# 配置安全访问的选项和VPN功能（中国）

## 目录

## 问题

分析思科安全访问中国部署的VPN功能的组织需要澄清加密支持和操作限制。具体来说，以下问题包括：部署在中国大陆的思科安全防火墙设备上是否正式支持IPsec VPN(IKEv1/IKEv2)、为什么通常建议使用GRE隧道、安全通信有哪些先决条件或替代方案。此外，从AWS中国的虚拟检查点防火墙迁移到FTD平台以与AWS Transit Gateway建立连接时，需要了解对GRE隧道的支持。

## 环境

- 中国思科安全接入（云交付的安全服务边缘解决方案）
- 思科在中国大陆的安全防火墙部署
- FTD平台迁移方案
- AWS China Transit Gateway连接要求
- 仅支持GRE的虚拟检查点防火墙环境

## 分辨率

Cisco Secure Access中国提供了全面的VPN功能以及特定的协议支持和配置选项：

### IPsec VPN支持

思科安全访问中国仅支持使用IKEv2协议的IPsec VPN。此部署模式不支持IKEv1。支持的IPsec参

数和配置选项在官方的Cisco Secure Access China文档中记录。

IPsec支持的主要特征：

- 独占支持IKEv2协议。
- 不需要特殊的固件或加密映像。
- 云交付的安全服务边缘(SSE)解决方案。
- 标准IPsec参数配置可用。

### 高可用性选项

为了提高可靠性，思科安全接入中国网络隧道组支持具有高可用性功能的主集线器和辅助集线器配置。

## 原因

未发现具体原因。

## 相关内容

- 思科安全访问中国IPsec参数
- 思科安全访问中国GRE配置
- 支持的IPsec参数文档
- 网络隧道组高可用性
- VPN部署用户指南
- 思科技术支持和下载

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）。