Disconnessioni intermittenti di Secure Access dietro i firewall aziendali con errori di timeout di inattività

Sommario

Problema

Ambiente

Risoluzione

- Passaggio 1: Implementa configurazione buffer TTL MX
- Passaggio 2: Configurare le esclusioni di dominio necessarie
- Passaggio 3: Verifica delle autorizzazioni per porte e protocolli
- Passaggio 4: Monitora e convalida risoluzione

Causa

Contenuto correlato

- Problema
- Ambiente
- Risoluzione
  - Passaggio 1: Implementa configurazione buffer TTL MX
  - Passaggio 2: Configurare le esclusioni di dominio necessarie
  - Passaggio 3: Verifica delle autorizzazioni per porte e protocolli
  - Passaggio 4: Monitora e convalida risoluzione
- Causa
- Contenuto correlato

Problema

I client Cisco Secure Access rilevano disconnessioni intermittenti e riconnessioni immediate quando gli endpoint sono connessi alla rete aziendale. Le disconnessioni avvengono in modo casuale e il client si riconnette automaticamente dopo circa 5 secondi. Questo comportamento viene osservato quando il traffico Internet viene inoltrato tramite Zero Trust Access (ZTA) ad Secure Access da endpoint posizionati dietro i dispositivi Cisco FirePower e Meraki MX.

Il registro eventi di Windows acquisisce gli errori specifici di "idleTimeout" durante questi eventi di disconnessione. Il modello di disconnessione non si verifica quando gli utenti si connettono da una connessione Internet domestica, indicando che il problema è specificamente correlato

all'infrastruttura di rete aziendale.

Il sintomo crea interruzioni delle attività aziendali per proteggere la connettività di accesso remoto per gli utenti che operano nell'ambiente di rete aziendale, mentre gli utenti remoti non sono interessati da questo problema di connettività.

Ambiente

- Cisco Secure Access - Implementazione vantaggiosa
- Software client Cisco Secure Internet Access (SIA)
- Infrastruttura di rete aziendale con appliance di sicurezza Cisco FirePower
- Appliance di sicurezza Meraki MX nel percorso di rete
- Configurazione ZTA (Zero Trust Access) che inoltra il traffico Internet ad accesso sicuro
- Endpoint Windows con funzionalità di registrazione eventi
- Scenari di connettività misti: rete aziendale (interessata) e connessioni Internet domestiche (non interessata)

Risoluzione

La risoluzione implicava l'implementazione di modifiche alla configurazione del dispositivo Meraki MX e la garanzia di esclusioni di dominio e di autorizzazioni di porta adeguate per l'integrazione Secure Access.

Passaggio 1: Implementa configurazione buffer TTL MX

Configurare un buffer TTL MX sul dispositivo Meraki MX per risolvere il comportamento della cache TTL DNS che contribuiva ai problemi di disconnessione intermittente. Questa modifica alla configurazione consente di risolvere i conflitti di tempo tra la memorizzazione nella cache della risoluzione DNS e le aspettative di connettività dei client Secure Access.

Passaggio 2: Configurare le esclusioni di dominio necessarie

Accertarsi che questi domini siano correttamente esclusi dall'intercettazione e aggiunti agli elenchi dei domini non decriptati su dispositivi Cisco FirePower e Meraki MX:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Domini aggiuntivi del servizio Secure Access identificati nella configurazione dei criteri

Passaggio 3: Verifica delle autorizzazioni per porte e protocolli

Configurare l'infrastruttura firewall aziendale in modo da consentire le porte e i protocolli di accesso sicuro richiesti tramite i dispositivi FirePower e Meraki MX. Verificare che il traffico diretto alla porta 443 per gli endpoint del servizio Secure Access venga gestito correttamente senza interferenze derivanti dall'ispezione di sicurezza che potrebbe causare condizioni di timeout.

Passaggio 4: Monitora e convalida risoluzione

Dopo aver implementato la configurazione del buffer TTL MX, monitorare il comportamento del client Secure Access per diversi giorni per verificare che il modello di disconnessione e riconnessione intermittente sia terminato.

Causa

Le disconnessioni intermittenti sono state causate da conflitti di comportamento della cache TTL (Time To Live) DNS tra l'infrastruttura di rete aziendale e le aspettative del servizio Secure Access. L'analisi tecnica di Cisco ha rilevato che i valori TTL DNS variano a causa del comportamento della cache del resolver e che si prevede un comportamento alternato degli indirizzi IP a causa dei meccanismi di bilanciamento del carico nell'architettura del servizio Secure Access.

Quando i dispositivi di rete aziendali (Cisco FirePower e Meraki MX) hanno elaborato le risposte

DNS per gli endpoint ad accesso sicuro, la memorizzazione nella cache e la gestione dei valori TTL hanno creato una mancata corrispondenza degli intervalli che ha causato condizioni di "idleTimeout". Questo conflitto di tempistica ha causato l'interpretazione della connessione da parte del client Secure Access come inattiva e l'avvio dei cicli di disconnessione/riconnessione.

Il problema era specifico degli ambienti di rete aziendali, in quanto le connessioni Internet domestiche in genere non implementano lo stesso livello di caching DNS e di ispezione del traffico che può interferire con la gestione dello stato della connessione client di accesso sicuro.

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).