

SWG configureren om conflicten met SSL VPN-verkeer te voorkomen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe incompatibiliteitsproblemen tussen Secure Web Gateway (SWG) en SSL VPN's met behulp van onderschepte poorten kunnen worden opgelost.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Umbrella SWG voor AnyConnect kan problemen ondervinden met incompatibiliteit met bepaalde SSL VPN's die gebruikmaken van poorten die zijn onderschept door de SWG-agent, zoals TCP 443. AnyConnect SWG kan de dekking niet op betrouwbare wijze activeren en toepassen. De betrouwbaarheid van het netwerk kan verslechteren of onbeschikbaar worden wanneer SWG actief is en VPN-verkeer via SWG verloopt. Niet-webverkeer wordt in dit scenario weggelaten. Dit probleem is van invloed op alle SSL VPN's die gebruikmaken van poorten 80 en 443.

Oplossing

Om te voorkomen dat SWG VPN-verkeer onderschept, configureert u een bypass voor uw VPN-domeinen en IP-adressen:

1. Navigeer in het Umbrella-dashboard naar Access Deployment > Domain Management > External Domains.
2. Voeg het domein en het IP-adres van uw VPN-head-endservers toe aan de lijst Externe domeinen. De IP-vermelding zorgt ervoor dat VPN-verkeer nooit wordt onderschept door de SWG-agent vanwege het grote aantal verbindingen.
3. Laat een uur wachten voordat de nieuwe instelling zich voortplant.

SSL VPN gebruiken met SWG:

1. Voeg het VPN-domein toe aan de lijst Externe domeinen.
2. Als het VPN head end domein een DNS Search Suffix is, voegt de client dit domein automatisch toe voor de duur van de verbinding.
3. Voeg de IP-adressen of het IP-bereik van het VPN-hoofdeinde toe aan de lijst Externe domeinen.

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.