安全访问和FortiGate防火墙之间的IPSec隧道身份验证失败

问题

Cisco安全访问和FortiGate防火墙之间的IPSec隧道建立失败，出现身份验证错误。FortiGate防火墙调试日志显示“身份验证失败”消息，尽管验证两端预共享密钥(PSK)匹配。第1阶段协商由于INVALID_KE_PAYLOAD错误而失败，导致隧道无法启动。两个端点之间的连接提议似乎匹配，但隧道建立过程未成功完成。

环境

- 思科安全访问
- FortiGate防火墙（由第三方管理）
- 带有冗余主端点和备用端点的IPSec隧道配置

分辨率

IPSec隧道连接问题已通过进行特定配置调整来解决INVALID_KE_PAYLOAD错误和身份验证问题。

第1阶段DH组配置

仅配置一个Diffie-Hellman(DH)组进行第1阶段协商。在第1阶段设置DH组20，而不是使用多个DH组或以前配置的DH组14。

配置修复

```
config vpn ipsec phase1-interface
    edit "sse-tunnel"
        set dhgrp 20
    next
end
```

NAT遍历配置

在IPSec隧道配置上启用NAT穿越(NAT-T)。这以前已禁用，但需要启用才能正确建立隧道。

完全前向保密配置

在第2阶段配置中禁用完全向前保密(PFS)以消除潜在的协商冲突。

原因

IPSec隧道故障是由多个配置不匹配和不兼容引起的：

- INVALID_KE_PAYLOAD错误：此第1阶段错误是由于Cisco安全访问和FortiGate终端之间的Diffie-Hellman组协商冲突引起的
- DH组不匹配：配置多个DH组并在原始配置中使用DH组14与Cisco安全访问要求不兼容
- NAT遍历设置：已禁用NAT穿越，导致网络环境中无法正确建立隧道

相关内容

- 使用FortiGate防火墙配置安全访问
- 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）。