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

本文档介绍思科安全访问重叠子网解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全访问管理。
- 防火墙/路由器管理。

Cisco 建议您：

- 对思科安全访问的管理访问。
- 对IPSec头端设备（防火墙或路由器）的管理访问

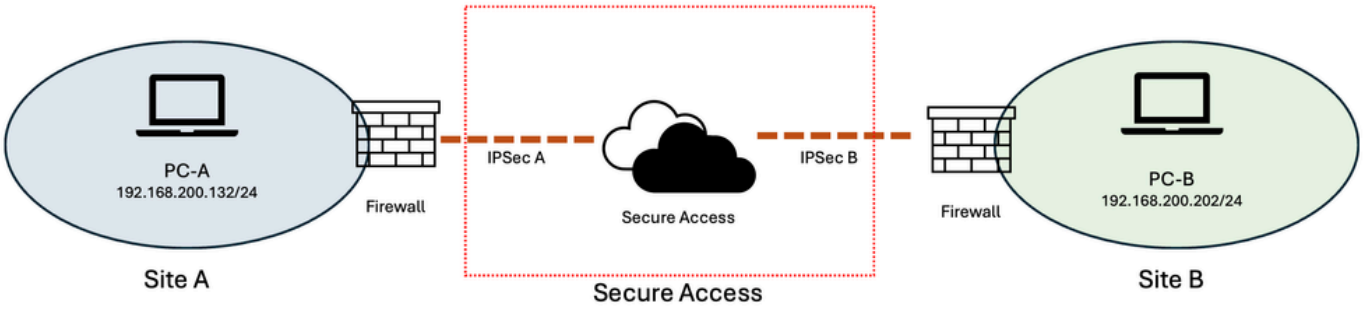
使用的组件

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，有两个具有相同IP子网192.168.200.0/24的不同分支站点，它们通过两个单独的IPSec隧道连接到Cisco安全访问。



图像 — 网络图

目标是从“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的用户访问位于站点B的资源时，该用户通过站点B虚拟子网(**10.40.40.0/24**)而不是直接使用重叠的192.168.200.0/24地址空间来访问资源。

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的发往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，尽管这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

由于Cisco安全访问的当前设计和限制，实现此场景需要在IPsec隧道和Cisco安全访问后的头端设备上进行配置。

前端设备是建立到Cisco安全访问的IPsec隧道的防火墙或路由器。除了在思科安全访问中配置D-NAT外，前端防火墙还必须对返回流量执行源NAT(S-NAT)。

因此，配置包含两个部分：

1. 在Cisco安全访问中分别为每个网络隧道配置目标NAT(D-NAT)。
2. 在防火墙上配置源NAT(S-NAT),以确保返回流量转换回虚拟地址空间。

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：

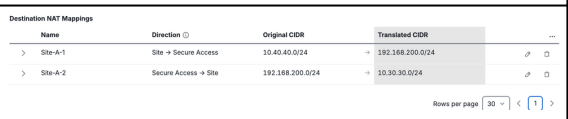
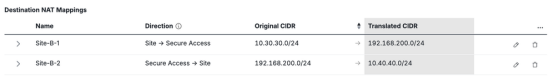
- IPSec-A =站点A的网络隧道组
- IPSec-B =站点B的网络隧道组

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：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 5：在Destination NAT Mappings下，单击Add Mappings。

步骤 6：使用此表为每个网络隧道组配置D-NAT映射：

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

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

配置防火墙

防火墙配置是必需的，因为当前在处理网络隧道组后面重叠的IP子网时存在限制。

当思科安全访问对传入数据包执行D-NAT时，转换后的目标地址用于将数据包传送到目标资源。但是，在此重叠子网方案中，不会自动对返回流量执行相应的反向转换。

因此，返回流量需要在防火墙上进行手动源NAT转换。

关键要求是，目标服务器使用客户端最初访问的虚拟IP地址（而不是服务器的实际IP地址）看到返回流量。

示例

假设以下情况：

- 站点A客户端：192.168.200.132
- 站点B Web服务器：192.168.200.202
- 站点B的虚拟子网：10.40.40.0/24
- 网络服务器的虚拟地址：10.40.40.202

站点A的客户端使用https://10.40.40.202访问站点B Web服务器

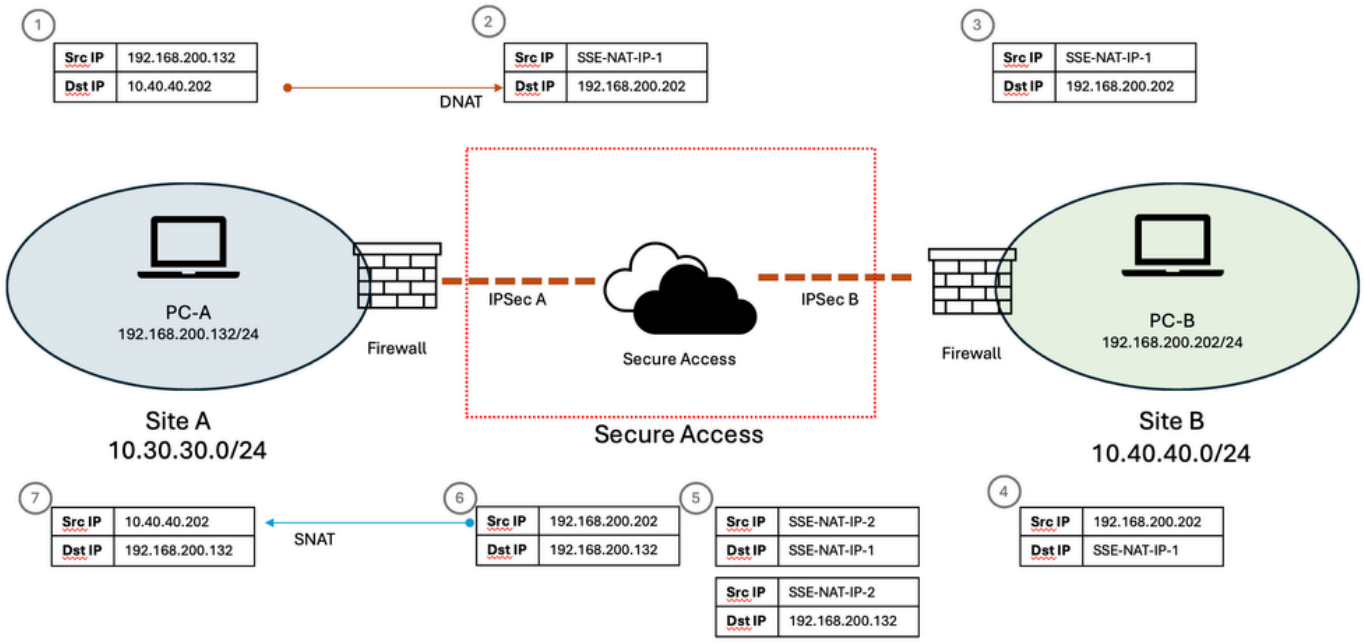
Cisco安全访问执行D-NAT 10.40.40.202 → 192.168.200.202

然后，数据包到达地址为192.168.200.202的Web服务器。

返回流量出现问题。如果防火墙上没有附加NAT，则Web服务器会使用Source:192.168.200.202

但是，客户端启动了到目标的连接：10.40.40.202

因此，需要转换返回流量，以便提供给客户端的源地址与虚拟地址192.168.200.202 → 10.40.40.202对应



图像 — 网络流

为此，防火墙对流向网络隧道组的流量执行源NAT。

在本示例中，所需的映射为192.168.200.0/24 → 10.40.40.0/24

这会在实际地址及其对应的虚拟地址之间创建反向的一对一关系。

一对一SNAT

如果防火墙支持整个子网的一对一源NAT，则单个NAT规则可以代表完整的/24地址范围。

例如：

实际来源	转换后的源
192.168.200.0/24	10.40.40.0/24

这会导致映射，例如192.168.200.202 → 10.40.40.202和192.168.200.203 → 10.40.40.203

相同的一对一关系适用于整个子网。

没有一对一SNAT的防火墙

如果防火墙不支持整个子网的一对一源NAT，则需要单独配置每个所需的映射。

例如，对于Web服务器：

- 源 IP：192.168.200.202
- 来源接口:网络隧道组
- 流量方向：入站
- 转换后的源IP:10.40.40.202

产生的转换为192.168.200.202 → 10.40.40.202

对于需要通过虚拟子网访问的每个资源，可采用相同的方法。

这可确保通信的两个方向都保持虚拟编址方案，并且客户端从建立连接时所使用的同一虚拟IP地址接收响应。

相关信息

Cisco安全访问NAT映射/网络隧道组配置：https://securitydocs.cisco.com/docs/csa/olh/168842.dita

思科安全访问网络隧道组配置和路由参考：https://securitydocs.cisco.com/docs/csa/olh/118900.dita

思科安全访问故障排除和基本数据收集指南：https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

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）。