Azure-gehostete FQDN-Verbindungsprobleme durch sicheren Zugriff mit Meraki-Integration

Inhalt

Problem

Bestimmte Azure-gehostete FQDNs sind nicht erreichbar, wenn der Benutzerdatenverkehr über Meraki an Cisco Secure Access weitergeleitet wird, obwohl der Datenverkehr in den Protokollen für sicheren Zugriff als "zulässig" angezeigt wird. Das Problem betrifft in erster Linie die RDP-Verbindung mit nicht standardmäßigen Ports zu diesen FQDNs.

Beim Durchsuchen von Protokollen nach FQDN im Secure Access-Portal werden nur DNS-Sicherheitsprotokolle mit dem Status "allowed" angezeigt. Die RDP-Verbindung zu denselben Zielen an nicht standardmäßigen Ports schlägt jedoch fehl. Wenn der FQDN in eine IP-Adresse aufgelöst wird und die Aktivitätssuche die Ziel-IP-Adresse verwendet, werden Cloud-Firewall-Protokolle angezeigt, die den Datenverkehr blockiert haben.

Umwelt

- Cisco Secure Access (SSE) mit Meraki-Integration
- Meraki Dashboard mit lokaler Breakout-Funktion
- Von Azure gehostete Entwicklungsressourcen, die RDP-Zugriff auf nicht standardmäßigen Ports erfordern
- Datenverkehr-Routing durch Meraki-Tunnel für sicheren Zugriff

Auflösung

Sofortige Lösung

Fügen Sie die betroffenen FQDNs zu den lokalen Break-out-Regeln von Meraki hinzu, um Secure Access für die in den nächsten Abschnitten beschriebenen Ziele zu umgehen.

Schritt 1: Zugriff auf das Meraki Dashboard

Navigieren Sie zum Meraki Dashboard, und suchen Sie nach dem lokalen Abschnitt mit der Breakout-Konfiguration.

Phase 2: Lokale Breakout-Regeln konfigurieren

Fügen Sie die problematischen FQDNs zu den lokalen Breakout-Regeln hinzu, um Secure Access-Routing zu umgehen. Durch diese Konfigurationsänderung wird der Zugriff für betroffene Benutzer umgehend wiederhergestellt, indem der Datenverkehr direkt von Meraki an das Internet weitergeleitet wird, wobei der Secure Access-Tunnel umgangen wird.

Fehlerbehebung und Analyse

Schritt 1: Protokollanalyse nach FQDN

Sichere Zugriffsprotokolle mithilfe des FQDN durchsuchen. Dies zeigt in erster Linie DNS-Sicherheitsprotokolle an und kann den Status "erlaubt" für Webdatenverkehr auf Port 443 anzeigen.

Phase 2: Protokollanalyse nach Ziel-IP

Lösen Sie den FQDN auf seine IP-Adresse auf, und verwenden Sie die Ziel-IP-Adresse anstelle

des FQDN für Suchaktivitäten. Dies zeigt Cloud-Firewall-Protokolle mit blockiertem Datenverkehr an, die den tatsächlichen Status des Datenverkehrs liefern.

Schritt 3: Überprüfen des Datenverkehrsflusses

Vergewissern Sie sich, dass das Problem nur auftritt, wenn der Datenverkehr dem Pfad folgt: Benutzer → Meraki → Tunnel → Sicherer Zugriff → Internet. Test, bei dem die Umgehung über ein lokales Breakout das Verbindungsproblem löst

Langfristige Lösung

Das beobachtete Verhalten wurde als erwartete Funktionalität innerhalb der aktuellen Secure Access-Implementierung identifiziert. Es wurde eine Funktionsanfrage (FR CSE-I-5543) eingereicht, um die Sichtbarkeit und funktionalen Bedenken in Bezug auf Folgendes zu klären:

- Diskrepanz zwischen FQDN-basierten und IP-basierten Protokollsuchen
- Uneinheitliche Berichte zur Einstufung des Datenverkehrs zwischen DNS Security- und Cloud Firewall-Protokollen
- Verbesserte Transparenz für RDP-Datenverkehr an nicht standardmäßigen Ports

Ursache

Das Problem ist auf eine Diskrepanz in der Art und Weise zurückzuführen, wie Secure Access den Datenverkehr für von Azure gehostete FQDNs verarbeitet und meldet, wenn auf nicht standardmäßige Ports über RDP zugegriffen wird. Beim Durchsuchen von Protokollen nach FQDN zeigt das System primär DNS-Sicherheitsprotokolle mit dem Status "allowed" für den Web-Datenverkehr an (in der Regel Port 443). Der tatsächliche RDP-Datenverkehr an nicht standardmäßigen Ports wird jedoch von Cloud-Firewall-Regeln verarbeitet, die nur bei der Suche nach der aufgelösten Ziel-IP-Adresse und nicht nach dem FQDN sichtbar sind.

Dadurch entsteht eine Sichtbarkeitslücke, bei der Administratoren "zulässigen" Datenverkehr bei FQDN-basierten Suchen sehen, während die eigentlichen RDP-Verbindungen durch Firewall-Richtlinien blockiert werden, die nur bei IP-basierten Protokollsuchen erkennbar sind. Das

Verhalten wird derzeit als erwartete Funktionalität betrachtet, es wurde jedoch eine Funktionsanforderung gesendet, um die Transparenz und Konsistenz der Datenverkehrsberichte über verschiedene Suchmethoden hinweg zu verbessern.

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.