Automatic certificate request / renewal (Let's Encrypt) isn't working

- Parallels Secure Workspace

Symptoms

- When navigating to the Workspace URL, the browser warns that an expired, invalid, or untrusted certificate is used.
- When trying to request a new Let's Encrypt certificate through **System Settings > Global > Certificates**, an error is shown.

Cause

Requesting a Let's Encrypt has failed.

Resolution

The automatic certificate renewal relies on the REST API of Let's Encrypt.
Mind that this option is only available for a single-node environment.

Parallels Secure Workspace checks once or twice a day whether certificates should be renewed.

There are two main requirements:

- The appliance must be able to connect to the Let's Encrypt servers (acme-v02.api.letsencrypt.org **- TCP port 443**).
  Verify this outgoing connectivity by running a tcpscan.
- The Let's Encrypt servers also need to be able to resolve the specified domain name (so a public DNS record is required) to fetch some data (ACME Challenge) from the appliance. Let's Encrypt will connect to the **public IP address** of the appliance on **TCP ports 80 and 443**. These port numbers can not be altered.

  The internal SSL offloading with enforced HTTPS can still be enabled on the appliance (**System Settings > Global > Connectivity**) so all other incoming requests will be redirected and will use HTTPS.

When troubleshooting, make sure there are also no geo-restrictions in place on the organization's firewall and that any port forwarding (destination NAT) on the firewall is done correctly. Unfortunately at this point Let's Encrypt doesn't offer a list of IPs that could be whitelisted.