Secure Access Intermittent verbreekt de verbinding achter bedrijfsfirewalls met inactieve time-outfouten

Inhoud

- uitgifte
- milieu
- resolutie
  - Stap 1: Implementeer MX TTL-bufferconfiguratie
  - Stap 2: Vereiste domeinuitsluitingen configureren
  - Stap 3: Controleer de toewijzingen voor poorten en protocollen
  - Stap 4: Resolutie controleren en valideren
- Oorzaak
- Gerelateerde inhoud

---

uitgifte

Cisco Secure Access-clients worden met tussenpozen verbroken en maken onmiddellijk opnieuw verbinding wanneer eindpunten zijn verbonden met het bedrijfsnetwerk. De verbindingen worden willekeurig verbroken, waarbij de client na ongeveer 5 seconden automatisch opnieuw verbinding maakt. Dit gedrag wordt waargenomen wanneer internetverkeer via Zero Trust Access (ZTA) wordt geproxy naar Secure Access vanaf eindpunten die zich achter Cisco FirePower- en Meraki MX-apparaten bevinden.

Het Windows-gebeurtenissenlogboek legt specifieke "idleTimeout"-fouten vast tijdens deze gebeurtenissen waarbij de verbinding wordt verbroken. Het ontkoppelingspatroon treedt niet op

wanneer gebruikers verbinding maken vanaf thuisinternetverbindingen, wat aangeeft dat het probleem specifiek verband houdt met de bedrijfsnetwerkinfrastructuur.

Het symptoom veroorzaakt een verstoring van de bedrijfsvoering om de connectiviteit op afstand te beveiligen voor gebruikers die binnen de bedrijfsnetwerkomgeving werken, terwijl externe gebruikers niet worden beïnvloed door dit connectiviteitsprobleem.

milieu

- Cisco Secure Access - Advantage-implementatie
- Cisco Secure Internet Access (SIA)-clientsoftware
- Bedrijfsnetwerkinfrastructuur met Cisco FirePower-beveiligingstoestellen
- Meraki MX-beveiligingsapparaten in het netwerkpad
- Zero Trust Access (ZTA)-configuratie die internetverkeer naar Secure Access proxyt
- Windows-eindpunten met mogelijkheid voor gebeurtenisregistratie
- Gemengde connectiviteitsscenario's: bedrijfsnetwerk (beïnvloed) en thuisinternetverbindingen (niet beïnvloed)

resolutie

De resolutie betrof het implementeren van configuratiewijzigingen op het Meraki MX-apparaat en het waarborgen van goede domeinuitsluitingen en poortwachtigheden voor Secure Access-integratie.

Stap 1: Implementeer MX TTL-bufferconfiguratie

Configureer een MX TTL-buffer op het Meraki MX-apparaat om het DNS TTL-cachinggedrag aan te pakken dat bijdroeg aan de problemen met de intermitterende ontkoppeling. Deze configuratiewijziging lost de tijdconflicten op tussen caching van de DNS-resolutie en de verwachtingen met betrekking tot de connectiviteit van de Secure Access-client.

Stap 2: Vereiste domeinuitsluitingen configureren

Zorg ervoor dat deze domeinen op de juiste manier worden uitgesloten van onderschepping en worden toegevoegd aan niet-ontsleutelde lijsten op zowel Cisco FirePower- als Meraki MX-apparaten:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Aanvullende domeinen van de Secure Access-service, zoals aangegeven in de beleidsconfiguratie

Stap 3: Controleer de toewijzingen voor poorten en protocollen

Configureer de bedrijfsfirewallinfrastructuur om de vereiste Secure Access-poorten en -protocollen mogelijk te maken via zowel FirePower- als Meraki MX-apparaten. Zorg ervoor dat het verkeer naar poort 443 voor Secure Access-service-eindpunten correct wordt afgehandeld zonder interferentie van beveiligingsinspecties die time-outvoorwaarden kunnen veroorzaken.

Stap 4: Resolutie controleren en valideren

Nadat u de MX TTL-bufferconfiguratie hebt geïmplementeerd, moet u het gedrag van de Secure Access-client gedurende enkele dagen controleren om te bevestigen dat het patroon van intermitterende verbreken en opnieuw verbinden is opgehouden.

Oorzaak

De onderbrekingen werden veroorzaakt door DNS TTL (Time To Live) caching gedrag conflicten tussen de corporate netwerk infrastructuur en Secure Access service verwachtingen. De Cisco engineering analyse onthulde dat DNS TTL-waarden variëren als gevolg van resolver caching gedrag, en afwisselende IP-adressen worden verwacht gedrag als gevolg van load balancing mechanismen in de Secure Access service architectuur.

Toen bedrijfsnetwerkapparaten (Cisco FirePower en Meraki MX) DNS-reacties voor Secure Access-eindpunten verwerkte, zorgde de caching en TTL-verwerking voor mismatches in de timing die resulteerden in "idleTimeout" -omstandigheden. Dit tijdsconflict zorgde ervoor dat de Secure Access-client de verbinding interpreteerde als inactief en de ontkoppelings-/herverbindingscycli initieerde.

Het probleem was specifiek voor zakelijke netwerkomgevingen, omdat thuisinternetverbindingen doorgaans niet hetzelfde niveau van DNS-caching en verkeersinspectie implementeren dat het beheer van de status van de Secure Access-clientverbinding kan verstoren.

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.