Échecs d'authentification du contrôle de posture du certificat d'accès sécurisé

Table des matières

Problème

Lors de la tentative de déploiement d'un accès sécurisé avec le profil de posture de point de terminaison à l'aide de la fonctionnalité d'inspection de certificat, toutes les tentatives de connexion échouent malgré le fait que les causes spécifiques de l'échec ne peuvent pas être identifiées dans les journaux de l'ensemble DART.Les utilisateurs tentent d'utiliser l'authentification d'IDP SAML tout en voulant également appliquer la validation de certificat via le mécanisme de vérification de posture, mais cette configuration entraîne des échecs d'authentification cohérents même lorsque les correspondances de certificat principal sont réussies.

Environnement

- Accès sécurisé Cisco - Accès à distance sécurisé du client (VPN, position, ressource privée)
- Intégration de l'authentification SAML IDP
- Profil de posture du terminal avec fonction d'inspection de certificat activée
- Certificats utilisateur avec champ UPN dans le SAN correspondant aux adresses e-mail
- Configuration du locataire d'accès sécurisé avec les utilisateurs, les groupes et les terminaux

Résolution

Les vérifications de la position des points de terminaison de certificat ne sont appliquées que lors de l'utilisation de l'authentification multicertificat, qui nécessite à la fois un certificat utilisateur et une validation de certificat machine. Étant donné que le scénario de déploiement implique des

utilisateurs disposant uniquement de certificats d'utilisateur et devant utiliser un profil VPN unique, la solution implique la mise en oeuvre de l'authentification SAML + certificat unique au lieu de s'appuyer sur la vérification du certificat de position.

Étapes de configuration d'authentification

Étape 1: Configurer SAML + authentification par certificat unique

Configurez la méthode d'authentification pour utiliser l'authentification SAML combinée à l'authentification par certificat unique plutôt que d'essayer d'appliquer la validation de certificat par des contrôles de position.

Étape 2: Configurer la correspondance UPN de certificat

Assurez-vous que le champ UPN dans le nom alternatif de l'objet (SAN) du certificat contient l'adresse e-mail de l'utilisateur qui correspond à la propriété d'authentification configurée pour l'utilisateur dans Secure Access sous Users, Groups, and Endpoint devices.

Étape 3: Champ Définir l'authentification principale

Configurez le champ principal pour l'authentification à l'aide de l'UPN du certificat, en vous assurant qu'il correspond à l'adresse e-mail de l'utilisateur dans la base de données utilisateur d'accès sécurisé.

Exigences relatives à la structure des certificats

La structure du certificat doit être configurée de sorte que la valeur UPN ou secondaire du certificat corresponde à la propriété d'authentification de l'utilisateur dans Secure Access. Si un utilisateur présente un certificat dont la valeur UPN ou secondaire ne correspond pas à la propriété d'authentification configurée pour cet utilisateur dans Secure Access, l'authentification sera rejetée.

Notes de configuration importantes

L'authentification multicertificat (IDP SAML + Multi-Cert Auth) serait requise si l'application du contrôle de certificat de position est nécessaire, mais cela nécessite des certificats utilisateur et machine. Pour les déploiements où les utilisateurs n'ont que des certificats d'utilisateur et ont besoin d'utiliser un profil VPN unique, l'authentification SAML + certificat unique fournit la solution appropriée tout en conservant des contrôles de sécurité basés sur les certificats.

Motif

Les vérifications de la position des points de terminaison de certificat ne sont appliquées que lorsque l'authentification multicertificat est configurée. Lors de l'utilisation de l'authentification SAML avec vérification de la position des certificats, le système attend la présence de certificats utilisateur et machine pour validation. Étant donné que le déploiement n'utilisait que des certificats utilisateur avec authentification SAML, la fonctionnalité d'inspection de certificat de posture a systématiquement échoué lors des tentatives d'authentification malgré une correspondance de certificat principal réussie, car le mécanisme de posture n'a pas été conçu pour fonctionner avec des scénarios d'authentification de certificat unique.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.