SDSN：動態，自適應的 Multicloud 資訊安全

從防火牆轉為用戶需求式安全政策，為雲端服務提供靈活的安全防護

挑戰

傳統的安全政策無法因應不同的安全工作流程來進行動態調整，因而必須針對實體部署、私有雲和公有雲等所有可能的部署選項，分別配置和管理不同的安全政策。

解決方案

用戶需求式（user-intent）的安全政策善用所有區域一致使用的統一 Metadata，來根據不同安全工作流程進行調整，以協助企業在 multicloud 時代全面克服各種安全挑戰。

優點

- 為所有雲端部署統一的安全政策模型
- 簡化管理和用戶可讀性
- 減少操作費用
- 藉由消除需逐一確認的配置變更需求，增進應用程式部署流程的效率
- 協助安全管理員改善安全工作流程
- 讓管理員能在重要狀況下迅速採取修正措施

傳統的防火牆安全政策高度依靠 IP 位址來進行判斷，但在當今的雲端世界，這種方法無法發揮效用。想克服 multicloud 時代的安全挑戰，企業必須能在不同的工作流程和部署選項之間，使用單一且靈活的 multicloud 安全政策模型，並且動態地調整安全政策。一旦網路受到攻擊時，具備迅速隔離威脅並採取修正措施的能力更是關鍵。

瞻博網路（Juniper Networks）新推出的軟體定義安全網路（Software-Defined Secure Network，SDSN），為企業提供一套強而有力的解決方案。有了 SDSN，安全管理員可透過動態存取群組，以及基於 Metadata 的直覺式統合安全政策模型，打造一個強大的安全工作流程，並植入各個雲端，以便嚴密操控其 multicloud 部署。

挑戰

傳統的防火牆安全政策高度依靠 IP 位址來進行判斷，但這個方法在過去十年間未曾見到重大改善。隨著使用者持續建立與終結動態虛擬實體，IP 位址也隨之不停改變，因此傳統安全政策早已不適用於當今的雲端世界。此外，每個環境都有自己的原生元件，例如 Amazon Web Services（AWS）或 VMware NSX 中的安全群組，而且使用傳統安全政策已難以容納更多安全標籤，大幅限制了企業的靈活反應能力。

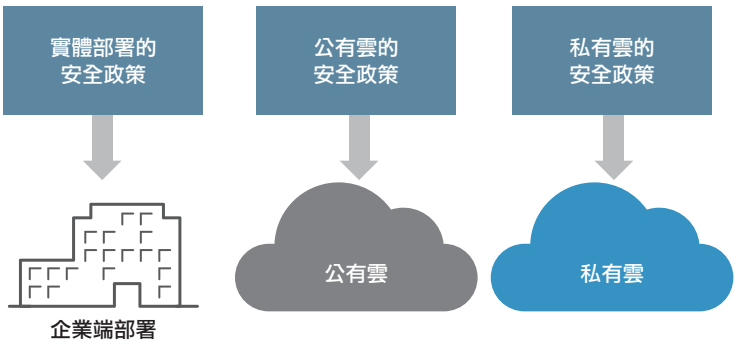
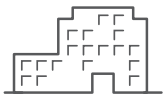


圖 1：安全政策需能夠針對不同的部署進行客製化

為了充分瞭解持續轉變的環境對網路安全會造成什麼樣的衝擊，首先須了解應用程式在企業中的部署方式。

開發了應用程式之後，應用程式開發小組會要求基礎設施小組分配必要的資源；而基礎設施小組會開始建構基礎設施，包括運算、儲存和網路資源，然後要求資安小組允許使用這些應用程式。資安小組會分析每一套應用程式，如有需要還會建立新的或是修改現有的安全政策，並且確認相關變更。

進行實體部署時，前述整個過程大約需要花費 4 到 6 個星期的時間，但如果在雲端環境進行部署，只需幾分鐘就能完成了。然而，在極度分散的環境中，基礎設施可能分別部署於多個雲端，使得資安管理員面臨更高的複雜性，因為他們必須檢視整體企業中安全政策的一致性，並且確認所有的配置變更。隨著部署於分散式系統的應用程式數量不斷成長，資安小組反而成為限制企業靈活性的障礙。



傳統 Waterfall 模型的應用程式部署

圖 2：典型的應用程式部署時程

安全政策行動的靜態本質，對於有效因應不同的安全工作流程，帶來了另一個新的挑戰。使用傳統防火牆安全政策時，當網路受到攻擊，資安管理員必須逐一過濾數千條規則、停用不需要的規則，以便隔離帶來威脅的來源。同樣的，安全管理員需要經常試驗安全政策設定，以便根據特定網路效能狀況，確認最佳的安全防護等級，並且視企業需求進行切換。在一個大規模的規則庫中手動進行變動非常耗時而且效率極差，在時間急迫或是需反覆執行的狀況下，這會造成極大困擾。

Juniper Networks 用戶需求式安全政策解決方案

Juniper Networks 利用一套全方位安全解決方案來克服這些挑戰，它基於用戶需求式安全政策，具有基於 Metadata 的安全政策模型和強大的動態安全政策調整功能。這套解決方案是 Juniper Software-Defined Secure Networking（SDSN）框架的一部分，其中包括以下元件：

- Juniper Networks® SRX 系列服務閘道器和 vSRX 虛擬防火牆，具備整合式下一代防火牆（NGFW）和統一威脅管理（UTM）等元件。這些產品提供：
  - 核心防火牆功能和 IPsec VPN，以及多功能網路服務，例如網址轉譯（NAT）和路由
  - 入侵偵測系統（IPS）2.0，可偵測並防堵網路入侵事件
  - 基於使用者角色的防火牆，可根據使用者角色和群組來分析、紀錄和強制執行存取控制
  - 利用整合式 Juniper Networks AppSecure 2.0 的應用程式控制和可視度，提供應用級分析、排序和防堵功能，以便安全地執行應用程式
  - 透過 UTM 執行防毒、防垃圾郵件和網站與內容過濾，以免遭受病毒、垃圾郵件和惡意網站與內容等威脅
  - 支援 Linux KVM、VMware、AWS 和 Azure 平台（vSRX）
  - 支援動態位址群組，有助於建立 "nocommit" 架構
- Juniper Networks Junos Space® Security Director 提供集中式單一虛擬管理介面，以便對網路中所有 SRX 實體系列和 vSRX 虛擬防火牆，進行安全功能與安全政策的部署、監控和配置。
  - Policy Enforcer 是 Security Director 的元件，可提供更深一層的集中式智慧功能，以便在交換器、路由器、WiFi 存取設備等不同廠商的網路元件上，部署和強制執行安全政策。
  - 在推出用戶需求式安全政策後，它還提供將 Metadata 用於安全政策的功能，並可使用 Dynamic Policy Actions（DPA）功能動態地對安全政策採取回應措施。
  - Security Director 包括可客製的儀表板，以提供詳細的下拉式威脅地圖和事件日誌，以及前所未有的網路安全狀態透視度。
  - 此外，它也可當作 Google Android 和 Apple iOS 系統的行動應用程式，讓您能透過行動裝置進行遠端監視。

基於 Metadata 的安全政策模型

Metadata 被定義從端點裝置相關屬性清單中過濾所有可能的數值，以便建立關鍵值資料庫。多數的雲端部署（VMware NSX、Juniper Contrail® 平台、Amazon AWS 等）都是使用其雲端的原生 Metadata。

在安全政策中充分利用 Metadata，可大幅增進已具備靜態識別特性（例如 IP 位址或位址物件）之傳統安全政策的成效。藉由遵循通用的 Metadata 標記，Security Director 的 SDSN Policy Enforcer 元件可用相同的安全政策配置企業中所有的防火牆，因此您無需費力地客製安全政策，使其能與雲端相容。網路或開發與 DevOps 管理者可輕易地將合適的 Metadata 指派給終端設備，讓預先配置的安全政策能立即開始使用。

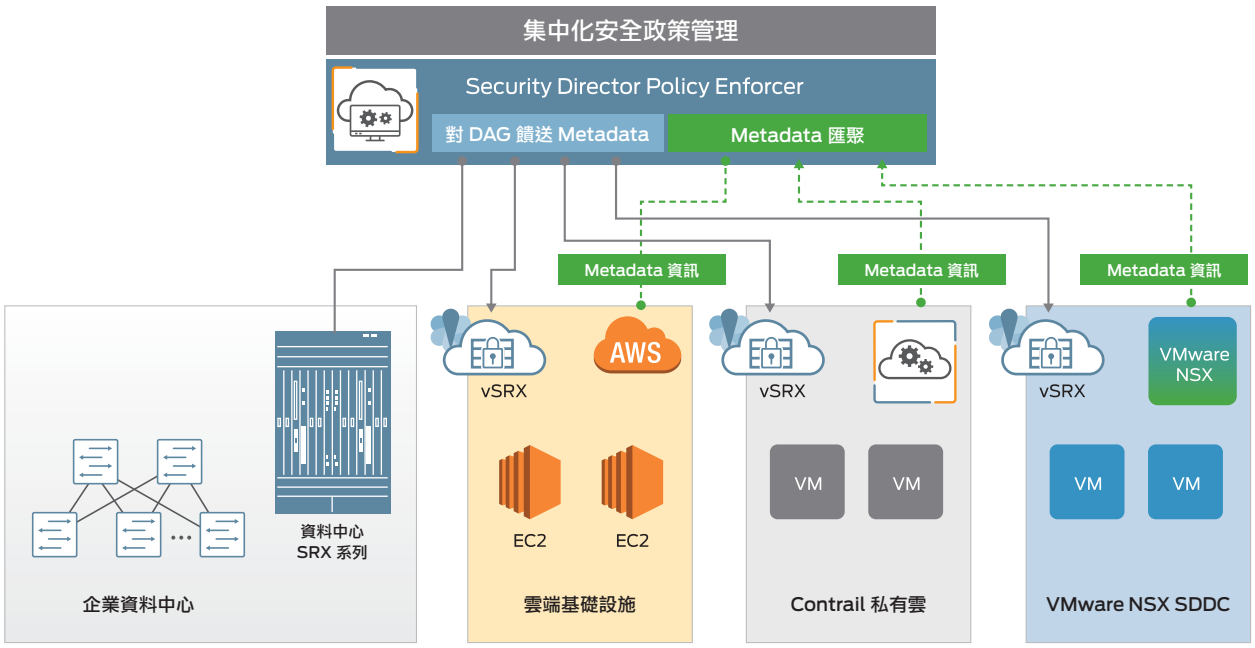


圖 3：對 SRX 系列和 vSRX NGFW 之動態位址群組進行 Metadata 匯聚和饋送（feed）

SRX 系列和 vSRX NGFW 的動態位址群組

SRX 系列實體和 vSRX 虛擬 NGFW 中的動態位址群組有助於實現可調整的安全政策，其中包含一張完整的 IP 位址清單。將動態位址群組用於安全政策後，便可任意增加或刪除 IP 位址，無需逐一進行確認。在經常動態建立或終結終端設備，導致 IP 位址不斷改變的情況下，這無疑是一大福音，因為添加數千個 IP 位址是極度耗時的工作。另外還有一個好處，SRX 系列和 vSRX 防火牆還可根據外部來源餽送的資料，動態地在位址群組中增加或更新 IP 位址。

映射至動態位址群組的 Metadata

Security Director Policy Enforcer 可當作匯聚伺服器，以便從不同來源（Contrail、VMware NSX、AWS 等）及其相關 IP 位址取得原生的 Metadata。接著這些資訊會被饋送到不同區域的 SRX 系列和 vSRX NGFW，它們可作為 Metadata 饋送伺服器和安全政策管理系統。

當應用程式從企業中的實體硬體設備轉移到雲端後，雲端的防火牆將使用應用終端設備提供的 Metadata 來決定適合終端設備傳送與接收之訊務的措施。如此可實現更順暢和靈活的應用程式轉移流程，而不用犧牲安全性。

使用有意義的 Metadata 也有助於瞭解使用者的意向，讓終端設備更容易辨認並可遵循安全政策來運作。

此解決方案也推出了在安全政策中使用邏輯操作符（logic operator）的功能，例如可在終端設備 Metadata 上進行“AND”和“OR” 操作。如此卓越的靈活性，大幅簡化了整體政策配置。

例如，如果為所有終端設備配置來源欄位，Metadata “Type”為“DB”，Metadata “PCI”為“no”，可在安全政策的來源或目的位址中加以指定。

下表讓管理員能快速一覽各種可能性，以便減輕企業安全負擔，並且有效提升操作靈活性。

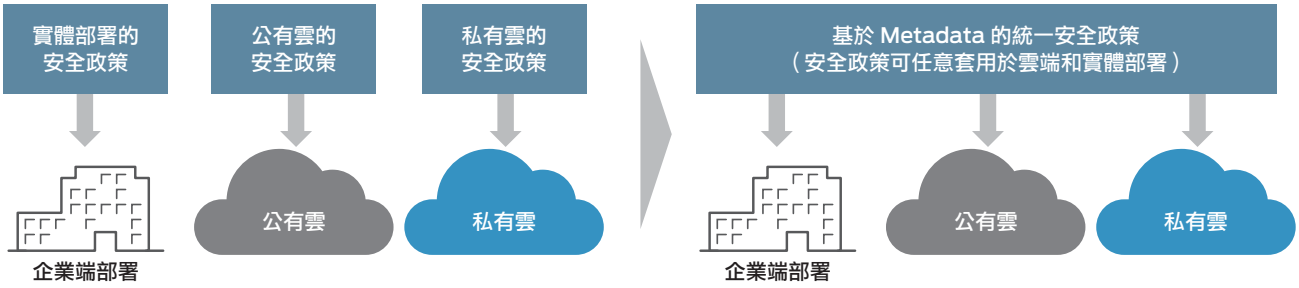


圖 4：基於 Metadata 的安全政策模型

安全政策使用如下表所示的靜態 IP：

#	來源	目的地	服務	防火牆	IPS
1	網路伺服器物件	資料庫位址物件	http	允許	無

後端位址物件至靜態 IP 的映射如下表所示（需配置資安小組）：

# 位址物件	映射
HR_SR_object	1.1.1.1
SQL_FIN_OBJECT	2.2.2.1

如需將新的模組加入應用程式時，DevOps 或網路管理員需配置必要的應用程式，並要求資安小組將 IP 位址加入許可清單中。管理員會對位址物件或靜態位址進行必要的變更並確認配置。基本上，逐一確認配置是個極為耗時的過程，進一步增加了安全負擔。

#	來源	目的地	服務	防火牆	IPS
1	PCI ==NO	TYPE == DB && PCI ==YES	任何	拒絕	無

Metadata 至位址的映射如下所示：

# 位址物件	IP 映射	Metadata 部署狀態	Metadata PCI	Metadata 類型
HR_SR_object	1.1.1.1	Production	無	網站
SQL_FIN_OBJECT	2.2.2.1	Production	是	資料庫

資安管理員根據來源和目的欄位的 Metadata 邏輯制訂安全政策。當 DevOps 或網路管理員指派新的終端設備給應用程式時，只有合適的 Metadata 才需要與新的終端設備建立關聯性，以便將它部署於應用程式集區。

使用資安小組核可的安全樣板或預設的基於 Metadata 的安全政策，可減少 3 到 4 個星期的配置和確認配置過程，不但可顯著縮短應用程式部署時間，還可確保更高的企業靈活性，並將操作支出降到最低。同樣的，只需簡單地刪除相關的 Metadata，便可將終端設備從應用程式集區中移除。

Dynamic Policy Actions

Security Director 的 Policy Enforcer 包括基於可配置的全域 NetSec 變數之 Dynamic Policy Action (DPA) 功能，可允許預先配置的安全政策在不同情況下採取不同的回應，如此便可對威脅進行主動出擊。此外，可對大量安全政策採取相對應行動的功能，則可動態簡化安全態勢，允許系統能在不同的攻擊情況下動態調整其回應措施。

當網路受到攻擊時，很重要的一點是，必須能夠迅速隔離威脅並採取修正措施。傳統的工作流程要求安全管理員以手動方式關閉所有不重要的商業應用程式，直到完成診斷為止。在一家正常企業中，可能有數以千計的安全政策負責監控不重要的應用，例如視訊或音頻串流、私人電子郵件，以及手機 app。如果認為網路受到攻擊，可使用 DPA，透過單一 NetSec 變數對大量的安全政策執行自訂的措施，以便保護基礎設施。

同樣的，在最佳化安全政策設定以提高效能和安全性，或是執行模式切換以便排列應用程式的優先順序時，DPA 也可藉由變更單一 NetSec 變數來達成目標。例如，在進行大量資料備份時，安全管理員可藉由設定 NetSec 變數來跳過內部訊務的額外 IPS 設定，等到備份完成後再切換回 “Full Security” 模式。安全管理員也可建立「實驗性」模式，以便在安全和效能設定之間找出方式最佳平衡點，然後預先配置安全政策，使其能根據此設定採取適當的動作。

這種快速切換的工作流程，不僅允許資安小組與企業中其他團隊密切合作，同時還讓安全管理員能在高壓狀況下，有效地採取回應措施。

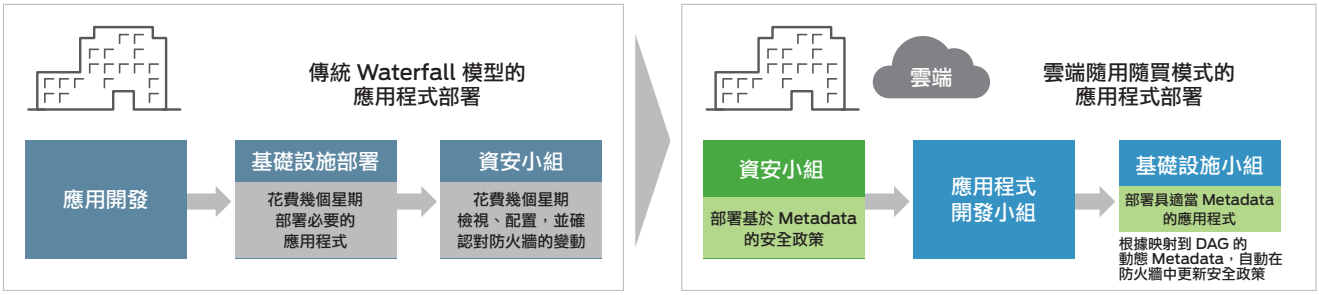


圖 5：基於 Metadata 的安全政策可顯著縮短應用程式部署時間

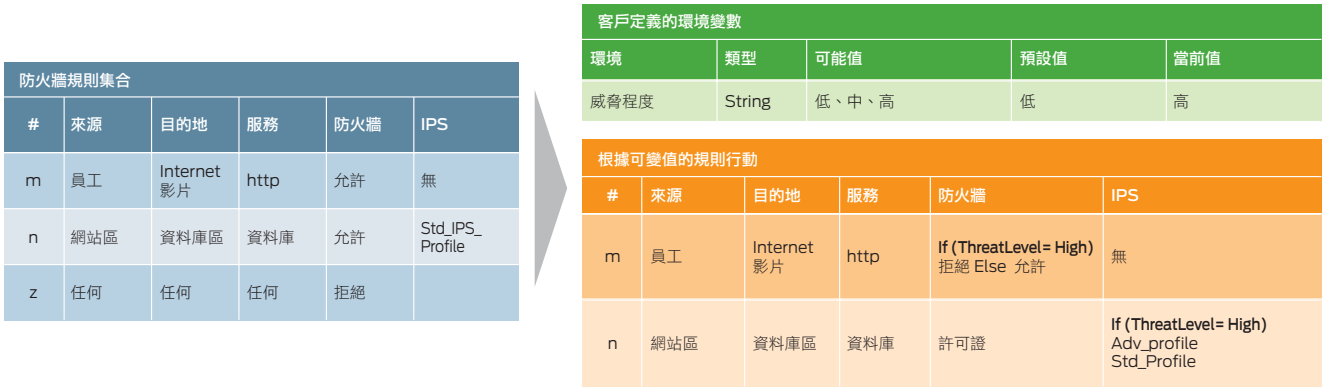


圖 6：對 SRX 系列和 vSRX NGFW 之動態存取群組進行 Metadata 匯聚和饋送（feed）

特色與優點

Juniper 用戶需求式安全政策解決方案具備以下的功能與優點：

- 藉由消除手動進行配置變更與確認的需求，確保靈活的應用程式部署
- 減少操作費用
- 將 Metadata 邏輯用於安全政策時，可改善使用者可讀性和靈活性
- 允許安全政策套用於不同區域，包括實體資料中心、私有雲和公有雲
- 可動態調整網路威脅等級，以便執行有效率的除錯和威脅隔離工作流程

結語 — Juniper 提供 multicloud 時代必備的統一安全解決方案

SRX 系列服務閘道器和 vSRX 虛擬防火牆支援先進的 L4 至 L7 安全功能，例如使用者防火牆、應用防火牆和 IPS，加上強而有力的底層功能，例如動態存取群組，有助於實現“no-commit” 結構，可提供理想的 cloud-ready NGFW。

有了基於 Juniper SDSN 的用戶需求式安全政策解決方案，安全管理員可透過動態存取群組，以及基於 Metadata 的直覺式統合安全政策模型，打造一個強大的安全工作流程，並植入各個雲端，以便嚴密操控其 multicloud 部署。

更多資訊

如需更多關於 Juniper Networks 安全解決方案的資訊，請瀏覽 www.juniper.net/us/en/products-services/security，或聯絡 Juniper 業務專員，以瞭解詳情。

關於 Juniper Networks

瞻博網路（Juniper Networks）致力於透過多元的產品、解決方案和服務，來改變網路連接的經濟效益，打破了業界一成不變的現狀。我們的團隊與客戶和合作夥伴共同推動技術創新，以提供自動化、可擴充的安全網路，進而提昇網路的靈活性、效能和價值。如欲獲得更多資訊，請瀏覽 Juniper Networks 網站，或是加入 Juniper Twitter 和 Facebook 粉絲團。

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510634-001-TC Dec 2017