Beveiligde toegang tot gereserveerde IP valideren met ZTA-client

Inhoud

uitgeven

De gebruiker probeert te valideren dat gereserveerde IP-adressen correct functioneren wanneer Cisco Secure Access wordt gebruikt met de Zero Trust Access ZTA TIA-client. De voor validatie gereserveerde IP's zijn:

- Reston, Virginia, Verenigde Staten: 151.186.128.84
- San Jose, Californië, VS: 151.186.131.49

De workflow omvat het routeren van internetverkeer via de ZTA TIA-client, niet de Umbrella Roaming-module. Umbrella SWG Module wordt uitgeschakeld zodra TIA actief is. Bij het uitvoeren van een externe IP-controle (zoals het gebruik van "whatsmyip") en het valideren van het activiteitenzoekrapport worden de verwachte gereserveerde IP-adressen niet in acht genomen.

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- subtechnologie: beveiligde toegang
- Voorbehouden IP's: 151.186.128.84 (Reston, VA), 151.186.131.49 (San Jose, CA)
- Internetverkeer dat wordt gerouteerd via een ZTA TIA-client (geen Umbrella Roaming-module)
- Geen specifieke softwareversie of hardwareplatform vermeld

resolutie

Deze stappen beschrijven de huidige workflow voor het valideren van gereserveerde IP-functionaliteit met Secure Access en ZTA-client, evenals de acties die worden ondernomen op basis van de casusgegevens.

Stap 1: IP-validatie via externe service proberen

1. Start een externe IP-controle met behulp van een openbare dienst (zoals "whatsmyip") en een activiteitenzoekrapport met behulp van een geavanceerd filter genaamd "Egress IP (Gereserveerd)" om te controleren of het internetverkeer dat via de ZTA-client wordt gerouteerd, afkomstig lijkt te zijn van het toegewezen gereserveerde IP-adres.

Beschrijving van de verwachte productie:

- Verwacht: de uitvoer moet X.X.X.X of X.X.X.X.X weergeven, afhankelijk van uw huidige geolocatie en configuratie voor beveiligde toegang.
- Werkelijk: de gereserveerde IP's worden niet weergegeven in de uitvoer.

Stap 2: Back-end provisioning controleren en bijwerken

Werk samen met TSE3 om deze taak uit te voeren.

De back-endconfiguratie moet worden bijgewerkt om ervoor te zorgen dat gereserveerde IP's worden toegepast voor ZTA TIA-verkeer (Traffic Internet Access). Dit proces kan coördinatie met het productmanagementteam en correctie van de systeemprovisioning omvatten. Als uw organisatie is voorzien voor RIP in DCv2, gebruikt u ZTA TIA.

case wordt NIET ondersteund. Dit is de hoofdoorzaak van het probleem. Om dit aan te pakken, schakelt u PM in om de provisioning naar AWS DC te corrigeren om RIP toe te passen voor ZTA TIA-verkeer.

Er is geen CLI-opdracht gevonden die de wijziging van niet-werkende CLI weergeeft.

Stap 3: Monitor voor wijzigingen in de backend

Wacht op de bevestiging dat de wijziging in de back-end is doorgevoerd, zodat de gereserveerde IP-toewijzing actief is voor ZTA TIA-verkeer.

Er is geen CLI-opdracht of -uitvoer beschikbaar die de back-endwijziging of succesvolle validatie weergeeft. Plaatsaanduiding voor toekomstige verificatiestappen.

Oorzaak

De oorzaak van het probleem is dat de gereserveerde IP-adressen momenteel niet worden toegepast op ZTA TIA-verkeer vanwege een vereiste wijziging in de back-endconfiguratie. Externe IP-validatie toont dus niet de verwachte gereserveerde IP's. De voorziening voor gereserveerde IP-toewijzing is in afwachting van correctie, volgens de workflow die in het geval is opgemerkt.

Verwante inhoud

- GA Release: Zero Trust Access voor alle internetbestemmingen
- 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.