配置兩個站點到站點隧道之間的流量迴轉傳輸

目錄

簡介

本文檔介紹如何在單個介面上的兩個VPN隧道之間轉發VPN流量。

必要條件

需求

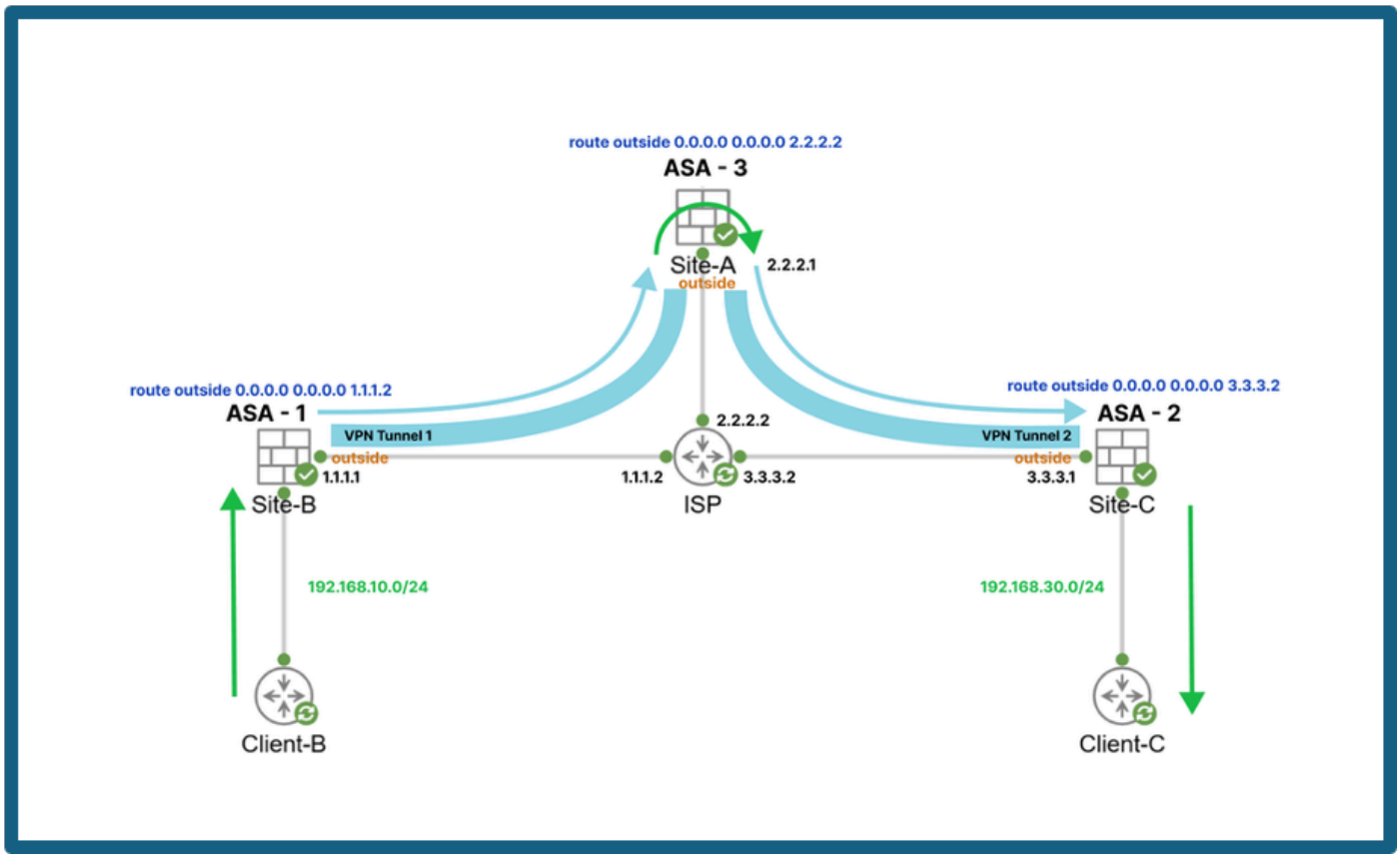
思科建議瞭解以下主題：
·對基於策略的站點到站點VPN有基礎瞭解
·使用ASA命令列體驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：
·自適應安全裝置(ASA)版本9.20
· IKEv1

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。

拓撲



拓撲

背景資訊

此組態會示範如何將流量從一站點到站點通道重新導向到同一裝置上的另一個通道。為了說明此設定，我們使用了代表站點A、站點B和站點C的三個ASA。

組態

本節概述了允許通過ASA-3（站點A）從ASA-1（站點B）到ASA-2（站點C）的流量所需的配置。

我們配置了兩個VPN隧道：

- VPN隧道1 :站點B和站點A之間的VPN隧道
- VPN通道2:站點C和站點A之間的VPN隧道

有關如何在ASA上建立基於策略的VPN隧道的詳細指導，請參閱Cisco文檔中的ASA配置部分：[在ASA和Cisco IOS XE路由器之間配置站點到站點IPSec IKEv1隧道]

ASA（站點B）配置

我們需要在ASA 1外部介面上的VPN隧道1的加密訪問清單中允許從Site-B網路到Site-C網路的流量。
在此案例中，介面是從192.168.10.0/24到192.168.30.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Nat異常：

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

VPN隧道1的加密對映：

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA（站點C）加密配置

在ASA 2外部介面上的VPN隧道2的加密訪問清單中，允許從Site-C網路到Site-B網路的流量。
在此案例中，介面是從192.168.30.0/24到192.168.10.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Nat異常：

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

VPN通道2的密碼編譯對應：

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA（站點A）加密配置

在VPN隧道1的加密訪問清單中允許從Site-C網路到Site-B網路的流量，在Site-A的ASA外部介面上的VPN隧道2的加密訪問清單中允許從Site-B網路到Site-C網路的流量，該流量與在_ ASA上配置的流量方向相反。

在此案例中，VPN通道1從192.168.30.0/24到192.168.10.0/24,VPN通道2從192.168.10.0/24到192.168.30.0/24

Crypto Access-list:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

VPN隧道1和2的加密對映配置：

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

除此之外，由於我們需要將流量從具有相同安全級別的同一介面的外部路由到外部，我們還需要配置命令：

```
same-security-traffic permit intra-interface
```

從站點B到站點C的流量

讓我們考慮從Site-B到Site-c的從192.168.10.0/24到192.168.30.0/24的流量。

站點B（源）

1.從192.168.10.0/24 network(Site-B)發起、目的地為192.168.30.0/24 network(Site-C)的流量會根據配置的路由表路由到ASA-1的外部介面。

2.一旦流量到達ASA-1，它就會匹配在ASA-1上配置的加密訪問清單110。這將觸發使用VPN隧道1對流量進行加密，該隧道會將資料安全傳送到Site-A。

站點A（中級）

1.來自站點A ASA外部介面192.168.10.0/24 to 192.168.30.0/24 arrives的加密流量。
2. 在Site-A，VPN隧道1解密流量以恢復原始負載。
3. 然後，在站點A的ASA外部介面使用VPN隧道2對解密的流量進行重新加密。

站點C（目標）

1. 來自192.168.10.0/24 to 192.168.30.0/24 reaches的加密流量通過Site-C的ASA-2的外部介面。

2. ASA-2使用VPN隧道2解密流量，並將資料包轉發到Site-C的LAN端，然後將其傳送到192.168.30.0/24 network內的目標目的地。

將流量從Site-C反向到Site-B

來源為Site-C(192.168.30.0/24) and)且目的地為Site-B(192.168.10.0/24)的反向流量會生成相同的流程，但方向相反：
1.在站點C，流量在傳送到站點A之前由VPN隧道2加密。
2.在站點A，流量通過VPN隧道2解密，然後使用VPN隧道1重新加密，然後轉發到站點B。
3.在Site-B，流量通過VPN隧道1解密並傳送到192.168.10.0/24 network。

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）。