通過L2L隧道的ASA VPN客戶端連線配置示例

目錄

簡介

本文說明如何配置思科自適應安全裝置(ASA)，以允許從Lan到Lan(L2L)對等地址進行遠端VPN客戶端連線。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA
- 遠端存取VPN
- LAN到LAN VPN

採用元件

本文檔中的資訊基於運行軟體版本8.4(7)的Cisco 5520系列ASA。

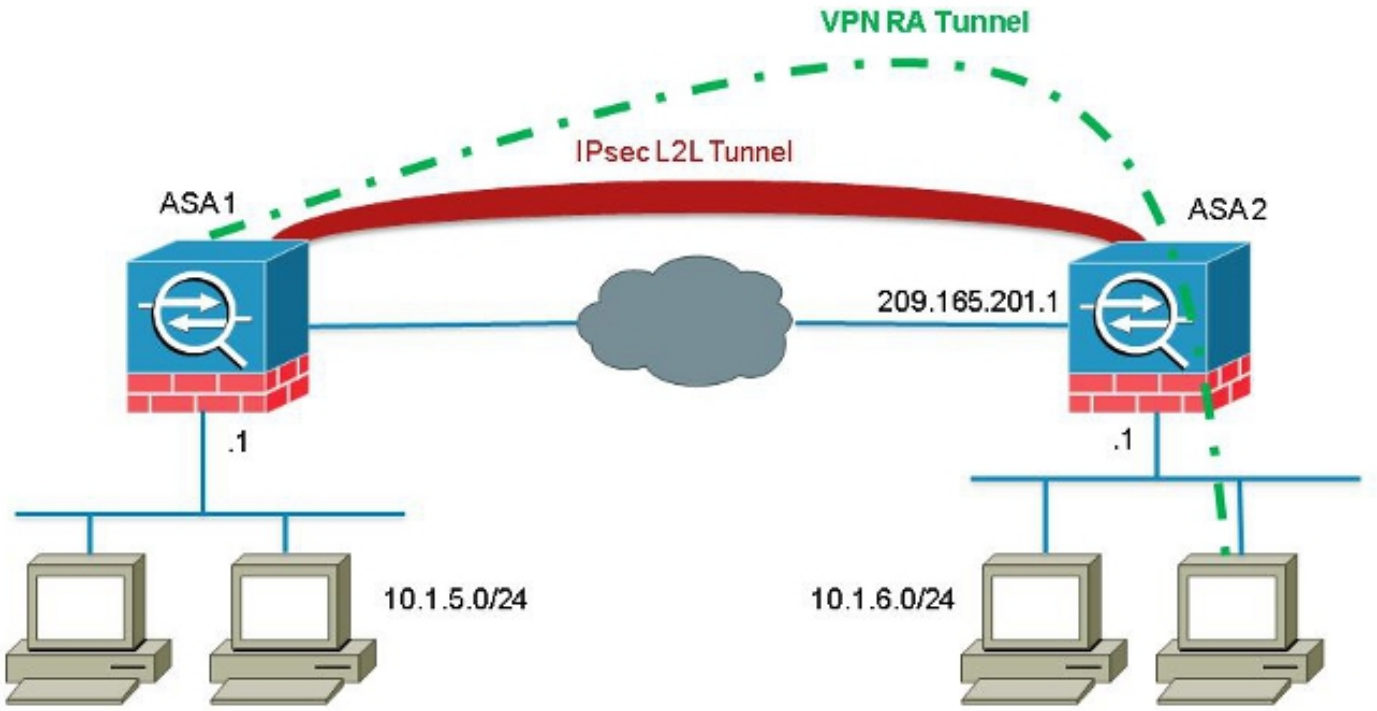
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

雖然VPN客戶端嘗試通過L2L隧道建立連線的情形並不常見，但管理員可能希望向某些遠端使用者

分配特定許可權或訪問限制，並指示他們在需要訪問這些資源時使用軟體客戶端。

> **附註**：此方案在過去是有效的，但在將頭端ASA升級到版本8.4(6)或更高版本後，VPN客戶端無法再建立連線。



思科錯誤ID CSCuc75090引入了行為更改。以前，對於專用網際網路交換(PIX)，當網際網路協定安全(IPSec)代理與加密對映訪問控制清單(ACL)不匹配時，它會繼續檢查清單後面的條目。這包括未指定對等體的動態加密對映的匹配項。

這被視為一個漏洞，因為遠端管理員可以訪問頭端管理員在配置靜態L2L時不想要的資源。

建立了一個修復程式，新增了一個檢查，以防止在沒有對等體的情況下與加密對映條目匹配，因為它已經檢查了與該對等體匹配的對映條目。但是，這會影響本文討論的場景。具體而言，嘗試從L2L對等地址連線的遠端VPN客戶端無法連線到頭端。

設定

使用本節配置ASA以允許從L2L對等地址進行遠端VPN客戶端連線。

新增新動態條目

為了允許來自L2L對等體地址的遠端VPN連線，必須新增包含相同對等體IP地址的新動態條目。

> **附註**：您還必須保留另一個沒有對等體的動態條目，以便來自Internet的任何客戶端也能連線。

以下是先前的動態加密對映工作組態範例：

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

以下是已配置新動態條目的動態加密對映配置：

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。