paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

移轉安全至 SASE 模式的實務指南

作者：Alex Ciobanu

目錄

第 1 章

SASE：網路與安全的典範轉移

簡介

隨著企業開始採用雲端和行動裝置，網路功能和安全性的交付方式也必須改變。數位轉型以及隨處工作的需求促進企業對於雲端的大規模利用，並且隨著企業以外的使用者和應用程式越來越多，將流量回傳至數據中心的舊架構模式便不再適用。雖然雲端網路安全產品已一躍成為具有潛力的解決方案，但這些產品也只不過是解決一部分的問題。同樣地，由於下列一些關鍵限制，使得許多現代化的安全存取解決方案無法實現企業所需的「隨處工作」體驗：

- 這些解決方案無法為所有應用程式提供存取和安全性，增加數據外洩的風險。
- 也無法提供完整、經驗證的企業級安全性，讓企業暴露在進階威脅之中。
- 它們為遠端工作者提供的存取層級和效能並不一致，不但會讓使用者感到困擾，更會增加 IT 部門的支援負擔。

是時候採用全新的方法。

安全存取服務邊緣 (SASE) 是一種新興的架構方法，可透過直接從雲端結合網路與安全服務的方式，協助企業解決這些問題。本指南適用於網路及安全專業人員，並介紹 SASE 的優勢以及如何使用 Palo Alto Networks 推出的 Prisma® Access 將您的網路安全架構移轉至 SASE 模式。

什麼是 SASE？

SASE 將軟體定義的廣域網路 (SD-WAN) 與防火牆即服務 (FWaaS)、安全網路閘道 (SWG)、雲端存取安全代理 (CASB) 和零信任網路存取 (ZTNA) 之類的安全服務整合至單一雲端交付服務。無論使用者、應用程式或裝置位於何處，SASE 都可以解決提供一致的安全存取方面的挑戰。

透過業界最完整的 SASE 架構，Palo Alto Networks 再次革新企業對於網路和安全基礎結構的轉型。Prisma Access 是一個雲端交付的安全平台，可提供企業需要的安全性來保護所有的流量、應用程式和使用者。Prisma SD-WAN 則是一個雲端交付的網路平台，可使用機器學習和自動化來簡化 WAN 連線並提供絕佳的使用者體驗。在將 Prisma Access 與 Prisma SD-WAN 進行深度整合後，Palo Alto Networks 可讓企業大規模地保護遠端工作者。Prisma Access 與 Prisma SD-WAN 的整合可提供業界最全面的 SASE 解決方案。

為何需要 SASE 來進行安全性的轉型？

傳統網路安全技術的設計無法有效地保護遠端工作者不受到現代化的安全威脅。此外，傳統防火牆和網路 Proxy 也無法針對全球性跨國企業的所有流量進行一致的檢查及控制。

傳統架構在保護分公司和零售點方面也會形成挑戰，因為原本這些架構就不是為了適應雲端的環境所設計。網路中每個獨立的實體都會需要新的架構、一組要部署的新政策，以及要設定的新介面。這會造成管理上的負擔，不但會增加成本和複雜度，更會形成企業的安全狀況的漏洞。

SASE 是一種平台式方法，可根據您的企業需求解決多個使用案例。這些需求一開始可能面對的緊急挑戰包括員工遠端存取、保護分公司直接網際網路存取，或改善網路安全性。Prisma Access 提供一個模組化平台，可讓您從對於企業最重要的使用案例開始，然後在新機會出現時解決其他的使用案例。

Prisma Access 的 SASE 使用案例

Prisma Access 可同時針對網路和使用者提供服務型的防護 (參閱圖 1)。

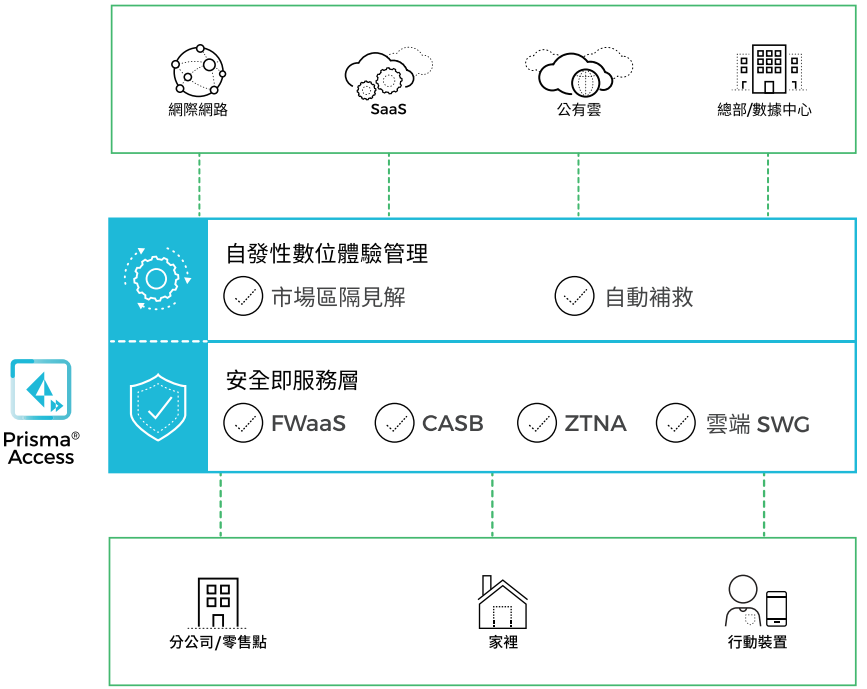


圖 1：Prisma Access 高層級架構

適用於行動使用者的 Prisma Access 可提供全面的雲端交付安全性，讓使用者無論在何處進行存取都可以安全地連線至他們需要的應用程式。Prisma Access 可同時支援受管理和和未受管理的裝置，以確保無論使用者是位於雲端、從數據中心交付 (或者兩者)，都可提供對於公司資源的一致安全性及無縫存取，同時提供最佳化的使用者體驗。在採用 ZTNA 方法時，Prisma Access 可根據定義的存取控制政策 (包括對於威脅以及數據遺失或憑證遭入侵徵兆的連線後監控)，提供對於應用程式和服務的存取權限。

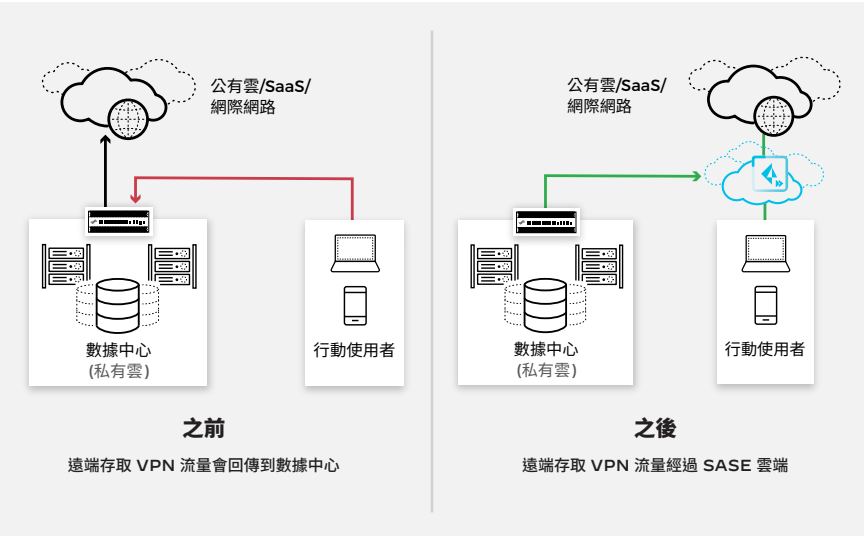


圖 2：行動使用者安全使用案例

適用於遠端網路的 Prisma Access 可針對分公司和遠端站台提供一致的連線和安全性。它可協助企業簡化對於全球安全政策和強制執行的部署與管理，以充分利用雲端優勢加速實現價值。企業在針對 WAN 連線和安全性進行大規模的管理時，也可以避免經常伴隨而來的複雜度和龐大管理成本。

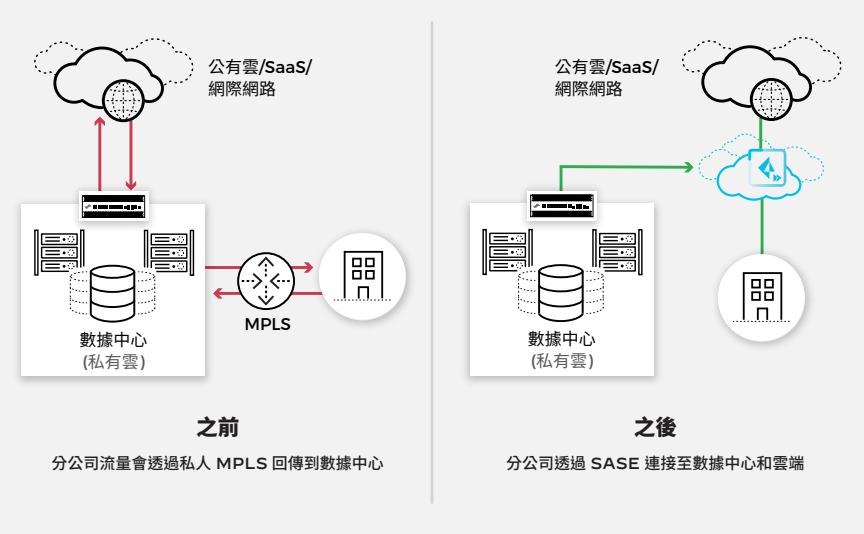


圖 3：遠端網路安全使用案例

更多資源

若要深入瞭解，請造訪我們的 Prisma Access 網站。

第 2 章

透過 Prisma Access 建構 SASE 部署

保護行動使用者

遠端工作型態的成長代表著對於應用程式的安全、高效能遠端存取比以往任何時候都更加重要。此外，應用程式也需要對於不當存取、威脅和惡意使用者的防護。

傳統方法對於遠端存取的挑戰，例如傳統的虛擬私人網路 (VPN) 不僅是在規模和容量方面，另外還包括缺乏內嵌安全性。Prisma Access 提供全球部署、雲端交付的服務並具備內建的高可用性、自動擴充和內嵌安全檢查等功能，因此可以克服這些挑戰。

藉由 Prisma Access，無論應用程式是在雲端、在網際網路還是在數據中心，使用者都可以安全不間斷地存取所有的應用程式。位於世界各地的使用者都可以連接至可用性最佳的雲端閘道，並執行一致的安全性，即使您所在的位置沒有區域網路也可運作。

Prisma Access 會使用 ZTNA 方法，以確保使用者只能根據政策獲得所需應用程式的存取權限。此外，系統會套用內嵌流量檢查以防範威脅和數據遺失，同時確保您的應用程式和數據不會受到未獲授權的存取或遭到潛在惡意活動的攻擊。

在使用 Prisma Access 的 ZTNA 功能時，系統會透過雲端平台導向使用者，因此您的應用程式會受到保護以避免公開曝露在網際網路中。一旦使用者透過 User-ID™ 技術進行驗證，無論他們位於何處，系統都會根據使用 App-ID™ 技術的第 7 層政策和裝置的角色或類型來允許他們存取應用程式。此外，系統也會套用連線後檢查來掃描威脅，並監控數據遺失和潛在的憑證竊取情況。

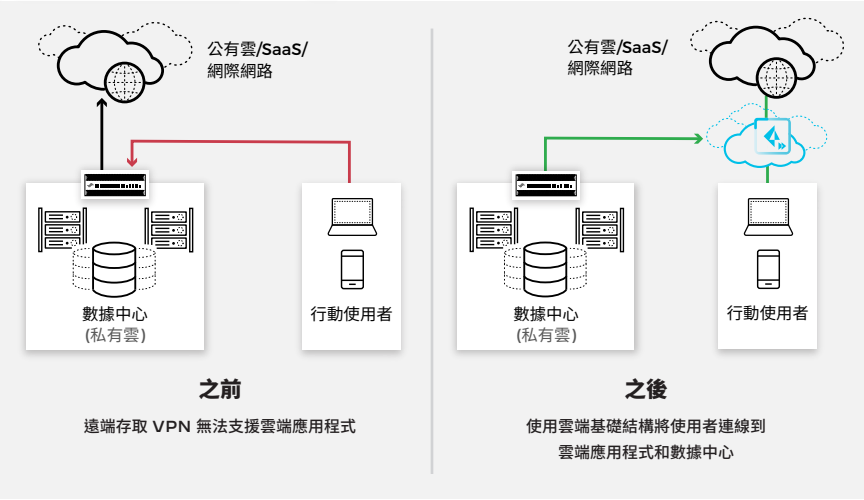


圖 4：可提供一致安全性的雲端基礎結構

使用者的智慧型手機、平板電腦或筆記型電腦可使用以下方式連接至 Prisma Access：

- **GlobalProtect 代理程式** — 端點代理程式會使用目前可用的最佳閘道來建立通往 Prisma Access 的安全通道。GlobalProtect 代理程式也會將使用者和裝置資訊列入考量以成為 ZTNA 的一部分。
- **無用戶端** — 透過啟用 SSL 的網路瀏覽器針對無法安裝代理程式的裝置提供安全的遠端存取。當您需要讓合作夥伴或承包商存取或安全地啟用自備裝置 (BYOD) 情況中的未受管理裝置時，這個選項就會很有用。
- **PAC 檔案** — 此連線方法會使用明確的 Proxy 方法，同時維護 Prisma Access 提供之同級最佳安全性。

保護遠端網路

企業傳統上會依賴 VPN 或多重通訊協定標籤交換 (MPLS)，為其網路提供安全的私人連線來存取數據、應用程式和網際網路。

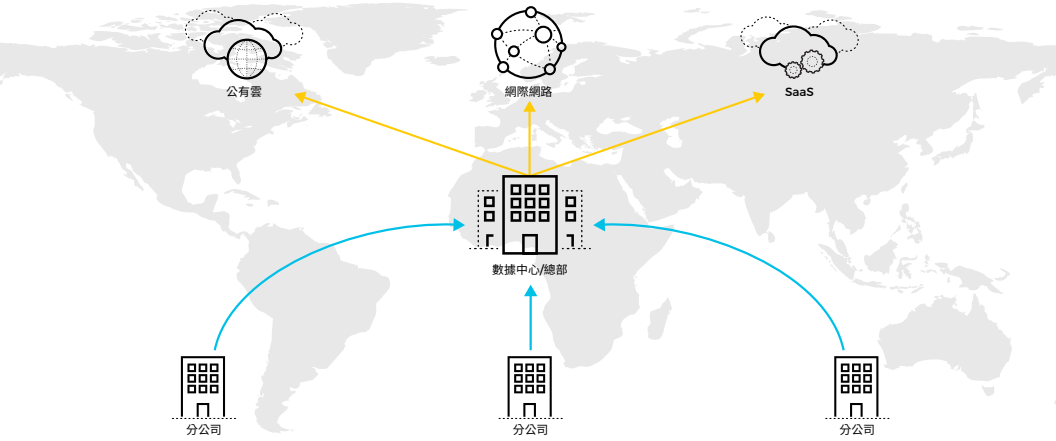


圖 5：傳統 WAN 方法

如圖 5 所示，此架構方法會帶來幾種挑戰，包括：

- 為了安全考量，在分公司中流入及流出的流量都會回傳到數據中心/總部，因而導致延遲性的增加
- MPLS 線路的維護過於昂貴且複雜
- 分公司之間的通訊並未受到保護

Prisma Access 可透過 IPsec 通道或 SD-WAN 將您的遠端位置上線，因此無論您位於世界上任何角落，它都可以讓您直接且安全地存取雲端、軟體即服務 (SaaS) 和網路資源。每個通道都可連接至其中一個雲端安全執行節點。Prisma Access 也可以將您的位置安全地連接至數據中心/總部。資源的存取是透過 Prisma Access 雲端和數據中心之間的個別 IPsec 通道 (稱為服務連線) 進行。

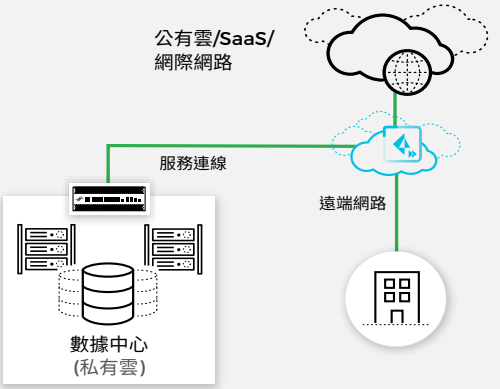


圖 6：保護任何地點的雲端存取

圖 6 顯示遠端網路如何連接至 Prisma Access。從路由的觀點來看，它可支援靜態路由和邊界閘道通訊協定 (BGP)。圖 7 顯示使用靜態路由的設定，Prisma Access 會對其進行重新分配，使網路中的其他資源和使用者可存取遠端位置。

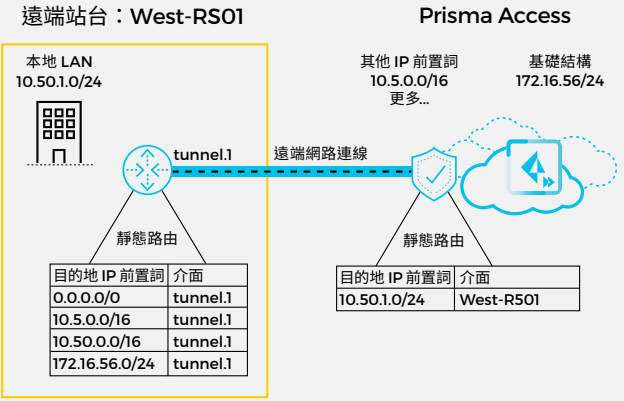


圖 7：連接至 Prisma Access 的遠端網路連線

利用 Prisma Access 來保護行動使用者和遠端網路的企業可取得以下優勢：

- 一致的安全性和進階威脅防護：無論使用者位於何處，您的政策皆會適用於所有流量。
- 數據遺失防護 (DLP)：全面性的數據保護會將您的敏感數據分類並在遠端使用者和位置之間移動這些數據時提供保護，以確保數據的絕對安全。
- DNS Security：進階分析和機器學習可提供保護，防止威脅入侵網域名稱系統 (DNS)。
- URL Filtering：系統會執行您接受的使用政策，並篩選對於惡意網域的存取。

更多資源

請參閱我們的 Prisma Access 參考架構

第 3 章

移轉最佳實務

確保 Prisma Access 的成功部署

在套用本章所描述的最佳實務功能之後，將可提供對於流量的可視性、對於潛在惡意活動的持續掃描、URL 篩選以及對於使用者的全球性地理涵蓋範圍。您可以從第一天就啟用 Prisma Access 中的所有功能。

圖 8：移轉最佳實務

1. 啟用所有安全政策的記錄

Prisma Access 會使用 Cortex® Data Lake 來收集、整合及轉換安全日誌數據。無論是已移轉或新設定的安全政策，我們都強烈建議啟用記錄功能。這將會提供對於網路中所有流量的可視性。您可以設定日誌轉送設定檔並將其指派至安全政策以輕鬆地啟用記錄功能。

如果您需要將 Prisma Access 日誌傳送至另一個位置 (例如安全資訊和事件管理 [SIEM] 系統)，您可以使用日誌轉送應用程式從 Cortex Data Lake 轉送日誌。

如果您要從傳統安全解決方案移轉規則 (我們將於第 4 章詳細說明)，您可以使用 Expedition 工具建立設定檔並在移轉期間自動將其指派至規則。這只會套用至 Panorama™ 網路安全管理所控管的 Prisma Access 部署。

2. 設定及啟用 Threat Prevention 和 Wildfire

無論是連接埠、通訊協定或應用程式，我們的 Threat Prevention 服務都可檢查所有流量以發現威脅，大幅超越一般的入侵防禦系統 (IPS)。WildFire® 惡意軟體防禦服務可提供雲端式威脅分析以找出零時差入侵和未知的惡意軟體。Threat Prevention 和 WildFire 應從第一天起就在安全規則上啟用。若無法在一開始就達到完全執行，我們強烈建議您可先在警示模式中啟用 Threat Prevention 和 WildFire，然後過一段時間後再移至完全執行。在結合 Threat Prevention 和 WildFire 後，您就可以為使用者提供一致且主動的防護以防範已知和未知的威脅。

3. 設定及啟用 URL Filtering

URL Filtering 可根據站台類別、功能和安全性為您的使用者提供安全的網路存取。雲端式服務結合運用靜態分析和機器學習進行識別，同時會自動封鎖惡意網站和網路釣魚網頁。您也可以嚴格控制允許使用者輸入公司憑證的站台類型以防止憑證網路釣魚竊取。您可以根據 URL 類別來執行您的安全政策。

4. 啟用應用程式與使用者識別

Prisma Access 可利用 Palo Alto Networks App-ID 引擎來識別周遊網路的應用程式，而無需考量連接埠、通訊協定、規避策略或加密 (SSL/TLS 或 SSH)。我們強烈地建議您將傳統安全規則移轉至 App-ID 或建立一個啟用 App-ID 的新安全規則。除了應用程式以外，您也可以設定 User-ID 來識別網路中的使用者，並決定誰可以存取某些應用程式。

5. 建立及部署解密策略

解密對於網路中完整控制及可視性的維護扮演相當重要的角色，且 Prisma Access 可支援所有流量的完整解密。您應設置及部署解密策略以識別所有應用程式，防止惡意的加密內容進入您的網路，或阻止敏感內容隱藏為加密流量而離開您的網路。

在開始解密流量時，您可以設定 Prisma Access 在工作階段中作為受信任第三方所需的認證。針對其他所有項目，我們已內建最佳實務解密設定，包括設定排除的選項，例如在解密時應排除的敏感內容或站台。

6. 為您的遠端工作者設定可在全球使用的位置

Prisma Access 可利用公有雲基礎結構為企業提供大規模的全球涵蓋範圍。為了將遠端工作者納入全球性地理涵蓋範圍，您可以啟用 100 個以上的 Prisma Access 位置供使用者進行連線。這可以為您的遠端工作者提供更佳的效能和安全性，同時為您的數據中心應用程式、公有雲、SaaS 應用程式和網際網路提供絕佳的通訊。圖 9 顯示位於各大洲的 Prisma Access 網路節點 (PoP)。

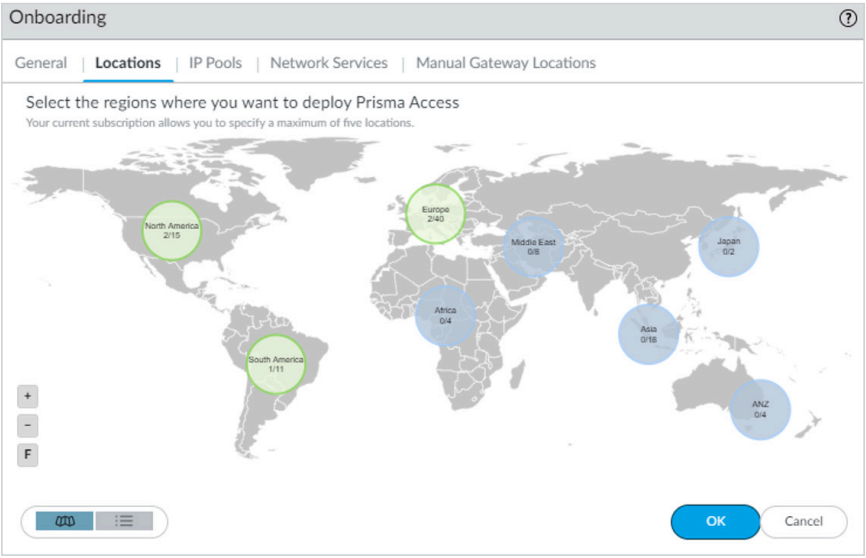


圖 9：分布於 76 個國家/地區的超過 100 個服務存取點

由於移轉至 SASE 模式需要進行詳盡的規劃和一些架構變更，因此越快著手進行越好。在下一章中，我們將分析從傳統架構和產品移轉至 Prisma Access 部署的建議方法，並著眼於網路和安全考量。

第 4 章

從傳統防火牆和 VPN 解決方案移轉至 Prisma Access

開始進行移轉

Palo Alto Networks 可提供兩種方式來部署及管理 Prisma Access：

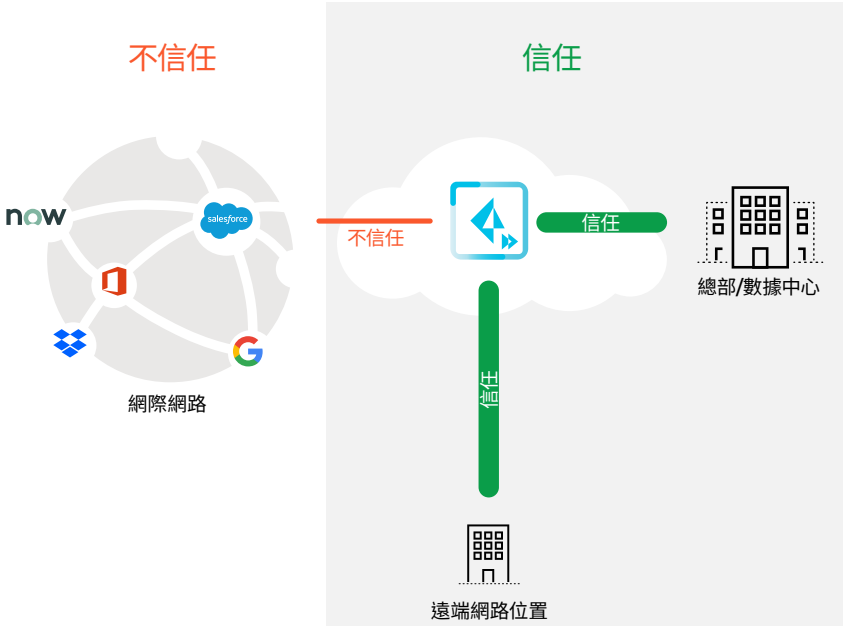
- Panorama 管理：若您已使用 Panorama 來管理您的 Palo Alto Networks 新世代防火牆，您可以透過 Panorama 管理來部署 Prisma Access 以利用您現有的政策。
- 雲端管理：若您並未使用 Panorama 或只是想要簡化的 Prisma Access 上線和管理體驗，可使用 Palo Alto Networks 中心的 Prisma Access 應用程式以快速且輕鬆地為您的 Prisma Access 使用者啟用網際網路存取，然後將連線延伸至總部、數據中心和分公司網路。

以下的移轉指南將會以 Panorama 管理的 Prisma Access 為基礎。

在從傳統防火牆解決方案移轉至 Prisma Access 時，必須注意與設定移轉有關的幾件事情。在一般基於區域的防火牆中，每個區域都有一個相關的介面。Prisma Access 可自動建立信任、不信任和無用戶端的 VPN 區域以簡化區域指派。使用者只需要建立區域對應就可達到一致的安全政策執行：

- **信任區域**包含公司網路中所有信任的 IP 位址、服務連線和行動使用者 (例如行動使用者 IP 集區、基礎結構、數據中心和遠端子網路)。

- **不信任區域**包含面向網際網路的所有介面。依預設，任何不受信任的 IP 位址或行動使用者在本質上都是不受信任的。
- **無用戶端 VPN 區域**可用於安全遠端存取 (例如承包商的應用程式存取)。



應用程式	安全政策區域	區域對應	行動
Office 365	已獲批准 - SaaS	不信任	允許
Salesforce	已獲批准 - SaaS	不信任	允許
Perforce	Eng-tools	信任	允許
LDAP	dc-apps	信任	允許

圖 10：在 Prisma Access 中自動建立的區域

圖 11 中顯示的轉型層級提供了轉換至 Prisma Access 的一種無縫且安全的方式，可將移轉風險降至最低並描述進階功能的逐步採用路徑，如第 3 章所述。

圖 11：轉型層級

從 Check Point 裝置移轉至 Prisma Access

本節將深入分析第 3 和第 4 層政策移轉考量，包括從 Check Point 產品移轉物件。雖然 Prisma Access 有許多獨特且動態的設定值必須個別進行設定，不過若您想要移轉任何現有的政策和物件，可以使用以下方式來完成。Palo Alto Networks 提供一種稱為 Expedition 的移轉工具，可用來將 Check Point 設定移轉至 Prisma Access。圖 12 顯示使用 Expedition 來移轉設定的高階流程。

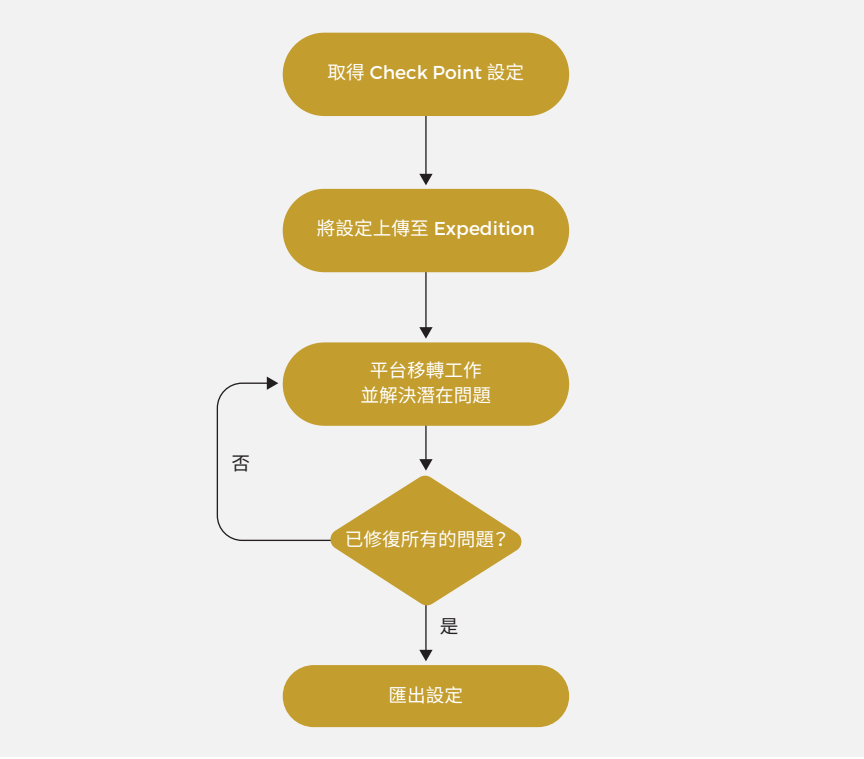


圖 12：透過 Expedition 進行移轉的高階方式

我們可以將此流程區分成三個步驟。

步驟 1：取得 Check Point 設定並將其上傳至 Expedition

必要的檔案將視 Check Point 軟體的版本而定：

- 針對低於 R80 的版本：
  - Objects_5_0.C
  - Policy.W
  - Rulebases_5_0.fws
  - Routes.txt
- 針對高於或等於 R80 的版本，請參考 Expedition Web-UI 中的指示以取得「R80.x 或更新版本」的選項。

步驟 2：執行移轉工作並解決潛在問題

第一個建議執行的動作就是檢查移轉日誌。這將會通知您有哪些問題是在轉換程序期間所發現，或者是否已自動修復設定的任何部分。圖 13 顯示與目的地 NAT 有關的一些日誌。這些日誌僅供參考之用，管理員並不需要執行任何動作。

MIGRATION LOGS

Level	Datetime	Message	Action
Task: Correcting Destination based on DNAT			
		Security Rule[69] covers the DNAT Rule(s)[9].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[10].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[11].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[12].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[13].	No Action required

圖 13：與目的地 NAT 有關的日誌

清除未使用的物件，其中包括在移轉期間其他建議執行的步驟。您可以從設定中移除下列未使用的物件：

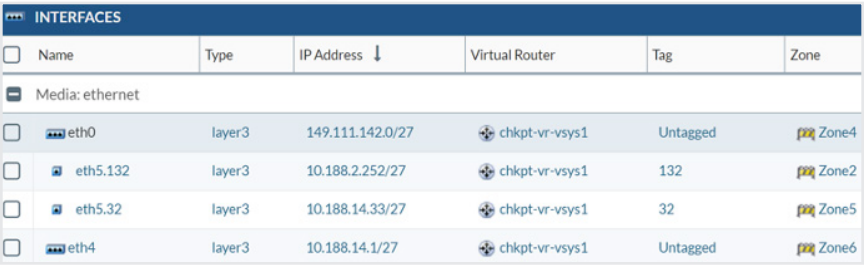
- 位址
- 位址群組
- 服務
- 服務群組
- 標籤

我們強烈建議您檢查及修復下列可能錯誤設定的移轉問題：

- 名稱重複的物件
- 無效的服務 (例如識別為服務而非應用程式的「Ping」)

從網路功能的觀點來看，Prisma Access 並不需要下列任何 Check Point 設定：

- **區域：**從 Expedition 匯出網路區域時，所有的區域都會命名為「Zone1」、「Zone2」、「Zone3」等等。這將會自動反映在安全政策中。不過，我們還是建議您變更這些區域名稱。系統會自動調整安全規則。在圖 14 的 Expedition 螢幕擷取畫面中，您可以看見從 Check Point 移轉的介面範例，以及一些新建立和對應的區域。
- **虛擬路由器：**Prisma Access 會自動處理所有介面設定、內部路由和 NAT。您不需要移轉任何路由表 (靜態或動態項目)。Prisma Access 中朝向數據中心或遠端網路的靜態或動態路由設定將會以手動方式設定。



INTERFACES

Name	Type	IP Address	Virtual Router	Tag	Zone
Media: ethernet					
eth0	layer3	149.111.142.0/27	chkpt-vr-vsys1	Untagged	Zone4
eth5.132	layer3	10.188.2.252/27	chkpt-vr-vsys1	132	Zone2
eth5.32	layer3	10.188.14.33/27	chkpt-vr-vsys1	32	Zone5
eth4	layer3	10.188.14.1/27	chkpt-vr-vsys1	Untagged	Zone6

圖 14：從 Check Point 移轉的介面

步驟 3：將設定上傳至 Panorama

雖然有多種方法可以將新預備的設定上傳至 Panorama，但我們仍建議採用以下其中一種方法：

- 從 Expedition 至 Panorama 的直接 API 呼叫
- 在 CLI 中使用「`load partial`」命令
  - 提供精確的方式，僅選取最終 XML 設定檔案的某些部分並上傳至 Panorama

圖 15 顯示了使用「load partial」命令的範例，也就是僅將個別和必要的部分從移轉的 Check Point 設定上傳至 Panorama (我們選擇了「Mobile_User_Device_Group」裝置群組)。在此案例中，我們已將匯出的 Expedition 設定檔案命名為「cp.xml」，且我們只將它匯入至 Panorama。

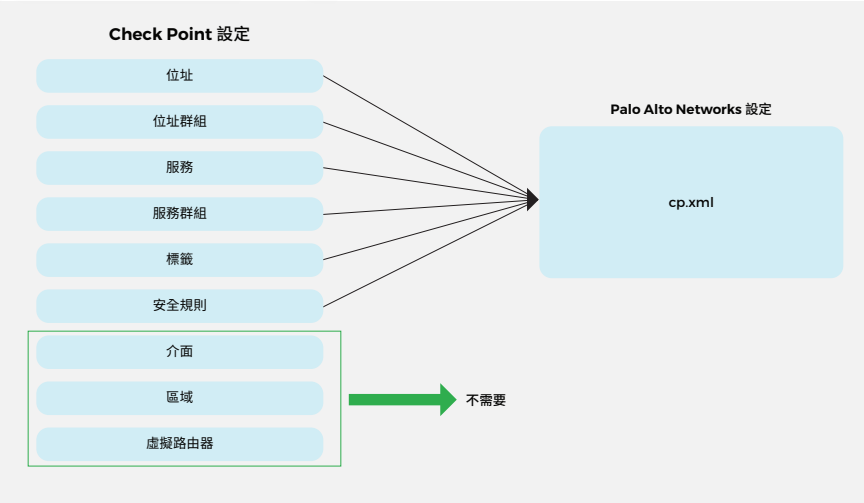


圖 15：僅必要的設定部分新增至最後的檔案

位址：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/address mode merge from cp.xml
```

位址群組：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/address-group mode merge from cp.xml
```

服務：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/service mode merge from cp.xml
```

服務群組：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/service-group mode merge from cp.xml
```

標籤：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
tag to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/tag mode merge from cp.xml
```

安全規則：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
rulebase/security/rules to-xpath /config/devices/entry[@
name='localhost.localdomain']/device-group/entry[@name='Mobile_
User_Device_Group']/post-rulebase/security/rules from cp.xml
```

我們已選擇將安全政策上傳為「post-rules」。安全區域將不會匯入，但會保存在新設定的政策中。由於我們在這個特殊設定中只移轉了七個區域，接下來唯一要做的就是在「Mobile_User_Template」範本設定中手動建立這些區域，並在 Prisma Access 外掛程式設定中執行區域對應。依預設，所有的新區域都會對應至不信任區域。

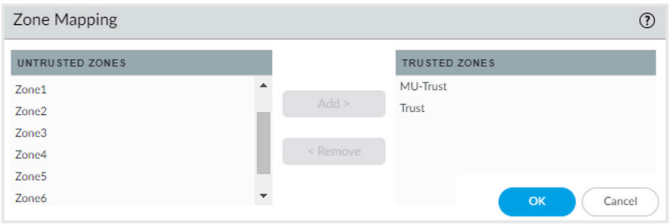


圖 16：新區域依預設對應至不信任區域。

從 Cisco ASA 裝置移轉至 Prisma Access

移轉 Cisco ASA 設定是一種簡單明瞭的程序。Cisco ASA 會利用存取控制清單 (ACL) 來允許或拒絕流量。使用 Expedition 可輕鬆地將這些 ACL 與對應的區域一併移轉至 Palo Alto Networks 格式。這些移轉會遵循我們之前為 Check Point 使用的相同流程。

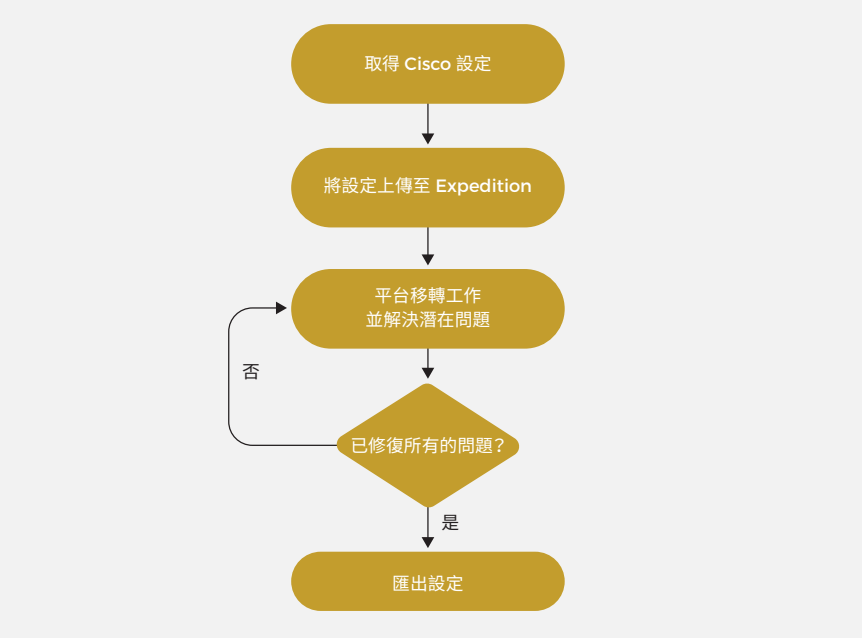


圖 17：透過 Expedition 進行移轉的高階方式

步驟 1：取得 Cisco ASA 設定並將其上傳至 Expedition

Cisco ASA 設定通常是在設備中執行「show running」命令所擷取。

步驟 2：執行移轉工作並解決潛在問題

在一般的設定中，我們會從介面設定取得對應的 Palo Alto Networks 區域。以下範例顯示了 Expedition 中介面設定的外觀：

```
介面 Gigabit Ethernet 0/3.1
  說明 DMZ-1
  vlan 74
  nameif dmz-1
  安全層級 50
  ip address 10.4.0.254 255.255.0.0 standby 10.4.0.253
```

在以上的 Expedition 輸出中，我們將在必要的區域「dmz-1」中擷取並採用安全規則。圖 18 顯示了 Expedition 中輸出的外觀。

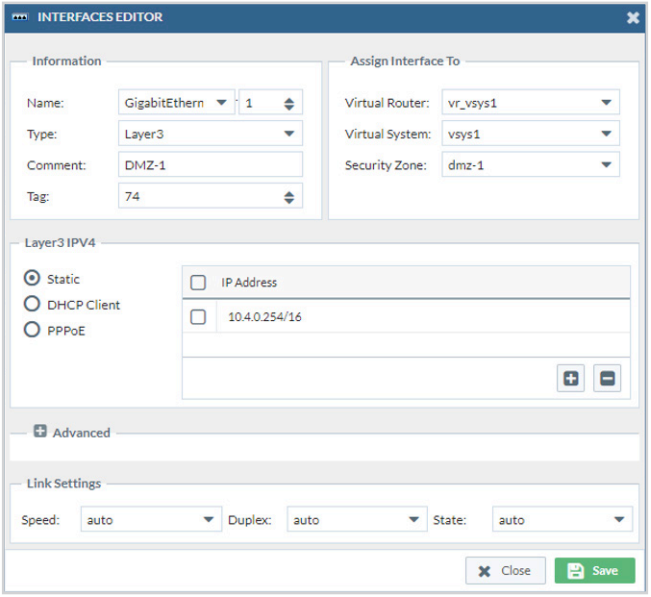


圖 18：Expedition 中的輸出

從網路功能的觀點來看，Prisma Access 並不需要下列 Cisco ASA 設定：

- **網路和虛擬路由器設定：**Prisma Access 會自動處理所有介面設定、內部路由和 NAT。您不需要移轉任何路由表 (靜態或動態項目) 或介面設定。Prisma Access 中朝向數據中心或遠端網路的靜態或動態路由設定將會以手動方式設定。

如以上所述，匯入的設定中存在的任何未使用物件都會被移除。建議您修復這些無效的物件。其中最常見的包括：

- 名稱重複的物件
- 無效服務

步驟 3：將設定上傳至 Panorama

在執行設定工作後，若要從設定載入特定物件/政策，可使用「`load partial`」命令。

雖然有多種方法可以將新預備的設定上傳至 Panorama，但我們仍建議採用以下其中一種方法：

- 從 Expedition 至 Panorama 的直接 API 呼叫
- 在 CLI 中使用「`load partial`」命令。
  - 提供精確的方式，僅選取最後 XML 設定檔案的某些部分並上傳至 Panorama

圖 19 顯示使用「`load partial`」命令的範例，也就是僅將個別和必要的部分從移轉的 Cisco 設定上傳至 Panorama (我們選擇「Mobile_User_Device_Group」裝置群組)。在此案例中，我們已將匯出的 Expedition 設定檔案命名為「cp.xml」，且我們只將它匯入至 Panorama。

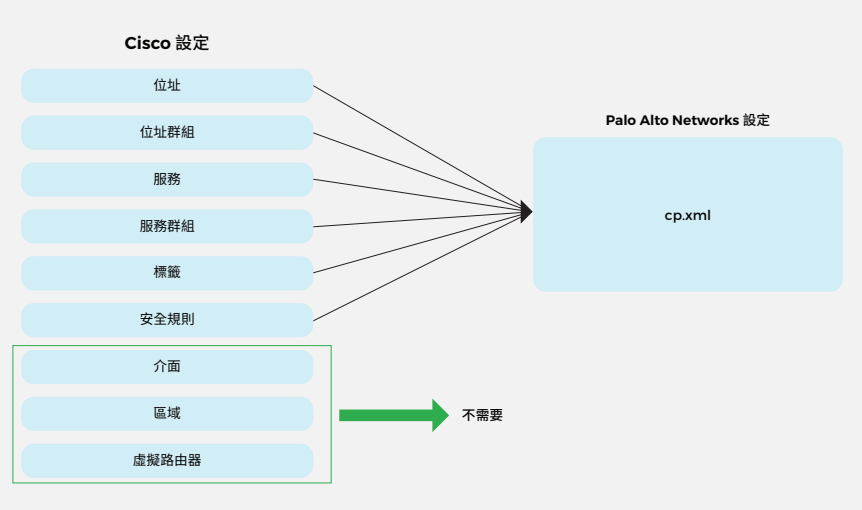


圖 19：僅必要的設定部分新增至最後的檔案

位址：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/address mode merge from cp.xml
```

位址群組：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/address-group mode merge from cp.xml
```

服務：

```
Admin@Pan# load config partial from-xpath /config/devices/entry[@
name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/service mode merge from cp.xml
```

服務群組：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/service-group to-xpath /config/devices/
entry[@name='localhost.localdomain']/device-group/entry[@
name='Mobile_User_Device_Group']/service-group mode merge
from cp.xml
```

標籤：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/tag to-xpath /config/devices/entry[@
name='localhost.localdomain']/device-group/entry[@
name='Mobile_User_Device_Group']/tag mode merge from cp.xml
```

安全規則：

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/rulebase/security/rules to-xpath /config/
devices/entry[@name='localhost.localdomain']/device-group/
entry[@name='Mobile_User_Device_Group']/post-rulebase/
security/rules from cp.xml
```

我們已選擇將安全政策上傳為「post-rules」。安全區域將不會匯入，但會保存在新設定的政策中。由於我們在這個特殊設定中只移轉七個區域，接下來唯一要做的就是在「Mobile_User_Template」範本設定中手動建立這些區域，並在 Prisma Access 外掛程式設定中執行區域對應。依預設，所有的新區域都會對應至不信任區域。

從傳統 VPN 解決方案移轉至 Prisma Access

行動使用者可使用 GlobalProtect 代理程式、無用戶端 VPN 或 PAC 檔案從任何地理位置連接至 Prisma Access。

從移轉的觀點來看，大部分從替代 VPN 解決方案的移轉都會以手動方式進行，因為廠商會使用完全不同方法來建構他們的 VPN 解決方案，且大部分的設定都互不相容。

不過，若您是從基於 Proxy 的解決方案移轉，Prisma Access 可讓您建立政策以根據包括 UDP 在內的所有通訊協定，而非只有 HTTP 或 HTTPS 來檢查流量。這意味著您不需要個別的解決方案來處理非網路流量，Prisma Access 會處理所有的工作。此外，當您從基於 Proxy 的解決方案移轉時，仍可以如第 3 章所述使用政策中的 URL 類別。在使用 GlobalProtect 代理程式時，可根據應用程式、程序名稱或路由，以最佳化的分割通道設定來取代任何 Proxy 規避設定。

若您之前並未使用任何移轉的政策，一旦您決定使用者用來連接 Prisma Access 的方式，就可以開始建立您自己的政策。您可以根據 ZTNA 原則來建立所有政策。除了啟用連線後監控來掃描威脅並監控數據遺失和潛在的憑證竊取情況以外，此方法還提供完整的內容檢查以識別網路中所有的使用者以及他們存取的應用程式。

如第 3 章所述，使用者身分 (相對於只有 IP 位址) 是 Prisma Access 所不可或缺的一部分。我們強烈建議您使用 User-ID 來識別使用者與其在網路中對應的群組，並利用此資訊來建立第 7 層政策。

您可以使用 Prisma Access 來設定多個政策類型：

- 如第 3 章所述，應用程式層級的安全政策可讓您強制執行規則並採取行動，且可視需求做為一般或特定政策。必須依序將這些政策與傳入流量進行比較。由於已套用符合流量的第一個規則，因此更特定的規則必須在更一般的規則之前套用。
- 可設定 QoS 政策以優先處理關鍵業務流量或要求低延遲的流量，例如 VoIP 或視訊會議。您也可以為企業關鍵應用程式保留最低程度的頻寬。企業的內部部署裝置依預設會遵循區別服務代碼點 (DSCP) 標記。
- 您可以設定解密政策來檢查流量以提供對於威脅的可視性，並控制通訊協定、驗證證書及處理故障。惡意內容將無法進入您的網路，敏感內容也不會隱藏為加密流量而離開您的網路。如第 3 章所述，使用網路中的解密政策會是目前的最佳實務。
- 若有需要，應用程式覆蓋政策可讓您覆蓋一般的 App-ID 來處理特定流量。在某些情況中，您可能會使用具有特定特徵碼的自訂應用程式。針對這類應用程式，若沒有任何可用的特徵碼，您可以使用應用程式覆蓋來進行較簡單的識別和報告。
- 在啟用驗證政策之後，最終使用者必須先通過驗證才能存取服務或應用程式。當使用者要求存取服務或應用程式時 (例如在造訪網頁時)，防火牆會評估驗證政策。根據相符的驗證政策規則，防火牆會提示使用者使用一種或多種方法進行驗證，例如登入和密碼、語音、SMS、推送或一次性密碼 (OTP) 驗證。

最佳實務政策規則也適用於大部分的政策類型，以協助您在雲端管理模式中透過 Prisma Access 迅速且安全地開始使用。

更多資源

請參閱我們的技術文件以深入瞭解 Panorama 管理或雲端管理的 Prisma Access。

第 5 章

將廣域網路轉換至 SASE 模式

克服舊型 WAN 的弱點

WAN 技術可用來互連位於企業總部、數據中心和遠端位置的網路。在所有提供 WAN 連線的服務中，MPLS 和公用網際網路已成為最常見的選項。服務供應商會使用 MPLS，在相同共用基礎結構中的客戶之間執行區隔和隔離以提供 WAN 服務。

總部、數據中心和分公司會使用客戶邊緣 (CE) 裝置來連接至 MPLS 網路中的供應商邊緣 (PE) 裝置。多個客戶可以共用 PE 裝置，但每個 CE 裝置都只專屬於單一客戶。從路由的觀點來看，最常使用的會是靜態路由和 BGP。

圖 20 中的實作方式顯示以下架構考量：

- 每個部署在不同地理位置的分公司都會使用 MPLS 連結以連接至數據中心和網際網路。
- 網際網路只能透過數據中心進行存取。任何直接網際網路連線都不會套用任何安全性 (例如行動使用者 IP 集區、基礎結構、數據中心和遠端子網路)。

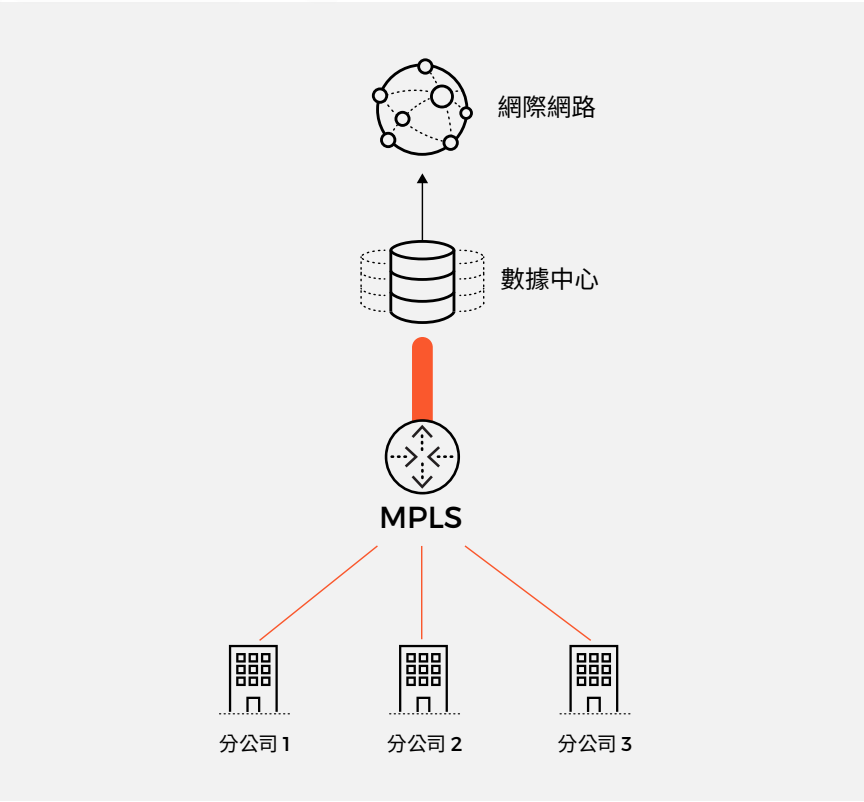


圖 20：MPLS 實作方式的簡易範例

這清楚地描述幾個架構性問題：

- 網際網路存取的回傳增加延遲性
- 遠端分公司適用的安全性不一致
- 分公司之間缺乏安全性檢查

您可以透過 Prisma Access 移轉至 SASE 模式，它可以從全球 76 個國家/地區超過 100 個地點提供雲端交付的網路骨幹。如此一來，您就可以將舊型 WAN 和安全服務完全移轉至雲端原生架構。

從架構觀點來看，將會發生以下改變：

- 每個分公司都會透過全球超過 100 個 PoP 的其中一個來連接至 Prisma Access。運用多個 PoP 可大幅提升靈活度。
- 專用的服務連線將可提供對於數據中心的存取，使每個分公司和行動使用者都能夠安全地存取資源。
- 遠端分公司和行動使用者將可使用本地網際網路分支連線。系統會直接從雲端適用安全性。
- 所有的遠端網路和行動使用者都適用一致的安全政策。
- 所有的功能都會以服務形式提供，包括擴充效能、維護資源的高可用性、套用必要的更新等等。

Prisma Access 與 SD-WAN 的整合

SD-WAN 技術可簡化 WAN 連線的管理和操作，並針對路由和路徑決策提供情報。在採用 SD-WAN 部署時，大部分的企業都會因為其 SaaS 應用程式的雲端位置而需要直接網際網路存取。

SD-WAN 解決方案可為企業提供許多優勢，例如節省成本、降低複雜度、提升部署的最佳化等，但它們必須受到適當地保護。雖然 Prisma Access 能夠與所有 SD-WAN 廠商整合，但本指南著重於 Prisma SD-WAN 所提供的更深層整合。

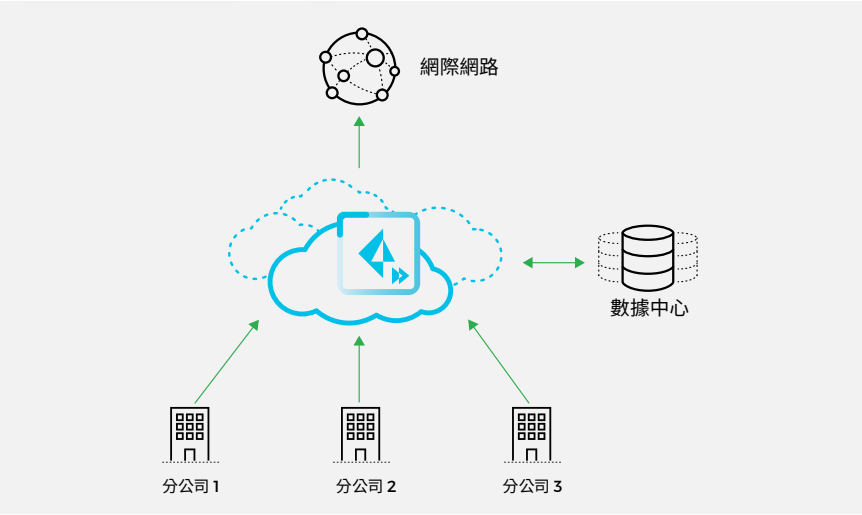


圖 21：更有效率的 WAN 架構與 Prisma Access 範例

Prisma SD-WAN (之前稱為 CloudGenix SD-WAN)，是一種新世代的解決方案，可協助您進行分公司和零售點的轉換、降低 WAN 整體擁有成本、簡化管理，同時取得對於網路流量的可視性。Prisma SD-WAN 能夠與 Prisma Access 完全整合，可針對分公司和零售點提供雲端交付安全性。

適用於 Prisma Access 的 Prisma SD-WAN CloudBlades 可讓您自動化遠端網路的部署並自動套用安全政策。此選項需要您部署一個內部部署的 Docker 容器或公有雲容器，以加快 Prisma Access 與 Panorama 所適用之 CloudBlade 之間的通訊。

下列各節將說明如何根據兩種架構情境來整合 Prisma SD-WAN 與 Prisma Access：

1. SD-WAN 與 Prisma Access 直接網際網路存取
2. SD-WAN 與區域軸輻式架構和 Prisma Access

SD-WAN 與 Prisma Access 直接網際網路存取

透過此選項，您可以使用 SD-WAN 設備提供的 IPsec 通道將遠端站台連接至 Prisma Access。此通道可用來將所有網際網路流量傳輸至 Prisma Access。數據中心應用程式流量會使用 SD-WAN 網狀架構直接傳輸至應用程式的目的地。

在此範例 (見圖 22) 中，Prisma Access 會部署一個遠端網路以連接至位於阿姆斯特丹的辦公室。此位置會使用地理上最接近的 PoP 連接至 Prisma SD-WAN 設備。

圖 23 顯示如何設定 Panorama 中的 Prisma Access 遠端網路以連接至位於阿姆斯特丹辦公室的 Prisma SD-WAN 設備。我們已使用荷蘭中心 PoP 並分配 50 Mbps 的頻寬。可設定靜態路由或 BGP，或者兩者。

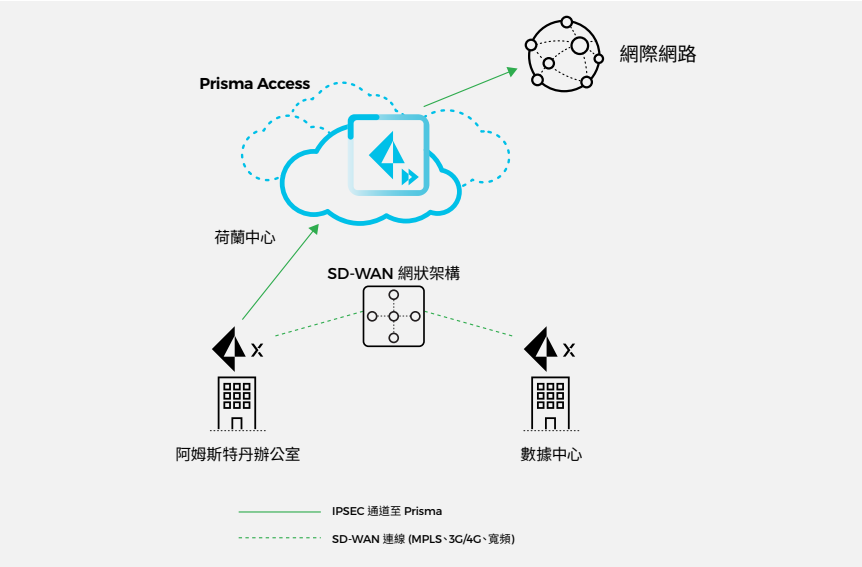


圖 22：Prisma Access 與 Prisma SD-WAN 的整合

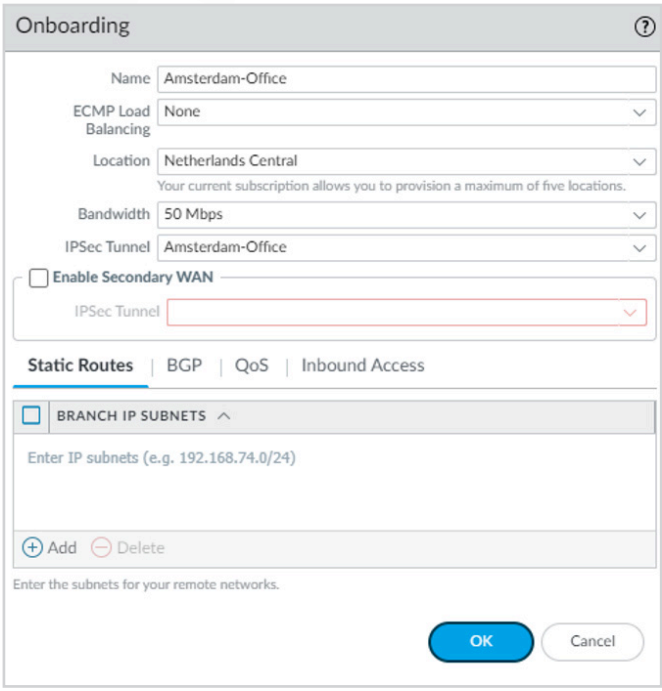


圖 23：已部署一個遠端網路的 Prisma Access

SD-WAN 與區域軸輻式架構和 Prisma Access

在此使用案例中，並非所有分公司都可直接連線至 Prisma Access。區域數據中心可在特定區域中彙總小型站台的網路流量。這類部署的一個範例就是區域分公司會有一個頻寬較低的網際網路連線。

在圖 24 中，兩個數據中心都各有一個通往個別 Prisma Access 位置的 IPsec 通道：一個通往美國東部地區，一個通往美國西部地區。每個站台上的 SD-WAN 邊緣裝置都會使用流量轉送政策來決定傳送至 Prisma Access 進行安全檢查的流量。

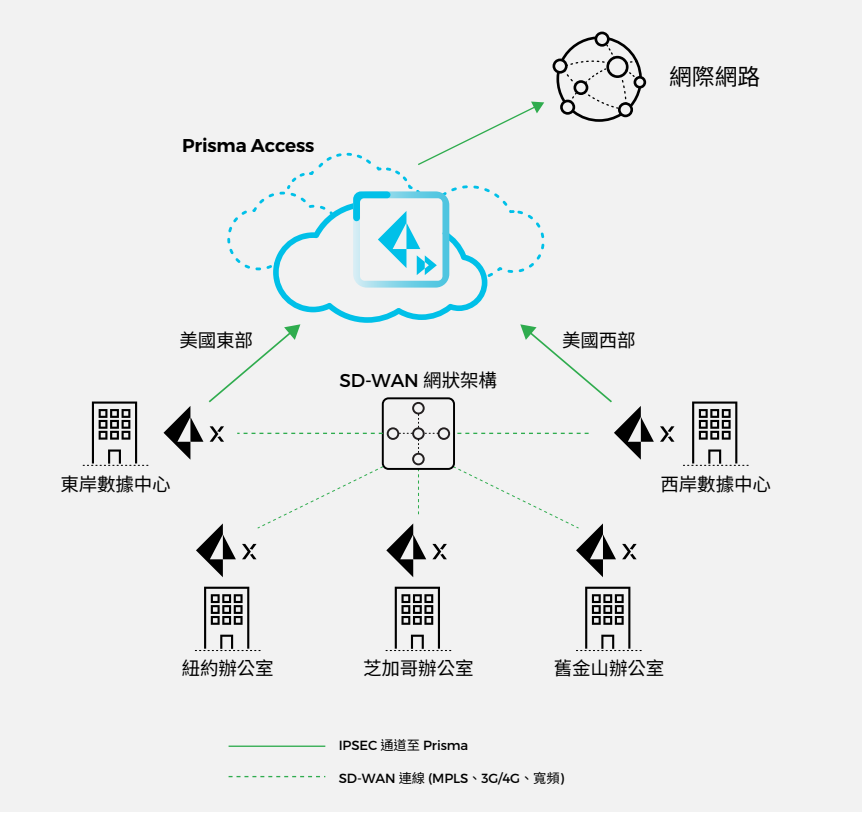


圖 24：區域軸輻式 SD-WAN 與 Prisma Access 的整合

更多資源

若要深入瞭解，請造訪我們的 Prisma SD-WAN 網站。

您也可以參閱我們的 Prisma SD-WAN 與 Prisma Access 部署指南。

特別感謝：

Jason Georgi
Matt De Vincentis
Shannon Bonfiglio
Tudor Andreescu
Don Meyer

關於 Palo Alto Networks

Palo Alto Networks 是全球網路安全產業的領導廠商，我們的技術不斷改變人員與企業的工作方式，打造以雲端為中心的未來格局。我們的目標是成為您網路安全合作夥伴的首選，為人們的數位生活方式提供安全保護。我們協助處理世界上最艱鉅的安全性挑戰，在持續的創新之中不斷掌握人工智慧、分析技術、自動化和協調技術上的最新突破。我們提供整合式平台，培養日益壯大的合作夥伴生態系統，因此始終能夠站在安全產業的最前線，為成千上萬企業的雲端、網路與行動裝置提供安全保護。我們的願景是讓世界一天比一天更安全。

如需瞭解更多資訊，請造訪 www.paloaltonetworks.com。


paloalto®
NETWORKS
PRISMA®
BY PALO ALTO NETWORKS