Herausforderungen bei der Identifizierung und Durchsetzung von Richtlinien pro Benutzer in Secure Web Gateway (SWG) für Umgebungen mit gemeinsam genutzten Computern mit SAML-Authentifizierung und PAC-basierter Datenverkehrsweiterleitung

Inhalt

Problem

In Cisco Secure Web Gateway (SWG)-Bereitstellungen, die Secure Access mit SAML-Authentifizierung und PAC-basierter oder Branch-to-Internet-Datenweiterleitung verwenden, wird nur der erste Benutzer, der an einem freigegebenen Computer angemeldet ist, für den Web-Datenverkehr und die Richtliniendurchsetzung richtig identifiziert. Beim Wechsel von Benutzern wird der nachfolgende Web-Datenverkehr weiterhin dem ursprünglichen Benutzer zugeordnet, selbst wenn die IP-Ersatz-Option deaktiviert ist und eine PAC-Datei verwendet wird. DNS-Abfragen geben den richtigen aktiven Benutzer über Umbrella Virtual an Appliance, aber Web- und Firewall-Protokolle ordnen die Aktivität dauerhaft dem vorherigen Benutzer zu. Die Anforderung besteht darin, zu ermitteln, ob die SWG die Identifizierung und Richtliniendurchsetzung pro Benutzer in Umgebungen mit gemeinsam genutzten Computern unterstützt und wie eine korrekte Benutzerzuordnung sichergestellt werden kann.

Umwelt

- Virtuelle Appliance für DNS-Auflösung.
- SAML-Authentifizierung für die Benutzeridentität.
- Mischung aus Datenweiterleitung mit PAC- und ohne PAC-Dateien.
- IP-Surrogat-Option aktiviert, wobei bestimmte Subnetze und Hosts für Cookie-Surrogat umgangen werden.
- Standortbasierte Geräte, keine Remote-Endgeräte oder -Benutzer

Auflösung

Das Problem wurde durch Benutzerschulungen und Konfigurationsanleitungen unter Berücksichtigung der folgenden Punkte behoben:

- Verwenden Sie die Cookie-Surrogat-Identifizierung mit PAC-Dateien. Der Datenverkehr kann in einen oder aus einem Netzwerktunnel weitergeleitet werden.
- Verwenden Sie die Cookie-Surrogat-Identifizierung ohne PAC-Dateien, aber der Datenverkehr muss durch einen Netzwerktunnel geleitet werden.
- Für die Zugriffsrichtlinie, für die Sie Cookie-Surrogate durchsetzen möchten, muss die SAML-Authentifizierung im Sicherheitsprofil aktiviert sein.
- Cookie-Surrogat-Datenverkehr ist nur für Browser-basierten Datenverkehr bestimmt. Eine separate Regel ist erforderlich, um Nicht-Cookie-Datenverkehr vom Computer (z. B. Team- oder WebEx-Datenverkehr) mit der Quellidentität als Netzwerk zu identifizieren.
- Das SWG-Modul darf nicht verwendet werden, damit Cookie-Ersatz funktioniert.
- Wenn IP-Surrogat ebenfalls aktiviert ist, müssen Sie die privaten IP-Adressen/Subnetze, die Cookie-Surrogat verwenden möchten, in der Umgehungsliste (Benutzer und Gruppen - Konfigurationsverwaltung - Erweiterte Einstellungen) hinzufügen.
- Die Umgehungsliste für Cookie-Surrogate stimmt auch mit kürzeren Präfixen überein. Beispiel: Wenn Sie
  10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
  hinzufügen.
- Das Cookie-Surrogat unterstützt das Umschalten eines Benutzers von einem Computer, ohne sich abmelden zu müssen, um mehrere Identitäten zu behalten.

Ein Großteil der Fehlerbehebung erfolgte durch Richtlinientests und die Aktivitätssuche.

Ursache

Die Hauptursache für eine falsche Benutzeridentifizierung in Umgebungen mit gemeinsam genutzten Computern liegt in der Benutzerschulung.

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.