思科客戶。

SNORT 新一代入侵防禦系統 (SNORT NGIPS) 是業界領先的開放原始碼 NGIPS，可執行流量分析、封包監聽/記錄，以及通訊協定分析。SNORT NGIPS 利用 Talos 威脅情報，藉由共享原則以幫助保護整個資安社群免於遭受發展中威脅的入侵。

身分識別服務引擎 (ISE) 可以根據環境在任何地方進行彈性的受信任存取。其透過意向型原則和合規性解決方案提供智慧型的整合保護。

Secure Access by Duo 使用遠端存取和單一登入提供多重要素驗證、端點能見度、自適型驗證和原則強制執行，以主動保護對應用程式的存取權。

Secure Network Analytics、Secure Workload 和 Application Centric Infrastructure (ACI) 協同工作，無論使用者身在何處，其應用程式工作負載在何處，皆可使用機器學習、行為建模，網路基礎架構遙測和分段功能，密切掌握狀況，戰勝新出現的威脅。

藉由投資思科資安平台和 Cisco Secure Firewall，實作針對未來設計的防火牆設定策略。您將獲得當今最強大的資安狀態，為明天做好萬全的準備。

第 5 節：立即開始建構防火牆的未來

思科將網路領導力和尖端的資安技術結合在一起，提供有史以來最安全的架構。無論是透過最佳化現有投資來增強網路資安，還是將路由器轉型為防火牆，思科都將繼續創新。

Cisco Secure Firewall 是建構網路的公司，專為您的數位化轉型企業而設計的網路資安。

深入瞭解 Cisco Secure Firewall，即刻著手您未來的防火牆設定。並在「2020 年全球網路趨勢報告」中，閱讀更多關於塑造未來網路的最新趨勢。