Connectivity requirements

- Parallels Secure Workspace

Resolution

Before starting a deployment of the Parallels Secure Workspace platform, a few connectivity requirements need to be checked and/or enabled. Please review this section to ensure proper installation and operation.

Connectivity Requirements during Installation:

During the installation of the Parallels Secure Workspace, the appliance should be able to connect to the DNS server(s), NTP server(s), and - if applicable - the external database server.

Connection	From	To
NTP: UDP port 123	The Workspace VM	Internal or external NTP service. Use the internal NTP service of the Active Directory domain controller(s), or rely on external NTP servers such as the pool.ntp.org servers. The NTP service should use the same time zone as the hypervisor (UTC is recommended).
DNS: UDP port 53	The Workspace VM	The DNS server that resolves the NTP server (when provided via FQDN*) and other relevant hostnames. Most commonly, the DNS servers integrated in the Active Directory are used.
HTTP : TCP port 8080	The browser of the admin	The Workspace VM
HTTP : TCP port 80	The browser of the admin	The Workspace VM

* FQDN = Fully Qualified Domain Name, e.g. ntp.mycompany.com

Connectivity Requirements during Operation and Configuration:

The Workspace appliance has a few requirements for correct operation. Before deployment, check whether the following ports can be opened.

Best practice: configure your firewall rules to only allow traffic from/to the ports that are needed for operation.

Connection	From	To
LDAP(S): TCP port 389 (or TCP port 636 for SSL encryption)	The Workspace VM	LDAP or Active Directory server(s) back-end
Kerberos: UDP/TCP port 88 and TCP port 464	The Workspace VM	Kerberos server (Only required when users need to be able to change password at next logon) **Important:** The Kerberos server should also have PTR (reverse DNS) and SRV records in place to locate the KDC server and define the protocol to use**
RADIUS (if used): UDP port 1812	The Workspace VM	RADIUS service for second-factor authentication
		CIFS/SMB file server(s) back-end

CIFS (if used): UDP port 137, TCP port 445	The Workspace VM	
WebDAV (if used): TCP port 80 or 443 (or different depending on WebDAV config)	The Workspace VM	WebDAV file server(s) back-end
RDP: TCP port 3389 (RDP/RemoteApp)	The Workspace VM	To application server(s) back-end
NTP: UDP port 123	The Workspace VM	Internal or external NTP service. Use the internal NTP service of the Active Directory domain controller(s), or rely on external NTP servers such as the pool.ntp.org servers. The NTP service should use the same time zone as the hypervisor (UTC is recommended).
HTTPS: TCP port 443	The Workspace VM	• The repository servers: https://psw.parallels.com (directly or via the configured HTTP proxy). Only mandatory during upgrades, but required for Anonymous Usage Reporting. • When using SaaS services, those services need to be reachable by Parallels Secure Workspace or via the configured HTTP proxy: ♦ Microsoft OneDrive for Business: ◊ <mydomain>**-my**.sharepoint.com ◊ login.microsoftonline.com ◊ graph.microsoft.com ♦ DUO Multi-Factor Authentication: ◊ <your_api>.duosecurity.com ♦ Automatic certificates through Let's Encrypt: ◊ *.api.letsencrypt.org (only directly, not through HTTP proxy)
HTTP(S): TCP port 80/443	The Workspace VM	Web applications reversed proxied by Parallels Secure Workspace
DNS: UDP port 53	The Workspace VM	Specify the DNS server that resolves all the relevant hostnames mentioned in this section. Most commonly, the DNS servers integrated in the Active Directory are used.
HTTP: TCP port 80 (long-living WebSocket)	The (end user browser) client***	• The Workspace VM • When using automatic certificate: the servers of Let's Encrypt
HTTPS: TCP port 443 (long-living WebSocket)	The (end user browser) client***	• The Workspace VM (Only when SSL Offloader is enabled) • When using automatic certificates: the servers of Let's Encrypt
SNMP (if used): UDP port 161	Monitoring System	The Workspace VM (Only if SNMP is enabled)
HTTP(s) : TCP port 80/443	All servers involved in Kerberos Authentication (AD and Application Servers)	The Workspace VM (http(s)://<workspace_url>/crl/<WORKSPACE_DOMAIN_NAME>.crl)

SSH: TCP port 22	The client	The Parallels Secure Workspace VM (Only necessary to access Parallels Secure Workspace using SFTP to obtain the environment backup)

* FQDN = Fully Qualified Domain Name, e.g. ntp.mycompany.com
** e.g. *kerberos-master.*(tcp|udp).staging.somewindowsdomain.com - For more information: https://technet.microsoft.com/en-us/library/cc961719.aspx
*** When this connection goes via an SSL-offloader, reverse proxy, firewalls, etc., please make sure that WebSockets are supported and that open WebSocket connections are not killed after a while.

For a **multi-node** deployment, all TCP, UDP, and ICMP traffic should be allowed between the nodes. This traffic is not encrypted. Each node has an internal firewall only allowing traffic from other nodes (based on the IP address).

While the appliance always listens for incoming requests on ports 80 (HTTP) or 443 (HTTPS), port forwarding originating from a different port is supported, e.g. https://remote.company.com:8443 .

Connectivity Requirements only during Remote Intervention:

In some cases, the support team will request direct SSH access to the appliance. For security, the appliance only allows access using public key authentication (with an optional intervention password on top of the public key authentication).

Connection	From	To
SSH: TCP port 22	Parallels network (IP address will be provided by support)	The Workspace VM
