

Paraplu proxy blokkeert Ninja Application Connectivity

Inhoud

uitgeven

Gebruikers kunnen een extern systeem niet uitvoeren met een gedownload installatiebestand wanneer ze zijn verbonden via Cisco Umbrella. De toepassing functioneert niet onder Paraplu-bescherming, met name wat betreft de toegang tot het externe systeem. Hetzelfde externe systeem werkt perfect zonder problemen wanneer de Cisco Umbrella-proxy is uitgeschakeld.

Pogingen tot probleemoplossing omvatten testen met een apart beleid waarbij de systeembeveiliging en de bestemming waren ingesteld op ANY, maar het probleem bleef bestaan. Bovendien werd geprobeerd het verkeer door Zero Trust Access (ZTA) te leiden, maar het probleem bleef ongewijzigd. Verkeer was toegestaan via Secure Access op TCP/443, maar verbindingen werden nog steeds geblokkeerd op het eindpunt.

milieu

- Cisco Umbrella met proxy-functionaliteit ingeschakeld
- Zero Trust Access (ZTA)-configuratie
- Beleid voor beveiligde toegang geconfigureerd voor TCP/443-verkeer

resolutie

De oplossing omvat het uitsluiten van specifieke NinjaOne-gerelateerde domeinen van de Umbrella-proxy om directe connectiviteit voor de toepassing voor externe toegang mogelijk te maken.

Stap 1: Identificeer de betrokken domeinen

Analyse van de pakketopname en HAR-bestanden onthult dat deze NinjaOne-gerelateerde domeinen worden beïnvloed door de Umbrella-proxy:

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

Stap 2: Domeinvrijstellingen configureren

Sluit de geïdentificeerde domeinen uit van zowel het beveiligingsbeleid voor Secure Web Gateway (SWG) Internet Security als de besturing van het internetverkeer door ZTA. Door deze configuratiewijziging kunnen deze domeinen de paraplu-proxy omzeilen en directe verbindingen tot stand brengen.



Opmerking: een DND-lijstconfiguratie (Do Not Decrypt) is niet effectief gebleken voor het oplossen van dit probleem. Verkeerssturing en ontheffing is de aanbevolen aanpak.

Stap 3: Configuratiewijzigingen toepassen

Implementeer de domeinvrijstellingen in de Umbrella-configuratie om het NinjaOne-gerelateerde verkeer uit te sluiten van proxy-verwerking. Hierdoor kan de toepassing voor externe toegang rechtstreekse verbindingen tot stand brengen met de vereiste services.

Stap 4: Resolutie valideren

Test de functionaliteit van de toepassing voor externe toegang na het toepassen van de uitzonderingen om ervoor te zorgen dat de juiste connectiviteit wordt hersteld terwijl de overkoepelende bescherming voor ander verkeer behouden blijft.

Oorzaak

Het probleem treedt op omdat NinjaOne-toepassingen voor externe toegang proxyverbindingen weigeren wanneer het verkeer via de Cisco Umbrella-proxy wordt geleid. De applicatie vereist directe connectiviteit met specifieke NinjaOne-domeinen om goed te kunnen functioneren. Wanneer deze verbindingen via Umbrella worden geproxydeerd, kan de service voor externe toegang niet de benodigde communicatiekanalen tot stand brengen, wat leidt tot toepassingsfouten, zelfs wanneer het beveiligingsbeleid is geconfigureerd om het verkeer toe te staan.

Verwante inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.