Errore di sincronizzazione della configurazione ZTNA di accesso sicuro con decrittografia SSL e tunnel di rete

Sommario

Problema

La registrazione di Cisco Secure Client Zero Trust Access (ZTA) è riuscita, ma si è verificato un errore durante la sincronizzazione della configurazione con risposte HTTP 502 e stato di connettività del server "BadResponse". I registri DART dall'endpoint di Windows 11 mostrano la corretta registrazione ma errori di sincronizzazione della configurazione ripetuti. Il problema si verifica solo quando l'endpoint è connesso al percorso di rete aziendale utilizzando il proxy Secure Access/Umbrella con i tunnel Meraki AutoVPN, mentre lo stesso endpoint completa correttamente la sincronizzazione della configurazione su una rete domestica senza infrastruttura proxy o tunnel.

Ambiente

- Cisco Secure Client ZTA versione 5.1.16.4434
- Windows 11 Enterprise Endpoint
- Appliance Meraki MX con integrazione AutoVPN
- SSE (Secure Access) con NTG (Network Tunnels Gateway)
- DNS Umbrella e Secure Access Web Security
- Decrittografia SSL e ispezione HTTPS abilitate sul percorso di rete aziendale
- DND (Do Not Decrypt List) fornito dal sistema non configurato inizialmente

Risoluzione

L'errore di sincronizzazione della configurazione è stato risolto implementando i byte di decrittografia SSL appropriati per i domini correlati a ZTA quando si utilizzano tunnel di rete con accesso protetto.

Passaggio 1: Identificazione impatto decrittografia SSL

Verificare che la decrittografia SSL causi gli errori di sincronizzazione della configurazione esaminando i log di Ricerca attività in Accesso sicuro per gli eventi di decrittografia correlati ai domini ZTA.

Passaggio 2: Configura elenco DND fornito dal sistema

Quando si utilizza Network Tunnels Gateway (NTG) con Secure Access, il DND fornito dal sistema deve essere abilitato per ignorare correttamente il traffico ZTA proveniente dall'ispezione SSL.

Passare a Dashboard di accesso protetto > Protetto > Non decrittografare elenchi e modificare l'elenco Non decrittografare fornito dal sistema.

Passaggio 3: Crea profilo di sicurezza per domini ZTA

Aggiungere i domini ZTA richiesti a un nuovo profilo di sicurezza utilizzando l'elenco DND fornito dal sistema:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

Passaggio 4: Applica profilo di sicurezza alla regola di test

Assegnare il profilo di sicurezza appena creato contenente il dominio ZTA a una regola di test per convalidare la configurazione.

Passaggio 5: Convalida sincronizzazione della configurazione

Verificare la sincronizzazione della configurazione e della registrazione ZTA dalla rete aziendale. La sincronizzazione può essere completata senza errori HTTP 502.

Passaggio 6: Coordinamento con il team Meraki

Per una copertura completa, coordinati con il supporto Meraki per convalidare gli URL e i domini ufficiali relativi a ZTA che possono essere ignorati dall'ispezione Secure Access. Fare riferimento alla seguente documentazione di Meraki:

- Regole firewall upstream per connettività cloud
- Aggiornamento URL dashboard Meraki - Conformità PCI

Causa

L'errore di sincronizzazione della configurazione è stato causato dalla decrittografia SSL e dalla trasmissione tramite proxy del traffico di accesso con attendibilità zero sulla rete aziendale. Quando si utilizza Network Tunnels Gateway (NTG) con Secure Access, i domini relativi a ZTA devono essere ignorati usando il DND (Do Not Decrypt List) fornito dal sistema. Senza questa configurazione di bypass, l'ispezione SSL modifica le catene di certificati e interferisce con la comunicazione del control plane ZTA, causando la ricezione di risposte HTTP 502 da parte del client durante i tentativi di sincronizzazione della configurazione.

Contenuto correlato

- Risoluzione dei problemi relativi a Secure Access Decryption e SSL

- Servizi di registrazione basati su client con Zero Trust per l'accesso sicuro
- Requisiti del dominio ZTA per l'accesso sicuro
- Risoluzione dei problemi relativi alla registrazione degli errori di Secure Access
- Risoluzione dei problemi di sincronizzazione della configurazione client sicura
- Raccolta dei log ZTNA dettagliati per la risoluzione dei problemi
- 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).