# セキュアアクセスとFortiGateファイアウォールの間でIPSecトンネル認証が失敗する

## お問い合わせ内容

Cisco Secure AccessとFortiGateファイアウォールの間でIPSecトンネルの確立が失敗し、認証エラーが発生します。FortiGateファイアウォールのデバッグログには、「authentication failed」メッセージが表示されますが、事前共有キー(PSK)が両側で一致していることが確認されます。フェーズ1ネゴシエーションがINVALID_KE_PAYLOADエラーで失敗し、トンネルがアップ状態になりません。接続のプロポーザルは両方のエンドポイント間で一致するようですが、トンネル確立プロセスは正常に完了していません。

## 環境

- シスコセキュアアクセス
- FortiGateファイアウォール（サードパーティで管理）
- 冗長なプライマリおよびバックアップエンドポイントを使用したIPSecトンネル設定

## 解決策

IPSecトンネル接続の問題は、INVALID_KE_PAYLOADエラーと認証の問題に対処するために特定の設定を調整することで解決されました。

### フェーズ1のDHグループの設定

フェーズ1ネゴシエーション用にDiffie-Hellman(DH)グループを1つだけ設定します。複数のDHグループや以前に設定したDHグループ14を使用する代わりに、フェーズ1でDHグループ20を設定します。

### 構成の修正

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

### NATトラバーサルの設定

IPSecトンネル設定でNATトラバーサル(NAT-T)を有効にします。これは以前はディセーブルにされていましたが、トンネルを正しく確立するためにイネーブルにする必要があります。

### 完全転送秘密の設定

潜在的なネゴシエーションの競合を排除するために、フェーズ2設定でPerfect Forward Secrecy(PFS)を無効にします。

## 原因

IPSecトンネル障害は、複数の設定の不一致と非互換性が原因で発生しました。

- INVALID_KE_PAYLOADエラー：このフェーズ1エラーは、Cisco Secure Accessエンドポイントと FortiGateエンドポイント間のDiffie-Hellman(DH)グループネゴシエーション競合が原因で発生しました
- DHグループの不一致：複数のDHグループが設定されており、元の設定でDHグループ14を使用するとCisco Secure Accessの要件に適合しませんでした
- NATトラバーサルの設定：NATトラバーサルが無効になっているため、ネットワーク環境でトンネルが適切に確立されませんでした

## 関連コンテンツ

- FortiGateファイアウォールによるセキュアアクセスの設定
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。