Proxypoorten configureren voor niet-standaard poortverkeer op WSA 1000V

Inhoud

uitgifte

Een WSA 1000V-proxy die op VMware werd gehost, verwerkte het clientverkeer correct op poorten 80 en 443, maar verwerkte het verkeer niet op niet-standaard poorten zoals poort 8890. Wanneer de toegang tot een bestemming met een niet-standaard poort in eerste instantie werd geblokkeerd door het beleid, de WSA correct gelogd de geblokkeerde aanvraag. Na het toevoegen van het IP-adres en de URL om een beleid toe te staan, is het verkeer echter nog steeds mislukt en zijn er geen overeenkomstige logs gegenereerd op de proxy. Dit gedrag suggereerde dat het verkeer niet werd bereikt of wordt verwerkt door de WSA nadat het allow-beleid werd gemaakt, wat van invloed is op de toegang van de client tot toepassingen met behulp van niet-standaard poorten.

milieu

- Cisco WSA 1000V-proxy gehost op VMware
- Software versie 15.0.0
- Verkeer op poorten 80 en 443 die normaal worden verwerkt.
- Niet-standaard poortverkeer (bijvoorbeeld poort 8890) dat niet door de proxy wordt verwerkt.
- Sta beleidsregels toe die zijn geconfigureerd voor getroffen bestemmingen.

resolutie

Het probleem is opgelost door de WSA te configureren voor ondersteuning van niet-standaard poorten in de instellingen voor het identificatieprofiel. De configuratie van de proxypoorten moest

worden bijgewerkt om de vereiste niet-standaard poortnummers op te nemen.

Configuratiestappen

Stap 1: Toegang tot de interface van Web Security Manager.

Stap 2: Navigeer naar de configuratie Identificatieprofielen.

Navigeer naar Web Security Manager > Identificatieprofielen.

Stap 3: Selecteer het gewenste identificatieprofiel waarvoor niet-standaard poortondersteuning nodig is.

Stap 4: Breid de geavanceerde configuratie-opties uit.

Vouw op de pagina Identificatieprofiel het tabblad Geavanceerd uit.

Stap 5: Configureer de instelling Proxy Ports.

Selecteer de koppeling naast Proxypoorten om toegang te krijgen tot de poortconfiguratie.

Stap 6: Voeg de vereiste niet-standaard poortnummers toe.

Voeg de specifieke poortnummers toe die clients gebruiken voor niet-standaard poortverbindingen (bijvoorbeeld 8890).

Stap 7: Opslaan en vastleggen van de configuratiewijzigingen.

Na het implementeren van deze configuratiewijzigingen kan de WSA verkeer op de opgegeven niet-standaard poorten verwerken en inspecteren, waardoor de proxy clientverbindingen goed kan verwerken en beleid kan toepassen op verkeer met behulp van deze poorten.

Oorzaak

De WSA 1000V is geconfigureerd met standaard proxypoortinstellingen die alleen standaard HTTP-poorten (poort 80) en HTTPS-poorten (poort 443) bevatten. De configuratie van de proxypoorten voor het identificatieprofiel omvatte niet de niet-standaard poorten die vereist zijn voor de clienttoepassingen. Zonder dat deze poorten expliciet zijn geconfigureerd in de geavanceerde instellingen van het identificatieprofiel, kon de WSA geen beleid voor verkeer onderscheppen, verwerken of toepassen met niet-standaard poorten, zelfs niet wanneer beleid voor de bestemmingen is geconfigureerd.

Gerelateerde 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.