Überprüfen der IPS-Entschlüsselung in Cisco Secure Access

Inhalt

Problem

Bei der Verwendung von Cisco Secure Access mit RAVPN (Remote Access VPN) über Secure Client müssen Organisationen überprüfen, ob IPS (Intrusion Prevention System)-Entschlüsselung und -Inspektion für den Datenverkehr zu bestimmten Websites korrekt durchgeführt werden. Die wichtigste Herausforderung besteht darin, zu bestätigen, dass die TLS-Entschlüsselungs- und Prüfprozesse nicht mit den Standard-UI-Protokollen, sondern mit anderen Methoden wie der Aktivitätssuche, ordnungsgemäß funktionieren. Zu den spezifischen Überprüfungsanforderungen gehören die Identifizierung clientseitiger Zertifikatprüfungen oder Debug-/Berichtsmechanismen, die die Testvalidierung unterstützen können, und die zusätzliche Bestätigung des IPS-Betriebs über die Verwaltungsschnittstelle hinaus.

Umwelt

- Cisco Secure Access (CSA) mit RAVPN-Funktion
- Cisco Secure Client für Remotezugriff-VPN-Verbindungen
- IPS-Entschlüsselungs- und Prüffunktionen aktiviert
- TLS-/SSL-Datenverkehr, der entschlüsselt werden muss, für die Sicherheitsüberprüfung
- Webdatenverkehr von RAVPN-Clients zu externen Websites

Auflösung

In Cisco Secure Access gibt es zwei Methoden zur Überprüfung der ordnungsgemäßen Funktion von IPS-Entschlüsselung und -Prüfung für den VPN-Verkehr des Remote-Zugriffs:

Methode 1: Suche nach Management-UI-Aktivität (primäre Methode)

Die Aktivitätssuche in der Cisco Secure Access-Verwaltungsoberfläche ist die zuverlässigste Methode zur Bestätigung von IPS-Entschlüsselungs- und Prüfungsvorgängen. Diese Schnittstelle zeigt detaillierte Protokolle und Analysen an, aus denen hervorgeht, wann der Datenverkehr von den Sicherheitsdiensten entschlüsselt und überprüft wurde.

So greifen Sie auf die Aktivitätssuche zu:

Navigieren Sie zum Management-Dashboard von Cisco Secure Access, und suchen Sie die Funktion für die Aktivitätssuche, um die Protokolle der Datenverkehrsüberprüfung und den Entschlüsselungsstatus für bestimmte Benutzersitzungen und Zielwebsites anzuzeigen.

Um Entschlüsselungsprotokolle zu aktivieren, kann diese Einstellung in den globalen Einstellungen aktiviert werden:

Dashboard -> Sicher -> Zugriffsrichtlinie -> Regelstandardwerte und globale Einstellungen -> Globale Einstellungen -> Entschlüsselungsprotokollierung.

Methode 2: Clientseitige Zertifikatverifizierung

Als zusätzliche Überprüfungsmethode können Sie clientseitige Zertifikatprüfungen durchführen, um sicherzustellen, dass der Datenverkehr entschlüsselt wird.

Wenn Cisco Secure Access den TLS-Datenverkehr erfolgreich entschlüsselt und inspiziert, wird dem Client ein eigenes Zertifikat anstatt des ursprünglichen Website-Zertifikats bereitgestellt.

So überprüfen Sie die Entschlüsselung durch die Zertifikatsüberprüfung:

1. Überprüfen Sie das Websitezertifikat.
Öffnen Sie die Zertifikatdetails im Browser, und überprüfen Sie den Aussteller und die Gültigkeitsdauer.

Wenn das Zertifikat von der Cisco Secure Access Root CA mit einer Gültigkeitsdauer von ca. 10 Tagen ausgestellt wird, weist es auf die Entschlüsselung des Intrusion Prevention-Systems auf Firewall-Ebene hin.

Beträgt die Gültigkeit des Zertifikats ca. 5 Tage, weist es auf eine auf Secure Web Gateway basierende Entschlüsselung hin.

2. Überprüfen des Zertifikatausstellers (DC-Benennung)

Diese clientseitige Zertifikatsüberprüfungsmethode dient als ergänzende Bestätigungstechnik neben der primären Aktivitätssuchmethode und bietet zusätzliche Sicherheit, dass die IPS-Entschlüsselungsprozesse wie erwartet funktionieren.

Intrusion Prevention System Nicht entschlüsseln:

Die Entschlüsselung für das Intrusion Prevention System wird durchgeführt, wenn -

- Es ist unter den globalen Einstellungen aktiviert UND

- Das Intrusion Prevention System ist für mindestens eine der Zugriffsrichtlinien aktiviert (obwohl die Regel deaktiviert ist, gilt diese Bedingung weiterhin)

Umgehen einer Domäne von der Entschlüsselung des Intrusion Prevention-Systems

Verwenden Sie das bereitgestellte System nicht entschlüsseln Liste und fügen Sie Domäne in das bereitgestellte System nicht entschlüsseln Liste.

Oder

Nutzung der quellenbasierten Entschlüsselung unter "Globale Einstellungen" für Cisco Secure Access -

HINWEIS: Dies funktioniert, wenn in der Netzwerk-Tunnelkonfiguration für sicheren Zugriff KEIN ausgehendes NAT konfiguriert ist.

Ursache

In Unternehmensumgebungen sind mehrere Prüfmethoden erforderlich, um die Durchsetzung von Sicherheitsrichtlinien zu validieren. Während Management-Benutzeroberflächenprotokolle

umfassende Transparenz bieten, bieten clientseitige Überprüfungsmethoden zusätzliche Bestätigungspunkte, die für Konformitätstests, Fehlerbehebung und Validierungsszenarien nützlich sein können, bei denen der direkte Zugriff auf Verwaltungsschnittstellen eingeschränkt sein kann oder bei denen mehrere Überprüfungspunkte für gründliche Testverfahren erforderlich sind.

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.