

内部DNS構成が原因でAzureのSecure Access仮想アプライアンス経由でプライベートリンクリソースにアクセスできない

内容

お問い合わせ内容

AzureにデプロイされたCisco Secure Access Virtual Appliance (VA)経由でトラフィックがルーティングされる場合、AzureのプライベートリンクリソースにAzureのワークスペースやワークロードからアクセスすることはできません。この問題は、トラフィックステアリング例外を設定してAzureプライベートドメインのセキュアアクセスをバイパスし、DNSバックオフを有効にし、VAでプライベートDNSを設定しても解決しません。

Secure Access VAの背後にあるAzureワークロードからAzureプライベートリンクエンドポイントにアクセスしようとする、解決と接続に失敗します。

環境

- Azureに導入されたCisco Secure Access Virtual Appliance(VA)
- AzureワークスペースとAzureでホストされるワークロード
- プライベートAzureリソース接続に対してAzureプライベートリンクが有効になっています
- AzureプライベートドメインのSecure Accessをバイパスするように構成されたトラフィック操作例外
- セキュアアクセスVA内で有効なDNSバックオフ
- Secure Access VAで設定されたプライベートDNSゾーン
- ソフトウェアバージョン：すべて（バージョンに依存しない問題）

解決策

この問題を解決するには、Cisco Secure Access VA内のDNS設定を更新して、Azureプライベートリンクドメインを解決できる内部DNSサーバエントリを含める必要がありました。次の手順は、実施されたトラブルシューティングと修正措置の詳細を示しています。

セキュアアクセスVA上のローカルDNS設定の診断

1. 既存のDNS設定を調べて、内部DNSサーバが設定されているかどうかを確認するには、セキュアアクセスVAで次のコマンドを使用します。

```
config localdns show
```

1. 出力例 (デバイス名を置き換えて):

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

セキュアアクセスVAへの内部DNSサーバエントリの追加

1. Azureプライベートリンクドメインの適切な解決を有効にするには、次のコマンドを使用して適切な内部DNSサーバーのIPアドレスを追加します:

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

1. <internal-DNS-server-IP>を、Azureプライベートリンクドメインを解決できる内部DNSサーバーの実際のIPアドレスに置き換えます。

AzureプライベートリンクドメインのDNS解決の確認

1. DNS構成を更新した後、セキュアアクセスVAを介してAzureプライベートリンクドメインを解決できることを確認します。次のコマンドを使用して、DNSサーバーの設定を確認します。
 - 。

```
config localdns show
```

1. 出力例 (デバイス名を置き換え):

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

1. DNSサーバなしのconfig localdns showから、解決が確認された動作状態への変更を示すCLIコマンドは見つかりませんでした。

Azureプライベートリンクリソースへの接続の検証

DNSが正しく解決されたら、Secure Access VAの背後にあるAzureワークロードから目的のAzureプライベートリンクエンドポイントへの接続をテストして、適切なアクセスを確保します。

原因

この問題の根本原因は、Cisco Secure Access VA内に内部DNSサーバ設定がないことにあります。VAはAzureプライベートドメインの条件付きフォワーダーで構成されましたが、Azureプライベートリンクドメインの適切なDNS解決に必要な内部DNSサーバがありませんでした。内部DNSサーバエントリを追加することで、問題が解決しました。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。