

Fehlerbehandlung bei SSL-Entschlüsselungszertifikat in sicherem Zugriff

Inhalt

Problem

Bei Benutzern treten zertifikatbezogene Fehlerseiten auf, wenn die SSL-Verschlüsselung in Cisco Secure Access aktiviert ist. Es sind mehrere Anfragen zu drei spezifischen Arten von Zertifikatfehlern eingegangen:

- Fehler beim Ablaufen des Ursprungsserverzertifikats
- CN/SAN-Zertifikatfehler, wenn der im Zertifikat aufgeführte Common Name oder Subject Alternative Names nicht mit der aufgerufenen Domäne übereinstimmen
- Der in das Zertifikat des Ursprungsservers eingebettete CRL-Link (Certificate Revocation List) verursacht Verbindungsprobleme.

Diese Zertifikatfehler ähneln Warnungen, die normalerweise in Webbrowsern angezeigt werden. Es stellt sich die Frage, ob Cisco Secure Access zertifikatbezogene Fehler behandeln kann, indem Warnseiten angezeigt werden (ähnlich wie Browser oder Content-Filter) und der Zugriff nach Anzeige der Warnung oder in allen Fällen erlaubt wird. Außerdem muss bekannt sein, wie sich SSL-Verschlüsselung verhält, wenn sie deaktiviert ist, und ob der Datenverkehr unabhängig von Zertifikatsproblemen weitergeleitet wird.

Umwelt

- Cisco Secure Access - Internetzugang (Roaming-Modul, VA, DNS, SWG, PAC, IPS, Zertifikate)
- Aktivierung der SSL-Entschlüsselungsfunktion
- Bei mehreren Domänen treten Probleme bei der Zertifikatsvalidierung auf.
- Ursprungsserver mit verschiedenen Zertifikatsproblemen, einschließlich Ablauf und

Auflösung

Einschränkungen bei der Behandlung von Zertifikatfehlern

Die zertifikatbezogene Fehlerbehandlung ist in Cisco Secure Access nicht verfügbar. Das Produkt unterstützt nicht:

- Anzeigen von browserähnlichen Warnseiten für Zertifikatprobleme
- Konfiguration zur Behandlung von domänenspezifischen Zertifikatfehlern
- Benutzerdefinierte Fehlerbehandlung auf Basis von Zieldomänen
- Warnseiten im Stil eines Inhaltsfilters mit Optionen zum Überschreiben durch den Benutzer

Problemumgehung zum Ausschluss der SSL-Verschlüsselung

Der empfohlene Ansatz besteht darin, problematische Domänen mithilfe der Verschlüsselungseinstellungen des Sicherheitsprofils von der SSL-Entschlüsselung auszuschließen. Dies kann wie folgt konfiguriert werden:

Navigieren Sie zum Abschnitt Sicherheitsprofil > Entschlüsselungseinstellungen, um bestimmte Domänen von der SSL-Überprüfung auszuschließen.

Wenn Domänen von der SSL-Verschlüsselung ausgeschlossen werden, geschieht dieses Verhalten:

- Datenverkehr für ausgeschlossene Domänen umgeht SSL-Prüfung vollständig
- Die Zertifikatsvalidierung wird von Secure Access nicht durchgeführt.
- Von Secure Access generierte Zertifikatfehlerseiten für Benutzer nicht vorhanden
- Die ursprünglichen Zertifikatfehler sind möglicherweise im Benutzerbrowser weiterhin

sichtbar, wenn die Zertifikatprobleme weiterhin bestehen

SSL-Entschlüsselung deaktiviert Verhalten

Wenn die SSL-Entschlüsselung für eine Domäne oder global deaktiviert ist, leitet Cisco Secure Access den Datenverkehr unabhängig von Zertifikatproblemen weiter. Das Produkt überprüft und validiert Zertifikate nicht, wenn die Entschlüsselung nicht aktiviert ist, sodass der gesamte HTTPS-Datenverkehr transparent übertragen werden kann.

Ursache

Die Zertifikatfehler werden durch legitime Probleme bei der Zertifikatsvalidierung auf den Ursprungsservern verursacht, darunter abgelaufene Zertifikate, CN/SAN-Diskrepanzen und Probleme mit der CRL-Verbindung. Cisco Secure Access führt im Rahmen des SSL-Verschlüsselungsprozesses eine Zertifikatsvalidierung durch. Wenn diese Validierungsfehler auftreten, generiert das Produkt Fehlerseiten, um potenziell unsichere Verbindungen zu verhindern. Dies ist das beabsichtigte Sicherheitsverhalten der SSL-Prüffunktion.

Verwandte Inhalte

- [Cisco Secure Access-Entschlüsselungskonfigurationsdokumentation](#)
- [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.