セキュアアクセス証明書検査ポスチャチェック認証の失敗

内容

お問い合わせ内容

証明書検査機能を使用してエンドポイントポスチャプロファイルでSecure Accessを展開しようとすると、DARTバンドルログで特定の原因を特定できないにもかかわらず、すべてのログイン試行が失敗します。ユーザは、ポスチャチェックメカニズムを使用して証明書の検証を実施する一方でSAML IDP認証を利用しようとしていますが、この設定では、バックエンド証明書が一致した場合でも一貫した認証エラーが発生します。

環境

- Cisco Secure Access – セキュアクライアントリモートアクセス (VPN、ポスチャ、プライベートリソース)
- SAML IDP認証統合
- 証明書検査機能が有効なエンドポイントポスチャプロファイル
- SANのUPNフィールドが電子メールアドレスに一致するユーザー証明書
- ユーザ、グループ、エンドポイントデバイスを使用したセキュアアクセステナントの設定

解決策

ポスチャでの証明書エンドポイントチェックは、ユーザ証明書とマシン証明書の両方の検証が必要な複数証明書認証を使用する場合にのみ適用されます。この導入シナリオでは、単一のVPNプロファイルを使用する必要があるユーザ証明書のみを持つユーザを対象としているため、ポスチャ証明書チェックに依存する代わりに、SAML +単一の証明書認証を実装することがソリューションに含まれます。

認証の設定手順

手順1:SAML +単一の証明書認証を設定する

ポスチャチェックによって証明書の検証を強制するのではなく、単一の証明書認証と組み合わせたSAML認証を使用するように認証方式を設定します。

ステップ2：証明書UPN照合の設定

証明書のサブジェクト代替名(SAN)のUPNフィールドに、ユーザー、グループ、およびエンドポイントデバイスの下のセキュアアクセスでユーザーに対して構成されている認証プロパティと一致するユーザーの電子メールアドレスが含まれていることを確認してください。

ステップ3：プライマリ認証フィールドの設定

証明書のUPNを使用して認証するプライマリフィールドを設定し、Secure Accessユーザデータベース内のユーザの電子メールアドレスに対応するようにします。

証明書構造の要件

証明書のUPNまたはセカンダリの値がセキュアアクセスのユーザの認証プロパティと一致するように、証明書構造を設定する必要があります。ユーザが提示した証明書のUPNまたはセカンダリの値が、セキュアアクセスで設定されているそのユーザの認証プロパティと一致しない場合、認証は拒否されます。

重要な設定に関する注意事項

ポスチャ証明書チェックの強制が必要な場合は、複数証明書認証（IDP SAML +複数証明書認証）が必要になりますが、これにはユーザ証明書とマシン証明書の両方が必要です。ユーザがユーザ証明書のみを所有し、単一のVPNプロファイルを使用する必要がある環境では、SAML +単一の証明書認証により、証明書ベースのセキュリティ制御を維持しながら、適切なソリューションが提供されます。

原因

ポスチャでの証明書エンドポイントチェックは、複数の証明書の認証が設定されている場合にのみ適用されます。ポスチャ証明書チェックを伴うSAML認証を使用する場合、システムは検証のためにユーザ証明書とマシン証明書の両方が存在することを想定します。導入ではSAML認証を持つユーザ証明書のみを使用したため、ポスチャ証明書のインスペクション機能は、単一の証明書認証シナリオで動作するように設計されていなかったため、バックエンド証明書の一致に成功しても、認証に失敗していました。

関連コンテンツ

- 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。