Private Link Resources Inaccessible via Secure Access Virtual Appliance in Azure Due to Internal DNS Configuration

Contents

Issue

Azure Private Link resources are not accessible from Azure workspaces and workloads when traffic is routed throug

Attempts to access Azure Private Link endpoints from Azure workloads behind the Secure Access VA result in faile

Environment

- Cisco Secure Access Virtual Appliance (VA) deployed in Azure
- Azure workspaces and Azure-hosted workloads
- Azure Private Link enabled for private Azure resource connectivity
- Traffic steering exceptions configured to bypass Secure Access for Azure private domains
- DNS backoff enabled within Secure Access VA
- Private DNS zones configured in Secure Access VA
- Software Version: ALL (issue is version-agnostic)

Resolution

The resolution involved updating the DNS configuration within the Cisco Secure Access VA to include internal DNS

Diagnose Local DNS Configuration on Secure Access VA

1. To examine the existing DNS configuration and confirm whether internal DNS servers are set, use this comma

```
config localdns show
```

1. Example output (with device name replaced):

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

Add Internal DNS Server Entries to Secure Access VA

1. To enable proper resolution of Azure Private Link domains, add the appropriate internal DNS server IP addres

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

1. Replace `<internal-DNS-server-IP>` with the actual IP address of your internal DNS server that can resolve Azure Private Link domains.

Verify DNS Resolution for Azure Private Link Domains

1. After updating the DNS configuration, verify that Azure Private Link domains can be resolved through the Se

```
config localdns show
```

1. Example output (device name replaced):

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

1. No CLI command found which shows the change from `config localdns show` with no DNS servers to a worki

Validate Connectivity to Azure Private Link Resources

Once DNS is resolving correctly, test connectivity from Azure workloads behind the Secure Access VA to the intend

Cause

The root cause of the issue was the absence of internal DNS server configurations within the Cisco Secure Access VA. The VA was configured with conditional forwarders for Azure private domains but lacked internal DNS servers necessary for proper DNS resolution of Azure Private Link domains. Adding the internal DNS server entries resolved the problem.

Related Content

- Cisco Technical Support & Downloads