

Problemen oplossen met APP_UNREACHABLE-storingen voor privé-apps in Secure Access

Inhoud

uitgifte

Wanneer gebruikers via Cisco Secure Access toegang proberen te krijgen tot Zero Trust Network Access (ZTNA)-toepassingen, krijgen ze een foutmelding "Application Unreach".

- De connector toont gezond / actief in het dashboard en de toepassing wordt bevestigd door de eigenaar.
- De storing kan van invloed zijn op alle gebruikers van één toepassing, terwijl andere toepassingen die door dezelfde connector worden bediend normaal werken.
- Bij implementaties van de connectorpool kunnen storingen met tussenpozen optreden — sessies slagen of mislukken afhankelijk van de connector in de pool die is geselecteerd.

milieu

- Cisco Secure Private Access-implementatie met ZTNA
- Particuliere bronnen geconfigureerd voor ZTNA-toegang
- Implementatie van resourceconnector voor toegang tot privébronnen

resolutie

Stap 1. Rechtstreekse bereikbaarheid testen vanuit het Connectors Network-segment

- De Resource Connector is een vergrendeld apparaat en biedt geen shell-toegang om opdrachten zoals curl of nc rechtstreeks uit te voeren. Voer in plaats daarvan de bereikbaarheidstest uit vanaf een testhost (of een tijdelijke VM) die in hetzelfde subnet/VLAN als de connector is geplaatst, zodat deze hetzelfde netwerkpad, dezelfde routerings- en firewallregels voor de toepassing volgt:

```
curl -v http://APP_IP:PORT/health  
nc -zv APP_IP PORT
```

- Als dit mislukt, wordt het probleem bevestigd in het netwerkpad of op de toepassingsserver — los dit eerst op voordat u een Secure Access-configuratie controleert.



Opmerking: een test van een ander subnet is niet overtuigend - firewallregels en routing worden per bron geëvalueerd, omdat de testbron de IP-plaatsing van de connector zo goed mogelijk moet spiegelen.

Stap 2. De configuratie van de privébronnen verifiëren

- Navigeer in het Dashboard voor beveiligde toegang naar Bronnen > Particuliere bronnen, open de betreffende privébron en vergelijk het geconfigureerde IP-, FQDN- en poortteken-voor-teken met het feitelijke bindadres en de poort van de actieve toepassing.
- Elke mismatch (verouderde IP na een servermigratie, verkeerde poort, HTTP versus HTTPS) produceert APP_UNREACHABLE, zelfs met een perfect gezond netwerkpad.

Stap 3. DNS-resolutie voor de connector valideren

- Als de privébron is gedefinieerd door FQDN, controleert u of de DNS-servers die aan de connector zijn toegewezen deze kunnen oplossen. Voer vanuit de CLI Resource Connector (VM-implementaties bieden een diagnostische CLI met ondersteunde standaard Linux-opdrachten voor probleemoplossing) het volgende uit:

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- Bevestig dat het juiste privé-IP is geretourneerd. Zorg ervoor dat de netwerkconfiguratiepunten van de connector op interne DNS-servers die FQDN's van particuliere toepassingen kunnen oplossen, worden geconfigureerd met openbare resolvers die geen interne zones kunnen oplossen.

Stap 4. Het Firewall-pad bekijken

- Bevestig de firewallregels (netwerkfirewalls en de hostfirewall op de toepassingsserver) om verkeer van het IP-adres van de connector naar het IP-adres van de toepassingsserver op de vereiste poort toe te staan.

Stap 5. Verkeer vastleggen met tcpdump op de Resource Connector

- Voer een pakketopname uit op de Resource Connector om de laatste-mijl verbindingspogingen naar de toepassing te observeren. Het hulpprogramma tcpdump is beschikbaar op de Resource Connector. Raadpleeg de handleiding [Tcpdump uitvoeren op Resource Connectors](#).



Tip: Als u de vastlegging deterministisch wilt maken in een implementatie van een connectorgroep, houdt u tijdelijk slechts één Resource Connector ingeschakeld in de groep, zodat alle sessies voor de resource deze doorlopen en voert u vervolgens de vastlegging gefilterd uit op de toepassingsserver en -poort.

-
- Voorbeeld:

```
tcpdump 'host x.x.x.x and tcp port 443'
```

(waarbij x.x.x.x de toepassingsserver IP is en 443 de poort van de toepassing)

- Interpreteer de resultaten: uitgaande SYN's zonder SYN-ACK geven een firewalldrop aan of de app luistert niet; een onmiddellijke RST geeft aan dat de host bereikbaar is, maar niets is gebonden aan de poort; helemaal geen pakketten richting de app geeft aan dat de sessie deze connector niet bereikt of dat DNS is opgelost naar een onverwacht adres.
- Schakel de resterende connectors in de groep opnieuw in zodra de opname is voltooid.

Oorzaak

- Firewall blokkeren Connector-to-app verkeer: Een netwerk of host-based firewall blokkeert de vereiste poort tussen de Connector host IP en de applicatie server IP.
- Configuratie van privébronnen komt niet overeen in beveiligde toegang: het IP, FQDN of de poort die is geconfigureerd in de definitie van privébronnen (Bronnen > Particuliere bronnen) komt niet overeen met wat de toepassing daadwerkelijk luistert (de app is bijvoorbeeld verplaatst naar een nieuw IP, of luistert naar 8443 terwijl 443 is geconfigureerd).
- DNS-oplossingsfout voor de connector: de privébron wordt gedefinieerd door FQDN, maar de connector-DNS-servers lossen geen FQDN's voor privétoepassingen op.
- Toepassingsserver down of niet luisteren: De server lijkt gezond door andere maatregelen, maar is niet gebonden aan de verwachte poort, of de service is gecrasht terwijl de host bleef.
- Gedeeltelijke bereikbaarheid in een connectorpool: Een of meer connectoren in de pool bevinden zich in een netwerksegment dat de toepassing niet kan bereiken, dus alleen sessies die aan die connectoren zijn toegewezen, mislukken.

Gerelateerde inhoud

- [Problemen oplossen en basisinformatie verzamelen voor Cisco Secure Access](#)
- [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.