Fehler bei der Secure Access Certificate Inspection-Statusüberprüfung der Authentifizierung

Inhalt

Problem

Beim Versuch, Secure Access mithilfe der Zertifikatprüfungsfunktion mit dem Endpunktsicherungsprofil bereitzustellen, schlagen alle Anmeldeversuche fehl, obwohl bestimmte Fehlerursachen in den DART-Paketprotokollen nicht identifiziert werden können.Benutzer versuchen, die SAML IDP-Authentifizierung zu verwenden, während sie gleichzeitig die Zertifikatvalidierung über den Statusprüfungsmechanismus durchsetzen möchten. Diese Konfiguration führt jedoch zu konsistenten Authentifizierungsfehlern, selbst wenn die Backend-Zertifikatübereinstimmungen erfolgreich sind.

Umwelt

- Cisco Secure Access - Sicherer Client-Remote-Zugriff (VPN, Status, private Ressource)
- SAML IDP-Authentifizierungsintegration
- Endgerätestatusprofil mit aktivierter Zertifikatprüfungsfunktion
- Benutzerzertifikate mit UPN-Feld in SAN-übereinstimmenden E-Mail-Adressen
- Tenant-Konfiguration mit sicherem Zugriff für Benutzer, Gruppen und Endgeräte

Auflösung

Die Statusüberprüfungen für Zertifikatendpunkte werden nur bei Verwendung der Authentifizierung mit mehreren Zertifikaten erzwungen, für die sowohl ein Benutzerzertifikat als auch eine

Computerzertifikatüberprüfung erforderlich ist. Da das Bereitstellungsszenario Benutzer mit nur Benutzerzertifikaten umfasst, die ein einzelnes VPN-Profil verwenden müssen, sieht die Lösung die Implementierung einer SAML + Single Certificate Authentication vor, anstatt auf Statuszertifikatprüfungen angewiesen zu sein.

Konfigurationsschritte für die Authentifizierung

Schritt 1: Konfiguration von SAML + Single Certificate Authentication

Konfigurieren Sie die Authentifizierungsmethode so, dass sie die SAML-Authentifizierung in Kombination mit einer einzelnen Zertifikatsauthentifizierung verwendet, anstatt zu versuchen, die Zertifikatsvalidierung durch Statusprüfungen durchzusetzen.

Phase 2: Zertifikat-UPN-Zuordnung konfigurieren

Stellen Sie sicher, dass das UPN-Feld im SAN (Subject Alternative Name) des Zertifikats die E-Mail-Adresse des Benutzers enthält, die mit der Authentifizierungseigenschaft übereinstimmt, die für den Benutzer in Sicherer Zugriff unter Benutzer, Gruppen und Endgeräte konfiguriert wurde.

Schritt 3: Feld für primäre Authentifizierung festlegen

Konfigurieren Sie das primäre Feld für die Authentifizierung mithilfe des UPN aus dem Zertifikat, und stellen Sie sicher, dass es der E-Mail-Adresse des Benutzers in der Secure Access-Benutzerdatenbank entspricht.

Anforderungen an die Zertifikatstruktur

Die Zertifikatstruktur muss so konfiguriert werden, dass der UPN- oder sekundäre Wert im Zertifikat mit der Authentifizierungseigenschaft für den Benutzer in Secure Access übereinstimmt. Wenn ein Benutzer ein Zertifikat präsentiert, das einen UPN- oder sekundären Wert aufweist, der nicht mit der konfigurierten Authentifizierungseigenschaft für diesen Benutzer in Secure Access übereinstimmt, wird die Authentifizierung abgelehnt.

Wichtige Konfigurationshinweise

Die Authentifizierung mehrerer Zertifikate (IDP SAML + Multi-Certificate Auth) ist erforderlich, wenn die Überprüfung von Statuszertifikaten erzwungen werden muss. Hierfür sind jedoch Benutzer- und Computerzertifikate erforderlich. Für Bereitstellungen, bei denen Benutzer nur über Benutzerzertifikate verfügen und ein einzelnes VPN-Profil verwenden müssen, bietet die SAML- + Einzelzertifikatauthentifizierung die passende Lösung, wobei jedoch zertifikatbasierte Sicherheitskontrollen beibehalten werden.

Ursache

Die Statusüberprüfung der Zertifikatendpunkte wird nur erzwungen, wenn die Authentifizierung mit mehreren Zertifikaten konfiguriert ist. Bei Verwendung der SAML-Authentifizierung mit Statuszertifikatprüfung erwartet das System, dass zur Validierung Benutzer- und Computerzertifikate vorhanden sind. Da bei der Bereitstellung nur Benutzerzertifikate mit SAML-Authentifizierung verwendet wurden, ist die Statuszertifikatprüfungsfunktion trotz erfolgreichen Backend-Zertifikatabgleichs immer wieder fehlgeschlagen, da der Statusmechanismus nicht für die Verwendung mit Einzelzertifikatauthentifizierungsszenarien konzipiert wurde.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.