

Il proxy Umbrella blocca la connettività delle applicazioni Ninja

Sommario

Problema

Gli utenti non sono in grado di eseguire un sistema remoto utilizzando un file di installazione scaricato quando sono connessi tramite Cisco Umbrella. L'applicazione non funziona sotto la protezione Umbrella, influenzando in modo specifico sull'accesso al sistema remoto. Lo stesso sistema remoto funziona perfettamente senza alcun problema quando il proxy Cisco Umbrella è disabilitato.

I tentativi di risoluzione dei problemi includevano il test con un criterio separato in cui la sicurezza del sistema e la destinazione erano impostate su ANY (QUALSIASI), ma il problema persisteva. Inoltre, è stato tentato il routing del traffico tramite ZTA (Zero Trust Access), ma il problema è rimasto invariato. Il traffico è stato consentito tramite l'accesso protetto su TCP/443, ma le connessioni erano ancora bloccate sull'endpoint.

Ambiente

- Cisco Umbrella con funzionalità proxy abilitata
- Configurazione ZTA (Zero Trust Access)
- Criteri di accesso sicuro configurati per il traffico TCP/443

Risoluzione

La risoluzione implica l'esclusione di specifici domini relativi a NinjaOne dal proxy Umbrella per consentire la connettività diretta per l'applicazione di accesso remoto.

Passaggio 1: Identifica domini interessati

L'analisi dell'acquisizione dei pacchetti e dei file HAR rivela che questi domini relativi a NinjaOne sono influenzati dal proxy Umbrella:

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Passaggio 2: Configura esenzioni dominio

Escludere i domini identificati dai criteri di sicurezza Internet Secure Web Gateway (SWG) e dal controllo del traffico Internet ZTA. Questa modifica alla configurazione consente a questi domini di ignorare il proxy Umbrella e stabilire connessioni dirette.



Nota: Una configurazione dell'elenco DND (Do Not Decrypt) è stata considerata inefficace per la risoluzione del problema. La direzione del traffico e l'esenzione sono l'approccio raccomandato.

Passaggio 3: Applica modifiche alla configurazione

Implementare le esenzioni del dominio nella configurazione Umbrella per escludere il traffico relativo a NinjaOne dall'elaborazione proxy. Ciò consente all'applicazione di accesso remoto di stabilire connessioni dirette ai servizi richiesti.

Passaggio 4: Convalida risoluzione

Verificare la funzionalità dell'applicazione di accesso remoto dopo aver applicato le esenzioni per garantire il ripristino della corretta connettività mantenendo la protezione Umbrella per il traffico di altro tipo.

Causa

Il problema si verifica perché le applicazioni di accesso remoto NinjaOne rifiutano le connessioni proxy quando il traffico viene instradato tramite il proxy Cisco Umbrella. L'applicazione richiede una connettività diretta a domini NinjaOne specifici per funzionare correttamente. Quando queste connessioni vengono inoltrate tramite Umbrella, il servizio di accesso remoto non è in grado di stabilire i canali di comunicazione necessari, con conseguente errore dell'applicazione anche quando i criteri di sicurezza sono configurati per consentire il traffico.

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).