Troubleshoot APP_UNREACHABLE Failures for Private Apps in Secure Access

Contents

Issue

When attempting to access Zero Trust Network Access (ZTNA) applications through Cisco Secure Access, users encounter an "Application Unreachable" error message.

- The Connector shows healthy/active in the dashboard, and the application is confirmed running by its owner.
- The failure can affect all users of one application while other applications served by the same Connector work normally.
- In connector-pool deployments, failures can appear intermittent — sessions succeed or fail depending on which connector in the pool is selected.

Environment

- Cisco Secure Private Access deployment with ZTNA
- Private resources configured for ZTNA access
- Resource connector deployment for private resource access

Resolution

Step 1. Test Direct Reachability from the Connectors Network Segment

- The resource Connector is a locked-down appliance and does not provide shell access to run commands such as **curl** or **nc** directly. Instead, perform the reachability test from a test host (or a

temporary VM) placed in the **same subnet/VLAN as the Connector**, so it obeys the same network path, routing, and firewall rules to the application:

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

- If this fails, the problem is confirmed in the network path or on the application server — fix this first before reviewing any Secure Access configuration.

Note: A test from a different subnet is not conclusive — firewall rules and routing are evaluated per source, as the test source must mirror the Connector's IP placement as closely as possible.

Step 2. Verify the Private Resource Configuration

- In the Secure Access dashboard, navigate to **Resources** > **Private Resources**, open the affected private resource, and compare the configured IP, FQDN, and port character-for-character against the running application's actual bind address and port.
- Any mismatch (stale IP after a server migration, wrong port, HTTP vs HTTPS) produces APP_UNREACHABLE even with a perfectly healthy network path.

Step 3. Validate DNS Resolution for the Connector

- If the private resource is defined by FQDN, verify that the DNS servers assigned to the Connector can resolve it. From the **Resource Connector CLI** (VM deployments provide a diagnostics CLI with supported standard Linux troubleshooting commands), run:

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

- Confirm the correct private IP is returned. Ensure the Connector's network configuration points at internal DNS servers that can resolve private application FQDNs; a Connector configured with public resolvers cannot resolve internal zones.

Step 4. Review the Firewall Path

- Confirm the firewall rules (network firewalls and the host firewall on the application server) permit traffic from the **Connector's IP address** to the application server IP on the required port.

Step 5. Capture Traffic with tcpdump on the Resource Connector

- Run a packet capture on the Resource Connector to observe the last-mile connection attempts toward the application. The **tcpdump** utility is available on the Resource Connector —refer to the Run tcpdump on Resource Connectors guide.

Tip: To make the capture deterministic in a connector-group deployment, temporarily keep only **one** Resource Connector enabled in the group so all sessions for the resource traverse it, then run the capture filtered on the application server and port.

- For example:

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

(where x.x.x.x is the application server IP and 443 is the application's port)

- Interpret the results: outbound SYNs with no SYN-ACK indicate a firewall drop or the app not listening; an immediate RST indicates the host is reachable but nothing is bound to the port; no packets at all toward the app indicates the session is not reaching this connector or DNS resolved to an unexpected address.
- Re-enable the remaining connectors in the group once the capture is complete.

Cause

- **Firewall blocking Connector-to-app traffic**: A network or host-based firewall blocks the required port between the Connector host IP and the application server IP.
- **Private resource configuration mismatch in Secure Access**: The IP, FQDN, or port configured in the private resource definition (**Resources > Private Resources**) does not match what the application actually listens on (for example, the app moved to a new IP, or listens on 8443 while 443 is configured).
- **DNS resolution failure for the Connector**: The private resource is defined by FQDN, but the Connector DNS servers not resolving private application FQDNs.

- **Application server down or not listening**: The server appears healthy by other measures but is not bound to the expected port, or the service crashed while the host stayed up.
- **Partial reachability in a connector pool**: One or more connectors in the pool sit in a network segment that cannot reach the application, so only sessions assigned to those connectors fail.

Related Content

- Troubleshoot and Collect Basic Information for Cisco Secure Access
- Cisco Technical Support & Downloads