在思科安全访问中具有重叠子网的站点到站点连接

目录

简介

先决条件

- 要求
- 使用的组件

开始使用前

准备和规划

配置步骤

- 配置思科安全访问

相关内容

简介

本文档介绍思科安全访问中的重叠子网解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全访问管理

Cisco 建议您：

- 对思科安全访问的管理访问

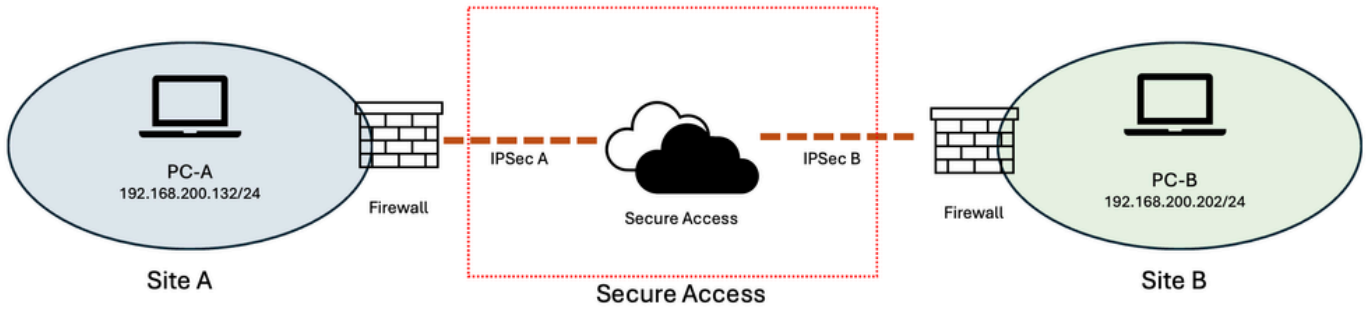
使用的组件

本文档不限于特定的软件和硬件版本。

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。

开始使用前

在本示例中，有两个使用相同IP子网192.168.200.0/24的分支机构站点，并通过两个单独的IPsec隧道连接到思科安全访问。



图像 — 网络图

目标是站点A的用户可以访问站点B中的资源，反之亦然。

准备和规划

由于两个站点使用相同的IP子网(192.168.200.0/24)，重叠的地址空间会阻止两个站点之间的直接通信。为了解决这一重叠问题，需要分配两个非重叠的虚拟子网来代表每个站点的资源。

对于此示例：

- 站点A:10.30.30.0/24
- 站点B:10.40.40.0/24
- 两个站点的实际子网：192.168.200.0/24

虚拟子网为每个站点提供唯一的地址空间，而实际资源继续使用其现有的192.168.200.0/24地址。

当站点A的用户访问站点B中的资源时，该用户通过站点B虚拟子网(10.40.40.0/24))访问资源，而不是直接使用重叠的192.168.200.0/24地址空间。

思科安全访问提供一对一目标NAT(D-NAT)功能，可将虚拟地址转换为对应的实际地址。D-NAT地址范围与原始子网的大小相同。在本示例中，虚拟网络和实际网络都是/24子网，提供虚拟和实际IP地址之间的一对一映射。

例如：

10.40.40.202 → 192.168.200.202

因此，D-NAT会将来自站点A发往10.40.40.202的请求转换为192.168.200.202，从而允许该请求到达站点B的相应资源，尽管两个站点使用相同的基础IP子网。

此方法可以为每个站点有效地创建虚拟的非重叠地址空间，同时保留资源的现有IP编址。它还在虚拟地址和实际地址之间提供一致的一对一关系，使配置更易于理解、管理和故障排除。

配置步骤

因此，配置包含两个部分：

1. 在一个网络隧道的思科安全访问中配置目标NAT(D-NAT)。（在本示例中，站点B）
2. 为其他网络隧道在Cisco安全访问中配置静态路由。（在本示例中为Site A）

配置思科安全访问

步骤 1：从Cisco Secure Access管理门户导航到Connect > Network Connections，然后选择Network Tunnel Groups选项卡。

步骤 2：编辑与使用重叠子网的站点的IPsec隧道相关联的网络隧道组。

在本例中：

- IPsec-A =站点A的网络隧道组
- IPsec-B =站点B的网络隧道组

步骤 3：点击所需网络隧道组旁边的三点菜单并选择编辑。

步骤 4：对于站点B，配置目标NAT映射,

步骤 4-1:从左侧菜单中选择Routing选项卡，并启用Network Address Translation(NAT)（如果尚未启用）。

步骤 4-2:在Destination NAT Mappings下，单击Add Mappings。

步骤 4-3:使用此表为网络隧道组配置D-NAT映射。

步骤 4-4:保存更改。

注意：配置每个网络隧道组的设置后，单击Save。出现确认窗口时，输入UPDATE确认更改。对其他网络隧道组重复相同的过程

步骤 5：对于站点A，配置静态路由,

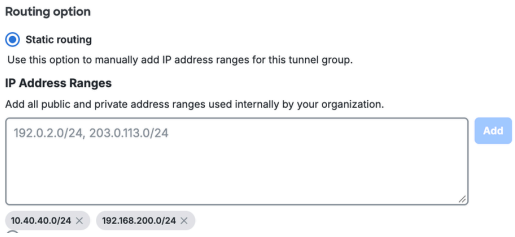
步骤 5-1:从左侧菜单中选择Routing选项卡，并启用Static Routing（如果尚未启用）。

步骤 5-2:在IP Address Ranges部分中输入subnets和virtual 子网。

步骤 5-3:使用此表配置网络隧道组的路由。

步骤 5-4:保存更改。

	站点A - IPsec隧道	站点B - IPsec隧道
目标NAT-1	不适用	站点→全访问 原始CIDR:192.168.200.0/24 转换后的CIDR:10.40.40.0/24
目标NAT-2	不适用	安全访→站点 原始CIDR:192.168.200.0/24 转换后的CIDR:10.30.30.0/24

路由	IP 地址范围: 10.40.40.0/24 192.168.200.0/24	不适用
	 IPsec隧道站点A — 静态路由配置	 IPsec隧道站点B - D-NAT配置

相关内容

[思科安全访问NAT映射/网络隧道组配置]

[思科安全访问网络隧道组配置和路由参考]

[思科安全访问故障排除和基本数据收集指南]

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）。