Remote interventions

- Parallels Secure Workspace

Resolution

Sometimes the support team must connect to the appliance to perform troubleshooting. In such a situation, the customer is requested to allow inbound connections from a specific IP from our organization to the appliance (TCP port 22). Usually, this can be done by enabling port forwarding (or destination NAT) on the firewall.

In the case of a multi-node environment, it is usually enough to allow inbound connections to a single node.

Only allow connections from our public IP **34.76.247.118** for the duration of the troubleshooting.

For security and liability reasons, we only connect directly from our headquarters and not through intermediate clients / jump hosts. We do not support other scenarios, as we believe it may compromise the security of the customer's own Parallels Secure Workspace appliances (virtual machines) or potentially those of others.

In your communication, confirm the public IP and port number that we can connect to once the necessary configuration is in place which allows us to connect.

It is possible to **optionally** configure a password for additional security: Configuring the intervention password .

After the intervention, it's highly recommended to simply disable the firewall rule again.
