通過IPsec LAN到LAN的ASA無客戶端SSL VPN流量配置示例

目錄

簡介

本檔案介紹如何連線到Cisco Adaptive Security Appliance(ASA)Clientless SSLVPN入口網站，並存取位於透過IPsec LAN到LAN通道連線的遠端位置的伺服器。

必要條件

需求

思科建議您瞭解以下主題：

- 無客戶端SSL VPN配置。
- LAN到LAN VPN配置

採用元件

本文檔中的資訊基於運行版本9.2(1)的ASA 5500-X系列，但它適用於所有ASA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。在對實際網路進行更改之前，請確保您已瞭解任何命令可能造成的影響。

背景資訊

來自無客戶端SSLVPN會話的流量通過LAN到LAN隧道時，請注意，存在兩個連線：

- 從客戶端到ASA
- 從ASA到目的主機。

對於ASA到目標主機連線，使用距離目標主機「最近」的ASA介面的IP地址。因此，LAN到LAN的相關流量必須包含從該介面地址到遠端網路的代理身份。

附註： 如果書籤使用智慧隧道，則仍會使用距離目標最近的ASA介面的IP地址。

設定

在此圖中，兩個ASA之間有一個LAN到LAN隧道，允許流量從192.168.10.x傳輸到192.168.20.x。

決定該通道相關流量的存取清單：

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

如果無客戶端SSLVPN使用者嘗試與192.168.20.x網路上的主機通訊，則ASA1使用209.165.200.225地址作為該流量的源。因為LAN到LAN存取控制清單(ACL)不包含209.168.200.225作為代理身分，所以流量不會透過LAN到LAN通道傳送。

為了透過LAN到LAN通道傳送流量，必須將新的存取控制專案(ACE)新增到相關流量ACL中。

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

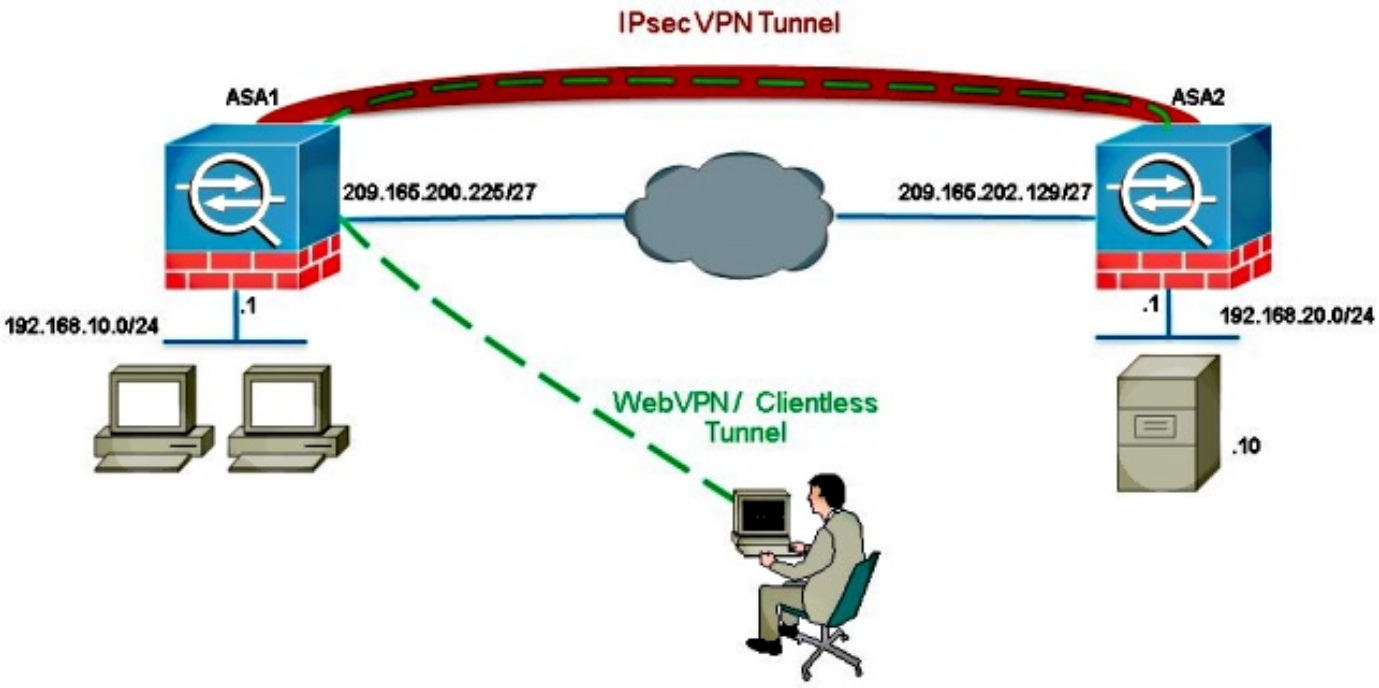
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

同樣的原理適用於無客戶端SSLVPN流量需要關閉其進入的相同介面的配置，即使它不應通過LAN到LAN隧道也是如此。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



通常，ASA2執行192.168.20.0/24的埠地址轉換(PAT)以提供網際網路訪問。在這種情況下，當來自ASA 2上192.168.20.0/24的流量進入209.165.200.225時，應將其排除在PAT進程之外。否則，響應將不會通過LAN到LAN隧道。例如：

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

- **show crypto ipsec sa**-使用此命令驗證是否已建立ASA1代理IP地址與遠端網路之間的安全關聯(SA)。檢查無客戶端SSLVPN使用者訪問該伺服器時加密和解密計數器是否增加。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果未生成安全關聯，則可以使用IPsec調試來查明失敗的原因：

- **debug crypto ipsec <level>**

  附註：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。