Konfigurieren von SSE Nicht entschlüsseln für IPS und SWG-Entschlüsselungsumgehung

Inhalt

Problem

Der HTTPS-Datenverkehr zu Zielen von Finanzkategorien stellt weiterhin ein Cisco SSE-Zertifikat anstelle des ursprünglichen Website-Zertifikats dar, auch nachdem die Finanzkategorie oder bestimmte Domänen einer DND-Liste (Do Not Decrypt) hinzugefügt und die entsprechende Zugriffsregel angewendet wurde. Dieses Verhalten wird beobachtet, wenn der Zugriff auf Websites über den Zero Trust Access Client (TIA) erfolgt, was sich insbesondere auf den Zugriff auf finanzierungsbezogene Websites wie https://onlinesbi.sbi.bank.in/ auswirkt, auf denen End-to-End-Zertifikattransparenz erforderlich ist.

Das erwartete Verhalten ist, dass beim Hinzufügen einer Website oder Inhaltskategorie zur DND-Liste das Zertifikat der ursprünglichen Website dem Browser anstelle des Cisco SSE-Zertifikats angezeigt werden kann. Das Cisco SSE-Zertifikat wird jedoch weiterhin angezeigt, was darauf hinweist, dass die Entschlüsselung des Datenverkehrs trotz der DND-Konfiguration weiterhin erfolgt.

Umwelt

- Cisco Secure Service Edge (SSE)
- TIA-Verbindungen (Zero Trust Access Client)
- Globale IPS-Entschlüsselung aktiviert
- IPS auf Grundlage von Zugriffsrichtlinien aktiv
- In der Liste "Nicht entschlüsseln" im Sicherheitsprofil konfigurierte Finanzkategorie
- Anwendung von Zugriffsregeln auf die entsprechenden Sicherheitsprofile

Auflösung

Die Lösung besteht darin, zu verstehen, dass Cisco SSE zwei verschiedene Arten der Entschlüsselung durchführt, und die entsprechenden Einstellungen für "Nicht entschlüsseln" für beide Arten der Entschlüsselung zu konfigurieren.

Informationen zu SSE-Entschlüsselungstypen

Cisco SSE führt zwei separate Entschlüsselungsprozesse durch:

- SWG-Entschlüsselung (Secure Web Gateway) - Webproxy-Entschlüsselung
- IPS-Entschlüsselung - Entschlüsselung des Intrusion Prevention-Systems

Entschlüsseln Sie keine Einträge, die in einem Sicherheitsprofil konfiguriert sind, nur für die SWG-Entschlüsselung und verhindern Sie keine IPS-Entschlüsselung. Wenn die globale IPS-Entschlüsselung aktiviert ist und IPS für eine beliebige Zugriffsrichtlinie aktiviert ist, erfolgt die IPS-Entschlüsselung weiterhin, sodass das Cisco SSE-Zertifikat dem Browser angezeigt wird.

Konfigurationsschritte

Schritt 1: Fügen Sie Websites oder Inhaltskategorien zur Liste der vom System bereitgestellten Nicht-Entschlüsselungen hinzu.

Die vom System bereitgestellte Liste "Nicht entschlüsseln" wird auf alle IPS-Profile angewendet. Durch Hinzufügen einer Website oder Inhaltskategorie zu dieser vom System bereitgestellten Liste wird das Zertifikat der ursprünglichen Website angezeigt, wodurch die IPS-Entschlüsselung effektiv umgangen wird.

Phase 2: Vergewissern Sie sich, dass keine weiteren Richtlinienänderungen erforderlich sind.

Es ist nicht erforderlich, in den Zugriffsrichtlinien auf die vom System bereitgestellte Liste "Nicht entschlüsseln" zu verweisen. Die Liste wird automatisch auf alle IPS-Profile angewendet.

Validierungstests

Mit diesen Validierungsmethoden kann die korrekte Konfiguration bestätigt werden:

Methode 1: Domäne zur Liste "Nicht entschlüsseln" des bereitgestellten Systems hinzufügen

Wenn Sie die spezifische Domäne zur Liste der vom System bereitgestellten Do Not Decrypt-Zertifikate hinzufügen, wird möglicherweise das Zertifikat der Ursprungswebsite anstelle des Cisco SSE-Zertifikats angezeigt.

Methode 2: Globale IPS-Entschlüsselung vorübergehend deaktivieren (nur für Tests)

Wenn die globale IPS-Entschlüsselung vorübergehend deaktiviert wird, wird auch das Ursprungszertifikat für den getesteten Standort angezeigt. Dies bestätigt, dass die IPS-Entschlüsselung die Ursache für die Cisco SSE-Zertifikatpräsentation war.

Voraussichtliche Ergebnisse

Nach der korrekten Konfiguration:

- Websites oder Inhaltskategorien, die der vom System bereitgestellten Liste der nicht zu entschlüsselnden Websites hinzugefügt wurden, präsentieren ihre ursprünglichen Website-Zertifikate.
- Sowohl die SWG- als auch die IPS-Entschlüsselung werden für die angegebenen Standorte oder Kategorien umgangen.
- Der Browser zeigt das eigentliche Website-Zertifikat anstelle des Cisco SSE-Zertifikats an.

Ursache

Das Problem liegt daran, dass die Cisco SSE zwei unterschiedliche Entschlüsselungsprozesse durchführt: SWG-Entschlüsselung und IPS-Entschlüsselung In Sicherheitsprofilen konfigurierte Einträge nicht entschlüsseln Umgehen Sie nur SWG-Entschlüsselung. Wenn die globale IPS-Entschlüsselung aktiviert ist und IPS für die Zugriffsrichtlinien aktiviert ist, wird die IPS-Entschlüsselung weiterhin unabhängig durchgeführt, sodass das Cisco SSE-Zertifikat dem Browser angezeigt wird, auch wenn Websites in den Sicherheitsprofil-DND-Listen enthalten sind.

Um beide Entschlüsselungstypen vollständig zu umgehen, müssen Websites oder

Inhaltskategorien der vom System bereitgestellten Liste der nicht zu entschlüsselnden Seiten hinzugefügt werden. Diese Liste gilt für alle IPS-Profile und verhindert die SWG- und IPS-Entschlüsselung.

Verwandte Inhalte

- Erstellung einer effektiven Liste nicht entschlüsseln für sicheren Zugriff
- Fehlerbehebung und Erfassung grundlegender Informationen für sicheren Zugriff
- 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.