Verbinding met Azure VPN-client mislukt met Secure Access Web Security ingeschakeld

Inhoud

uitgeven

Na de migratie van Umbrella naar SSE en het inschakelen van Web Security met een nieuw toegewezen SIA-licentie, kunnen Azure VPN Client-verbindingen niet worden gemaakt voor gebruikers wanneer Web Security is ingeschakeld. Het probleem met de connectiviteit van Azure VPN-clients is van invloed op alle clients, waardoor deze geen verbinding kunnen maken met de VPN. Wanneer de Cisco Secure Access Client wordt verwijderd van clientcomputers, wordt de VPN-connectiviteit hersteld, wat aangeeft dat de Secure Access-client de verbinding met Azure VPN-services blokkeert.

Als u Web Security uitschakelt of de installatie van de Cisco Secure Access-client ongedaan maakt, wordt de VPN-verbinding hersteld, maar dit heeft gevolgen voor de toegang van gebruikers tot bronnen via Azure VPN wanneer beveiliging via Web Security nodig is.

milieu

- Cisco Secure Access (voorheen SIA) met Web Security ingeschakeld
- Azure VPN Client
- Migratie van paraplu naar SSE afgerond
- Nieuw toegewezen SIA-licentie

resolutie

De oplossing omvat het toevoegen van het openbare IP-adres van de Azure VPN-gateway aan de

SSE/SWG-uitzonderingslijst om te voorkomen dat verkeer wordt onderschept dat VPN-verbindingen blokkeert.

Stap 1: Identificeer het Azure VPN Gateway IP-adres

Bepaal het publieke IP-adres van de Azure VPN-gateway.

Stap 2: IP-gebaseerde uitzondering toevoegen aan SSE/SWG

1.- Voeg het openbare IP-adres van Azure Virtual Gateway toe aan de uitzonderingenlijst SSE/SWG in de Cisco Secure Access-omgeving.

2.- Meld u aan bij het Cisco Secure Access Dashboard - Klik op Verbinden - Connectiviteit voor eindgebruikers - Internet Security - Uitzondering toevoegen. Dit voorkomt dat de Secure Web Gateway verkeer onderschept en inspecteert dat bestemd is voor de Azure VPN-gateway.

Stap 3: VPN-connectiviteit testen

Nadat u de op IP gebaseerde uitzondering hebt toegepast, test u de Azure VPN-verbinding om te controleren of clients met succes VPN-verbindingen kunnen maken met Web Security ingeschakeld.

Stap 4: testen uitbreiden

Het testen van de IP-gebaseerde uitzondering uitbreiden tot extra gebruikers in de omgeving om consistente functionaliteit te garanderen voordat de oplossing als voltooid wordt beschouwd.

Oorzaak

Het probleem treedt op omdat het SWG-uitzonderingsmechanisme (Secure Web Gateway) vereist dat een DNS-zoekopdracht voor een domein wordt uitgevoerd om een cachevermelding van domein naar IP te maken. Wanneer de Azure VPN-client rechtstreeks verbinding maakt met het IP-adres zonder een DNS-query voor de VPN-URL uit te voeren, kan de SWG-module het domein niet toewijzen aan het IP-adres. Als gevolg hiervan blijft de SWG het verkeer naar het IP-adres inspecteren en onderscheppen, waardoor de VPN-verbinding niet tot stand kan komen.

Analyse van pakketregistratie toonde geen DNS-query's voor de VPN-URL en geen zichtbaar SWG-interceptieverkeer voor de Azure-gateway IP, wat bevestigt dat de SWG de verbinding blokkeerde vanwege het ontbreken van de juiste toewijzing van domeinen naar IP in de cache.

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.