Problemi di connettività FQDN ospitata in Azure tramite accesso sicuro con integrazione Meraki

Sommario

Problema

Gli FQDN specifici ospitati in Azure diventano irraggiungibili quando il traffico degli utenti viene instradato tramite Meraki a Cisco Secure Access, nonostante i registri di accesso protetto mostrino che il traffico è "consentito". Il problema riguarda principalmente la connettività RDP che utilizza porte non standard per questi FQDN.

Quando si esegue la ricerca dei registri in base al nome di dominio completo (FQDN) nel portale di accesso protetto, vengono visualizzati solo i registri di protezione DNS con lo stato "consentito". Tuttavia, la connettività RDP alle stesse destinazioni sulle porte non standard non riesce. Quando l'FQDN viene risolto in un indirizzo IP e la ricerca attività utilizza l'IP di destinazione, vengono visualizzati i log del firewall del cloud che bloccavano il traffico.

Ambiente

- Cisco Secure Access (SSE) con integrazione Meraki
- Dashboard Meraki con funzionalità breakout locale
- Risorse di sviluppo ospitate da Azure che richiedono accesso RDP su porte non standard
- Routing del traffico attraverso il tunnel Meraki per un accesso sicuro

Risoluzione

Soluzione immediata

Aggiungere gli FQDN interessati alle regole di interruzione locali di Meraki per ignorare l'accesso sicuro per le destinazioni specifiche descritte nelle sezioni seguenti.

Passaggio 1: Accesso a Meraki Dashboard

Passare al dashboard Meraki e individuare la sezione di configurazione della disgregazione locale.

Passaggio 2: Configura regole di interruzione locali

Aggiungere gli FQDN problematici alle regole di interruzione locali per ignorare il routing di accesso sicuro. Questa modifica alla configurazione ripristina immediatamente l'accesso per gli utenti interessati instradando il traffico direttamente da Meraki a Internet, ignorando il tunnel Secure Access.

Risoluzione dei problemi e analisi

Passaggio 1: Analisi del log per FQDN

Cercare i registri attività accesso sicuro utilizzando il nome di dominio completo. Questo mostra principalmente i registri di sicurezza DNS e può visualizzare lo stato "consentito" per il traffico Web sulla porta 443.

Passaggio 2: Analisi del log per IP di destinazione

Risolvere il nome di dominio completo (FQDN) nel relativo indirizzo IP e cercare i registri attività utilizzando l'indirizzo IP di destinazione anziché il nome di dominio completo. Ciò rivela i log del cloud firewall che mostrano il traffico bloccato, fornendo l'effettiva eliminazione del traffico.

Passaggio 3: Verifica flusso traffico

Confermare che il problema si verifica solo quando il traffico segue il percorso: Utente → Meraki → Tunnel → Secure Access → Internet. Il test che consente di evitare l'accesso tramite breakout locale risolve il problema di connettività.

Risoluzione a lungo termine

Il comportamento osservato è stato identificato come funzionalità prevista nell'implementazione di Secure Access corrente. È stata aperta una richiesta di funzionalità (FR CSE-I-5543) per risolvere i problemi di visibilità e di funzionalità relativi a:

- Discrepanza tra le ricerche di log basate su FQDN e su IP
- Segnalazione incoerente dell'eliminazione del traffico tra la sicurezza DNS e i registri del firewall del cloud
- Maggiore visibilità del traffico RDP su porte non standard

Causa

Il problema deriva da una discrepanza nel modo in cui Secure Access elabora e segnala il traffico per gli FQDN ospitati in Azure quando vi si accede tramite RDP su porte non standard. Quando si esegue la ricerca dei log in base al nome FQDN, il sistema visualizza principalmente i log di sicurezza DNS che mostrano lo stato "consentito" per il traffico Web (in genere la porta 443). Tuttavia, il traffico RDP effettivo su porte non standard viene elaborato dalle regole del firewall del cloud, visibili solo quando si esegue la ricerca in base all'indirizzo IP di destinazione risolto anziché al nome di dominio completo (FQDN).

Ciò crea un gap di visibilità in cui gli amministratori vedono il traffico "consentito" nelle ricerche basate su FQDN mentre le connessioni RDP effettive vengono bloccate dai criteri firewall che sono evidenti solo nelle ricerche dei log basati su IP. Il comportamento è attualmente considerato funzionalità prevista, ma è stata inviata una richiesta di funzionalità per migliorare la visibilità e la coerenza dei report del traffico tra i diversi metodi di ricerca.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).