安全访问迪拜DC故障修复步骤

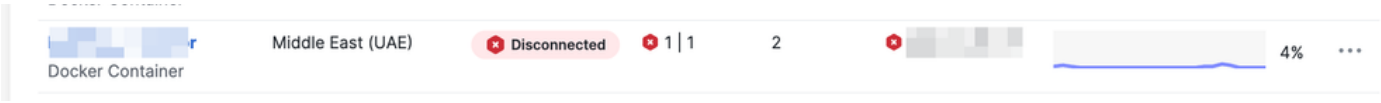
目录

简介

本文档包含3月2日Secure Access Dubai DC事件的补救步骤。
https://status.sse.cisco.com/incidents/7h28mb7mr5zl

资源连接器

已部署的资源连接器将显示为从安全访问控制面板断开连接：



已部署的资源连接器绑定到单个安全访问区域，并且不能通过配置更改进行修改。

为了修复此问题，受影响的客户需要遵循以下概述的步骤：

1.部署新的资源连接器

2.在新区域（孟买或海德拉巴）创建连接器组

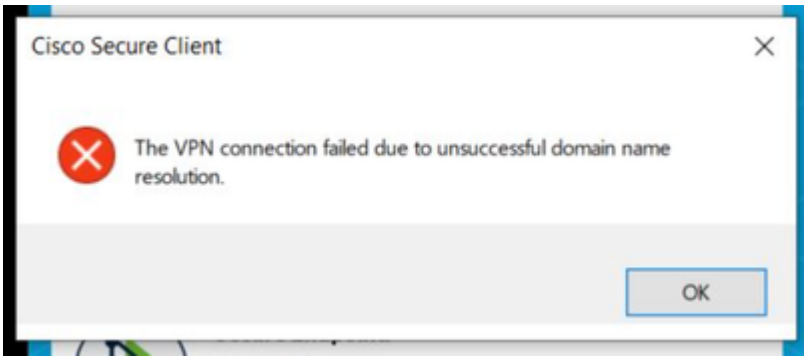
2.将专用资源分配给新的连接器组

有关部署资源连接器的详细步骤，请参阅《资源连接器部署指南》：

远程访问VPN配置文件

远程访问VPN客户端可能由于不同错误而无法建立连接。

示例错误：



仅在迪拜DC拥有远程访问VPN配置文件的组织：

请按以下步骤操作：
·选择最近的可用数据中心（孟买或海德拉巴）作为迁移目标。
·配置VPN IP池和配置文件以匹配组织的当前会话负载，镜像现有的ME-Central设置。

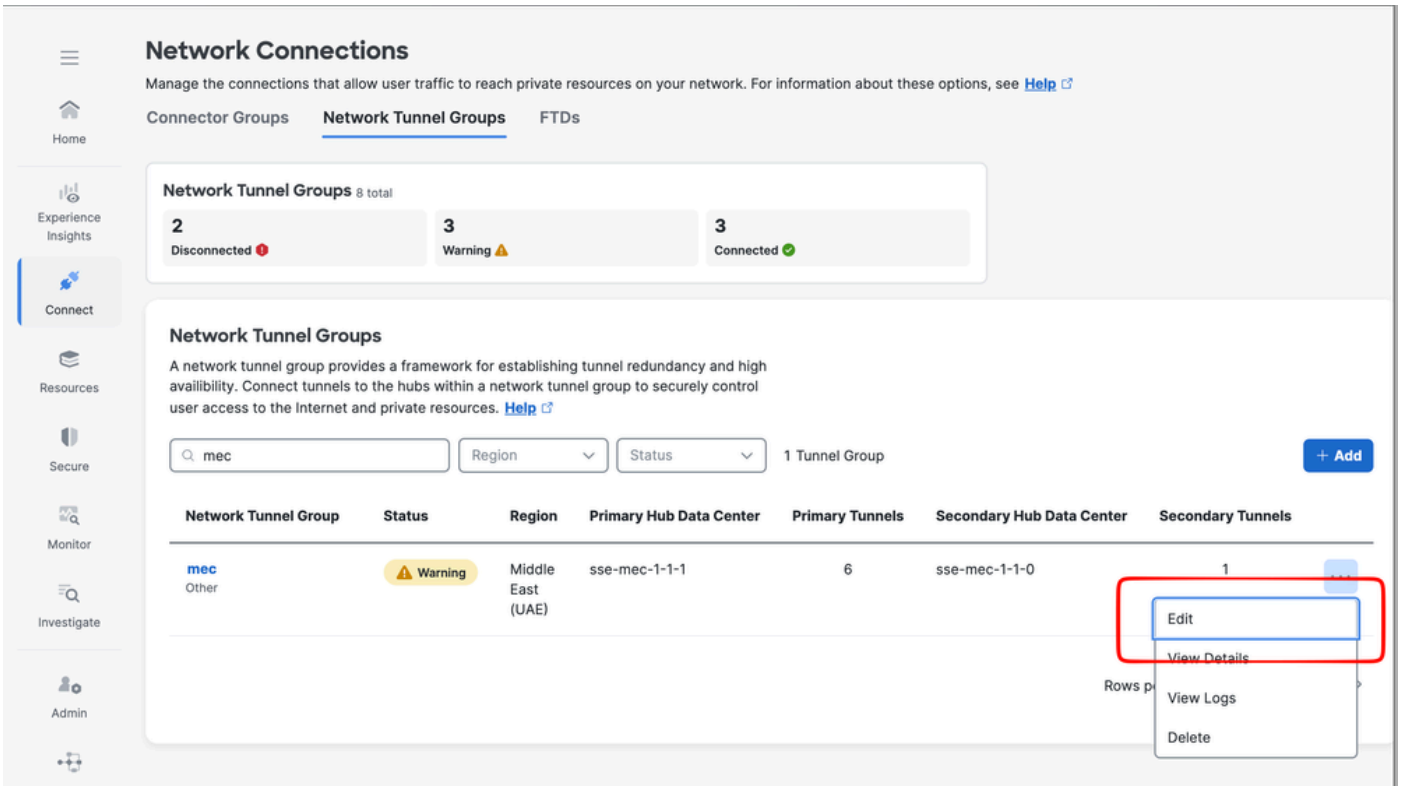
有关配置新VPN配置文件的详细步骤，请参阅《远程访问VPN部署指南》：

网络隧道组

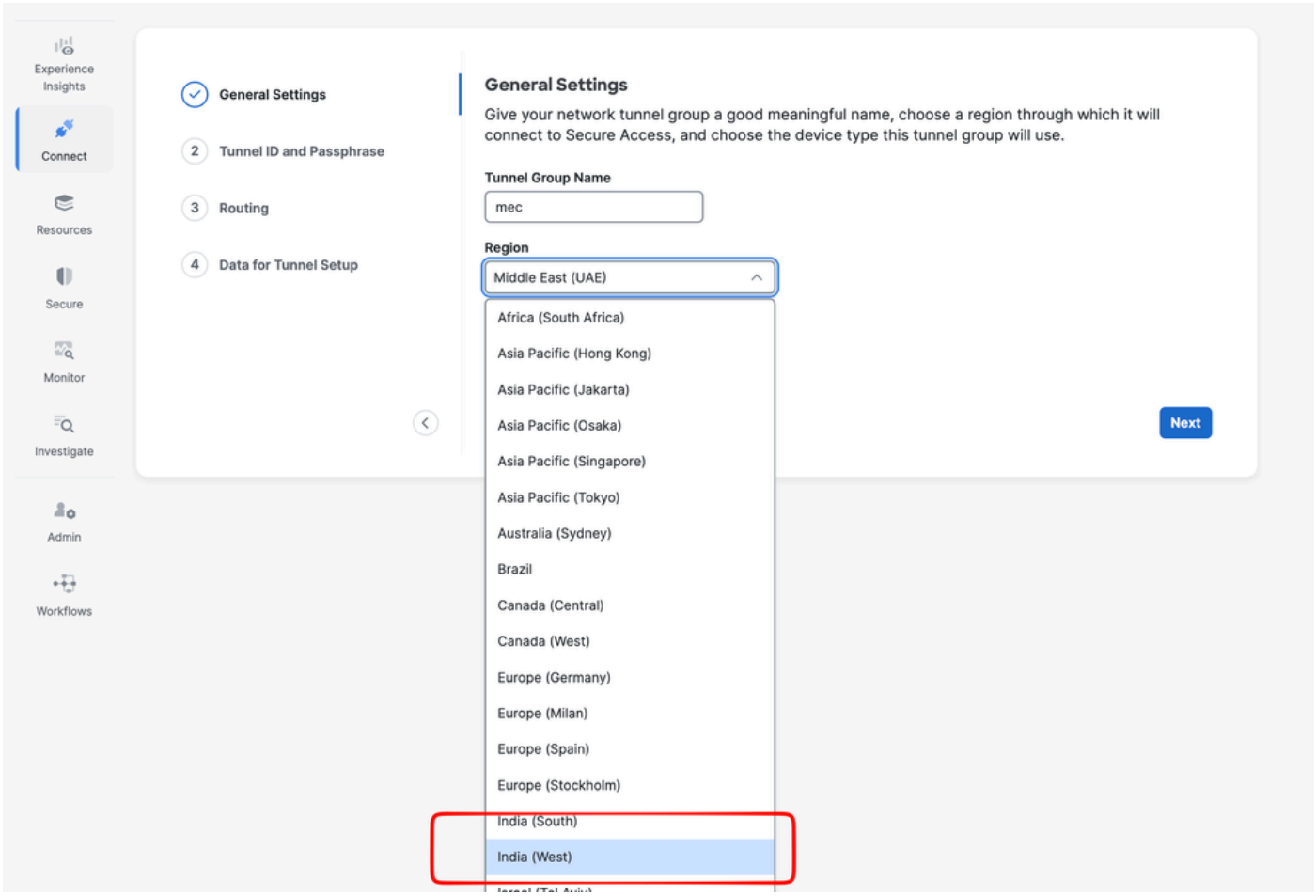
请按照以下步骤更改网络隧道组区域:

·按如下所述转到NTG选项：

·编辑您现有的中东(UAE)区域隧道。

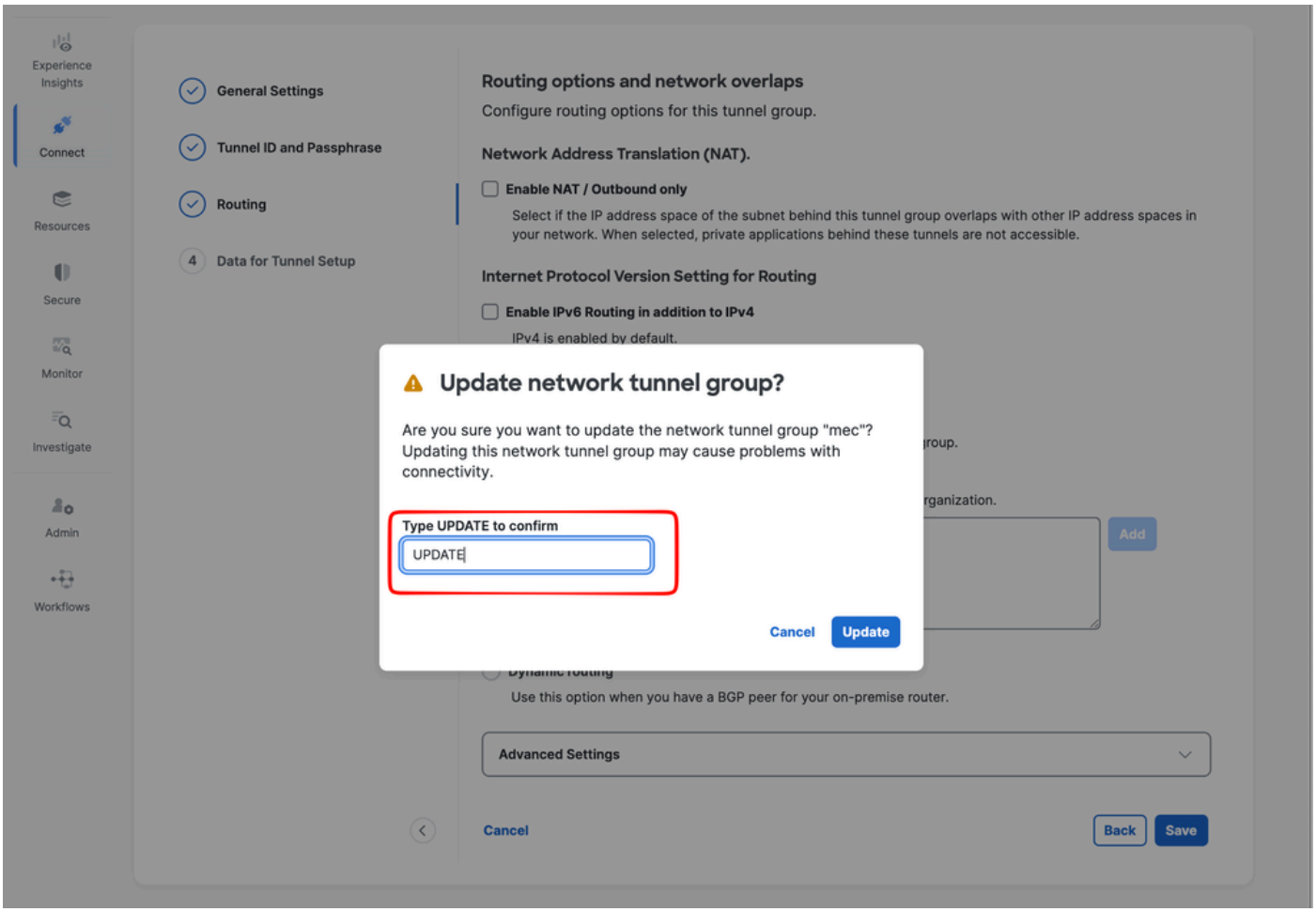


·将中东地区（阿联酋）改为印度（西部）。

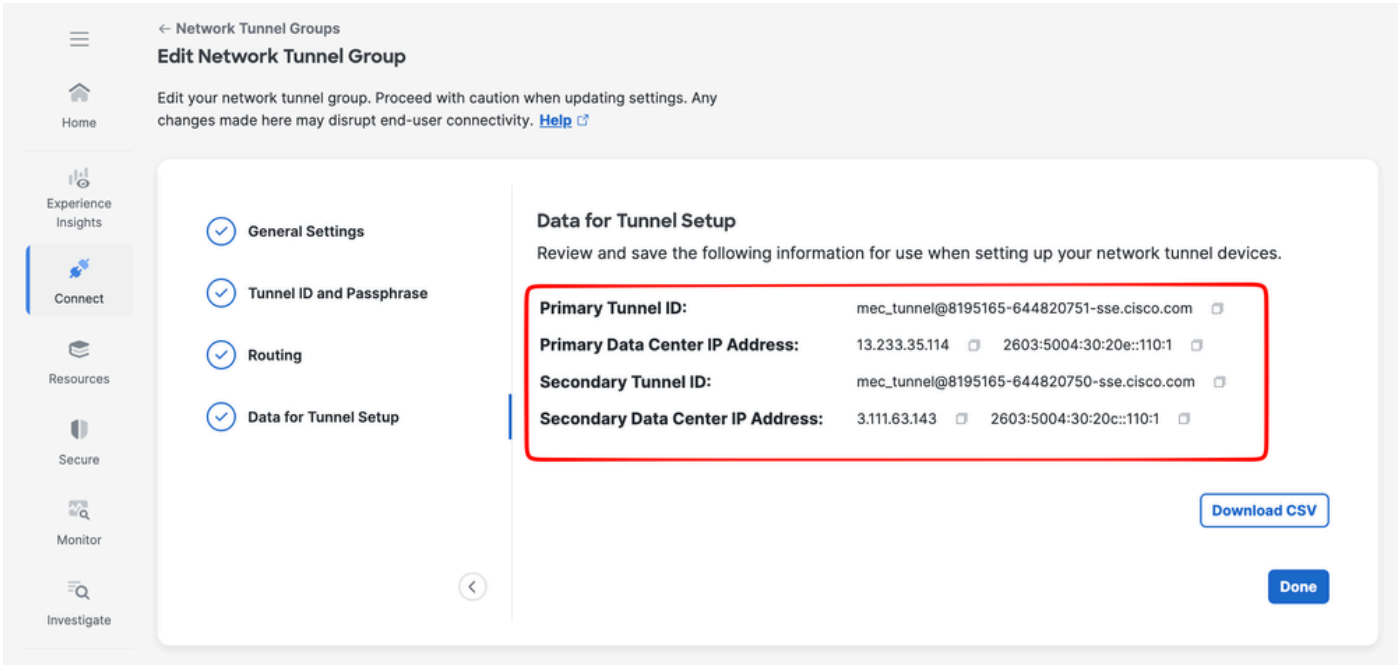


·请勿修改其他设置；保存配置。

·出现提示时，键入“UPDATE”并确认。



·使用所示的新印度（西部）IP地址更新您的IPSEC CPE设备。



·如果使用多区域回传或路由映射，请根据思科SSE的新设置更新BGP社区值。

安全Web网关

使用漫游安全模块的客户端将自动连接到下一个最近且可用的安全访问数据中心。
目前客户不需要采取任何措施。

零信任访问客户端

使用零信任访问模块的客户端将自动连接到下一个最近且可用的安全访问数据中心。
目前客户不需要采取任何措施。

相关信息

- 状态思科安全访问

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）。