Client-basierte ZTA Secure Access - Konfiguration und Verhalten

Inhalt

Problem

Beim Einsatz für den Internetzugriff wurden Fragen zum Verhalten und den Konfigurationsmöglichkeiten der clientbasierten Zero Trust Access (ZTA)-Statusfunktion von Cisco Secure Access gestellt. Zu den spezifischen Bedenken zählten:

- Hiermit wird festgelegt, ob Anforderungen an den Betriebssystemstatus eine konfigurierbare Kulanzfrist von bis zu 365 Tagen unterstützen, während der Geräte das ZTA-Modul weiterhin für den Zugriff auf Internetziele verwenden können, auch wenn sie nicht die erforderliche Betriebssystemversion erfüllen.
- Legt fest, ob Statusanforderungen, die nicht mit dem Betriebssystem übereinstimmen, wie z. B. Firewall oder Systemkennwort, zu einer sofortigen Blockierung des Zielzugriffs führen, wenn diese nicht erfüllt werden.
- Legt fest, ob benutzerdefinierte Warnmeldungen oder andere Aktionen als die Blockierung (z. B. die Überwachung) für Ausfälle bei Statusanforderungen über die Benutzeroberfläche für sicheren Zugriff konfiguriert werden können.

Umwelt

- Cisco Secure Access mit ZTNA-Funktion (Zero Trust Access)
- Client-basierte ZTA-Statusimplementierung
- Einsatzszenario für Internetzugriff
- Statusanforderungen, einschließlich Betriebssystem, Firewall und Systemkennwort

Auflösung

Die in den nächsten Abschnitten beschriebenen Klarstellungen beziehen sich auf das Verhalten bei und die Konfigurationsfunktionen von Secure Access auf Client-Basis für den ZTA-Status.

Kulanzfrist für Betriebssystemstatus

Das beschriebene Verhalten hinsichtlich der Betriebssystemstatusanforderungen ist korrekt. Bei der Konfiguration eines Betriebssystemstatus wird eine konfigurierbare Kulanzfrist von bis zu 365 Tagen unterstützt. Während dieser Kulanzfrist können Geräte, die nicht die erforderliche Betriebssystemversion erfüllen, während des Upgrades auf die Zielversion weiterhin das ZTA-Modul für den Zugriff auf Internetziele verwenden.

Statusanforderungen für nicht betriebene Systeme

Bei anderen Statusbedingungen als dem Betriebssystem (z. B. Firewall, Systemkennwort und anderen Sicherheitskontrollen) wird der Zugriff auf Ziele sofort gesperrt, wenn diese Anforderungen nicht erfüllt werden. Diese Statusarten unterstützen nicht die für die Betriebssystemanforderungen verfügbaren Funktionen für die Kulanzfrist.

Statusfehleraktionen und benutzerdefinierte Meldungen

Aktionen bei Ausfällen von Statusanforderungen werden über die Konfiguration der Zugriffsrichtlinie gesteuert.

Die Zugriffsrichtlinie unterstützt verschiedene Aktionstypen, darunter:

- Zulassen
- Blockieren
- Warnen
- Isolieren

Benutzerdefinierte Warnmeldungen und Benachrichtigungsseiten für Statusfehler können über die Sicherheitseinstellungen für Zugriffsrichtlinien konfiguriert werden. Die Verwaltung der Warn- und Benachrichtigungsseite erfolgt über die Dokumentations- und Konfigurationsschnittstelle Manage Notification Pages.

Dies bedeutet, dass andere Aktionen als die Blockierung (z. B. die Überwachung über die Warnaktion) verfügbar sind und konfiguriert werden können, im Gegensatz zur ursprünglichen Einschätzung, dass nur Blockierungsaktionen möglich waren.

Ursache

Die Fragen ergaben sich aus der Notwendigkeit, die spezifischen Verhaltensunterschiede zwischen Betriebssystemstatusanforderungen und anderen Statustypen zu verstehen und die verfügbaren Konfigurationsoptionen für die Behandlung von Statusfehlern zu klären, die in der Benutzeroberfläche für sicheren Zugriff nicht sofort erkennbar sind.

Verwandte Inhalte

- Verwalten der Dokumentation zu Benachrichtigungsseiten 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.