Geografische toegangsbeperking voor zero trust-toegang en VPN-verbindingen

Inhoud

uitgifte

Organisaties die geografische toegangsbeperkingen vereisen voor Zero Trust Access (ZTA)- en VPN-verbindingen, kunnen merken dat het bestaande ZTA- en VPN-beleid moet worden uitgeschakeld wanneer ze proberen landgebaseerde toegangscontroles te implementeren. Gebruikers ervaren volledig verlies van toegang tot vereiste bronnen wanneer beleid is uitgeschakeld vanwege het onvermogen om native geografische restrictieopties te vinden binnen de Secure SSE-productinterface. De specifieke eis om de toegang te beperken tot verbindingen die alleen afkomstig zijn uit een bepaald land, kan niet worden geconfigureerd met behulp van ingebouwde productmogelijkheden, wat resulteert in een wijdverbreide impact van de gebruiker wanneer bestaande beleidsregels worden gedeactiveerd in een poging om dergelijke beperkingen te implementeren.

milieu

- Cisco Secure Access Service Edge (SASE) / Secure SSE-product
- Zero Trust Access (ZTNA)-implementatie
- VPN-services waarvoor geografische toegangscontrole vereist is
- Privébeleid voor toegang tot bronnen
- Organisatie die landspecifieke toegangsbeperkingen vereist

resolutie

Het Cisco Secure SSE-product biedt momenteel geen native functionaliteit om de toegang tot

privébronnen te beperken op basis van de geografische locatie of het land van de gebruiker. De in de volgende paragrafen beschreven benaderingen kunnen worden overwogen om deze beperking aan te pakken.

Aanvraag voor functie indienen

Er moet een aanvraag voor functies worden ingediend bij Cisco om geografische beperkingsmogelijkheden voor ZTA- en VPN-toegang toe te voegen. Dit verbeteringsverzoek wordt door het productteam beoordeeld op mogelijke opname in toekomstige releases. Organisaties kunnen samenwerken met hun Cisco Account Manager om te helpen bij het prioriteren van dergelijke functieverzoeken op basis van zakelijke vereisten.

Overweging voor handmatige oplossing

Een mogelijke handmatige oplossing omvat het toevoegen van landspecifieke openbare IP-adresbereiken als netwerkobjectgroepen in toegangsbeleid.

Stap 1: Het verkrijgen van het land openbare IP-adres varieert van de juiste Regional Internet Registry (RIR).

Stap 2: Maak netwerkobjectgroepen met de geïdentificeerde IP-bereiken. Configureer netwerkobjectgroepen binnen de configuratie van het toegangsbeleid om de specifieke IP-adresbereiken op te nemen die aan het doelland zijn toegewezen.

Stap 3: Pas de netwerkobjectgroepen toe op het toegangsbeleid. Wijzig het bestaande toegangsbeleid om te verwijzen naar de gemaakte netwerkobjectgroepen, waardoor de toegang tot verbindingen uit de opgegeven IP-bereiken effectief wordt beperkt.

Belangrijke beperkingen

Deze handmatige aanpak heeft aanzienlijke beperkingen, omdat deze afhankelijk is van statische definities van het IP-bereik en geen rekening kan houden met dynamische IP-toewijzingen, mobiele gebruikers of VPN-services die geografische beperkingen kunnen omzeilen. Bovendien vereist deze methode voortdurend onderhoud om de nauwkeurigheid van het IP-bereik te garanderen.

Tijdelijk beleidsbeheer

Zolang er geen permanente oplossing beschikbaar is, moeten organisaties voorkomen dat alle ZTA- en VPN-beleidsregels tegelijkertijd worden uitgeschakeld. Overweeg in plaats daarvan om een gefaseerde aanpak te implementeren waarbij kritisch toegangsbeleid actief blijft terwijl geografische restrictievereisten worden aangepakt met alternatieve middelen of in afwachting van productverbeteringen.

Oorzaak

De Cisco Secure SSE-productarchitectuur bevat geen native geografische toegangsbeheermogelijkheden voor toegang tot privébronnen. Het beleidskader voor producttoegang is ontworpen rond gebruikersidentiteit, apparaathouding en netwerkgebaseerde controles, maar bevat geen geografische locatie als beleidshandhavingsparameter. Dit vertegenwoordigt een lacune in de productcapaciteit in plaats van een configuratieprobleem of een softwaredefect.

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.