

Firewall requirements for Parallels Remote Application Server 19

- Parallels Remote Application Server 19.0
- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 19.2

By default, **Remote Application Server** will install with a **Secure Gateway** and a **Connection Broker**. There can only be one master **Connection Broker** in a farm; however, multiple **Secure Gateway** access points and resource **Connection Brokers (RDSH Agent)** can be deployed where needed.

Below are the firewall requirements for each of the separate **Remote Application Server** functions:

All Components: TCP 135, 445 - remote agent push.

Parallels Client

Source	Destination	Protocols	Ports	Description
Parallels Client	HALB	TCP, UDP	80, 443	Management and user session connections
		TCP, UDP	20009	Device Manager shadowing via Firewall
	RAS Secure Gateway Forwarding mode	TCP, UDP	80, 443	Management and user session connections
		TCP, UDP	3389	Optional - Used for user session if RAS is not installed
		UDP	20000	Secure Gateway lookup broadcast.
	RAS Secure Gateway Normal mode	TCP, UDP	80, 443,	Management and user session connections
		TCP, UDP	3389	Optional - Used for user session if RAS is not installed
		TCP, UDP	20009	Device Manager shadowing via Firewall
	Session host (VDI, RDS, RemotePC)	UDP	20000	Secure Gateway Lookup Broadcast
		TCP, UDP	3389	Used for user session connections in RAS
	Azure Virtual Desktop Services	TCP	443	Azure Virtual Desktop Gateway connections
		UDP	3390	Used for user session connections in RAS
	Microsoft site	TCP	443	Download Microsoft Remote Desktop Client
	Parallels site	TCP	80, 443	Check for updates and download Parallels Client

Web (external)

Source	Destination	Protocols	Ports	Description
Web browser (HTML5) and Let's Encrypt service	RAS Web Admin Service [RAS Management Portal]	TCP	20443	Admin access to HTML5-based Management Portal
	HALB	TCP	80, 443	End-user access to Parallels RAS Web Admin Service (Optional - required when using Let's Encrypt)

	RAS Secure Gateway	TCP	80, 443	End-user access to Parallels RAS Web Client (Optional - required when using Let's Encrypt)
HALB				
Source	Destination	Protocols	Ports	Description
HALB	HALB	VRRP	112	HALB-to-HALB communication is used for management and user session connections.
	RAS Secure Gateway in Forwarding Mode	TCP, UDP	80, 443	Management and user session connections.
	RAS Secure Gateway in Normal Mode	TCP, UDP	80, 443	Management and user session connections.
		TCP, UDP	20009	Device Manager shadowing via Firewall
RAS Secure Gateway				
Source	Destination	Protocols	Ports	Description
RAS Secure Gateway in Forwarding mode	RAS Secure Gateway in Normal mode	TCP, UDP	80, 443	Management and user session connections.
		TCP, UDP	3389	Optional - Used for user session if RAS Secure Gateway is in Forwarding mode.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected data.
RAS Secure Gateway in Normal mode	Remote Desktop Services	TCP, UDP	3389	RDP Connections.
	RAS Connection Broker	TCP	20002	RAS Connection Broker service port (Normal mode only).
		TCP, UDP	20009	Device Manager shadowing via Firewall
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected data.
	Localhost	TCP	20020	Communication with HTML5 Gateway
RAS Connection Broker				
Source	Destination	Protocols	Ports	Description
RAS Connection Broker	AD DS controllers	TCP	389, 3268	LDAP
		TCP	636, 3269	LDAPS
		TCP, UDP	88, 53	Kerberos
		UDP		DNS
	RAS Connection Broker	TCP	20001	Redundancy service.
			20030	Communication between RAS Connection Broker and RAS Secure Gateway.
	Parallels Licensing Server	TCP	443	RAS Connection Broker (primary Connection Broker) Server (https://ras.parallels.com).
				Note: Not required for Tenant Broker.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected data.
	RAS RD Session Host Agent	TCP, UDP	30004	Server for Connection Broker requests.
	RAS Provider Agent	TCP, UDP	30006	Provider Agent communication port.

	RAS Remote PC Agent	TCP, UDP	30004	Remote PC Agent Communication P
	2FA Server(s)	TCP, UDP	8080, 80	Deepnet/ Safenet
			1812, 1813	Radius
	RAS Enrollment Server	TCP	30030	RAS Connection Broker Sends RAS
	RAS Reporting	TCP	30008	Master RAS Connection Broker com
	RAS Remote Installer Service	TCP	30020	Remote agent pushing
	RAS RD Session Host Agent	TCP	135, 445, 49179	Remote Install Push/Takeover of Sof
	RAS Guest Agent			
	RAS Remote PC Agent			
	RAS Connection Broker			
	RAS Secure Gateway			
	RAS Enrollment Server			
	SMTP	TCP	587	Notifdispatcher is the service that ser
	Let's Encrypt Service	TCP	443	Communication between the Let's En server.
RAS Console				
Source	Destination	Protocols	Ports	Description
RAS Console	RAS Reporting	TCP	30008	RAS Console is connected to the prin (installed on the same host as SSRS) the settings).
	SSRS	TCP	443	Reports retrieval.
	HALB	TCP, UDP	31006	Used for configuration.
	Parallels Client	TCP	50005	Shadowing from the RAS Console in
	RAS RD Session Host Agent	UDP, TCP	30004	Used for the "Check Agent" task.
				Used to manage components.
	RAS Guest Agent	UDP	30009	Used for the "Check Agent" task.
		TCP	30010	Used to manage components.
	RAS Remote PC Agent	UDP, TCP	30004	Used for the "Check Agent" task.
				Used to manage components.
	RAS Provider Agent	UDP, TCP	30006	Used for the "Check Agent" task.
				Used to manage components.
	MFA Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius
	Microsoft site	TCP	80, 443	Check for updates and download Par
	Parallels site	TCP	80	Check for updates and download Par
	RAS Secure Gateway	TCP	80, 443	Set the log level or clear/retrieve the
				Prefers to connect to the normal port is disabled
	RAS Performance Monitor	TCP	20002, 20001	Communication with Connection Br
	RAS Connection Broker	TCP	20002, 20001	Communication with Connection Br

	RAS Enrollment Server	TCP, UDP	30030	Used for the "Check Agent" task.
	Wyse Broker	UDP	1234 (outbound only)	Used to manage components and for Wyse broker discovery request broadcast Wyse broker discovery reply packet
	SMTP	TCP	68 (inbound only) 587	RAS Console can send test emails using SMTP
SSRS				
Source	Destination	Protocols	Ports	Description
SSRS	Microsoft SQL Server	TCP	1433	RAS Console is connected to the RA Reporting Service database
RAS Reporting				
Source	Destination	Protocols	Ports	Description
RAS Reporting Service	MS SQL	TCP	1433	Store RAS activity information
	SSRS	TCP	8085, 443	Enumeration of reports (incl. custom reports)
RAS Web Administration Service (REST/Management Portal)				
Source	Destination	Protocols	Ports	Description
RAS Web Administration Service	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS Provider Agent	TCP	30006	Log retrieval
	RAS Connection Broker	TCP	20002, 20001 30020	Communication with PA and Redundant Agent Used during publishing to browse for agents
	RAS RD Session Host Agent	TCP	135, 445	30020 - remote agent pushing (pre-RAS) Remote Install Push/Takeover of Software
	RAS Guest Agent			
	RAS Remote PC Agent			
	RAS Connection Broker			
	RAS Secure Gateway			
	RAS Enrollment Server			
	RAS Reporting Service	TCP	3000	Integration of RAS Reporting in Management Console

RAS PowerShell

Source	Destination	Protocols	Ports	Description
RAS PowerShell	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS Remote PC Agent	TCP	30004	Log retrieval
	RAS Provider Agent	TCP	30006	Log retrieval
	RAS Connection Broker	TCP	20002, 20001	Communication with PA and Redundant Agent Used during publishing to browse for agents

RAS Provider Agent

Source	Destination	Protocols	Ports	Description
RAS Provider Agent	RAS Connection Broker	TCP	20003	Connection Broker communication port
	RAS Guest Agent	TCP	30010	TCP is used to send the commands.
		UDP	30009	UDP is used during the initial handshake
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected data
	Hyper-V	TCP	135, 49152-65535	Used to check if the guest is powered on
	Nutanix	TCP	9440	Used to check if the guest is powered on
	VMWare	TCP	443	Used to check if the guest is powered on
	Microsoft Azure	TCP	443	Used to check if the guest is powered on
	AWS	TCP	443	Used to check if the guest is powered on
	Scale	TCP	443	Used to check if the guest is powered on
	Remote PC over VDI	TCP	135, 49152-65535	Used to check if the guest is powered on

RAS Enrollment Server

Source	Destination	Protocols	Ports	Description
RAS Enrollment Server	AD DS controllers	TCP	389, 3268	LDAP
		TCP	636, 3269	LDAPS
		TCP, UDP	88	Kerberos
		UDP	53	DNS
	RAS Connection Broker	TCP	20003	Settings synchronization and performance
		UDP	20003	Deny Connection Request
	Certificate Authority (CA)	TCP	135	DCOM/RPC ports
		TCP	dynamic range	
			49152 - 65535	

RAS RD Session Host Agent

Source	Destination	Protocols	Ports	Description
RAS RD Session Host Agent	RAS Connection Broker	TCP, UDP	20003	Used for communications with RAS Connection Brokers.
	Localhost	TCP	30005	For internal commands (memshell, printer redirector).
	FSlogix	TCP	443	Download FSlogix installer
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	RAS Enrollment Server	TCP	30030	RAS RD Session Host Agent (PrIsSCDriver) connects to get login credentials.

RAS Guest Agent

Source	Destination	Protocols	Ports	Description
RAS Guest Agent (used by Azure Virtual Desktop)	Provider Agent	TCP, UDP	30006	Communication with Provider Agent
				Subnet broadcast is sent to find Provider Agent
				Regular UDP heartbeats
	Localhost	TCP	30005	For internal commands - memshell, printer redirector)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB
	RAS Enrollment Server	TCP	30030	RAS Guest Agent (PrIsSCDriver) connects to get logon credentials
	FSlogix	TCP	443	Download FSlogix installer

RAS Remote PC Agent

Source	Destination	Protocols	Ports	Description
RAS Remote PC Agent	RAS Connection Broker	TCP, UDP	20003	Used for communications with RAS Connection Brokers
	Localhost	TCP	30005	For internal commands - memshell, printer redirector)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB
	RAS Enrollment Server	TCP, UDP	30030	RAS Remote PC (PrIsSCDriver) connects to get logon credentials
	FSlogix	TCP	443	Download FSlogix installer

Tenant Broker

Source	Destination	Protocols	Ports	Description
Tenant - RAS Connection Broker	Tenant Broker - RAS Connection Broker	TCP	20003	Tenant's RAS Connection Broker communicates with Tenant Broker to join Tenant Broker, synchronize configuration and statuses

Azure Virtual Desktop

The Azure virtual machines you create for Azure Virtual Desktop must have access to the following URLs in the Azure commercial cloud:

Address	Outbound TCP port	Purpose	Service tag
*. wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent traffic	AzureCloud
* xt.blob.core.windows.net	443	Agent traffic	AzureCloud
* eh.servicebus.windows.net	443	Agent traffic	AzureCloud
* xt.table.core.windows.net	443	Agent traffic	AzureCloud
* xt.queue.core.windows.net	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud
169.254.169.254	80	Azure Instance Metadata service endpoint	N/A
168.63.129.16	80	Session host health monitoring	N/A

The following table lists optional URLs that your Azure virtual machines can have access to:

Address	Outbound TCP port	Purpose	Azure Gov
*. microsoftonline.com	443	Authentication to Microsoft Online Services	login.microsoftonline.us
*. events.data.microsoft.com	443	Telemetry Service	None
www.msftconnecttest.com	443	Detects if the OS is connected to the internet	None
*. prod.do.dsp.mp.microsoft.com	443	Windows Update	None
login.windows.net	443	Sign in to Microsoft Online Services, Microsoft 365	login.microsoftonline.us

*. <u>sfx.ms</u>	443	Updates for OneDrive client software	<u>oneclient.sfx.ms</u>
*. <u>digicert.com</u>	443	Certificate revocation check	None
*. <u>azure-dns.com</u>	443	Azure DNS resolution	None
*. <u>azure-dns.net</u>	443	Azure DNS resolution	None

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.