Geografische Zugangsbeschränkung für nicht vertrauenswürdigen Zugriff und VPN-Verbindungen

Inhalt

Problem

Unternehmen, die geografische Zugriffsbeschränkungen für ZTA- (Zero Trust Access) und VPN-Verbindungen benötigen, können feststellen, dass vorhandene ZTA- und VPN-Richtlinien deaktiviert werden müssen, wenn sie versuchen, länderbasierte Zugriffskontrollen zu implementieren. Wenn Richtlinien deaktiviert werden, weil in der Secure SSE-Produktoberfläche keine Optionen für native geografische Beschränkungen gefunden werden können, geht der Zugriff auf die erforderlichen Ressourcen vollständig verloren. Die spezifische Anforderung, den Zugriff auf Verbindungen, die nur von einem bestimmten Land ausgehen, zu beschränken, kann nicht mit integrierten Produktfunktionen konfiguriert werden. Dies hat weit reichende Auswirkungen für die Benutzer, wenn bestehende Richtlinien deaktiviert werden, um solche Einschränkungen zu implementieren.

Umwelt

- Cisco Secure Access Service Edge (SASE)/Secure SSE-Produkt
- ZTNA-Implementierung (Zero Trust Access)
- VPN-Services, die eine geografische Zugriffskontrolle erfordern
- Richtlinien für den Zugriff auf private Ressourcen
- Organisation, die länderspezifische Zugriffsbeschränkungen benötigt

Auflösung

Cisco Secure SSE bietet derzeit keine nativen Funktionen, um den Zugriff auf private Ressourcen je nach geografischem Standort oder Land des Benutzers einzuschränken. Die in den nächsten Abschnitten beschriebenen Ansätze können in Betracht gezogen werden, um diese Einschränkung zu beheben.

Einsendung der Funktionsanforderung

Um Funktionen für ZTA- und VPN-Zugriffe hinzuzufügen, muss eine Funktionsanfrage bei Cisco eingereicht werden. Diese Verbesserungsanfrage wird vom Produktteam hinsichtlich einer möglichen Aufnahme in zukünftige Versionen bewertet. Organisationen können mit ihrem Cisco Account Manager zusammenarbeiten, um solche Funktionsanforderungen entsprechend zu priorisieren.

Überlegungen zur manuellen Problemumgehung

Eine mögliche manuelle Problemumgehung besteht darin, länderspezifische öffentliche IP-Adressbereiche als Netzwerkobjektgruppen in Zugriffsrichtlinien hinzuzufügen.

Schritt 1: Rufen Sie die öffentlichen IP-Adressbereiche des Landes im entsprechenden regionalen Internet-Register (RIR) ab.

Phase 2: Erstellen Sie Netzwerkobjektgruppen, die die angegebenen IP-Bereiche enthalten. Konfigurieren Sie die Netzwerkobjektgruppen in der Zugriffsrichtlinienkonfiguration so, dass sie die spezifischen IP-Adressbereiche enthalten, die dem Zielland zugewiesen sind.

Schritt 3: Wenden Sie die Netzwerkobjektgruppen auf die Zugriffsrichtlinien an. Ändern Sie vorhandene Zugriffsrichtlinien, um auf die erstellten Netzwerkobjektgruppen zu verweisen, und beschränken Sie so effektiv den Zugriff auf Verbindungen, die von den angegebenen IP-Bereichen ausgehen.

Wichtige Einschränkungen

Dieser manuelle Ansatz hat erhebliche Einschränkungen, da er auf statischen IP-Bereichsdefinitionen basiert und keine dynamischen IP-Zuweisungen, mobilen Benutzer oder VPN-Services berücksichtigen kann, die geografische Beschränkungen umgehen könnten.

Darüber hinaus erfordert diese Methode laufende Wartung, um die Genauigkeit des IP-Bereichs sicherzustellen.

Temporäres Richtlinienmanagement

Solange keine permanente Lösung verfügbar ist, müssen Unternehmen vermeiden, alle ZTA- und VPN-Richtlinien gleichzeitig zu deaktivieren. Erwägen Sie stattdessen die Implementierung eines schrittweisen Ansatzes, bei dem kritische Zugriffsrichtlinien aktiv bleiben, während Anforderungen geografischer Einschränkungen durch alternative Methoden erfüllt werden oder auf Produkterweiterungen warten.

Ursache

Die Cisco Secure SSE-Produktarchitektur umfasst keine nativen geografischen Zugriffskontrollfunktionen für den Zugriff auf private Ressourcen. Das Rahmenwerk für Produktzugriffsrichtlinien basiert auf der Benutzeridentität, dem Gerätestatus und netzwerkbasierten Kontrollen, berücksichtigt jedoch nicht den geografischen Standort als Parameter zur Richtliniendurchsetzung. Dies stellt eher eine Lücke bei den Produktfunktionen als ein Konfigurationsproblem oder einen Softwarefehler dar.

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.