



Parallels Remote Application Server

Solutions Guide

v15

Parallels IP Holdings GmbH

Vordergasse 59

8200 Schaffhausen

Switzerland

Tel: + 41 52 632 0411

Fax: + 41 52 672 2010

www.parallels.com

Copyright © 1999-2016 Parallels IP Holdings GmbH and its affiliates. All rights reserved.

This product is protected by United States and international copyright laws. The product's underlying technology, patents, and trademarks are listed at <http://www.parallels.com/trademarks>.

Microsoft, Windows, Windows Server, Windows NT, Windows Vista, and MS-DOS are registered trademarks of Microsoft Corporation.

Apple, Mac, the Mac logo, Mac OS, iPad, iPhone, iPod touch, FaceTime HD camera and iSight are trademarks of Apple Inc., registered in the US and other countries.

Linux is a registered trademark of Linus Torvalds.

All other marks and names mentioned herein may be trademarks of their respective owners.

Contents

Introduction	4
About This Guide	4
What is Parallels Remote Application Server.....	4
Advantages of Parallels Remote Application Server Based Computing.....	5
Parallels Remote Application Server Components	6
How Does It Work.....	7
Parallels Client Connection Flow.....	9
Client Connection Modes	10
Deployment Scenarios	12
General Considerations.....	12
How to Read Diagrams and Tables.....	12
Parallels RAS Deployment Scenarios.....	15
Single Farm with One Microsoft Remote Desktop Services Server	15
Single Farm with Two Microsoft Remote Desktop Services Servers	17
Single Farm with Mixed Desktops.....	18
Single Farm with Public & Private Parallels Secure Client Gateways	19
Single Farm with Dual Parallels Secure Client Gateways.....	21
High Availability with Multiple Gateways.....	24
High Availability with Single or Dual F/W DMZ.....	26
Mixed Scenarios.....	33
Deploying Parallels RAS Reporting Service	43
One Site with Multiple Microsoft RDS Servers	43
Multiple Sites with Multiple Microsoft RDS Servers	45
Port Reference and SSL Certificates.....	48
Port Reference.....	48
SSL Certificates	49
Index	52

CHAPTER 1

Introduction

In This Chapter

About This Guide	4
What is Parallels Remote Application Server	4
Advantages of Parallels Remote Application Server Based Computing	5
Parallels Remote Application Server Components	6
How Does It Work	7

About This Guide

This guide is intended for system administrators deploying and managing Parallels Remote Application Server (Parallels RAS) in their organizations. It begins with the introduction to Parallels RAS and its key components and then outlines the basic principles of operation of these components. The main topics of this guide describe the various deployment scenarios, complete with diagrams and description of components used in each scenario. The guide concludes with the information about communication ports used by Parallels Remote Application Server and provides information about using SSL certificates.

What is Parallels Remote Application Server

Parallels Remote Application Server is a market leader for Windows application publishing on any device, anywhere. It works with major hypervisors and Microsoft Remote Desktop Services, providing PC, Mac, and mobile users with a seamless experience while increasing security and reducing IT costs. It's simple and empowers users with the freedom and flexibility to work how they want.

With Parallels RAS, remote desktops and applications can be accessed from any device running virtually any operating system, including Windows, Linux, OS X, iOS, Windows Phone, Android, Chrome. Additionally, web access is available via Parallels Web Portal, as well as clientless access via HTML5.

For an in-depth information about the rich Parallels RAS features, please read the Parallels Remote Application Server Administrator's Guide, which can be downloaded from the Parallels website.

Advantages of Parallels Remote Application Server Based Computing

Server-based computing

Less administration, higher availability, reduced TCO.

Simplified administration

Central management of users, server-based OS patch management, application updates, virus definition updates, and backups.

Higher security

All data is kept on a server side with centralized security and backup management. Only mouse clicks, keyboard keystrokes, and desktop/application screenshots are transmitted to and from the client device, thus preventing data leakages, viruses, Trojans, and other vulnerabilities on clients.

Hardware independence

Support for virtually all platforms on client devices, including Windows, Linux, OS X, iOS, Windows Phone, Android, Chrome, and HTML5, all with minimum hardware requirements.

Easy access

Employees, customers, and partners telecommute/roam more easily with follow-me apps and desktops on any device from anywhere.

Extended Windows PC Lifecycle

Achieve cost savings in hardware replacement by converting Windows PCs into pseudo thin clients. Continue using Windows legacy operating systems to securely run virtual applications while also restricting access to native OS features. What's more, the administrator can choose which applications a user runs locally and remotely on a PC.

Proactive monitoring

Parallels RAS Reporting helps IT administrators to proactively tackle any potential issue before it occurs, providing reports and statistics on resources and services shown under one roof in the Parallels RAS console.

End user support

Windows Client Management enables client device shadowing (user session control) and power management for help desks, making routine end user assistance easier.

Parallels Remote Application Server Components

Farm is a collection of Parallels RAS components maintained as a logical entity with a unique database and licensing.

Site is a managing entity usually based on a physical location. Each site consists of at least a Publishing Agent, a Secure Client Gateway, and agents installed on terminal servers, virtualization servers, and Windows PCs. There can be multiple sites in a given farm.

Parallels RAS Console is the primary graphical user interface to use to configure and access Parallels Remote Application Server features.

RAS Publishing Agent is a service that provides access to published applications and desktops and load balances application traffic. High availability can be achieved by adding a backup RAS Publishing Agent to a site.

RAS Terminal Server Agent is a service installed on a Microsoft RDS server that enables publishing of the server resources (applications and desktop). RAS Publishing Agent also collects the necessary information from the server on which it's running and sends it to the RAS Publishing Agent, which uses it for load balancing and some other purposes.

RAS Remote PC Agent is a service installed on a physical Windows computer or a Windows virtual machine. It enables publishing of the computer resources (applications and desktop). RAS Remote PC Agent also collects the necessary information from the computer on which it's running and sends it to the RAS Publishing Agent, which uses it for load balancing and some other purposes.

RAS Guest Agent is a service installed in the guest operating system of a virtual machine, which is used as a VDI template on a hypervisor. The guest agent enables resource publishing from the VDI desktops and collects information required by the Publishing Agent. You can find a detailed information about VDI templates in the Parallels Remote Application Server Administrator's Guide.

RAS VDI Agent is a service application on Hyper-V and a virtual appliance on VMware and XenServer. RAS VDI Agent provides an interface for managing a hypervisor through its native API and also collects and sends information to the RAS Publishing Agent.

RAS Secure Client Gateway is a service that acts as a proxy between the Parallels Client software running on client devices and Parallels Remote Application Server. The gateway encrypts the communications using SSL. Multiple RAS Secure Client Gateways can work in high availability mode with Parallels HALB.

Parallels HALB (High Availability Load Balancing) is a secure virtual appliance provided by Parallels for the following supported hypervisors: Hyper-V, VMware, XenServer. The HALB virtual appliance is placed between client devices and RAS Secure Client Gateway. Multiple HALB appliances can run simultaneously, one acting as the master and the others as slaves. The more HALB appliances a Parallels RAS installation has, the lower the probability that end users will experience downtime. Master and slave appliances share a common or virtual IP address (also called VIP). Should the master HALB appliance fail, a slave is promoted to master and takes its place seamlessly without affecting end user connections.

Parallels RAS Web Portal is a web page that provides access to published resources via a web browser.

Parallels Device Manager is a Parallels RAS feature that allows the administrator to manage Windows computers. Windows XP up to Windows 10 are supported.

Parallels Desktop Replacement is a sub-feature of Parallels Device Manager (see above). It allows the administrator to convert a standard desktop into a limited device similar to a thin client without replacing the operating system on it.

How Does It Work

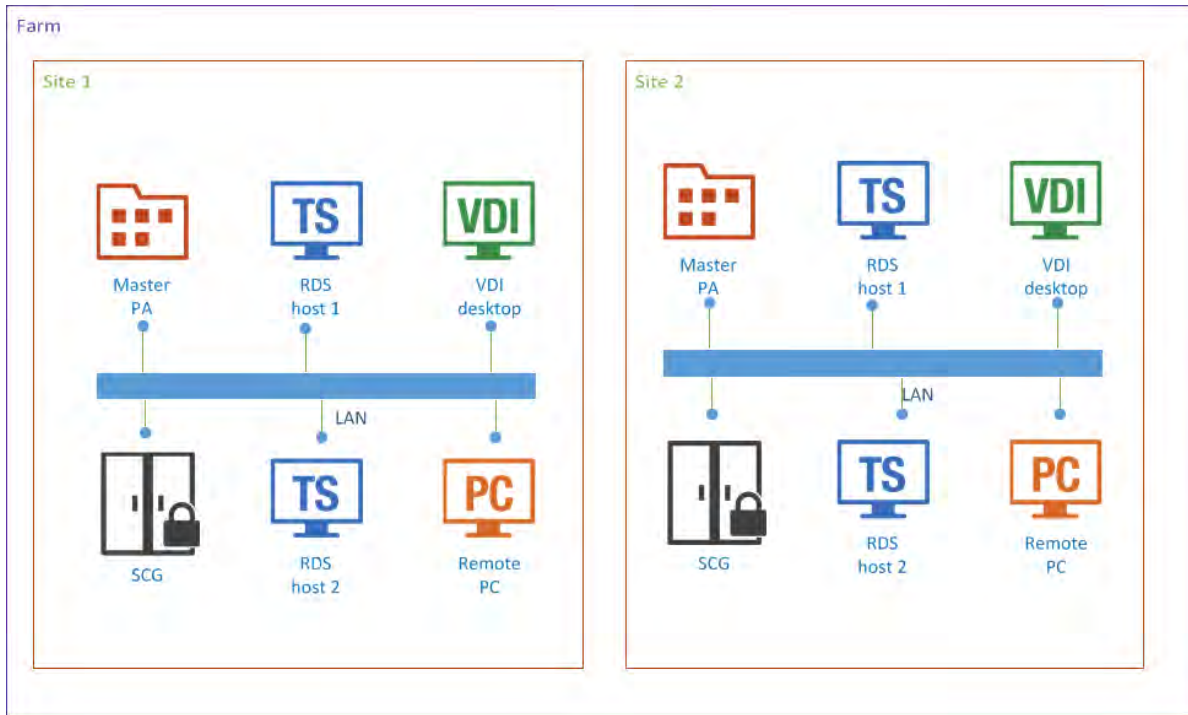
When a user connects to Parallels Remote Application Server from Parallels Client, they are presented with published resources (applications, desktops, documents, or published URLs). The user selects a resource and runs or opens it (depending on the resource type). The system load balances user requests automatically and launches the requested resource from a least-loaded host. The user is then presented with their requested resource seamlessly via RDP protocol, given that the resource is actually running on a remote server rather than locally on the user's device.

The Parallels Remote Application Server building blocks are (see the previous section for a detailed explanation):

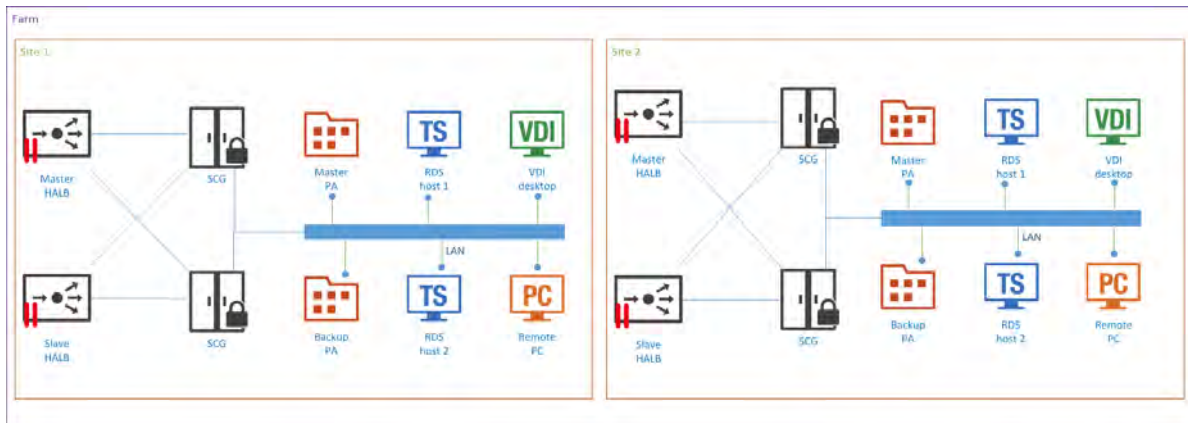
- Farm
- Site
- Agents

The first server added to a farm creates a new site and becomes the master RAS Publishing Agent in that site. The server also becomes the farm's Licensing Server handling device connection licenses. Every Publishing Agent in the farm (when more than one exists) keeps a synchronized copy of the Parallels RAS configuration database. When the administrator makes any changes to the Parallels RAS configuration in the Parallels RAS console, the changes are replicated to all other Publishing Agents.

The following diagram illustrates a Parallels RAS installation with two sites (Site 1 and Site 2), each consisting of a master Publishing Agent (Master PA), RAS Secure Client Gateway (SCG), Terminal Server (TS - RDS host 1), a second Terminal Server (TS - RDS host 2), VDI (Virtual Network Infrastructure) server, and a Windows PC.



Adding more RAS Publishing Agents and RAS Secure Client Gateways adds redundancy to the system. HALB is an optional component, which can be added to load balance application traffic.



Note: Resources (Terminal Servers, Remote PCs, VDI desktops) that are members of one site cannot be shared with other sites. For example, the RDS host 1 server is a member of Site 1, which means that it cannot be accessed by users who are connecting through a Secure Client Gateway and a Publishing Agent located in Site 2.

Parallels Client Connection Flow

The client connection flow consists of two stages: application enumeration and application launching. The following describes each stage in detail. Please note that the steps described below equally apply to all other types of published resources (not just applications), including remote desktops, documents, Web applications, and network folders.

Application Enumeration

Application enumeration is the process of getting the list of published resources that a particular user can use. During this stage, the following steps take place:

- 1** A user launches Parallels Client on their device and double-clicks a RAS connection (provided it has been configured).
- 2** Parallels Client connects to the RAS Secure Client Gateway or the HALB appliance, if one is installed.
- 3** If HALB is installed, the HALB appliance forwards the Parallels Client to the Secure Client Gateway according to load balancing rules. If HALB is not engaged with SSL offload (HALB is not installed or the pass-through mode is in place), an SSL session between the client and RAS Secure Client Gateway is established.
- 4** RAS Secure Client Gateway builds a connection tunnel with a Publishing Agent to initiate client authentication.
- 5** The Parallels Client transmits user credentials to the Publishing Agent.
- 6** If the user authentication is successful, the Publishing Agent returns the application list to the Parallels Client via the Secure Client Gateway SSL tunnel.
- 7** The application list is displayed in the Parallels Client window on the user's device, so the user can select an application to launch.

Application Launching

This stage comprises of the following steps:

- 1** The user launches an application.
- 2** The Parallels Client sends the request via the Secure Client Gateway tunnel to the Publishing Agent.
- 3** The Publishing Agent selects the least loaded RDS server and then sends its IP address back to the Parallels Client via Secure Client Gateway.
- 4** Depending on the connection mode selected on the client side (see **Client Connection Modes** below), the Parallels Client connects to the RDS server directly or via RAS Secure Client Gateway and passes the user credentials to it.
- 5** The RDS server verifies the received credentials and, if they are valid, starts an RDP session.

Client Connection Modes

Parallels Client can connect to Parallels Remote Application Server using one of the following connections modes:

- Direct
- Direct SSL
- Gateway
- Gateway SSL

Direct

To use a direct connection, Parallels Client must be able to directly access the server hosting the RAS Secure Client Gateway.

The connection is established as follows:

- 1** Parallels Client connects to a Secure Client Gateway through port 80 and negotiates a connection to establish a session.
- 2** Parallels Client then initiates an RDP session directly with a Terminal Server or a VDI host through port 3389.
- 3** Client disconnects from the gateway and establishes a new session with the server.

The direct mode is the most efficient connection because the RAS Secure Client Gateway is used only temporarily for a short period of time.

Direct SSL Mode

The direct SSL mode is the same as the direct mode but uses SSL encryption. To use a direct SSL mode, Parallels Client must also be able to directly access the RAS Secure Client Gateway server.

The connection is established as follows:

- 1** Parallels Client connects to a RAS Secure Client Gateway through port 443. Client and gateway negotiate a connection to establish a session.
- 2** Parallels Client initiates an RDP session directly with a Terminal Server or a VDI host through port 3389.
- 3** Parallels Client disconnects from the gateway and establishes a new session with the server.

Gateway Mode

When Parallels Client cannot directly access the server hosting the RAS Secure Client Gateway, it must use the gateway mode. The gateway mode is the simplest connection mode available. An administrator need to open only a single port, which is usually port 80.

The connection is established as follows:

- 1** Parallels Client connects to the RAS Secure Client Gateway on port 80 and negotiates a connection to establish a session.
- 2** Parallels Client requests the gateway to establish an RDP session through port 3389 with a terminal server or a VDI host using the same connection, thus forming a tunnel.
- 3** All communications between Parallels Client and the server then carried out using the established tunnel.

Gateway SSL Mode

The gateway SSL mode is the same as the gateway mode but uses SSL encryption.

The connection is established as follows:

- 1** Parallels Client connects to the RAS Secure Client Gateway on port 443.
- 2** Once an SSL tunnel is established, the client and gateway negotiate to establish a secure session.
- 3** Parallels Client requests the gateway to establish an RDP session through port 3389 with a terminal server or a VDI host using the same connection, thus forming a tunnel.
- 4** All communications between Parallels Client and the server then carried out using the established tunnel.

Mixed Mode: Direct and Gateway SSL

Parallels Remote Application Server is able to handle multiple connection modes simultaneously. For better utilization of RAS Secure Client Gateways, using the direct mode for LAN clients is recommended whenever possible. For better security, using the gateway SSL mode is recommended for WAN clients.

CHAPTER 2

Deployment Scenarios

This chapter describes common Parallels Remote Application Server deployment scenarios.

In This Chapter

General Considerations	12
How to Read Diagrams and Tables	12
Parallels RAS Deployment Scenarios	15

General Considerations

Regardless of the size of a particular Parallels RAS installation, redundancy among core components of your setup is recommended to ensure the greatest possible uptime. For small deployments, all roles can be installed on a single server, whereas role segregation is recommended for large setups.

The physical location of a Parallels Remote Application Server farm, including terminal servers and VDI desktops, must be selected based on the location of back-end resources, such as databases and file servers. This means that if a front-end application connects to a database or works with files on a file server, the terminal server on which it will be installed should be located close to the database (or the file server) on the intranet with fast, reliable, low latency LAN connections. For example, let's say you have a client-server application that you want to make available to your users. To do so, you will install the client part on a terminal server and publish it for your users. The database will continue to run on a dedicated server. To guarantee fast and reliable database access, the terminal server and the database server must be close to each other on the local network.

How to Read Diagrams and Tables

The topics describing deployment scenarios include diagrams and tables. The instructions below explain how to read them.

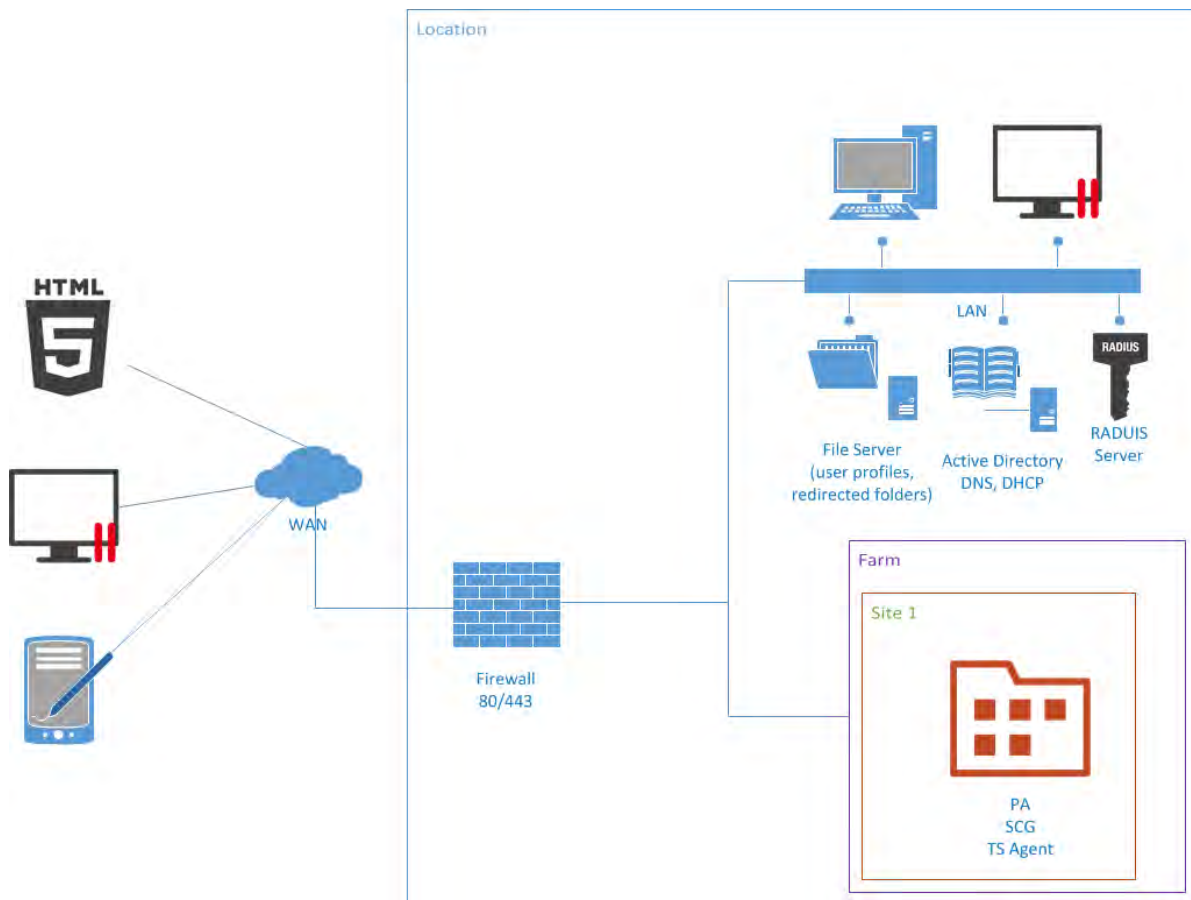
Abbreviations

The following table describes the abbreviations used in the diagrams.

Abbreviation	Description
PA	RAS Publishing Agent
SCG	RAS Secure Client Gateway
SGW	Same as SCG above
TS Agent	RAS Terminal Server Agent
Remote PC	Remote Windows computer
VDI	Virtual Desktop Infrastructure. This includes a server running a hypervisor and virtual machines running guest operating systems (virtual guests).
TS	Terminal Server
RDS host	Remote Desktop Services server
HALB	High Availability and Load Balancing

Diagrams

To understand the diagram layout, consider the following sample diagram:



The left side of the diagram displays clients that can connect to Parallels Remote Application Server. In the example above, the clients are (from top to bottom):

- HTML5 enabled web browser
- Windows, Linux, or Mac computer
- Mobile device

The **Location** rectangle denotes a physical location, such as an office.

The **Farm** rectangle represents a Parallels RAS farm, which is comprised of one or more sites.


The **Site** rectangle represents a site with individual servers and components contained on them. In the example above, the site has a single server with RAS Publishing Agent (PA), RAS Secure Client Gateway (SCG), and RAS Terminal Server Agent (TS Agent) installed on it.

The **LAN** bar represents a local area network with the usual resources connected to it, including servers and desktops, desktop computers with Parallels Client installed on them, file servers, AD domain server, DNS, etc.

The lines between icons denote the communication channels between individual components.

Server Components Tables

Together with a diagram, each topic describing a deployment scenario also includes one or more tables describing server components involved in a particular scenario. Consider the following sample table:

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Windows Installer (standard installation)
	Parallels Publishing Agent	
Parallels Terminal Server Agent		

The icon in the leftmost column corresponds to a component depicted on the diagram (see the diagram sample above). In this case, it's the server hosting the RAS Publishing Agent and the rest of the components described earlier.

The table header (in bold) indicates the type of the physical server used. In the example above, it's a Microsoft Remote Desktop Services Server.

The **Component Installed** column lists Parallels Remote Application Server components that must be installed on the server.

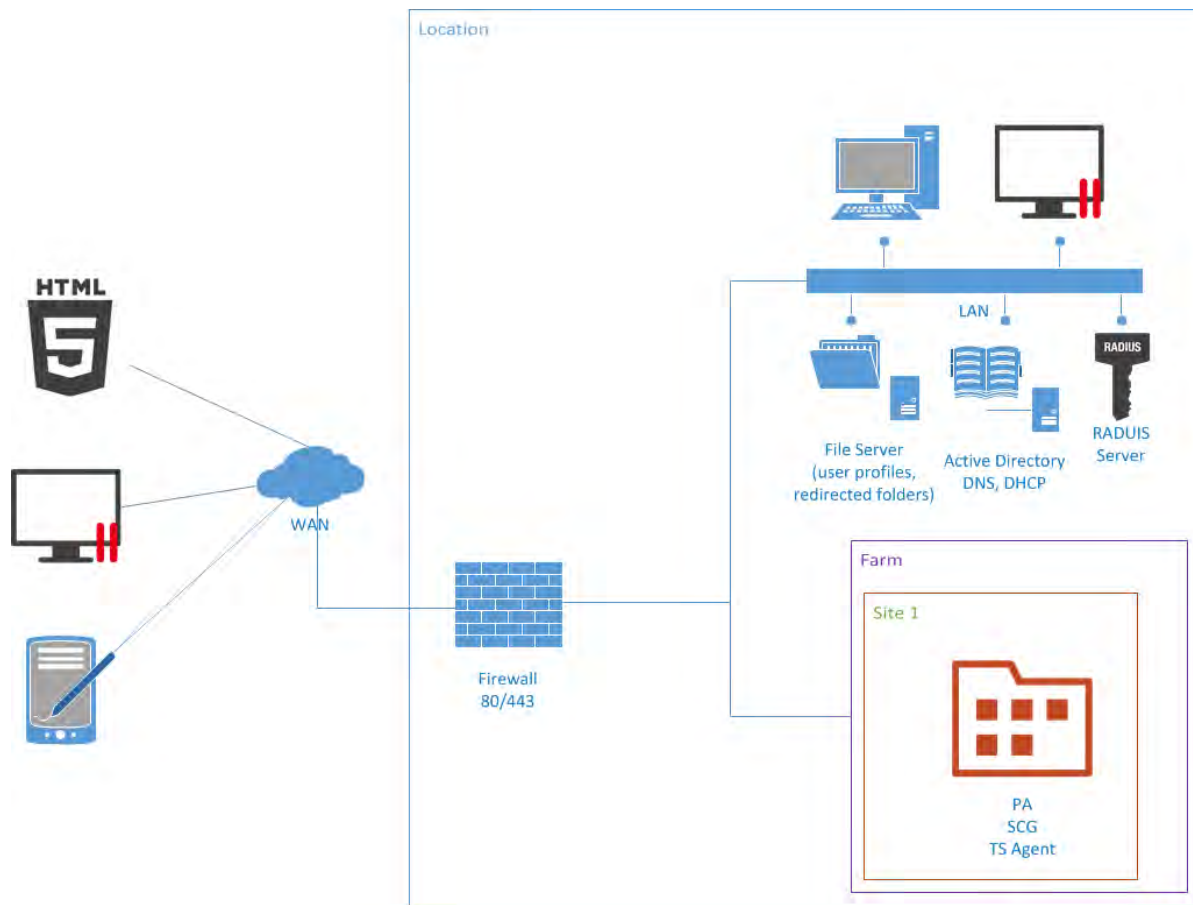
The **Installation Method** column specifies how a component (or components) must be installed. The following installation methods are used to install Parallels RAS components:

- **Windows Installer (standard installation).** This is the standard Windows installer (MSI installer package) that you run in Windows to install an application. The "standard installation" part indicates that the **Standard** option should be selected when using the installer, which means that the default installation options will be used.
- **Windows Installer (custom installation).** This is the same type of installation as the one above, but you must select **Custom** when using the installer. The custom installation allows you to select the component(s) to install. This installation type is used when no push installation can be performed for any reason (e.g. a server cannot be logged into over the network).
- **Push Installation.** A component is installed remotely from the RAS console by pushing the MSI installer packages to a remote server and then performing an unattended installation of the component on it.
- **Virtual appliance.** A pre-configured virtual appliance for VMware or XenServer. You can download a virtual appliance for the hypervisor you are using from the Parallels website by visiting the following URL: <http://www.parallels.com/products/ras/download/server/links/>


Parallels RAS Deployment Scenarios

Single Farm with One Microsoft Remote Desktop Services Server

This scenario uses a single server for publishing applications and desktops. SSL and HTML5 Gateway are enabled by default with a self-signed server certificate. The server certificate should be deployed on client devices. Enterprise certificate or third party trusted Certificate Authority can be used for external access (for details, see the **SSL Certificates** section (p. 49)).

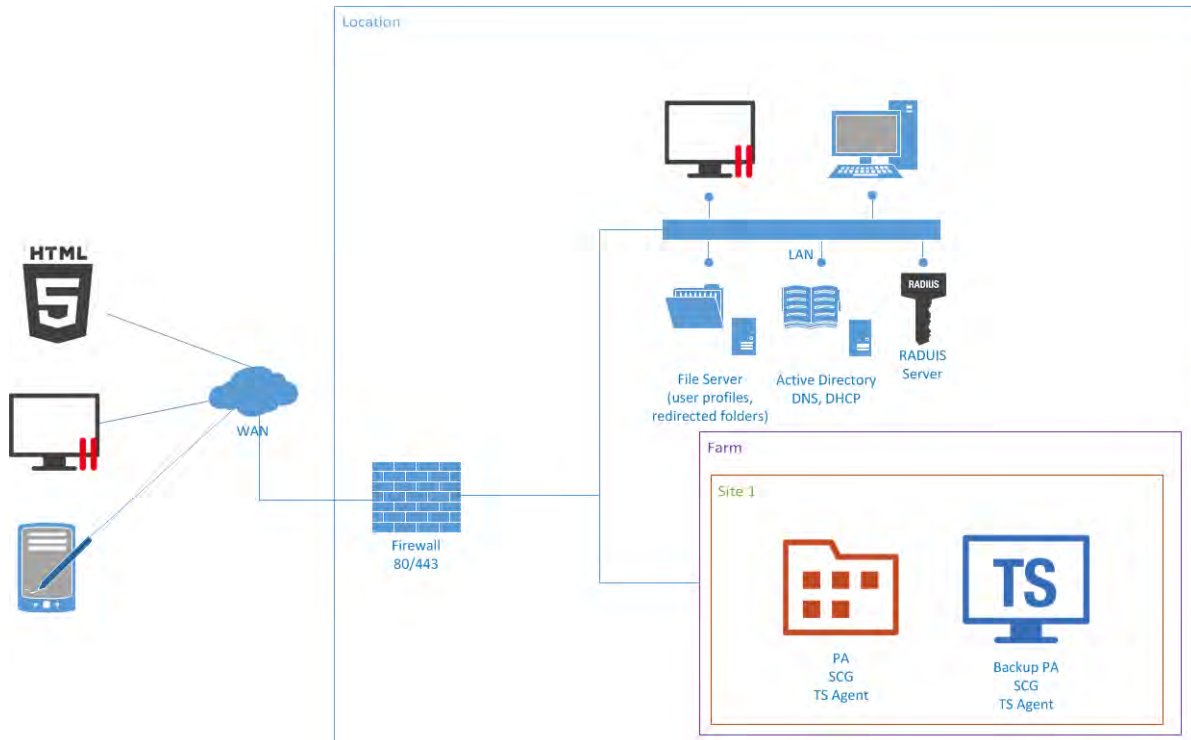


Server Components


	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Windows Installer (standard installation)
	Parallels Publishing Agent	
Parallels Terminal Server Agent		


Single Farm with Two Microsoft Remote Desktop Services Servers

This scenario can be implemented by an organization that needs to load balance published applications and desktops between two Microsoft RDS servers. For high availability, backup RAS Publishing Agent and RAS Secure Client Gateway should be installed on the second server.



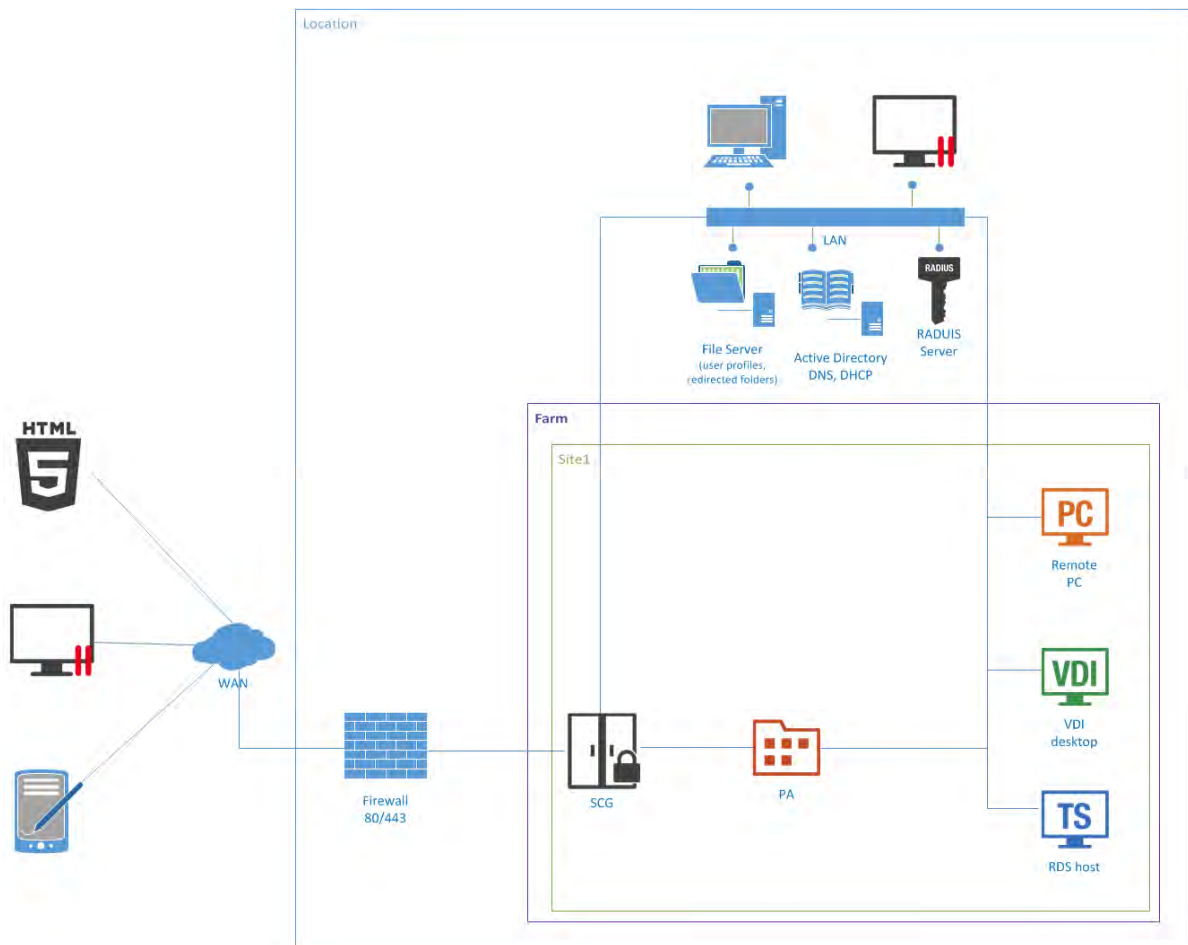
Server Components

Microsoft Remote Desktop Services Server		
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Windows Installer (standard installation)
	Parallels Publishing Agent	
	Parallels Terminal Server Agent	


Microsoft Remote Desktop Services Server		
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation
	Parallels Secure Client Gateway, including HTML5 Gateway	
	Parallels Publishing Agent (serves as a backup Publishing Agent)	

Single Farm with Mixed Desktops


By using this scenario you can publish applications and desktops from virtual environments, Microsoft RDS servers, and Windows desktops or laptops located in your office.



Server Components

	Parallels Remote Application Server	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway Parallels Publishing Agent	Windows Installer (standard installation)

	Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent Parallels Guest Agent	Push installation or virtual appliance Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

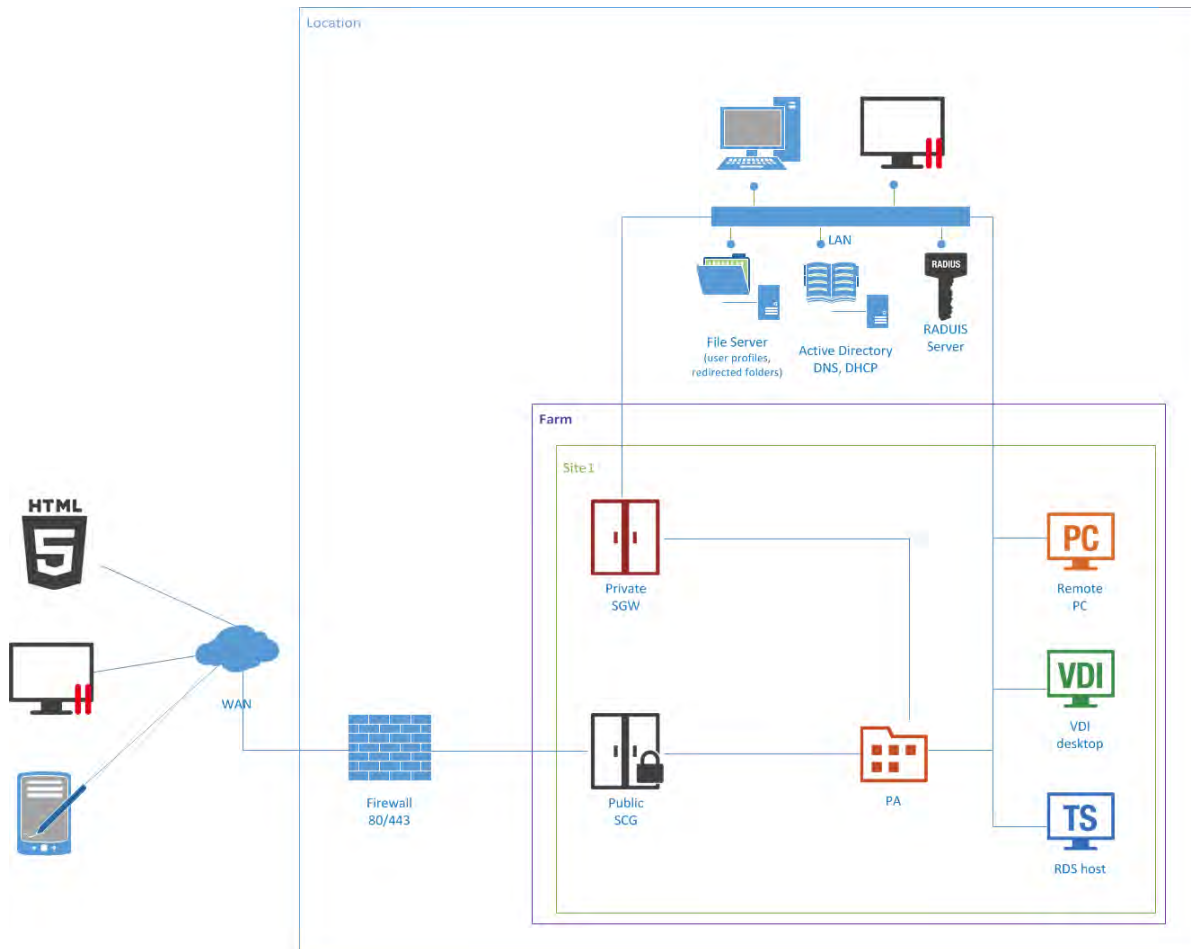
Single Farm with Public & Private Parallels Secure Client Gateways

To handle more connections on Secure Client Gateways, using a designated Parallels Secure Client Gateway is recommended for intranet users (private) with direct client connection mode.


Deployment Scenarios


To apply stricter security settings to servers with Internet access, using a designated Secure Client Gateway is recommended for Internet users (public) with Gateway SSL client connection mode.

The appropriate RAS connection settings can be applied either centrally via Client Policy in the Parallels Application Server Console or manually in the Parallels Client.




Server Components

Parallels Remote Application Server		
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Windows Installer (standard installation)
	Parallels Publishing Agent	

	Private Parallels Secure Client Gateway (Direct Mode)	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Public Parallels Secure Client Gateway (Gateway Mode)	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

Single Farm with Dual Parallels Secure Client Gateways

This scenario enables high availability for client connections using RAS connection settings on either the Parallels Client side or DNS round robin.

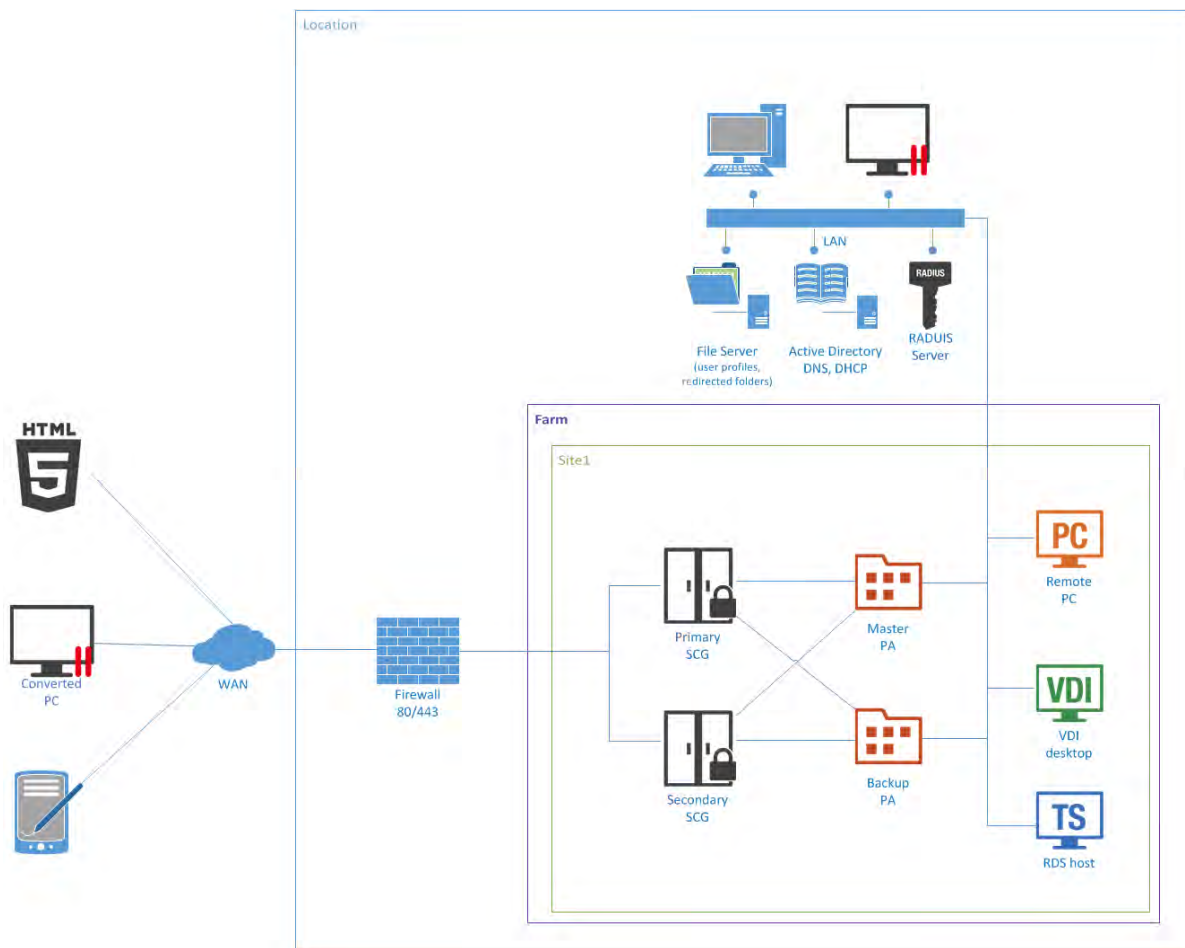
To enable high availability for client connections using RAS connection settings, the Parallels Clients should be configured to connect to primary and secondary Secure Client Gateways using the primary and secondary connection settings in the RAS connection properties.

Deployment Scenarios

In this case, primary and secondary Parallels Secure Client Gateways must be configured to connect to the same Parallels Publishing Agents (using the Advanced Client Gateway Settings). When the Primary Parallels Secure Client Gateway is not available, Parallels Clients can connect to the farm using the Secondary Parallels Secure Client Gateway.


The client settings can be applied either centrally (via Client Policy in the Parallels Application Server Console) or manually.


To enable high availability for client connections using DNS round robin, two new host records must be created in the DNS forward lookup zone with the same name (e.g. RemoteAccess.example.com) but with two different IP addresses of primary and secondary Parallels Secure Client Gateways.





Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation

	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

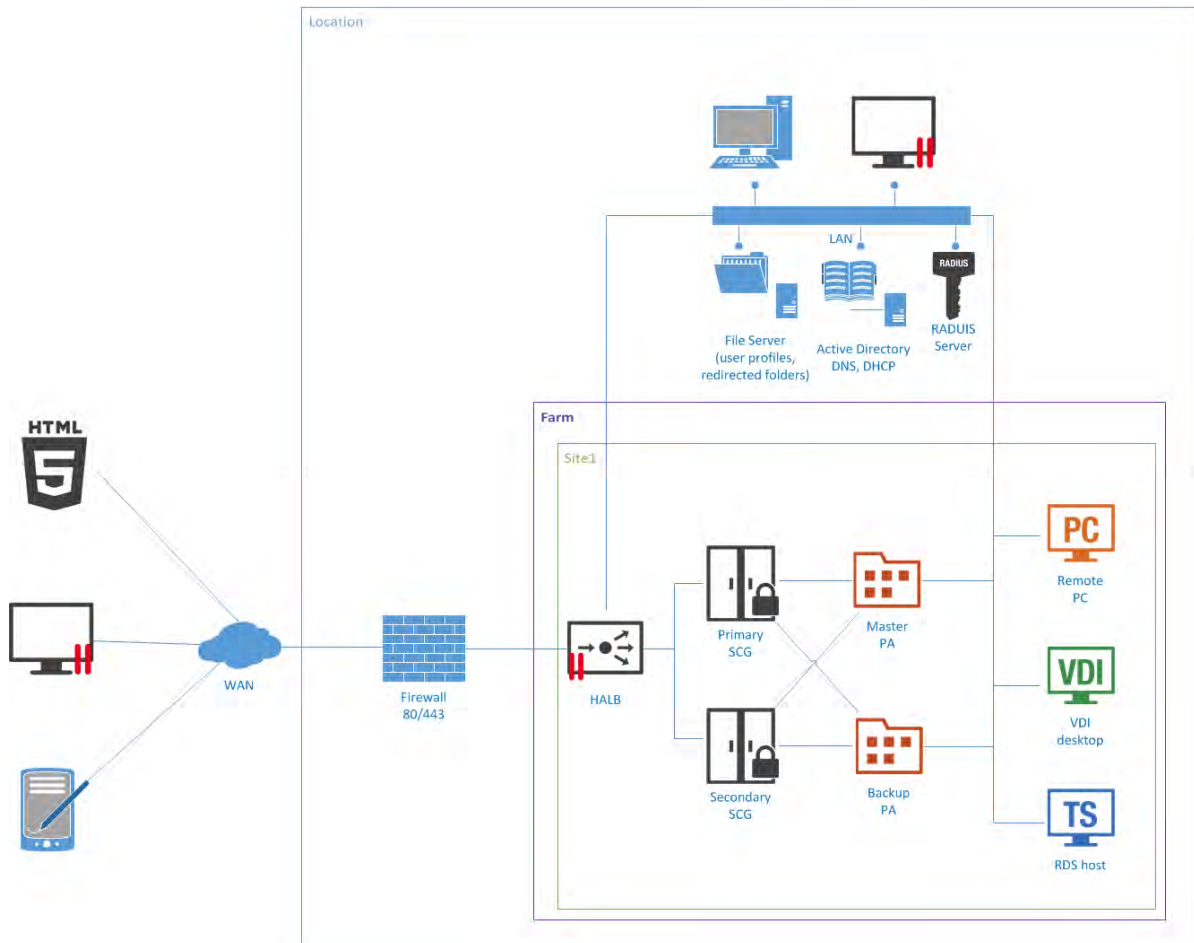
	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

High Availability with Multiple Gateways

This scenario is ideal for high availability environments with more than 300 concurrent users connected in SSL mode. Each client gateway should optimally handle 300 to 500 concurrent user connections* (see the note below). This can be scaled horizontally accordingly.

Both LAN and WAN users connect to the virtual address of a high availability and load balancing virtual appliance in an internal network.




*300 users through SSL tunneled gateway mode or 500 standard gateway connections, assuming the gateway machine is only acting as such (with no other demanding services using these machines).


All Parallels Secure Client Gateways must be configured to connect to the same Parallels Publishing Agents (using the Advanced Client Gateway Settings—see above).


Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)


	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation


	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

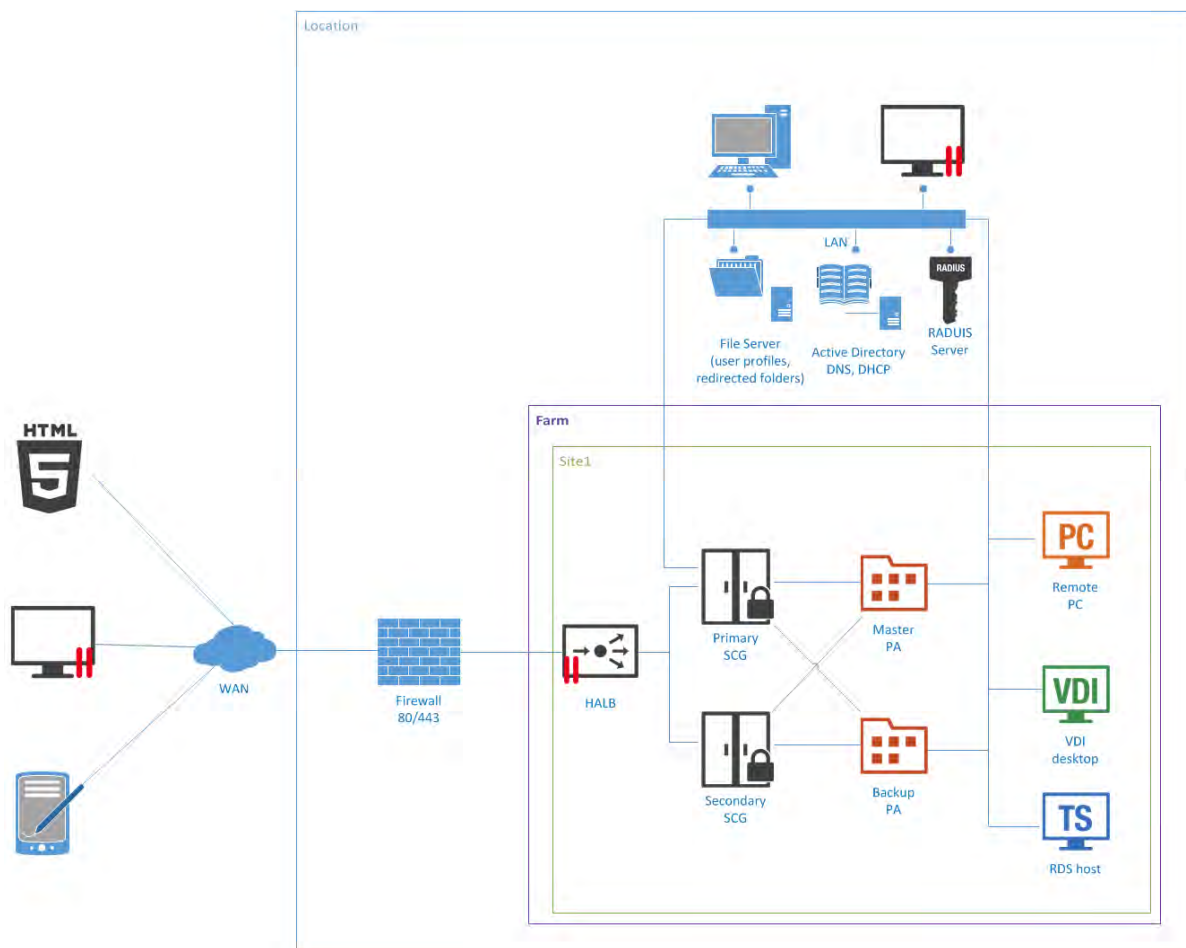
	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

High Availability with Single or Dual F/W DMZ

Many companies use the DMZ layout to separate servers that handle exposed services from those that handle internal services. There are two types of DMZ: single and dual-firewall, with the latter being more expensive but more secure (with the dual firewall approach, using two different firewall technologies allows you to avoid one weakness or one type of attack breaking both firewalls). A firewall between Parallels Secure Client Gateways and the intranet must allow gateways and systems to connect to a Publishing Agent using the standard port.

Single Firewall DMZ


In a single firewall DMZ scenario, the firewall system must be capable of routing connections properly from Parallels Secure Client Gateways to Parallels Publishing Agents. The firewall system is also responsible for connections from the Internet to the virtual IP address presented by a HALB virtual appliance or other generic protocol load balancing scenarios.





In a configuration of this type, HALB is installed in front of Parallels Secure Client Gateways in the internal network. The WAN users connect to HALB VIP, whereas LAN users use primary and secondary gateways configured in the primary and secondary connections settings of the RAS connection properties. The Parallels Client settings can be configured either centrally (via Client Policy in the Parallels RAS console), or locally on a device where Parallels Client is running. To add high availability for HALB, a second appliance can be deployed.


Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows installer (standard installation)

	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation


	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

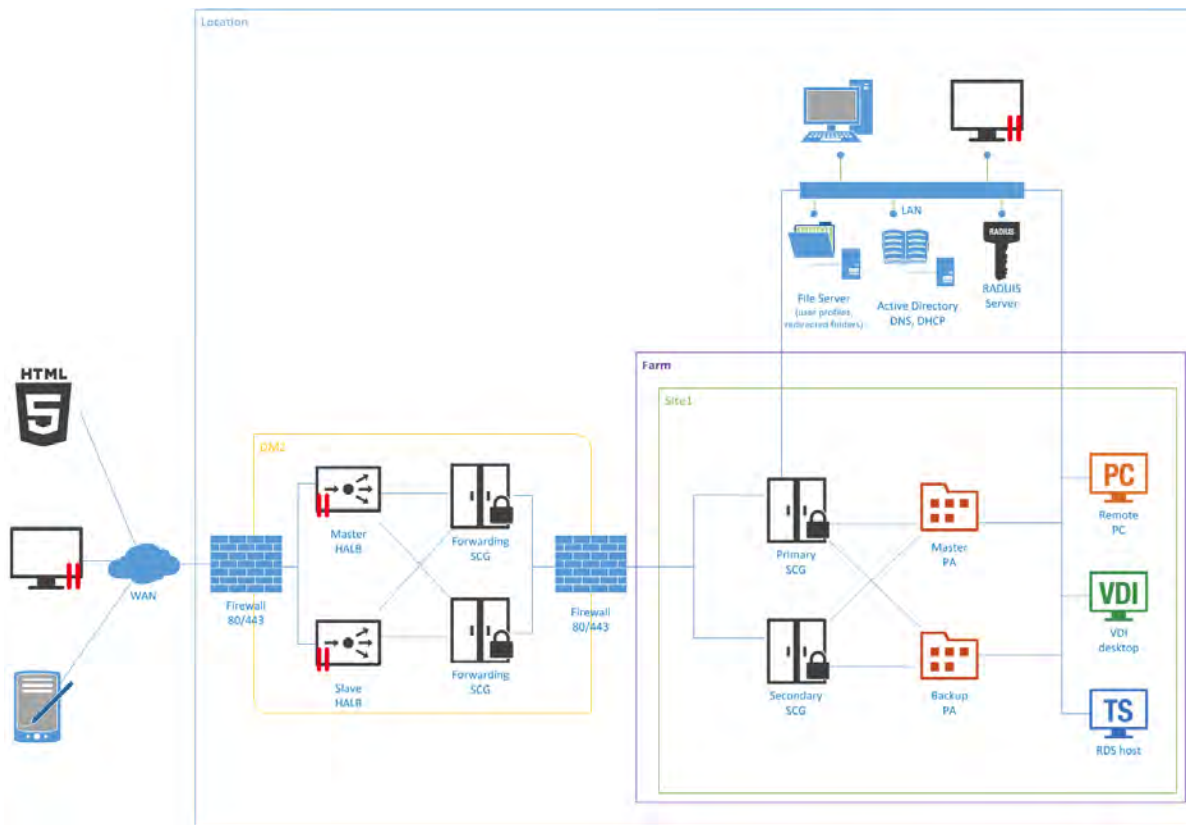
	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

Dual Firewall DMZ


In a dual firewall scenario, settings are simpler, and protection from external malicious agents is higher. Dual Firewall DMZ requires a Forwarding Parallels Secure Client Gateway server installed in the perimeter network to pass client connections to a Parallels Secure Client Gateway residing in the internal network.


In such a configuration, a HALB pair is installed in front of Forwarding Parallels Secure Client Gateways in DMZ. The WAN users connects to HALB VIP, whereas LAN users Primary and Secondary Gateways as Primary and Secondary connection settings of the RAS connection properties. RAS connection properties can be configured either centrally (using Client Policy in the Parallels Application Server Console) or manually.


Forwarding Parallels Secure Client Gateways forward network traffic using the **Forward requests to next RAS Secure Client Gateway in chain** option in the **Advanced** tab of the **Forwarding RAS Secure Client Gateway** properties.





Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation


	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation


	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

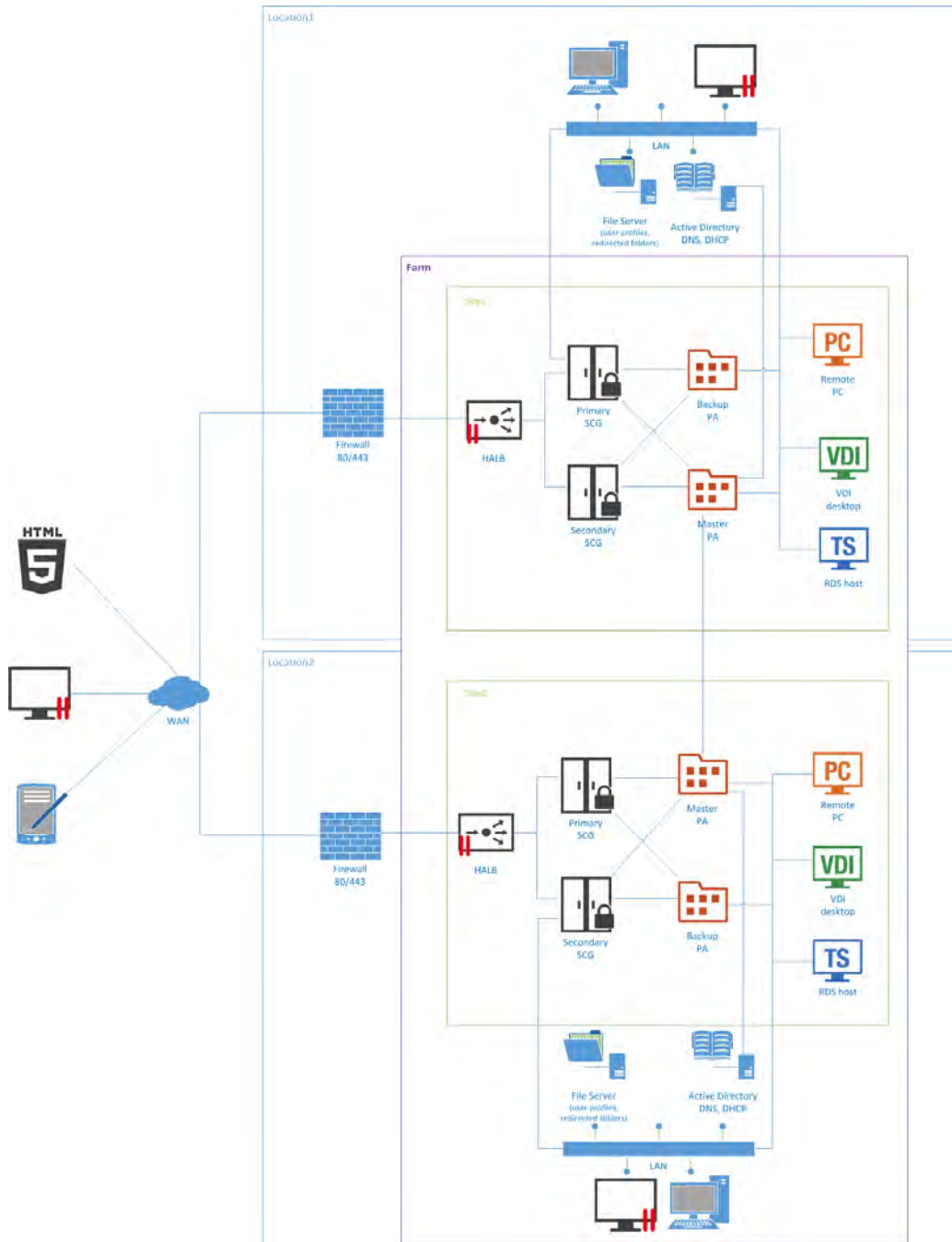
	Forwarding Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	<p>Push installation or (if cannot be pushed) Windows Installer (custom installation).</p> <p>When running the installer in Windows, select Custom and then select RAS SecureClientGateway.</p>

	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

Mixed Scenarios

Multisite Scenario

This scenario is suited for environments where published resources are distributed between two or more physical locations. Different administrators can administer a Parallels RAS farm containing multiple sites.



Each site consists of at least RAS Publishing Agent, RAS Secure Client Gateway (or multiple gateways), and agents installed on RDS or VDI servers, or Windows PCs.

Note: To add high availability for HALB, a second appliance can be deployed in each site.

If the resource set is similar, the users can use both sites via the single RAS connection. The following settings should be used in the RAS connection properties on the Parallels Client:

LAN users of the Site1

- Primary connection – local Primary Secure Client Gateway
- Secondary connections:
 - Local Secondary Secure Client Gateway
 - HALB VIP of the Site2

LAN users of the Site2

- Primary connection – local Primary Secure Client Gateway
- Secondary connections:
 - Local Secondary Secure Client Gateway
 - HALB VIP of the Site1

WAN users


- Primary connection - HALB VIP of the Site1
- Secondary connections - HALB VIP of the Site2


RAS connection settings can be configured either centrally (via Client Policy in the Parallels Remote Application Server Console) or manually.


Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation


	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

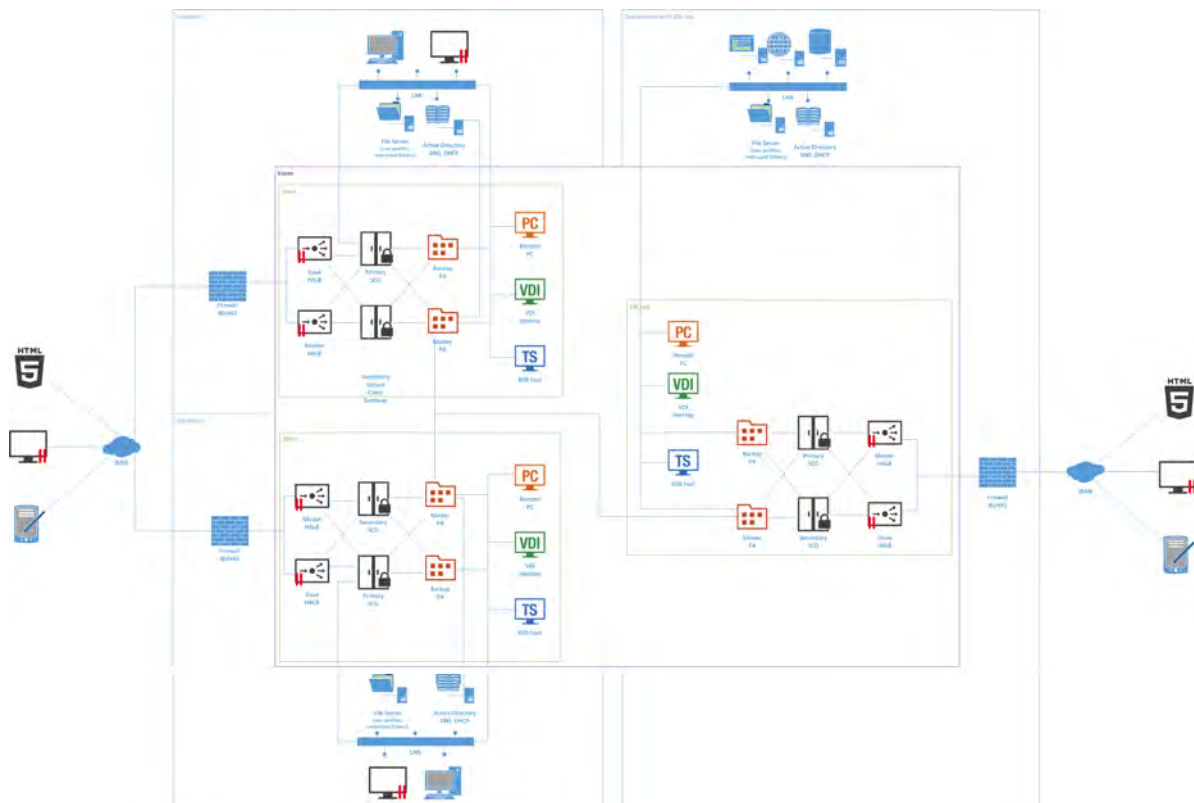
	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

Business Continuity and Disaster Recovery

A Parallels Remote Application server farm placement depends on the location of a back-end resource. Therefore, it is possible to continue operations by adding an additional remote location where the back-end resources are replicated (the appropriate software and hardware solutions are out of the scope of this document) and placing one more Parallels Remote Application Server site in this location.


Setting up a disaster recovery site, and then configuring the Parallels Client to use the closest site as the primary connection and the disaster recovery site as the secondary connection, allows users to always be connected to the primary site and to continue working using the disaster recovery site in case of failure.


WAN users can be invited to use both sites and setup HALB VIP of the first site as Server Address and HALB VIP of the second site as Secondary Server IP in the RAS connection settings on the Parallels Client side. The RAS connection settings can be configured either centrally (via Client Policy in the Parallels Remote Application Server Console) or manually.





Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)


	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Remotely pushed


	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

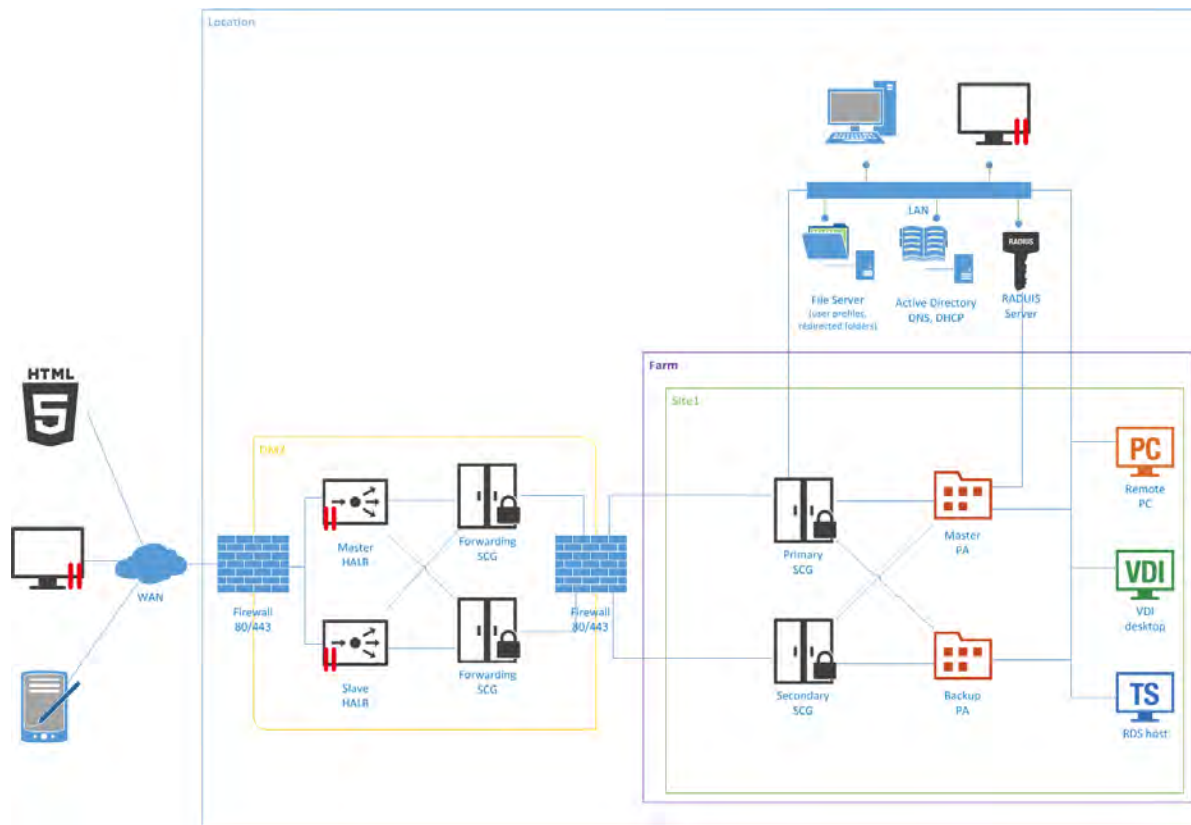
	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

Secure Setup with Dual Firewall DMZ and Second-Level Authentication

Second-level authentication provides a high level of protection via different types of security tokens for two-factor authentication. Users have to authenticate through two successive stages to get the application list. In addition to a standard user name and password, or a smart card authentication, second-level authentication uses a one-time password generated by a token. The second level of authentication can be provided by DualShield, Safenet, or a RADIUS server.

A RADIUS server is recommended to be placed in the Intranet with the Publishing Agent and Active Directory domain controller to speed up application enumeration.



In a configuration of this type the second-level authentication via a RADIUS server is checked first. If the check is successful, authentication takes place at the Active Directory level using either a user name and password or a smart card.

Client Manager and Desktop Replacement

The Client Manager feature allows the administrator to convert Windows devices running Windows XP up to Windows 10 into a thin-client-like OS. After the Windows Device Enrollment has been performed, features like Desktop Replacement, Kiosk Mode, Power Off, Reboot, and Shadow become available.

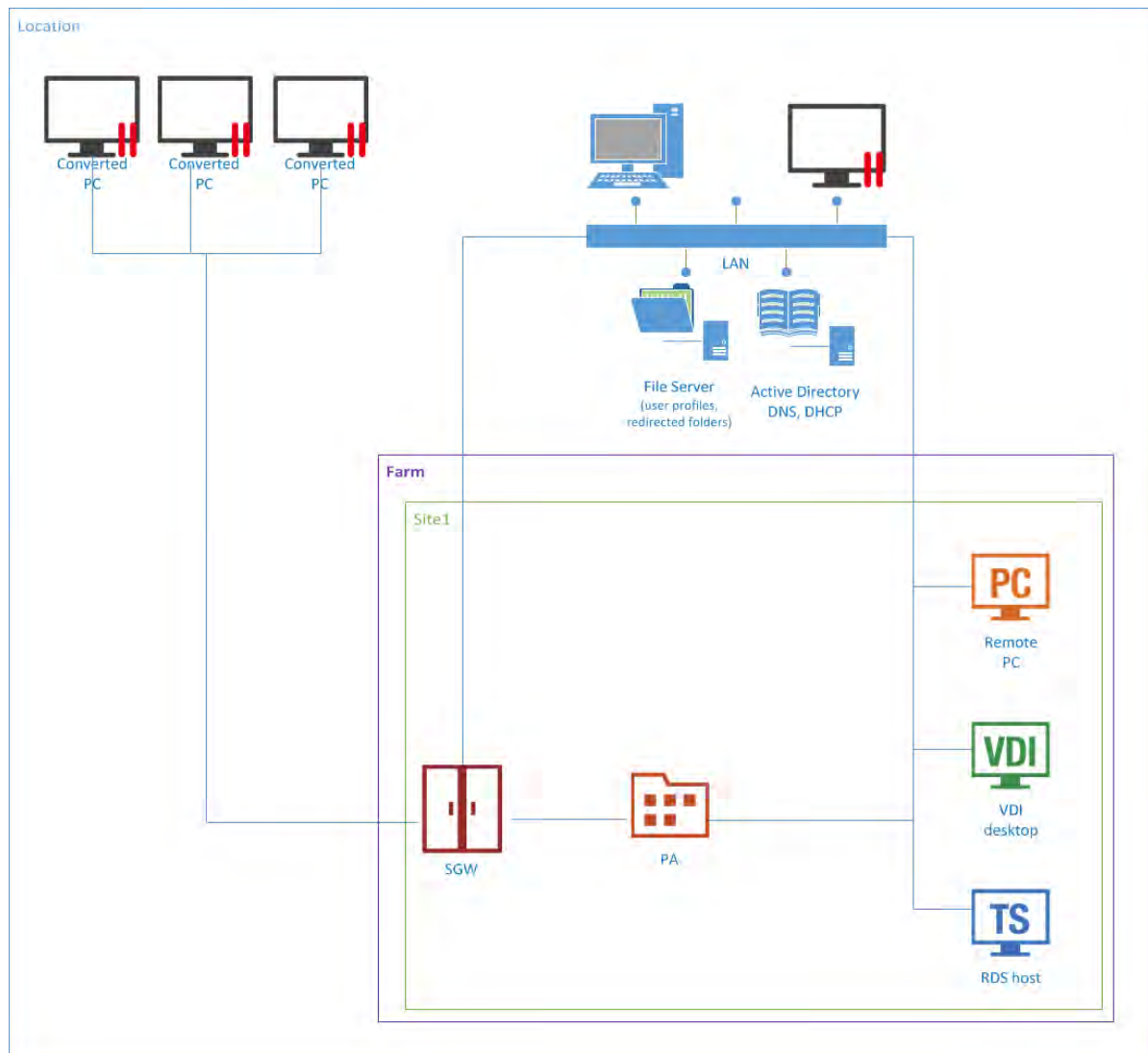
Shadowing

Shadowing provides access to the full Windows client device desktop and allows controlling applications running locally on the system, as well as any remote applications published from Parallels Remote Application Server. Shadowing requires a direct connection between the machine on which the Parallels RAS console is running and the device itself.


Desktop Replacement


The Replace Desktop option limits users from changing system settings or installing new applications. Replacing the Windows Desktop with Parallels Client transforms the Windows operating system into a thin-client-like OS without replacing the operating system itself. This way, users can only deploy applications from the client, thus providing the administrator with a higher level of control over connected devices.


Additionally, Kiosk mode prevents users from shutting down or rebooting their computers.




Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)


	Private Parallels Secure Client Gateway (Direct Mode)	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation


	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

Client Components

	Windows/Linux PC or Mac	
	Component Installed	Installation Method
	Parallels Client	Windows installer (standard installation).

	Converted Windows PC	
	Component Installed	Installation Method
	Parallels Client	Windows installer (standard installation).

CHAPTER 3

Deploying Parallels RAS Reporting Service

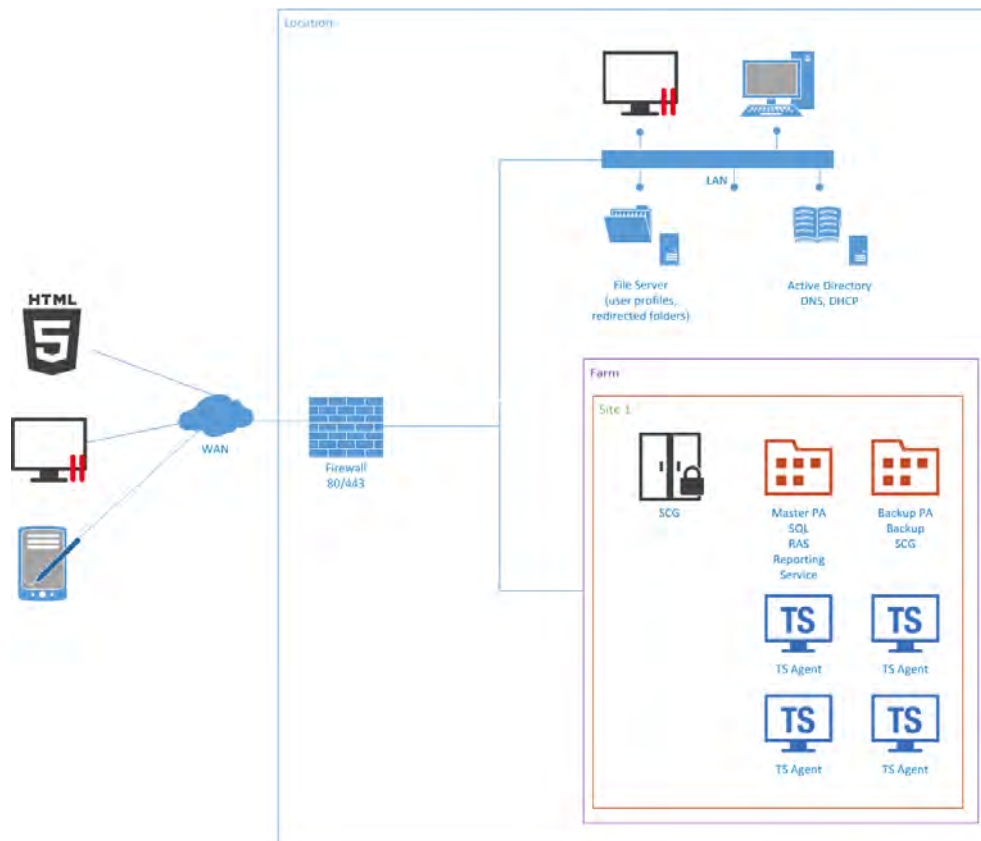
This chapter describes common scenarios for deploying the Parallels Remote Application Server Reporting Service.

In This Chapter

One Site with Multiple Microsoft RDS Servers.....	43
Multiple Sites with Multiple Microsoft RDS Servers	45


One Site with Multiple Microsoft RDS Servers


RAS Reporting Service relies on Microsoft SQL Server and Reporting Services. In small environments, a database instance and RAS Reporting Service can be installed on the same machine where Parallels Remote Application Server is running.




Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

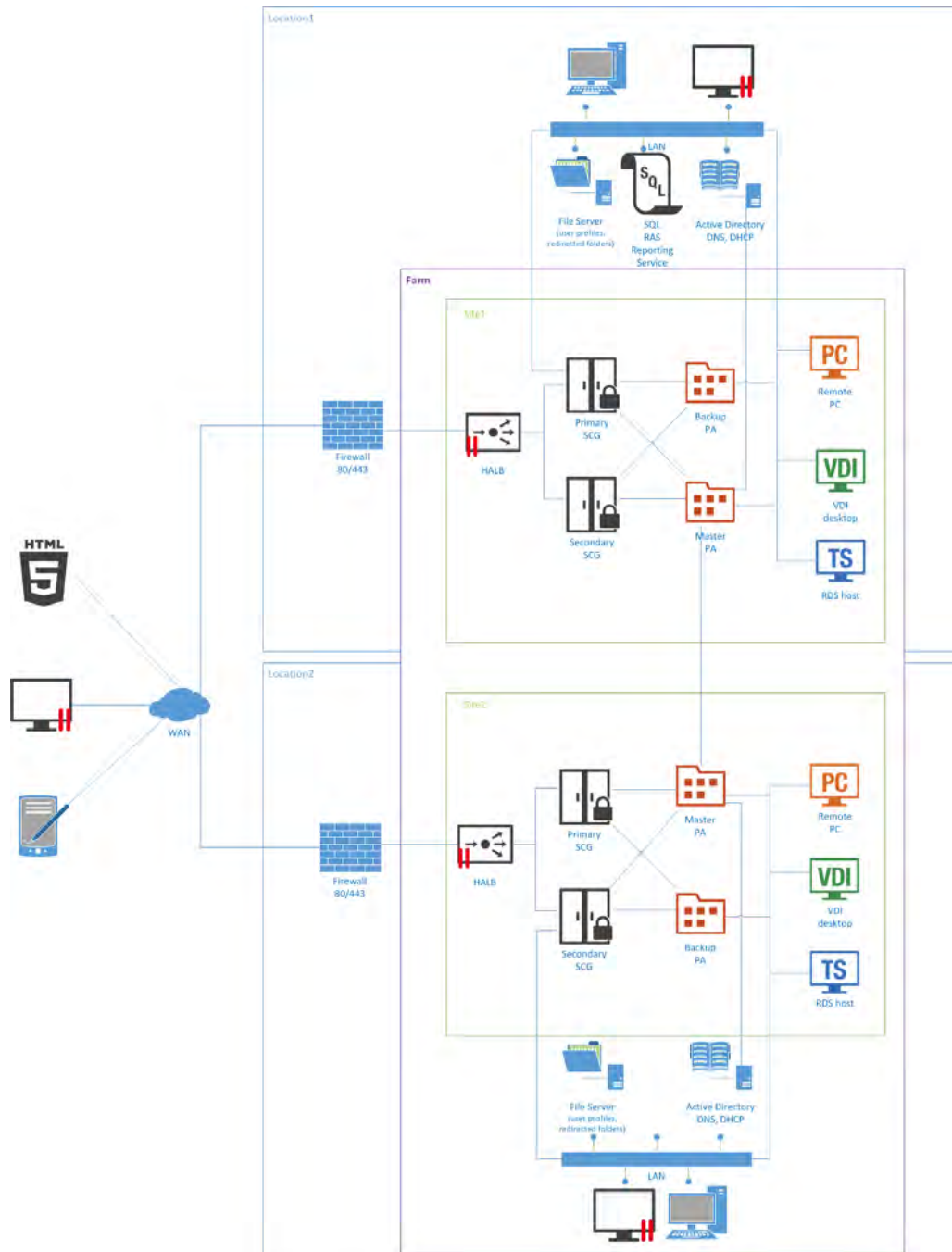
	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation

	Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation


	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation


Multiple Sites with Multiple Microsoft RDS Servers


For installations running in a multiserver farm environment, installing MS SQL Server on a dedicated machine is recommended.





Server Components

	Master Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Windows Installer (standard installation)

	Backup Publishing Agent	
	Component Installed	Installation Method
	Parallels Publishing Agent	Push installation

	Primary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation


	Secondary Parallels Secure Client Gateway	
	Component Installed	Installation Method
	Parallels Secure Client Gateway, including HTML5 Gateway	Push installation

	Microsoft Remote Desktop Services Server	
	Component Installed	Installation Method
	Parallels Terminal Server Agent	Push installation

	Hypervisor Host with VDI Desktops	
	Component Installed	Installation Method
	Parallels VDI Agent	Push installation or virtual appliance
	Parallels Guest Agent	Push installation

	Windows PC	
	Component Installed	Installation Method
	Parallels Remote PC Agent	Push installation

	SQL and RAS Reporting Service	
	Component Installed	Installation Method
	Parallels RAS Reporting Service	Windows Installer (standard installation)

	High Availability and Load Balancing Virtual Appliance	
	Component Installed	Installation Method
	Ready to use virtual appliance	Virtual appliance

CHAPTER 4

Port Reference and SSL Certificates

This chapter provides reference information about port used by Parallels Remote Application Server and describes how SSL certificates are used in Parallels RAS.

In This Chapter

Port Reference	48
SSL Certificates.....	49

Port Reference

The following table lists ports and protocols used in Parallels Remote Application Server deployments.

Component	Ports	Protocols
Firewall (Remote Install Push/Takeover of Software)	135, 445, 49179	TCP
HALB	112	VRRP
HALB	31006	TCP, UDP
Secure Gateway, HALB	80, 443	TCP, UDP
Secure Gateway, HALB, Terminal Server Agent, Guest Agent, Remote PC agent	3389	TCP, UDP
Secure Gateway	20000, 20020	
Publishing Agent	20001, 20002	TCP
Terminal Server Agent, Publishing Agent	20003	UDP
Secure Gateway, HALB, Publishing Agent (RAS Console and Client Manager, including shadowing)	20009	TCP, UDP
Terminal Server Agent, Guest Agent, Remote PC agent	30004	TCP,UDP
Terminal Server Agent, Guest Agent, Remote PC agent	30005	TCP
VDI Agent	30006	TCP, UDP
VDI Agent	30008	TCP
Publishing Agent (RAS Console and Reporting)	30008	TCP
Parallels Client (Client Manager, shadowing)	50005	TCP

SSL Certificates

This section explains how to use SSL certificates in Parallels Application Server deployments. You should read this section if you are setting up a RAS environment to test one or more of the deployment scenarios described earlier in this guide.

By default, a self-signed certificate is installed on a RAS Secure Client Gateway. Each RAS Secure Client Gateway has its own certificate, which should be added to Trusted Root Authorities on the client side to avoid security warnings.

To simplify the Parallels Client configuration, using a certificate issued either by a third party Trusted Certificate Authority or Enterprise Certificate Authority (CA) is recommended.

If an Enterprise CA certificate is used, Windows clients receive a Root or Intermediate Enterprise CA certificate from Active Directory. Client devices on other platforms require manual configuration.

If a third-party certificate issued by a well-known Trusted Certificate Authority (e.g. Verisign) is used, the client device trusts using Trusted Certificate Authority updates for the platform.

Using Third-Party Trusted Certificate Authority

- 1 In the RAS Console, navigate to **Farm > Gateway > Properties** and click the **SSL/TLS** tab.
- 2 Select your SSL settings options – TLS 1.1 and TLS 1.2 are recommended.
- 3 Choose CSR.
- 4 Fill in the data.
- 5 Copy and paste the CSR into a text editor and save the file for your records.
- 6 Paste the CSR into the party Vendors Website page or email it to the vendor.
- 7 Request a return certificate in the following format: Apache, with the private, public and intermediate CA all in one file, with extension `.pem`.
- 8 When you receive the file, place it in a secure folder for backup retrieval.
- 9 Click **Import Public Key** and navigate to the folder (or navigate to a secondary location where you have a copy of the single all-in-one cert) and insert the `.pem` file into the **Certificate key** field.
- 10 Click **Apply** and **Test**.

Note: The private key should already be populated from your initial CRS request.

Using Enterprise Certificate Authority

Use IIS to receive a certificate from Enterprise CA. The certificate should be exported in the `pfx` format and then converted into the PEM format using the OpenSSL tool, available at <http://gnuwin32.sourceforge.net/packages/openssl.htm>

Note: The `trusted.pem` file on the Parallels Client side must include the intermediate certificate to be able to verify the cert from the third party vendor. If the intermediate certificate for the vendor is not in the `trusted.pem` file, you will have to paste it in manually, or create a `trusted.pem` template file with the proper Intermediate Certificates and then replace the old `trusted.pem` file with the newly updated one. This file resides in `Program Files\Parallels` or `Program Files(x86)\Parallels` on the client side.

To convert a PFX file to a PEM file, follow these steps on a Windows machine:

- 1 Run the OpenSSL tool.
- 2 Create the `c:\certs` folder and copy the `cert.pfx` file into it.
- 3 Open a command prompt and change the director to `GnuWin32\bin` by entering `cd %ProgramFiles%\GnuWin32\bin`
- 4 Type the following command to convert the PFX file to an unencrypted PEM file:

```
openssl pkcs -in c:\certs\cert.pfx -out c:\certs\cert.pem -nodes
```
- 5 When prompted for the import password, enter the password you used when exporting the certificate to a PFX file. You should receive a message that says MAC verified OK.

Enable SSL on Parallels Secure Client Gateway with cert.pem

- 1 On the Parallels Client Gateway page, enable secure sockets layer (SSL) and click [...] to browse for the pem file.
- 2 Place the single file generated in the **Private Key** and **Public Key** fields.
- 3 Click **Apply** to apply the new settings.
- 4 Your browser may not support displaying this image.

Parallels Clients Configuration

In case the certificate is self-signed, or the certificate issued by Enterprise CA, Parallels Clients should be configured as described below.

- 1 Export the certificate in Base-64 encoded X.509 (.CER) format.
- 2 Open the exported certificate with a text editor, such as notepad or WordPad, and copy the contents to the clipboard.

To add the certificate with the list of trusted authorities on the client side and enable Parallels Client to connect over SSL with a certificate issued from an organization's Certificate Authority.

- 1** On the client side in the directory "C:\Program Files\Parallels\Remote Application Server Client\" there should be a file called `trusted.pem`. This file contains certificates of common trusted authorities.
- 2** Paste the content of the exported certificate (attached to the list of the other certificates).

Index

A

About This Guide - 4
Advantages of Parallels Remote Application
Server Based Computing - 5

B

Business Continuity and Disaster Recovery -
37

C

Client Connection Modes - 10
Client Manager and Desktop Replacement -
40

D

Deploying Parallels RAS Reporting Service -
43
Deployment Scenarios - 12
Dual Firewall DMZ - 29

G

General Considerations - 12

H

High Availability with Multiple Gateways - 24
High Availability with Single or Dual F/W DMZ
- 26
How Does It Work - 7
How to Read Diagrams and Tables - 12

I

Introduction - 4

M

Mixed Scenarios - 33
Multiple Sites with Multiple Microsoft RDS
Servers - 46
Multisite Scenario - 33

O

One Site with Multiple Microsoft RDS Servers
- 44

P

Parallels Client Connection Flow - 9
Parallels RAS Deployment Scenarios - 16
Parallels Remote Application Server
Components - 6
Port Reference - 50
Port Reference and SSL Certificates - 50

S

Secure Setup with Dual Firewall DMZ and
Second-Level Authentication - 39
Single Farm with Dual Parallels Secure Client
Gateways - 21
Single Farm with Mixed Desktops - 18
Single Farm with One Microsoft Remote
Desktop Services Server - 16
Single Farm with Public & Private Parallels
Secure Client Gateways - 19
Single Farm with Two Microsoft Remote
Desktop Services Servers - 17
Single Firewall DMZ - 27
SSL Certificates - 51

W

What is Parallels Remote Application Server -
4