

Testing Access

<https://campus.barracuda.com/doc/93201601/>

Test Connectivity from the Device to the CloudGen Access Proxy

1. Get the CloudGen Access Proxy details from the CloudGen Access Enterprise Console.
2. Try to open an SSL connection to the proxy and confirm that the first lines reference CloudGen Access Root Certificate Authority.

```
openssl s_client -showcerts -connect <proxy_host>:<proxy_port>
```

If the request fails or the operation times out, that means that you are not reaching the CloudGen Access Proxy.

Check the following:

- The Proxy Host DNS record is being resolved to the correct IP address.
- The Proxy Host IP address, if using IP instead of DNS, is correct.
- Proxy Host IP address is accessible to you. This usually means it needs to be publicly accessible.
- Proxy Port, defined in the console, is open in your network. Public networks usually allow only 80 and 433 outbound. Using other ports for the proxy might make it inaccessible for clients.
- NAT configuration in the device/service that is exposing the CloudGen Access Proxy.
- Firewall rules to allow inbound communication to the configured CloudGen Access Proxy.

Check if the Device Is Trying to Access the Resource with the CloudGen Access App

Check the IP address for the failing resource. It should return an IP in the following range:

- 255.0.0.0/8 for Unix/Linux-based systems
- 198.18.0.0/15 for Microsoft-based systems

```
? nslookup myresource.private
Server: 192.0.2.5
Address: 192.0.2.5#53
Name: myresource.private
Address: 255.0.0.12
```

Next steps:

- Confirm that the CloudGen Access App is running and the tunnel is started.

- Check that the CloudGen Access App is enrolled in a tenant.
- Confirm the resource is created in the CloudGen Access Enterprise Console.
- Resource list update on CloudGen Access App can take up to 15 minutes. Force refresh if your CloudGen Access App version allows it.

Test Connectivity from Envoy Proxy to the Resource

The Envoy Proxy needs to be able to reach the resource with the configured properties.

Take note of the following resource:

- **Resource Name** - My Resource
- **Public Host** - myresource.private
- **Resource Host** - myresource.internal
- **External Port** - 80
- **Internal Port** - 3000
- **Access Proxy** - US-EAST-1-PROXY

Envoy Proxy must be able to resolve the **Resource Host** record.

```
? nslookup myresource.internal
Server - 10.0.0.1
Address - 10.0.0.1#53
Name - myresource.internal
Address - 10.0.0.20
```

For an HTTP resource, an HTTP request can be sent using curl.

```
? curl myresource.internal:3000
HTTP/1.1 200 OK
[...]
```

For a redis resource, netcat can be used for connecting.

```
? nc myresource.internal 3000
PING
+PONG
```

Next steps:

- Check that the DNS server is correctly configured.
- Confirm that intermediate firewall rules are not blocking access to the resource.
- For HTTPS connection, the **Public Host** needs to match the configured hostname in the

resource certificate. However, the **Resource Host** just needs to be something the CloudGen Access Proxy can resolve and access.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.