

Fehlerbehebung bei APP_UNREACHABLE-Fehlern für private Anwendungen in sicherem Zugriff

Inhalt

Problem

Beim Versuch, über Cisco Secure Access auf ZTNA-Anwendungen (Zero Trust Network Access) zuzugreifen, wird die Fehlermeldung "Application Unreachable" (Anwendung nicht erreichbar) angezeigt.

- Der Connector wird im Dashboard als inaktiv/inaktiv angezeigt, und die Ausführung der Anwendung wird vom Besitzer bestätigt.
- Der Ausfall kann sich auf alle Benutzer einer Anwendung auswirken, während andere Anwendungen, für die derselbe Connector verwendet wird, normal funktionieren.
- Bei Connector-Pool-Bereitstellungen können Fehler zeitweilig auftreten - Sitzungen werden erfolgreich durchgeführt oder fallen aus, je nachdem, welcher Connector im Pool ausgewählt ist.

Umwelt

- Bereitstellung von Cisco Secure Private Access mit ZTNA
- Private Ressourcen, die für den ZTNA-Zugriff konfiguriert sind
- Bereitstellung von Ressourcenkonnektoren für den Zugriff auf private Ressourcen

Auflösung

Schritt 1: Testen der direkten Erreichbarkeit aus dem Connectors-Netzwerksegment

- Der Ressourcen-Connector ist eine gesperrte Appliance und bietet keinen Shell-Zugriff, um Befehle wie curl oder nc direkt auszuführen. Führen Sie stattdessen den Erreichbarkeitstest von einem Test-Host (oder einer temporären VM) aus, der im gleichen Subnetz/VLAN wie der Connector platziert ist, sodass für die Anwendung derselbe Netzwerkpfad, das gleiche Routing und die gleichen Firewall-Regeln befolgt werden:

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

- Wenn dies fehlschlägt, wird das Problem im Netzwerkpfad oder auf dem Anwendungsserver bestätigt. Beheben Sie dieses Problem zuerst, bevor Sie eine Konfiguration für sicheren Zugriff überprüfen.



Anmerkung: Ein Test aus einem anderen Subnetz ist nicht schlüssig - Firewall-Regeln und Routing werden pro Quelle ausgewertet, da die Testquelle die IP-Platzierung des Connectors so genau wie möglich spiegeln muss.

Schritt 2: Überprüfen der Konfiguration der privaten Ressource

- Navigieren Sie im Dashboard für sicheren Zugriff zu Ressourcen > Private Ressourcen, öffnen Sie die betroffene private Ressource, und vergleichen Sie die konfigurierte IP, den FQDN und den Port von Zeichen zu Zeichen mit der Bindungsadresse und dem Port der ausgeführten Anwendung.
- Jegliche Diskrepanz (veraltete IP nach einer Servermigration, falscher Port, HTTP gegen HTTPS) erzeugt APP_UNREACHABLE selbst bei einem einwandfreien Netzwerkpfad.

Schritt 3: Validieren der DNS-Auflösung für den Connector

- Wenn die private Ressource durch FQDN definiert ist, stellen Sie sicher, dass sie von den dem Connector zugewiesenen DNS-Servern aufgelöst werden kann. Führen Sie in der Resource Connector CLI (VM-Bereitstellungen bieten eine Diagnose-CLI mit unterstützten

Standard-Linux-Befehlen zur Fehlerbehebung) folgende Schritte aus:

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

- Bestätigen Sie, dass die richtige private IP zurückgegeben wurde. Stellen Sie sicher, dass die Netzwerkkonfiguration des Connectors auf interne DNS-Server verweist, die private Anwendungs-FQDNs auflösen können. Ein mit öffentlichen Resolvern konfigurierter Connector kann interne Zonen nicht auflösen.

Schritt 4: Überprüfen des Firewall-Pfads

- Bestätigen Sie, dass die Firewall-Regeln (Netzwerk-Firewalls und die Host-Firewall auf dem Anwendungsserver) Datenverkehr von der IP-Adresse des Connectors zur IP-Adresse des Anwendungsservers am erforderlichen Port zulassen.

Schritt 5: Erfassen von Datenverkehr mit tcpdump auf dem Ressourcen-Connector

- Führen Sie eine Paketerfassung auf dem Ressourcen-Connector aus, um die Verbindungsversuche auf der letzten Meile zur Anwendung zu beobachten. Das Dienstprogramm tcpdump ist im Ressourcen-Connector verfügbar. Weitere Informationen finden Sie im Leitfaden [Run tcpdump on Resource Connectors](#).



Tipp: Um die Erfassung deterministisch in einer Connector-Group-Bereitstellung zu machen, halten Sie vorübergehend nur einen Ressourcenkonnektor in der Gruppe aktiviert, sodass alle Sitzungen für die Ressource diese durchlaufen. Führen Sie dann die Erfassung gefiltert auf dem Anwendungsserver und Port aus.

-
- Beispiele:

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

(wobei x.x.x.x die IP-Adresse des Anwendungsservers und 443 der Port der Anwendung ist)

- Interpretieren Sie die Ergebnisse: Ausgehende SYNs ohne SYN-ACK weisen darauf hin, dass eine Firewall ausfällt oder die App nicht zuhört. Eine sofortige RST zeigt an, dass der Host erreichbar ist, aber nichts an den Port gebunden ist; Wenn keine Pakete in Richtung der App gesendet werden, bedeutet dies, dass die Sitzung diesen Connector nicht erreicht oder der DNS in eine unerwartete Adresse aufgelöst wurde.
- Aktivieren Sie die übrigen Anschlüsse in der Gruppe erneut, sobald die Erfassung abgeschlossen ist.

Ursache

- Firewall blockiert Connector-to-App-Datenverkehr: Eine Netzwerk- oder Host-basierte Firewall blockiert den erforderlichen Port zwischen der Host-IP des Connectors und der IP-Adresse des Anwendungsservers.
- Nicht übereinstimmende private Ressourcenkonfiguration in sicherem Zugriff: Die in der Definition der privaten Ressourcen (Ressourcen > Private Ressourcen) konfigurierte IP, der FQDN oder der Port stimmt nicht mit dem überein, was die Anwendung tatsächlich abhört (z. B. die App, die auf eine neue IP verschoben wurde, oder die 8443 abhört, während 443 konfiguriert ist).
- Fehler bei der DNS-Auflösung für den Connector: Die private Ressource wird durch den FQDN definiert, aber die Connector DNS-Server lösen keine FQDNs privater Anwendungen auf.
- Anwendungsserver ist ausgefallen oder hört nicht zu: Der Server scheint aufgrund anderer Messgrößen fehlerfrei zu sein, ist jedoch nicht an den erwarteten Port gebunden, oder der Dienst ist abgestürzt, während der Host aktiv geblieben ist.
- Teilweise Erreichbarkeit in einem Connector-Pool: Ein oder mehrere Connectors im Pool befinden sich in einem Netzwerksegment, das die Anwendung nicht erreichen kann, sodass nur Sitzungen fehlschlagen, die diesen Connectors zugewiesen sind.

Verwandte Inhalte

- [Fehlerbehebung und Erfassung grundlegender Informationen für Cisco Secure Access](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.