配置两个站点到站点隧道之间的流量发夹

目录

简介

本文档介绍如何在单个接口上的两个VPN隧道之间转发VPN流量。

先决条件

要求

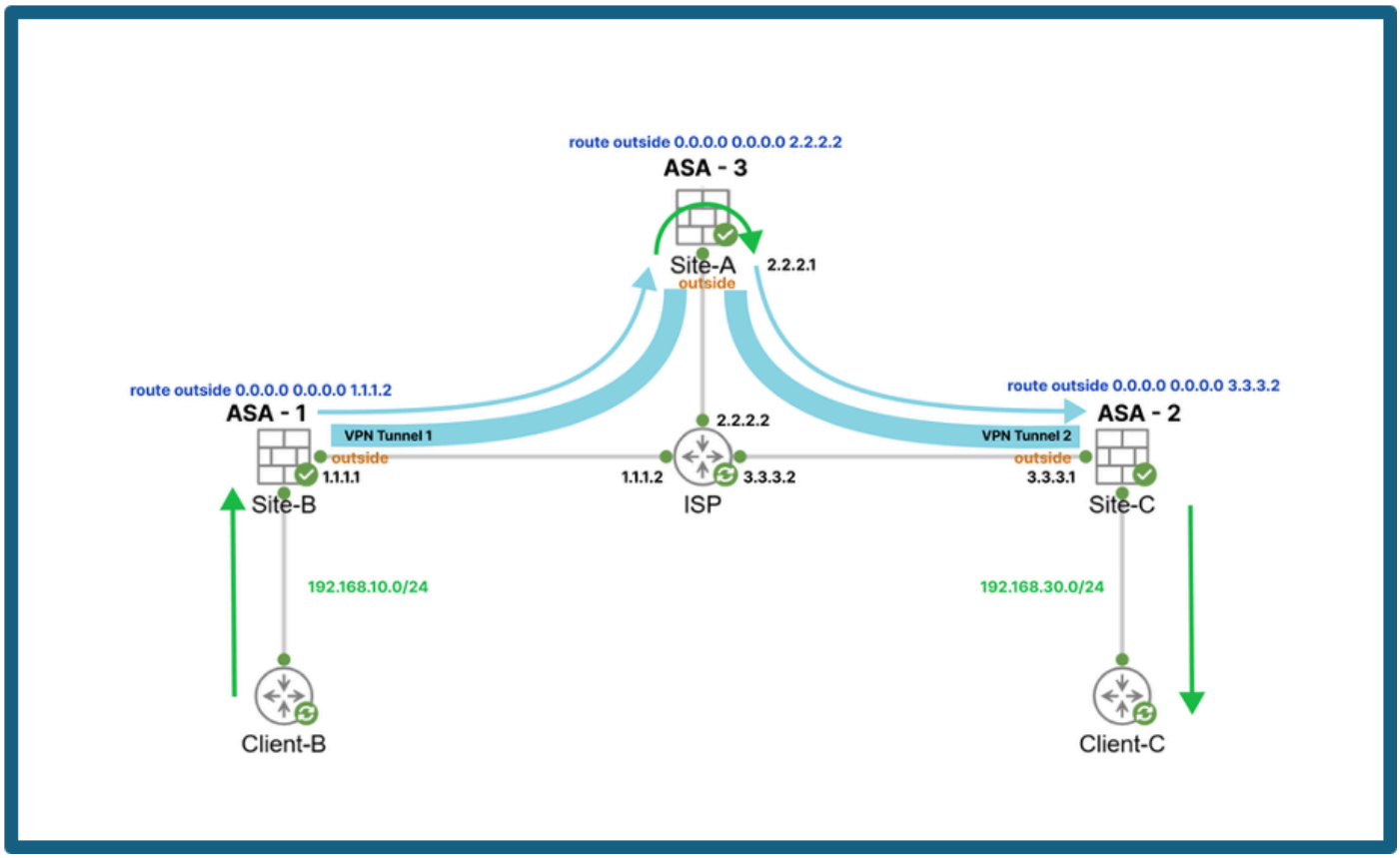
建议掌握下列主题的相关知识：
·基本了解基于策略的站点到站点VPN
·使用ASA命令行的体验

使用的组件

本文档中的信息基于以下软件和硬件版本：
·自适应安全设备(ASA)版本9.20
· IKEv1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

拓扑



拓扑

背景信息

此配置演示如何将流量从一个站点到站点隧道重定向到同一设备上的另一个站点。为了说明此设置，我们使用了代表站点A、站点B和站点C的三个ASA。

配置

本节概述允许通过ASA-3（站点A）从ASA-1（站点B）到ASA-2（站点C）的流量所需的配置。

我们配置了两个VPN隧道：

- VPN隧道1:站点B和站点A之间的VPN隧道
- VPN隧道2:站点C和站点A之间的VPN隧道

有关如何在ASA上创建基于策略的VPN隧道的详细指导，请参阅Cisco文档中的ASA配置部分：[在ASA和Cisco IOS XE路由器之间配置站点到站点IPSec IKEv1隧道]

ASA（站点B）配置

我们需要在ASA 1外部接口上的VPN隧道1的加密访问列表中允许从站点B网络到站点C网络的流量。
在本场景中，它从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异常：

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

VPN隧道1的加密映射：

```
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（站点C）加密配置

在ASA 2外部接口上的VPN隧道2的加密访问列表中，允许从站点C网络到站点B网络的流量。
在本场景中，它从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异常：

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

VPN隧道2的加密映射：

```
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（站点A）加密配置

在VPN隧道1的加密访问列表中允许从站点C网络到站点B网络的流量，在站点A的ASA外部接口的VPN隧道2的加密访问列表中允许从站点B网络到站点C网络的流量，该列表与我们在_ ASA上配置的方向相反。

在本场景中，对于VPN隧道1，从192.168.30.0/24到192.168.10.0/24，对于VPN隧道2，从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的加密映射配置：

```
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，由于我们需要将流量从具有相同安全级别的同一接口的外部路由到外部，因此还需要配置以下命令：

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

从站点B到站点C的流量

让我们考虑从Site-B向Site-c发起从192.168.10.0/24到192.168.30.0/24的流量。

站点B（源）

1.从192.168.10.0/24 network(Site-B)发起并发往192.168.30.0/24 network(Site-C)的流量会根据配置的路由表路由到ASA-1的外部接口。

2.一旦流量到达ASA-1，它就会与ASA-1上配置的加密访问列表110匹配。这将触发使用VPN隧道1对流量进行加密，VPN隧道1会将数据安全发送到站点A。

站点A（中级）

1.来自站点A ASA外部接口上192.168.10.0/24 to 192.168.30.0/24 arrives的加密流量。
2. 在Site-A上，VPN隧道1解密流量以恢复原始负载。
3. 然后，使用VPN隧道2在站点A的ASA的外部接口重新加密解密的流量。

站点C（目标）

1. 来自192.168.10.0/24 to 192.168.30.0/24 reaches的加密流量到达Site-C的ASA-2的外部接口。

2. ASA-2使用VPN隧道2解密流量并将数据包转发到Site-C的LAN端，然后将其传送到192.168.30.0/24 network内的预定目标。

将流量从Site-C反向到Site-B

从Site-C(192.168.30.0/24) and)发往Site-B(192.168.10.0/24)的反向数据流会导致相同的过程，但方向相反：
1.在Site-C，流量在发送到Site-A之前由VPN隧道2加密。
2.在站点A，流量由VPN隧道2解密，然后在转发到站点B之前使用VPN隧道1重新加密。
3.在Site-B，流量通过VPN隧道1解密并传送到192.168.10.0/24 network。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。