Configuratie van de stuurgedrag en uitzonderingenlijst voor veilig toegangsverkeer

Inhoud

uitgeven

Gebruikers hebben verduidelijking nodig over het gedrag van Cisco Secure Access Traffic Steering wanneer ze de ZTA gebruiken om alle internetbestemmingen te beveiligen met standaardconfiguraties voor uitzonderingen. Er rijzen specifieke vragen over:

- Of beslissingen over verkeerssturing zijn gebaseerd op IP-adressen van bestemming na DNS-resolutie.
- Hoe DNS-verkeer zelf wordt afgehandeld in het stuurproces.
- Of aanvullende lokale domeinvermeldingen moeten worden geconfigureerd buiten de standaard .local-domeinvermelding in de uitzonderingenlijst.

De configuratie in kwestie bevindt zich op: Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > (profielen zonder vertrouwen) > Beveiligde internettoegang > Verkeerssturing > ZTA gebruiken om alle internetbestemmingen te beveiligen

De lijst met standaarduitzonderingen bevat privé-IP-adresbereiken (klasse A, B en C) en het .local-domein, en gebruikers moeten het operationele gedrag van deze instellingen begrijpen.

milieu

- Cisco Secure Access
- Zero Trust Access (ZTA)-configuratie
- Traffic Steering-functie ingeschakeld
- Standaard uitzonderingenlijst met privé-IP-bereiken en .local-domein

resolutie

Het stuurgedrag van Cisco Secure Access Traffic werkt als volgt:

besluitvormingsproces inzake verkeerssturing

Verkeersstuurbeslissingen worden genomen op basis van het IP-adres van de bestemming na DNS-resolutie. Het systeem evalueert de werkelijke IP-bestemming die voortvloeit uit de DNS-naamresolutie om te bepalen of het verkeer door de Zero Trust Access-beveiligingsstack moet worden geleid.

DNS-verkeersafhandeling

DNS-query's zelf zijn niet onderhevig aan verkeerssturing. Wanneer eindpunten DNS-servertoewijzingen ontvangen via DHCP die verwijzen naar interne DNS-servers (meestal met behulp van privé-IP-adressen), omzeilen deze DNS-communicatie het stuurmechanisme voor het verkeer en worden ze lokaal afgehandeld.

Configuratie van uitzonderingenlijst

De lijst met standaarduitzonderingen bevat:

- Privé IP-adresbereiken (Klasse A: 10.0.0.0/8, Klasse B: 172.16.0.0/12, Klasse C: 192.168.0.0/16)
- Het .local domein

Voor organisaties die aangepaste lokale domeinen (interne domeinnamen) gebruiken, moeten aanvullende domeinvermeldingen worden toegevoegd aan de uitzonderingenlijst om ervoor te zorgen dat intern verkeer niet onnodig door de beveiligingsstack wordt geleid. Het standaard .local-item dekt standaard lokale netwerkdetectieprotocollen, maar omvat mogelijk niet alle interne domeinen van de organisatie.

Configuratieverificatie

Om de juiste configuratie te controleren:

Navigeer naar Verbinding maken > Eindgebruikersconnectiviteit > Toegang zonder vertrouwen > Veilige internettoegang > Verkeerssturing.

Controleer de uitzonderingenlijst om ervoor te zorgen dat deze alle benodigde privé-IP-bereiken en lokale domeinnamen bevat die specifiek zijn voor de interne infrastructuur van uw organisatie.

Oorzaak

Dit is een informatieverzoek over het operationele gedrag van de Cisco Secure Access Traffic Steering-functies. De behoefte aan verduidelijking komt voort uit de complexiteit van de verkeerssturingslogica en de interactie tussen DNS-resolutie, IP-gebaseerde routeringsbeslissingen en mechanismen voor uitzonderingsafhandeling.

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.