Private Link-Ressourcen über virtuelle Appliance für sicheren Zugriff in Azure aufgrund interner DNS-Konfiguration nicht zugänglich

Inhalt

Problem

Auf Azure Private Link-Ressourcen kann von Azure-Arbeitsbereichen und -Workloads aus nicht zugegriffen werden, wenn der Datenverkehr über eine in Azure bereitgestellte virtuelle Appliance (VA) von Cisco Secure Access weitergeleitet wird. Dieses Problem besteht trotz der Konfiguration von Ausnahmen für die Datenverkehrssteuerung zum Umgehen von sicherem Zugriff für private Azure-Domänen, der Aktivierung des DNS-Backoffs und der Konfiguration von privatem DNS in der VA weiter.

Versuche, von Azure-Workloads hinter der VA für sicheren Zugriff auf Azure Private Link-Endpunkte zuzugreifen, führen zu einer fehlgeschlagenen Auflösung und Konnektivität.

Umwelt

- Cisco Secure Access Virtual Appliance (VA) in Azure bereitgestellt
- Azure-Arbeitsbereiche und Azure-gehostete Workloads
- Azure Private Link aktiviert für private Azure-Ressourcenkonnektivität
- Ausnahmen für die Datenverkehrssteuerung, die konfiguriert wurden, um den sicheren Zugriff für Azure Private-Domänen zu umgehen
- DNS-Backoff in Secure Access-VA aktiviert
- Konfiguration privater DNS-Zonen in der VA für sicheren Zugriff
- Software-Version: ALLE (Problem ist versionsunabhängig)

Auflösung

Die Lösung umfasste die Aktualisierung der DNS-Konfiguration in der Cisco Secure Access VA, um interne DNS-Servereinträge einzuschließen, die Azure Private Link-Domänen auflösen können. In diesen Schritten werden die Fehlerbehebung und die durchgeführten Korrekturmaßnahmen im Detail beschrieben:

Diagnose der lokalen DNS-Konfiguration in der VA für sicheren Zugriff

1. Verwenden Sie den folgenden Befehl in der VA für sicheren Zugriff, um die vorhandene DNS-Konfiguration zu überprüfen und zu überprüfen, ob interne DNS-Server eingestellt sind:

```
config localdns show
```

1. Beispielausgabe (Gerätename ersetzt):

```
device# config localdns show
No internal DNS servers configured.
Conditional forwarders present for Azure private domains.
```

Hinzufügen interner DNS-Servereinträge zur sicheren Zugriffs-VA

1. Fügen Sie mit dem folgenden Befehl die entsprechenden internen IP-Adressen des DNS-Servers hinzu, um die ordnungsgemäße Auflösung von Azure Private Link-Domänen zu aktivieren:

```
config localdns add <internal-DNS-server-IP>
```

1. Ersetzen Sie `<internal-DNS-server-IP>` durch die tatsächliche IP-Adresse Ihres internen DNS-Servers, der Azure Private Link-Domänen auflösen kann.

Überprüfen der DNS-Auflösung für Azure Private Link-Domänen

1. Überprüfen Sie nach dem Aktualisieren der DNS-Konfiguration, ob Azure Private Link-Domänen über die VA für sicheren Zugriff aufgelöst werden können. Verwenden Sie diesen Befehl, um die DNS-Serverkonfiguration zu bestätigen:

```
config localdns show
```

1. Beispielausgabe (Gerätename ersetzt):

```
device# config localdns show
Internal DNS servers configured:
- x.x.x.x
Conditional forwarders present for Azure private domains.
```

1. Es wurde kein CLI-Befehl gefunden, der den Wechsel von `Konfigurationsgebietsschemas` ohne DNS-Server in einen funktionierenden Zustand mit bestätigter Auflösung anzeigt.

Überprüfen der Verbindung mit Azure Private Link-Ressourcen

Sobald DNS korrekt aufgelöst wurde, testen Sie die Verbindung von Azure-Workloads hinter der VA für sicheren Zugriff zu den beabsichtigten Azure Private Link-Endpunkten, um den ordnungsgemäßen Zugriff sicherzustellen.

Ursache

Die Ursache des Problems war das Fehlen interner DNS-Serverkonfigurationen in der Cisco Secure Access VA. Die VA wurde mit bedingten Weiterleitungen für private Azure-Domänen konfiguriert, es fehlten jedoch interne DNS-Server, die für eine ordnungsgemäße DNS-Auflösung von Azure Private Link-Domänen erforderlich sind. Durch Hinzufügen der internen DNS-Servereinträge konnte das Problem behoben werden.

Verwandte Inhalte

- 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.