Clientgebaseerde ZTNA-verkeersstuurproblemen met beveiligde client

Inhoud

uitgifte

Client-based Zero Trust Network Access (ZTNA) biedt geen toegang tot interne toepassingen wanneer deze worden benaderd met een FQDN- of direct IP-adres, terwijl dezelfde toepassingen bereikbaar blijven via een VPN-verbinding.

De specifieke symptomen die zijn waargenomen zijn:

- Secure Client ZTNA kan geen interne toepassingen bereiken via FQDN of direct IP wanneer de verbinding met VPN wordt verbroken.
- Browsergebaseerde ZTNA-toegangsfuncties werken correct voor dezelfde toepassingen.
- Er worden geen ZTNA-gebeurtenissen weergegeven in activiteitenlogboeken wanneer de VPN is uitgeschakeld, wat aangeeft dat het clientverkeer niet via het ZTNA-pad wordt geleid.
- Privé-app-definities zijn geverifieerd om VPN-routeerbare bronnen te matchen met de juiste IP / poort / FQDN-configuraties.
- Het ZTNA-beleid is bevestigd dat het overeenkomt met de toewijzingen van de testgebruiker en de groep.

Het probleem isoleert specifiek voor Secure Client ZTNA-verkeerssturing of handhavingsmechanisme, omdat browsergebaseerde ZTNA valideert dat backend-publicatie en -handhaving goed werken.

milieu

- Technologie: beveiligde toegang - Zero Trust Network Access (ZTNA)

- Componenten: clientgebaseerde ZTNA, houding, inschrijving, toegang tot privébronnen
- Veilige client met naast elkaar bestaande VPN-profielen
- Privétoepassingen toegankelijk via zowel FQDN als direct IP-adressering
- Browsergebaseerde ZTNA-functionaliteit bevestigd werken
- Beleidshandhaving geconfigureerd in de modus Meest specifieke matchhandhaving

resolutie

De resolutie betrof configuratieaanpassingen van het ZTA-profiel en beleidsvalidatie. De stappen die in de volgende secties worden beschreven, zijn uitgevoerd om de op clients gebaseerde ZTNA-functionaliteit te herstellen.

Stap 1: Voeg privébronnen toe aan ZTA-profiel

Private Resources werden toegevoegd aan de ZTA-profielconfiguratie. Na deze wijziging begonnen geblokkeerde gebeurtenissen te verschijnen in de activiteitenlogboeken en screenshots, wat aangeeft dat het clientverkeer nu goed werd gerouteerd via het ZTNA-pad.

Stap 2: Beleidsverificatie en testen

Een tijdelijke "vergunning voor elke" regel werd toegevoegd om de verkeersstroom te valideren. Hoewel deze regel actief was, functioneerde ZTNA-toegang op basis van clients correct, wat bevestigt dat het verkeersstuurmechanisme werkte, maar dat de beleidshandhaving moest worden aangepast.

Stap 3: Verfijning van het beleid

De regel voor tijdelijke vergunningen werd geschrapt en het specifieke toegangsbeleid werd gevalideerd. De private resource werd bevestigd toegankelijk te zijn onder het toegangsbeleid genaamd Private Resources_Cyril met behulp van de meest specifieke matchhandhavingsmodus

van het platform.

Stap 4: Configuratievalidatie

De gebruiker bevestigde dat de client-gebaseerde ZTNA-toegang consistent begon te werken nadat de configuratie was gewijzigd. Het probleem is opgelost zonder aanvullende beleidswijzigingen of systeemwijzigingen.

Oorzaak

De hoofdoorzaak was een onvolledige configuratie van de privébron in het ZTA-profiel. Zonder de juiste Private Resources gedefinieerd in het ZTA-profiel, werd het clientverkeer niet door het ZTNA-handhavingspad gestuurd, waardoor het terugviel op lokale routeringsmechanismen. Dit resulteerde erin dat het verkeer het ZTNA-beleid volledig omzeilde, wat verklaarde waarom er geen ZTNA-gebeurtenissen in de activiteitenlogboeken verschenen toen VPN werd losgekoppeld.

Het probleem was specifiek voor client-based ZTNA verkeer stuurinrichting configuratie, terwijl browser-based ZTNA bleef functioneren omdat het gebruik maakt van een ander verkeer afhandeling mechanisme dat goed was geconfigureerd.

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.