思科安全訪問中帶有重疊子網的站點到站點連線

目錄

簡介

本文檔介紹思科安全訪問重疊子網解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全存取管理。
- 防火牆/路由器管理。

思科建議您：

- 對思科安全訪問的管理訪問。
- 對IPSec頭端裝置（防火牆或路由器）的管理訪問

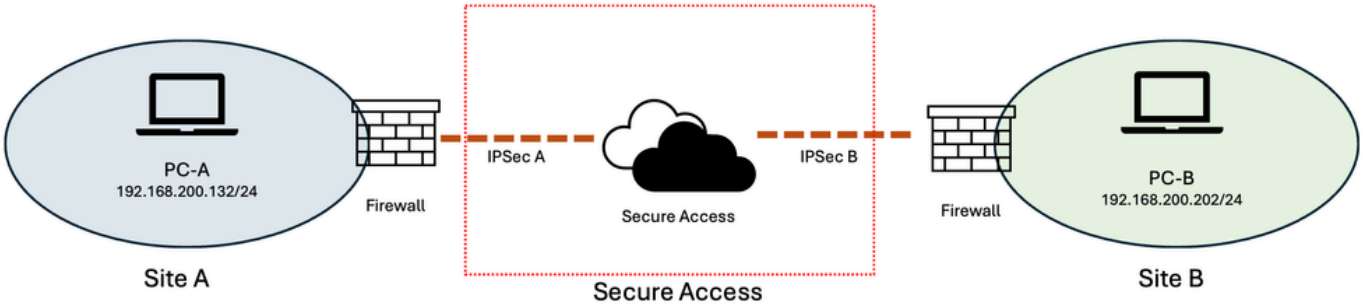
採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

開始之前

在本示例中，具有相同IP子網192.168.200.0/24的兩個不同分支站點通過兩個單獨的IPSec隧道連線到Cisco安全訪問。



影象 — 網路圖

目標是來自「站點A」的使用者可以訪問「站點B」中的資源，反之亦然。

準備和規劃

由於兩個站點使用相同的IP子網(192.168.200.0/24)，重疊的地址空間會阻止兩個站點之間的直接通訊。為了解決這一重疊問題，將分配兩個非重疊的虛擬子網來表示每個站點的資源。

在本例中：

- 站點A:10.30.30.0/24
- 站點B:10.40.40.0/24
- 兩個站點的實際子網：192.168.200.0/24

虛擬子網為每個站點提供唯一的地址空間，而實際資源繼續使用現有的192.168.200.0/24地址。

當站點A的使用者訪問位於站點B的資源時，該使用者通過站點B虛擬子網(**10.40.40.0/24**)而不是直接使用重疊的192.168.200.0/24地址空間來訪問資源。

Cisco安全存取提供一對一目的地NAT(D-NAT)功能，可將虛擬位址轉譯為對應的實際位址。D-NAT地址範圍與原始子網的大小相同。在本示例中，虛擬網路和實際網路都是/24子網，提供虛擬和實際IP地址之間的一對一對映。

舉例來說：

10.40.40.202 → 192.168.200.202

因此，D-NAT將來自站點A的發往10.40.40.202的請求轉換為192.168.200.202，從而允許該請求到達站點B的相應資源，儘管這兩個站點使用相同的基礎IP子網。

此方法有效地為每個站點建立了一個虛擬的非重疊地址空間，同時保留了資源的現有IP編址。它還在虛擬地址和實際地址之間提供一致的一對一關係，使配置更易於理解、管理和故障排除。

設定步驟

由於Cisco Secure Access的當前設計和限制，要實現此方案，需要在IPsec隧道和Cisco Secure Access後的頭端設備上進行配置。

頭端裝置是建立到Cisco Secure Access的IPsec隧道的防火牆或路由器。除了在思科安全訪問中配置D-NAT外，頭端防火牆還必須對返回流量執行源NAT(S-NAT)。

因此，該配置包含兩個部分：

1. 在Cisco安全訪問中為每個網路隧道單獨配置目標NAT(D-NAT)。
2. 在防火牆上配置源NAT(S-NAT),以確保返回流量轉換回虛擬地址空間。

配置思科安全訪問

步驟 1:從Cisco Secure Access管理門戶導航至Connect > Network Connections，然後選擇Network Tunnel Groups頁籤。

步驟 2:編輯與使用重疊子網的站點的IPsec隧道相關聯的網路隧道組。

在此範例中：

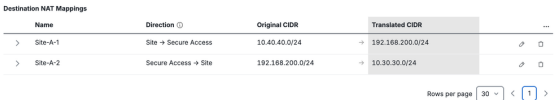
- IPSec-A =站點A的網路隧道組
- IPSec-B =站點B的網路隧道組

步驟 3:按一下所需的Network Tunnel Group旁邊的三個點選單，然後選擇Edit。

步驟 4:從左側選單中，選擇Routing頁籤，並啟用Network Address Translation(NAT)（如果尚未啟用）。

步驟 5:在Destination NAT Mappings下，按一下Add Mappings。

步驟 6:使用下表為每個網路隧道組配置D-NAT對映：

	站點A - IPSec隧道	站點B - IPSec隧道
目標NAT-1	站點→全訪問 原始CIDR:10.40.40.0/24 轉換後的CIDR:192.168.200.0/24	站點→全訪問 原始CIDR:10.30.30.0/24 轉換後的CIDR:192.168.200.0/24
目標NAT-2	安全訪→站點 原始CIDR:192.168.200.0/24 轉換後的CIDR:10.30.30.0/24	安全訪→站點 原始CIDR:192.168.200.0/24 已翻譯的CIDR:10.40.40.0/24
	 IPsec隧道站點A - D-NAT配置	 IPsec隧道站點B - D-NAT配置

附註：配置每個網路隧道組的設定後，按一下Save。當出現確認視窗時，輸入UPDATE以確認更改。對其他網路隧道組重複相同過程

配置防火牆

由於當前在處理網路隧道組後重疊的IP子網時存在限制，因此需要配置防火牆。

當Cisco安全訪問對傳入資料包執行D-NAT時，轉換後的目標地址用於將資料包傳送到目標資源。但是，在此重疊子網方案中，不會自動為返回流量執行相應的反向轉換。

因此，返回流量需要在防火牆上手動進行源NAT轉換。

關鍵要求是目標伺服器使用客戶端最初訪問的虛擬IP地址而不是伺服器實際IP地址來檢視返回流量。

範例

假設有以下幾點：

- 站點A客戶端：192.168.200.132
- 站點B Web伺服器：192.168.200.202
- 站點B虛擬子網：10.40.40.0/24
- Web伺服器的虛擬地址：10.40.40.202

站點A的客戶端使用https://10.40.40.202訪問站點B Web服務器

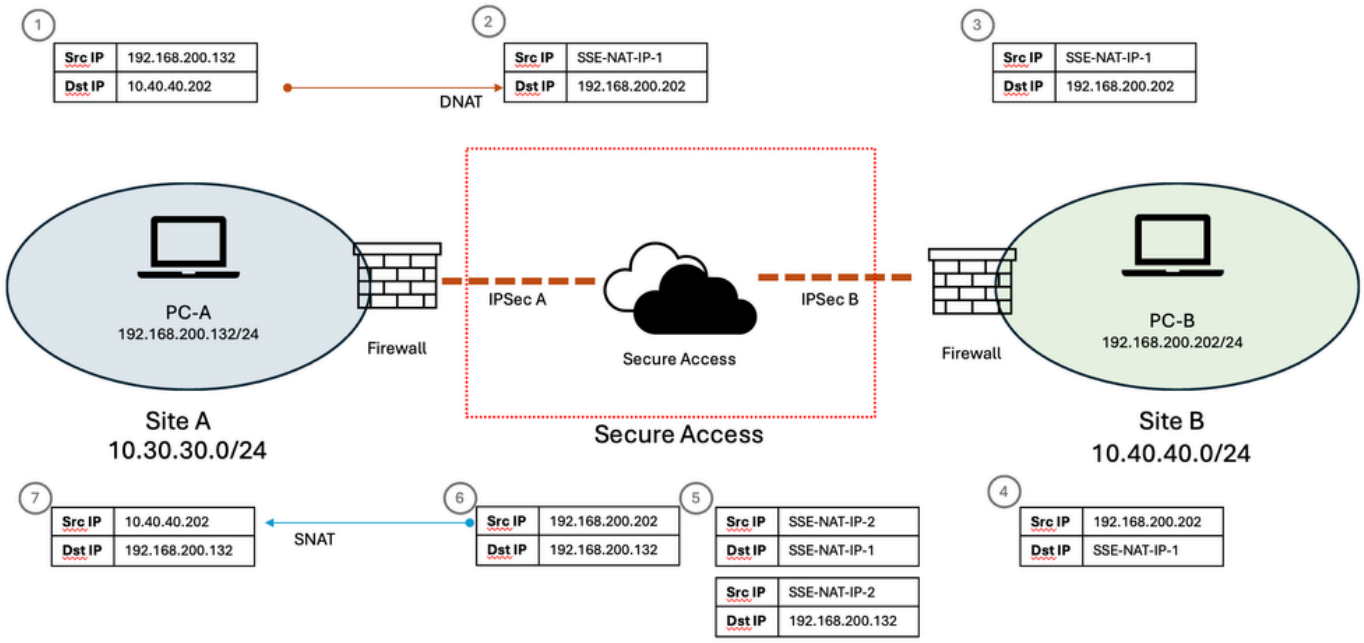
Cisco安全訪問執行D-NAT 10.40.40.202 → 192.168.200.202

然後，資料包到達地址為192.168.200.202的Web伺服器。

傳回流量發生問題。如果防火牆上沒有額外的NAT，Web伺服器會使用Source:192.168.200.202

但是，客戶端啟動了到Destination:10.40.40.202

因此，需要轉換返回流量，以便呈現給客戶端的源地址對應於虛擬地址192.168.200.202 → 10.40.40.202



影象 — 網路流

為此，防火牆對流向網路隧道組的流量執行源NAT。

在本示例中，所需的對映是192.168.200.0/24 → 10.40.40.0/24

這樣會在實際地址與其對應的虛擬地址之間建立反向的一對一關係。

一對一SNAT

如果防火牆支援整個子網的一對一源NAT，則單個NAT規則可以表示完整的/24地址範圍。

舉例來說：

實際來源	轉換後的源
192.168.200.0/24	10.40.40.0/24

這會導致對映如192.168.200.202 → 10.40.40.202和192.168.200.203 → 10.40.40.203

同一一對一關係適用於整個子網。

沒有一對一SNAT的防火牆

如果防火牆不支援整個子網的一對一源NAT，則需要單獨配置每個所需的對映。

例如，對於Web伺服器：

- 來源 IP:192.168.200.202
- 源介面：網路通道組
- 流量方向：傳入
- 轉換後的源IP:10.40.40.202

產生的轉換為192.168.200.202 → 10.40.40.202

對於需要通過虛擬子網訪問的每個資源，均可應用相同的方法。

這可確保通訊的兩個方向都保持虛擬編址方案，並且客戶端從建立連線時使用的同一個虛擬IP地址接收響應。

相關資訊

Cisco安全訪問NAT對映/網路隧道組配置：https://securitydocs.cisco.com/docs/csa/olh/168842.dita

思科安全訪問網路隧道組配置和路由參考：https://securitydocs.cisco.com/docs/csa/olh/118900.dita

思科安全訪問故障排除和基本資料收集指南：https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。