安全訪問和FortiGate防火牆之間的IPSec通道身份驗證失敗

問題

在Cisco安全訪問和FortiGate防火牆之間建立IPSec隧道失敗，出現身份驗證錯誤。FortiGate防火牆調試日誌顯示「身份驗證失敗」消息，儘管驗證前共用金鑰(PSK)在兩端都匹配。階段1協商失敗，出現INVALID_KE_PAYLOAD錯誤，導致隧道無法啟動。兩個端點之間的連線建議似乎匹配，但隧道建立過程未成功完成。

環境

- Cisco Secure Access
- FortiGate防火牆（由第三方管理）
- 帶有冗餘主端點和備用端點的IPSec隧道配置

解析

IPSec通道連線問題已通過進行特定配置調整來解決INVALID_KE_PAYLOAD錯誤和身份驗證問題。

第1階段DH組配置

只為階段1交涉設定一個Diffie-hellman(DH)群組。在階段1上設定DH組20，而不是使用多個DH組或以前配置的DH組14。

配置修復

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

NAT遍歷配置

在IPSec隧道配置上啟用NAT穿越(NAT-T)。以前禁用了此功能，但需要啟用它才能正確建立隧道。

完善前向保密配置

在第2階段配置中禁用完全轉發保密(PFS)以消除潛在的協商衝突。

原因

IPSec通道故障是由多個配置不匹配和不相容引起的：

- INVALID_KE_PAYLOAD錯誤：由於思科安全訪問和FortiGate端點之間的Diffie-Hellman組協商衝突，發生了第1階段錯誤
- DH組不匹配：配置多個DH組並在原始配置中使用DH組14與Cisco安全訪問要求不相容
- NAT遍歷設定：已禁用NAT穿越，從而阻止在網路環境中建立正確的隧道

相關內容

- 使用FortiGate防火牆配置安全訪問
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。