



Parallels Remote Application Server

Solutions Guide

v16.5

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 672 20 30
www.parallels.com

Copyright © 1999-2019 Parallels International GmbH. 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/about/legal/>.

Microsoft, Windows, Windows Server, Windows Vista are registered trademarks of Microsoft Corporation.
Apple, Mac, the Mac logo, OS X, macOS, iPad, iPhone, iPod touch 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

What is Parallels RAS.....	5
Advantages of Parallels RAS Solution.....	5
Parallels RAS Components	6
Understanding Deployment Scenario Diagrams	8
Parallels RAS Basic Concepts	11
Parallels Client Connection Flow.....	14
Client Connection Modes	15
Deployment Scenarios	17
General Considerations	17
Parallels RAS Deployment Scenarios.....	17
Single Farm with One RD Session Host.....	17
Single Farm with Two RD Session Hosts.....	19
Single Farm with RD Session Host Auto Scaling.....	20
Single Farm with VDI Desktops.....	21
Single Farm with Remote PC Desktops.....	22
Single Farm with Mixed Desktops.....	24
Single Farm with Public & Private RAS Secure Client Gateways	25
Single Farm with Dual RAS Secure Client Gateways.....	26
High Availability with Multiple Gateways.....	27
High Availability with Single or Dual F/W DMZ.....	28
Mixed Scenarios.....	32
Capacity Considerations	39
Deploying Parallels RAS Reporting Service	42
One Site with Multiple RD Session Hosts	43
Multiple Sites with Multiple RD Session Hosts	44
Port Reference and SSL Certificates	47
Port Reference.....	47
Parallels Client	47
Web Browsers.....	48
RAS Secure Client Gateway	48

Contents

RAS Publishing Agent	49
RAS Console.....	50
RAS Agents: RD Session Host, VDI, Guest, Remote PC	51
HALB	51
Common Communication Ports	52
Active Directory and Domain Services Ports.....	52
SSL Certificates	52
Index	55

CHAPTER 1

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 how these components operate. The main topics of this guide describe various Parallels RAS deployment scenarios, complete with diagrams and other information. The guide concludes with the information about communication ports used by Parallels RAS and the information about using SSL certificates.

In This Chapter

What is Parallels RAS	5
Advantages of Parallels RAS Solution	5
Parallels RAS Components.....	6
Understanding Deployment Scenario Diagrams	8
Parallels RAS Basic Concepts	11

What is Parallels RAS

Parallels RAS 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, macOS, iOS, 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 RAS Solution

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, macOS, iOS, 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 RAS 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 RAS Publishing Agent, RAS Secure Client Gateway, and agents installed on RD Session Hosts, 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 RAS features.

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

RAS RD Session Host Agent is installed on an RD Session Host and enables publishing of server resources (applications and desktop). RAS RD Session Host 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 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 installed in the guest operating system of a virtual machine. RAS Guest Agent enables resource publishing from VDI desktops, VDI RD Session Hosts and collects information required by RAS Publishing Agent.

RAS VDI Agent collects information from the Parallels RAS Infrastructure and is responsible for controlling VDI through its native API. It also acts as a gateway between a RAS Secure Client Gateway (or the client in direct mode) and an RDP server from the guest VM or VDI depending on a VDI implementation. RAS VDI Agent is a part of RAS Publishing Agent, so it is installed when you install the RAS Publishing Agent. This built-in RAS VDI Agent can be used to control multiple VDI hosts in a Parallels RAS farm. This applies to all hypervisors supported by Parallels RAS except **QEMU KVM with libvirt** and **Nutanix Acropolis**. With these two hypervisors, a dedicated RAS Publishing Agent must be installed on a VDI host directly. If needed, a dedicated RAS VDI Agent can also be installed on any VDI host, in which case the agent can be used to manage that host only. See **RAS VDI Agent dedicated** below.

RAS VDI Agent dedicated appears as an installation option in the Parallels RAS installer. It serves the same purpose as the built-in RAS VDI Agent described above. The difference is, you can only use a dedicated agent to control the VDI host on which it is installed.

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

High Availability Load Balancing (HALB) is an appliance that provides load balancing for RAS Secure Client Gateways. Parallels HALB virtual appliance is available for the following hypervisors: Hyper-V, VMware, XenServer. HALB deployment is per site, which means that a site must have at least one Parallels HALB appliance deployed. Multiple HALB deployments can run simultaneously, one acting as the master and others as slaves. The more HALB deployments a site has, the lower the probability that end users will experience downtime. Master and slave HALB deployments share a common or virtual IP address (VIP). Should the master HALB deployment fail, a slave is promoted to master and takes its place.

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.

Understanding Deployment Scenario Diagrams



Terms and Abbreviations














Deployment scenario diagrams include terms and abbreviations, which are explained in the following table.

PA	RAS Publishing Agent.
SCG	RAS Secure Client Gateway (including HTML5 gateway).
Private SGW	Private RAS Secure Client Gateway (used for direct client connections).
RDSH, RDS host RDSH Agent	RD Session Host (formerly Terminal Server). RAS RD Session Host Agent installed on an RD Session Host.
Remote PC	A remote Windows computer with RAS Remote PC Agent installed.
VDI	Virtual Desktop Infrastructure (a VDI host with a hypervisor running virtual machines). Each virtual machine must have RAS Guest Agent installed.
HALB	High Availability Load Balancing. An appliance that provides load balancing for RAS Secure Client Gateways.
Converted PC	A PC with Windows converted to a thin-client-like OS.

Icons

The following table describes the icons used in deployment scenario diagrams.

Parallels RAS Server Components	
	A server hosting RAS Publishing Agent. May also host other Parallels RAS components depending on a deployment.
	RAS Secure Client Gateway (including HTML5 gateway) used for secure (SSL) client connections.

	Private RAS Secure Client Gateway, used for direct client connections.
	RD Session Host with RAS RD Session Host Agent installed.
	A remote Windows computer with RAS Remote PC Agent installed. Not to be confused with Converted PC described below (a similar icon in red color).
	Virtual Desktop Infrastructure (a VDI host with a hypervisor running virtual machines). Each virtual machine must have RAS Guest Agent installed.
	High Availability Load Balancing. An appliance that provides load balancing for RAS Secure Client Gateways.
Parallels RAS Client Devices	
	A desktop computer (Windows, Linux, Mac) with Parallels Client installed.
	A PC with Windows converted to a thin-client-like OS. Not to be confused with a remote PC described above (a similar icon in orange color).
	A converted PC (same as above) with Kiosk mode enabled.
	HTML5 enabled web browser.
	Mobile device (iOS, Android).
Other Components	
	Active Directory, DNS, and DHCP server(s).
	RAS Reporting Server (uses Microsoft SQL Server).
	RADIUS server (used for second-level authentication).



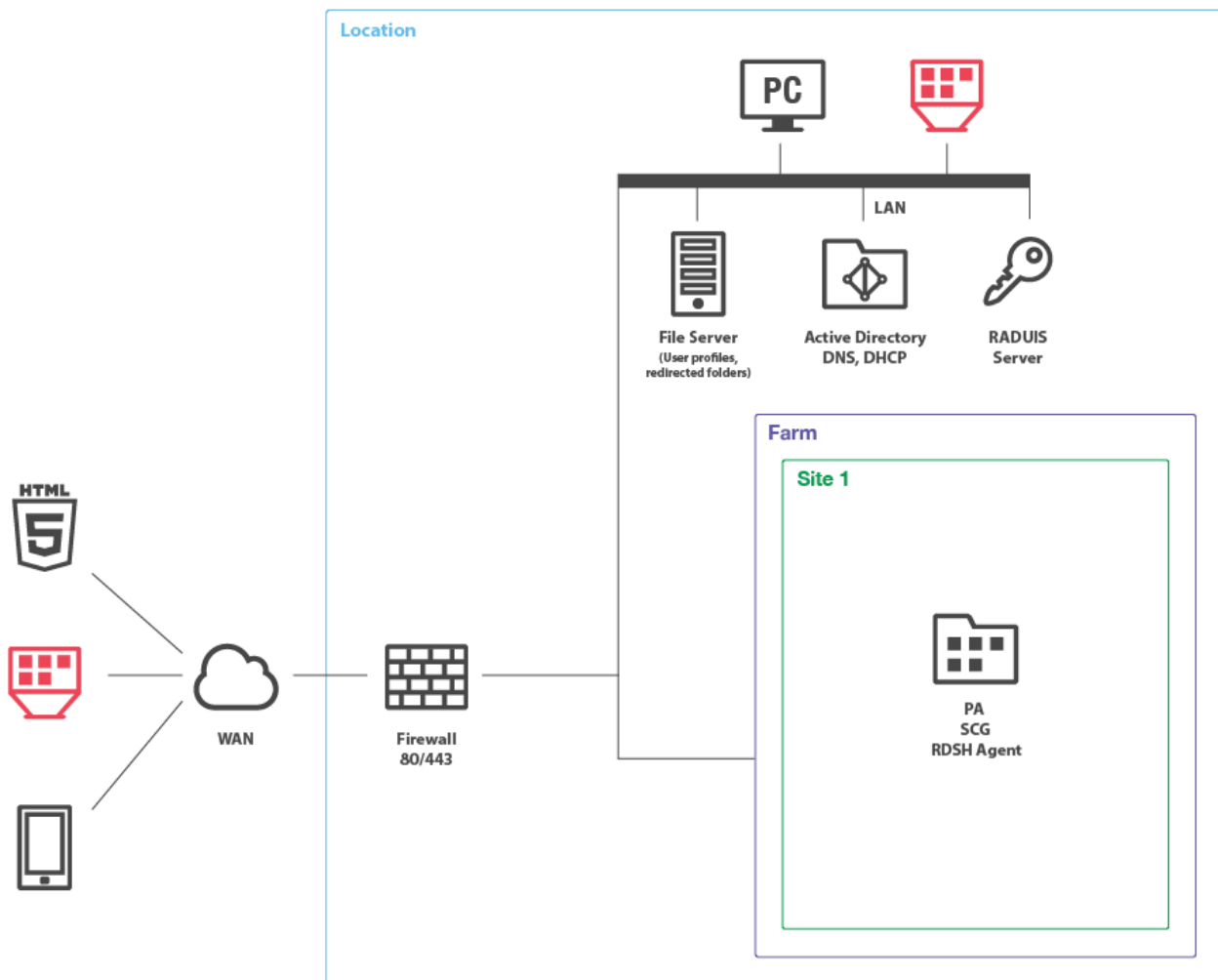
	File server for storing user profiles and redirected folders.
	Firewall (ports 80 and 443 are open).

Diagram Layout

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



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

- HTML5 enabled web browser
- A converted Windows PC running in Kiosk mode
- A mobile device (iOS, Android)

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 1** rectangle represents a site with individual servers and components. In the example above, the site has a single server with RAS Publishing Agent (PA), RAS Secure Client Gateway (SCG), and RAS RD Session Host Agent installed.

The **LAN** bar represents a local area network with the following computers and servers connected to it:

- Desktop computer
- Converted Windows PC running in Kiosk mode.
- File server
- Active Directory, DNS, and DHCP server(s)
- RADIUS server

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

The **Installation Notes** section describes how a component (or components) must be installed on a corresponding server. The following installation methods are used to install Parallels RAS server components:

- **Parallels RAS Installer (standard installation).** This is a standard MSI installer package that you run in Windows to install an application.
- **Windows Installer (custom installation).** This is the same type of installer as described above, but you must choose the **Custom** installation type, which allows you to select which component(s) you want to install.
- **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 on it.
- **Virtual appliance.** A preconfigured 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 Basic Concepts

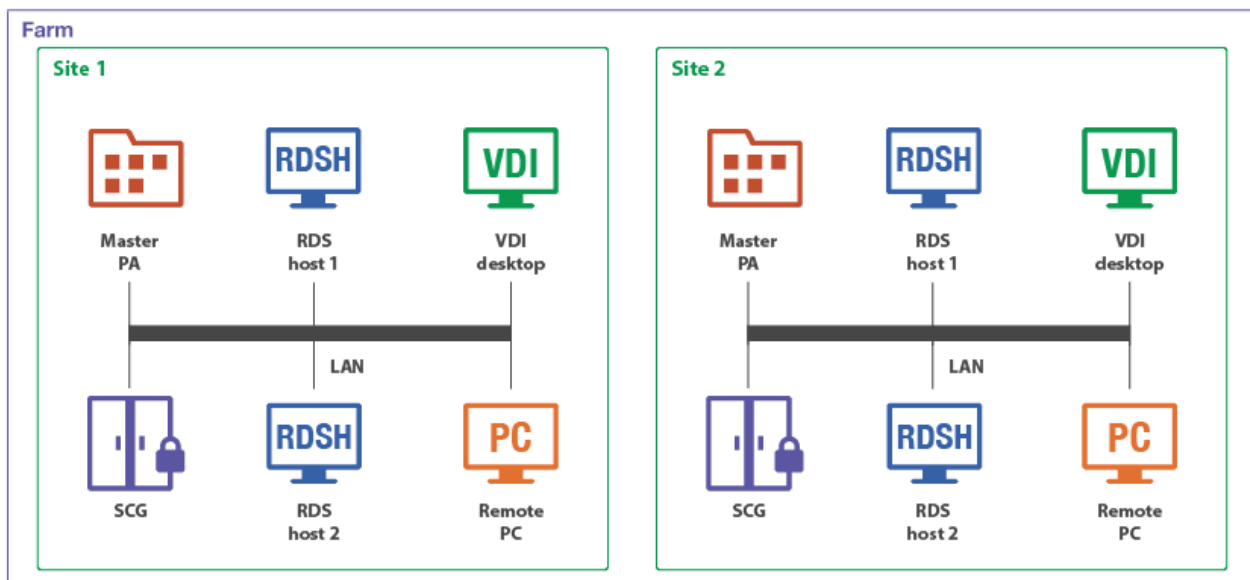
When a user connects to Parallels RAS from Parallels Client, they are presented with published resources (applications, desktops, documents, or published URLs). The user selects a resource and launches it. The system load-balances user requests automatically and launches the requested resource from a 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 RAS building blocks are (see the previous section for a detailed explanation):

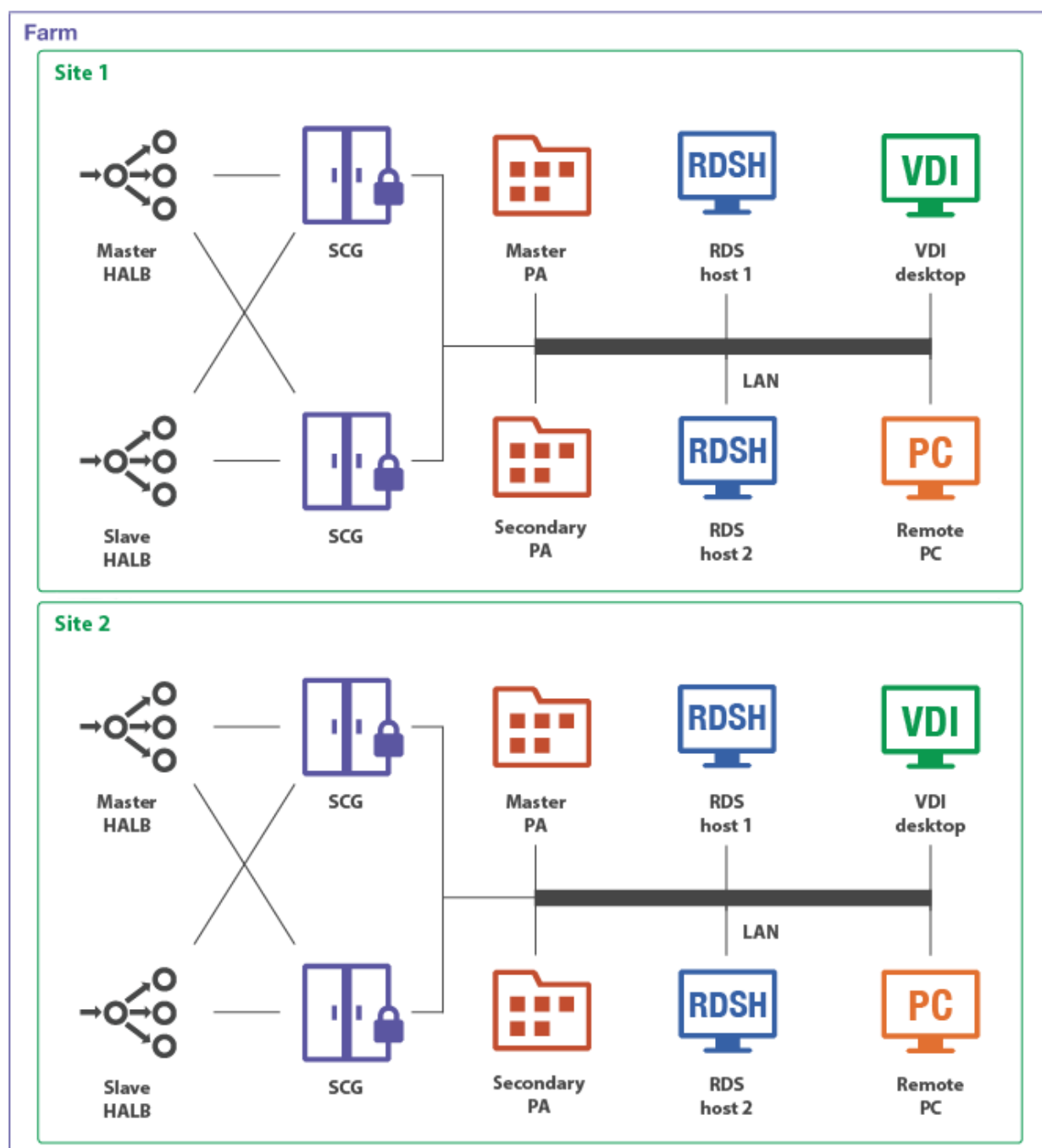
- Farm
- Site
- Agents

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), RD Session Host (RDS host 1), a second RD Session Host (RDS host 2), VDI (Virtual Desktop 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 (RD Session Host, 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 RD Session Host 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 RD Session Host directly or via RAS Secure Client Gateway and passes the user credentials to it.
- 5 The RD Session Host verifies the received credentials and, if they are valid, starts an RDP session.

Client Connection Modes

Parallels Client can connect to Parallels RAS 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 resources on an RD Session Host or a guest VM.

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 with an RD Session Host or a guest VM through port 3389.
- 3** Finally, Parallels 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 resources on an RD Session Host or a guest VM.

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 with an RD Session Host or a guest VM 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 an RD Session Host or a guest VM, 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 an RD Session Host or a guest VM 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 an RD Session Host or a guest VM 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 RAS 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 RAS deployment scenarios.

In This Chapter

General Considerations	17
Parallels RAS Deployment Scenarios	17

General Considerations

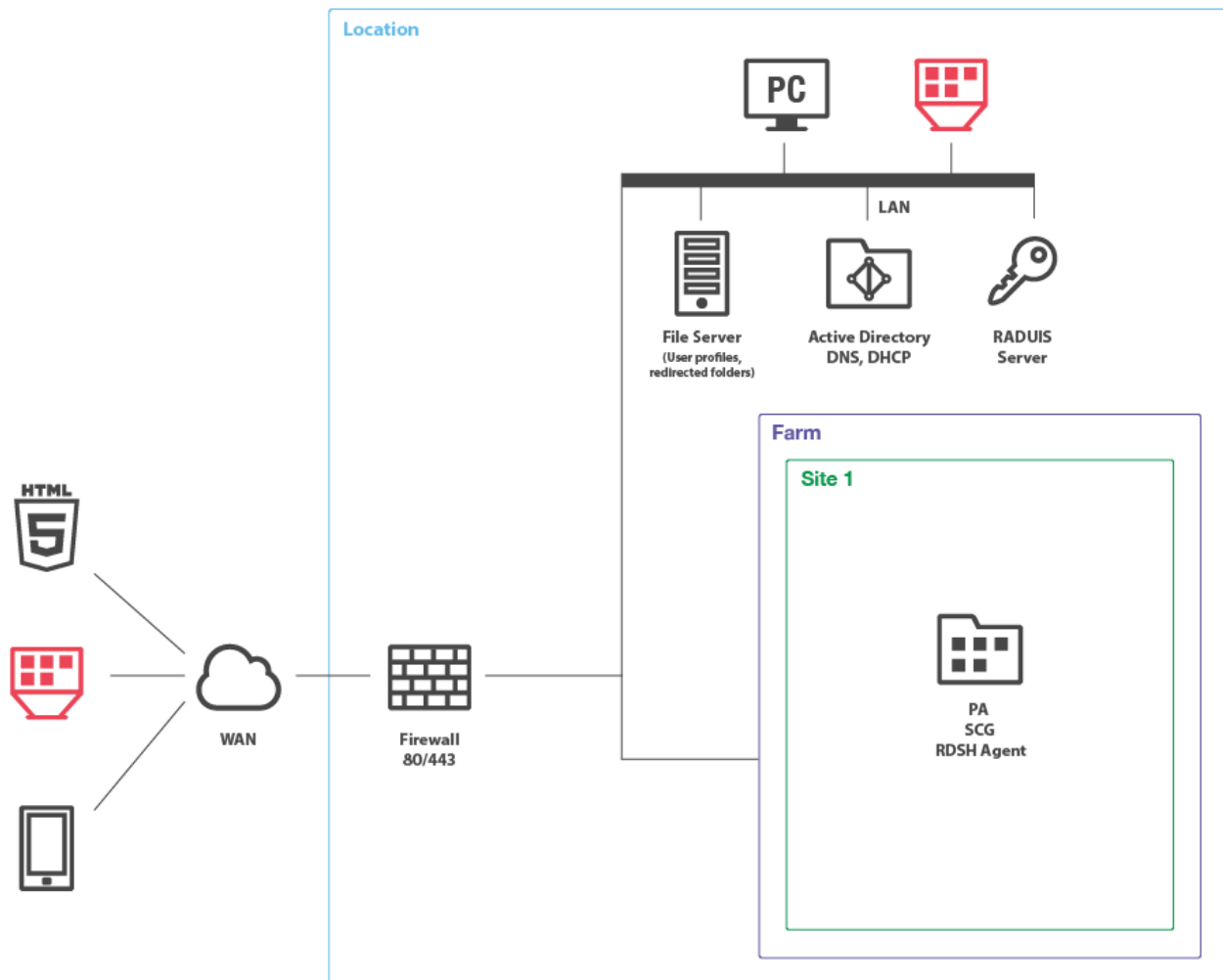
Regardless of the size of a Parallels RAS installation, redundancy among core components of your setup is recommended to ensure the greatest possible uptime. For small deployments, all roles can be installed on a single server, whereas role segregation is recommended for large setups.

The physical location of a Parallels RAS farm, including RD Session Hosts 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 RD Session Host 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 an RD Session Host and publish it for your users. The database will continue to run on a dedicated server. To guarantee fast and reliable database access, the RD Session Hosts server and the database server must be close to each other on the local network.

Parallels RAS Deployment Scenarios

Single Farm with One RD Session Host

This scenario uses a single RD Session Host 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, please see the **SSL Certificates** section (p. 52)).

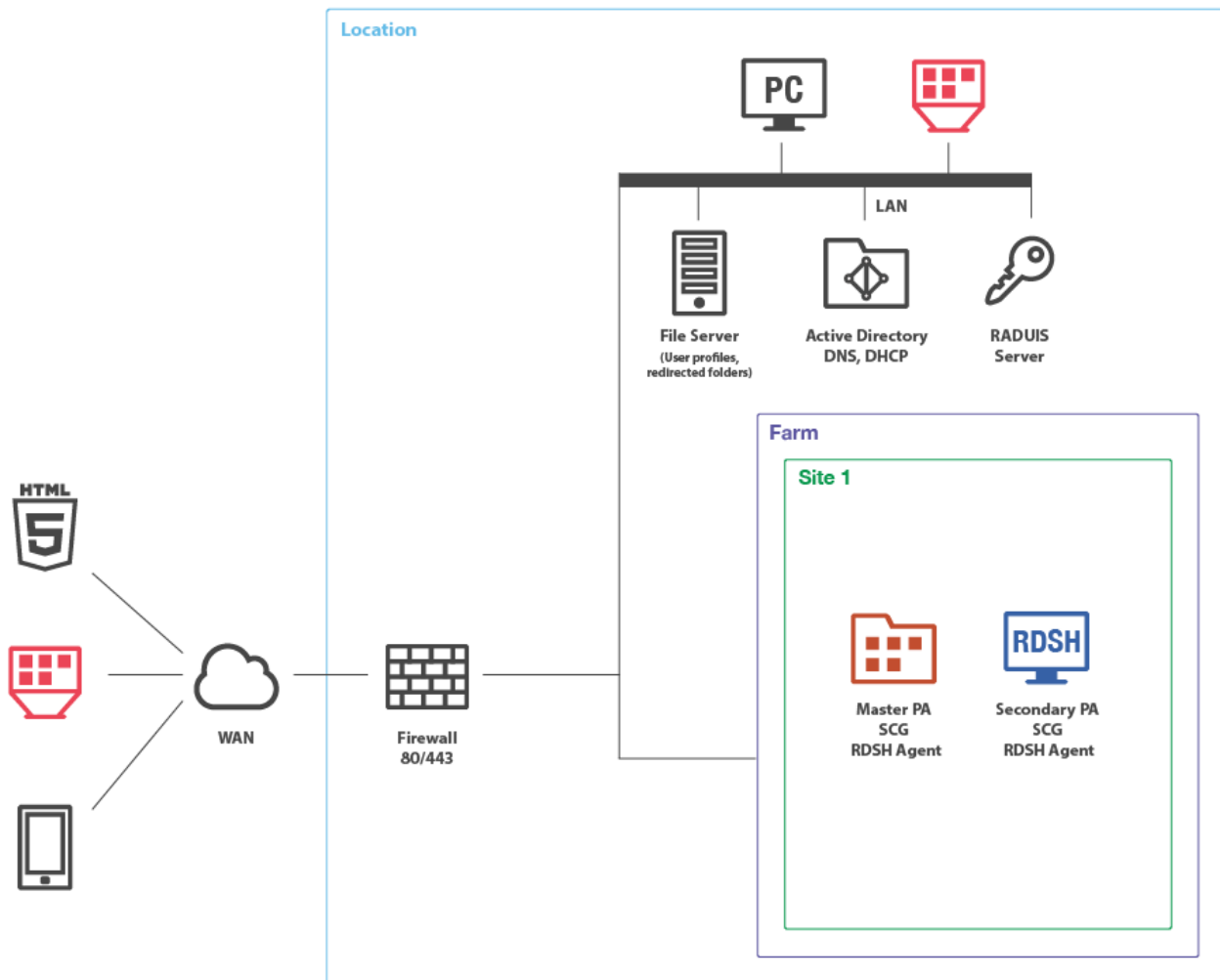


Installation Notes

All server Parallels RAS components are installed using the Parallels RAS installer (standard installation).

Single Farm with Two RD Session Hosts

This scenario can be implemented by an organization that needs to load-balance published applications and desktops between two RD Session Hosts. For high availability, a secondary RAS Publishing Agent and RAS Secure Client Gateway should be installed on the second server.



Installation Notes

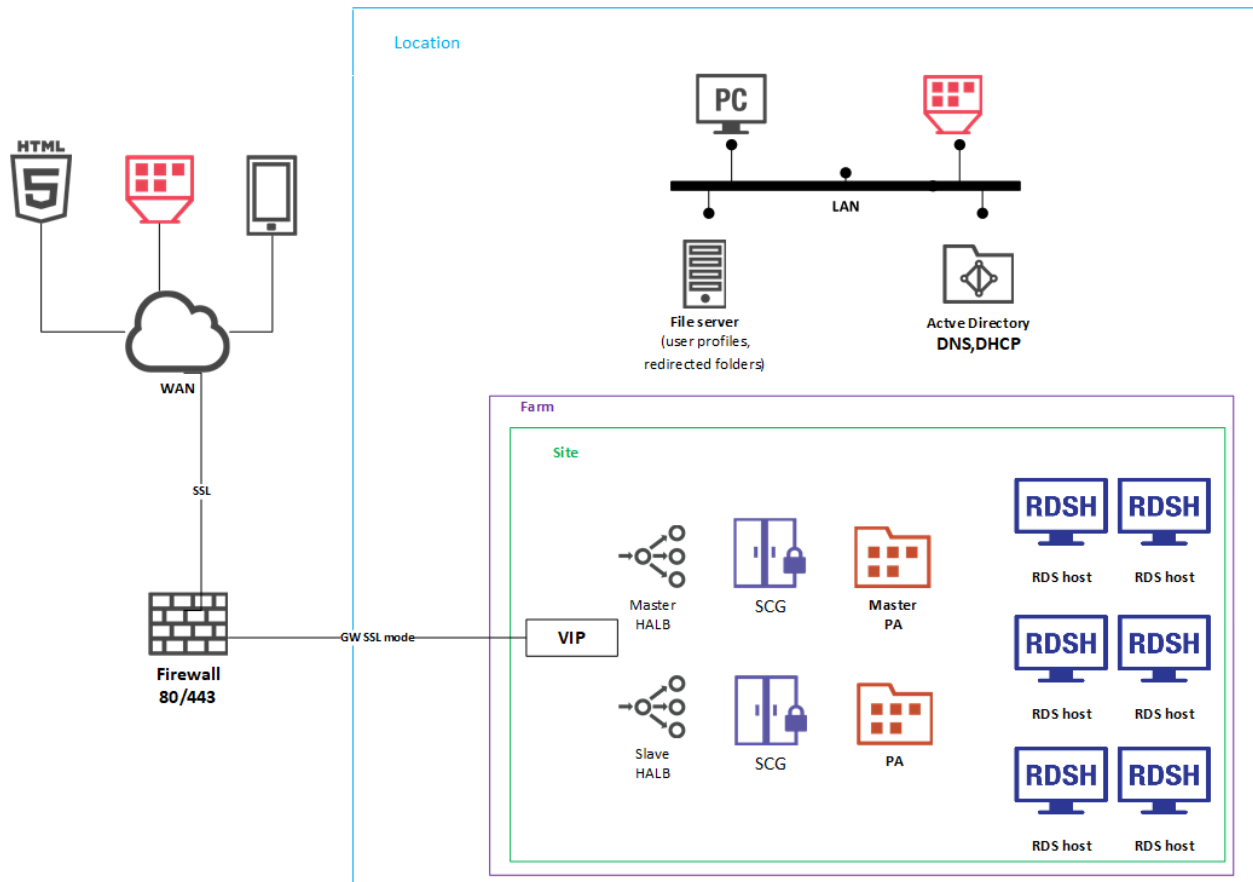
The components on the primary RD Session Host (where the master RAS Publishing Agent is installed) are installed using the Parallels RAS installer (standard installation).

The components on the secondary RD Session Host are push-installed from the RAS console.

Single Farm with RD Session Host Auto Scaling

This scenario can be implemented by an organization that needs to use single image management for RD Session Hosts and dynamic resource allocation for published applications and desktops.

For high availability, a secondary HALB appliance, RAS Publishing Agent, and RAS Secure Client Gateway should be deployed.



Installation Notes

The components on the master RAS Publishing Agent are installed using the Parallels RAS installer (standard installation).

A new type of RAS Template adds support for an RD Session Host running in a guest VM where both the RAS Guest Agent and RD Session Host Agent are push-installed in the VM from the RAS Console.

An RD Session Host Group is assigned a RAS Template and is then used for publishing of applications and desktops.

RD Session Host creation, maintenance and deletion is done via the RAS Template.

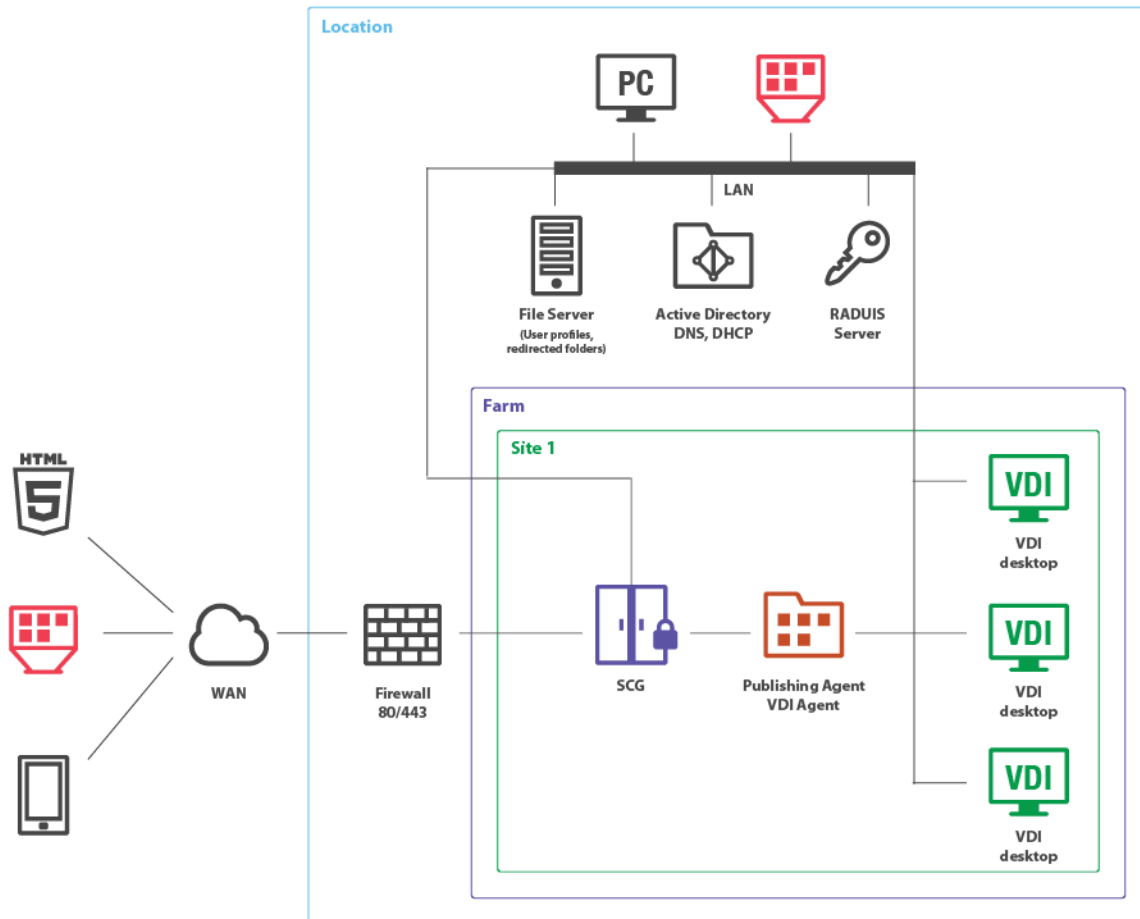
An RD Session Host Group assigns RD Session Hosts on demand providing more resources on the workload increase and unassigns RD Session Hosts on the workload decrease.

Single Farm with VDI Desktops

VDI pools are targeted for application and desktop publishing from virtual desktops (full or linked clones) which are located in a single data center.

VDI desktops have the following advantages:

- Rapid deployment of a common supported desktop environment across the company's network using a single Windows 7, 8, or 10 desktop image for creating virtual machines (VMs) on a hypervisor.
- Centralized deployment of updates and changes to Windows VDI desktops — all you need to do is update a single image.
- In case of failure, the VDI desktops can be easily restored using a single image backup.



Installation Notes

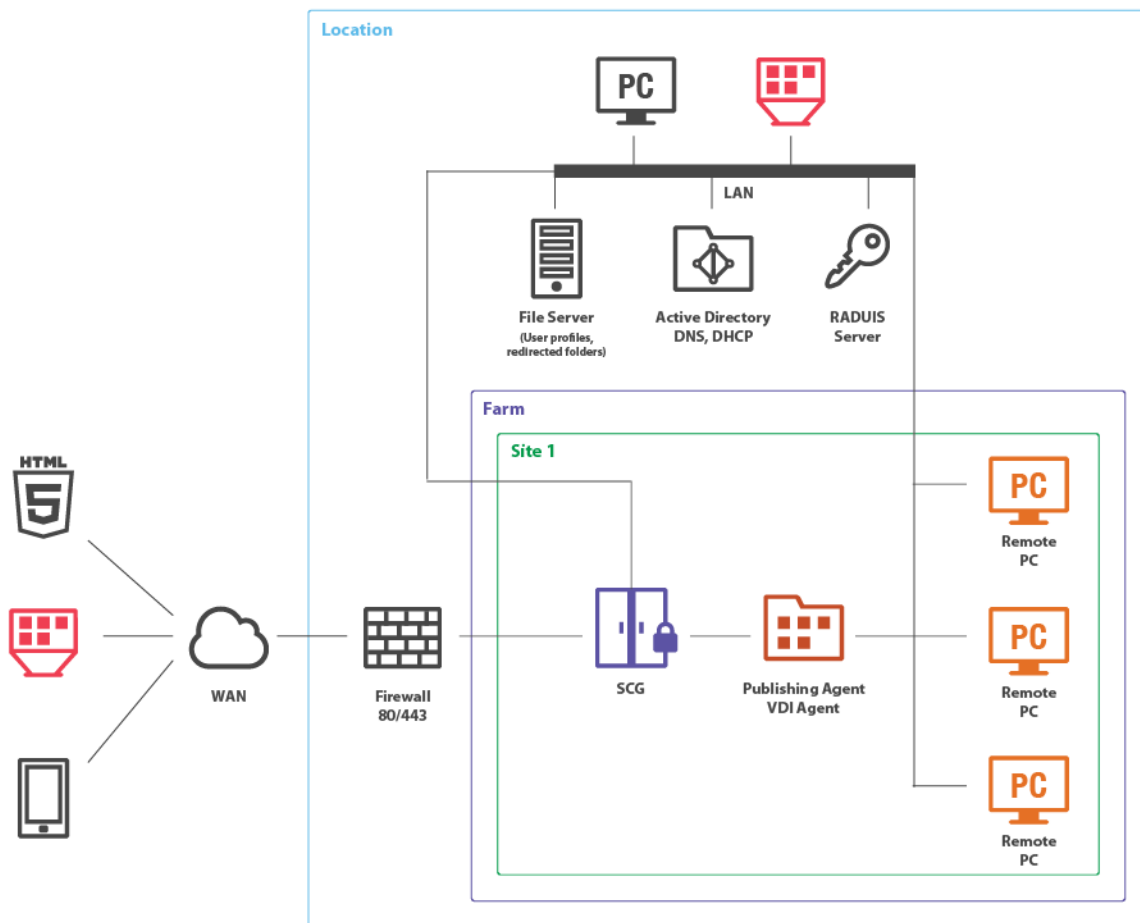
RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

RAS Secure Client Gateway, RAS Guest Agent are push-installed from the RAS console.

Single Farm with Remote PC Desktops

A Remote PC is a physical desktop running Windows that can be used for remote application and desktop publishing. In addition to individual Remote PCs, where every PC is published for a single user and must be specified for publishing, we've added Remote PC pools to Parallels RAS.

Remote PC pools are targeted for application and desktop publishing from Remote PCs which are located in a single data center. Remote PC pools provide the most effective hardware utilization for companies that use shift work (e.g. companies that provide 24/7 service) or when users are located in different time zones. A user is assigned a Remote PC on the first use. After a shift ends, the PC is either released back to the pool to be re-used by a user from the next shift or, depending on the admin settings, the persistence is kept (3 days by default).



Installation Notes

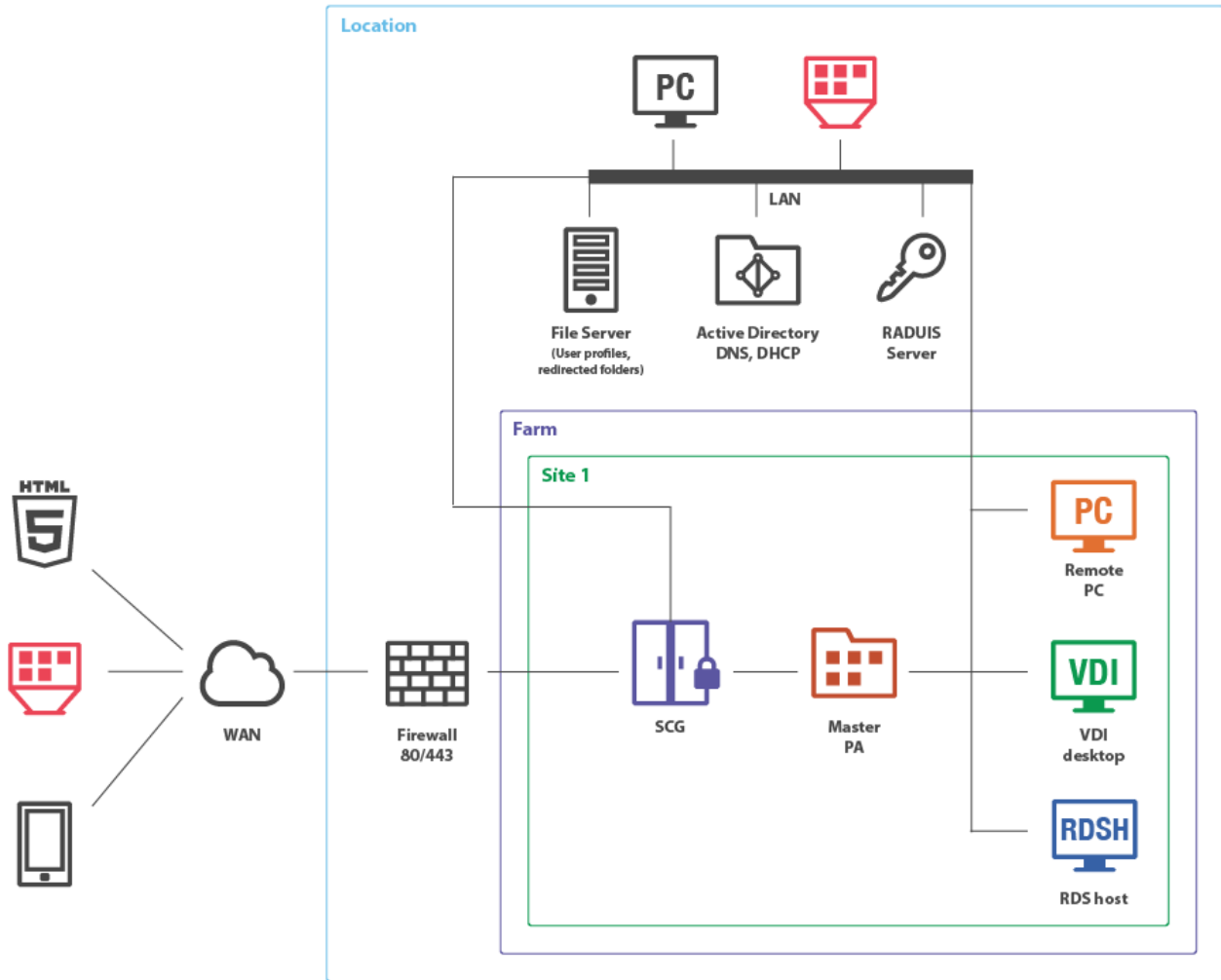
The RAS Guest Agent is used with Remote PC pools instead of the Remote PC Agent. Pool membership is built from either a PC list (manually adding individual PCs or importing the list from a CSV file) or based on an Active Directory OU location (the list is refreshed by the RAS Publishing Agent every 5 minutes).

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

RAS Secure Client Gateway, RAS Guest Agent are push-installed from the RAS console.

Single Farm with Mixed Desktops

By using this scenario you can publish applications and desktops from virtual machines, RD Session Hosts, and Windows desktop computers located in your office.



Installation Notes

RAS Secure Client Gateway and master RAS Publishing Agent are installed using the Parallels RAS installer (standard installation).

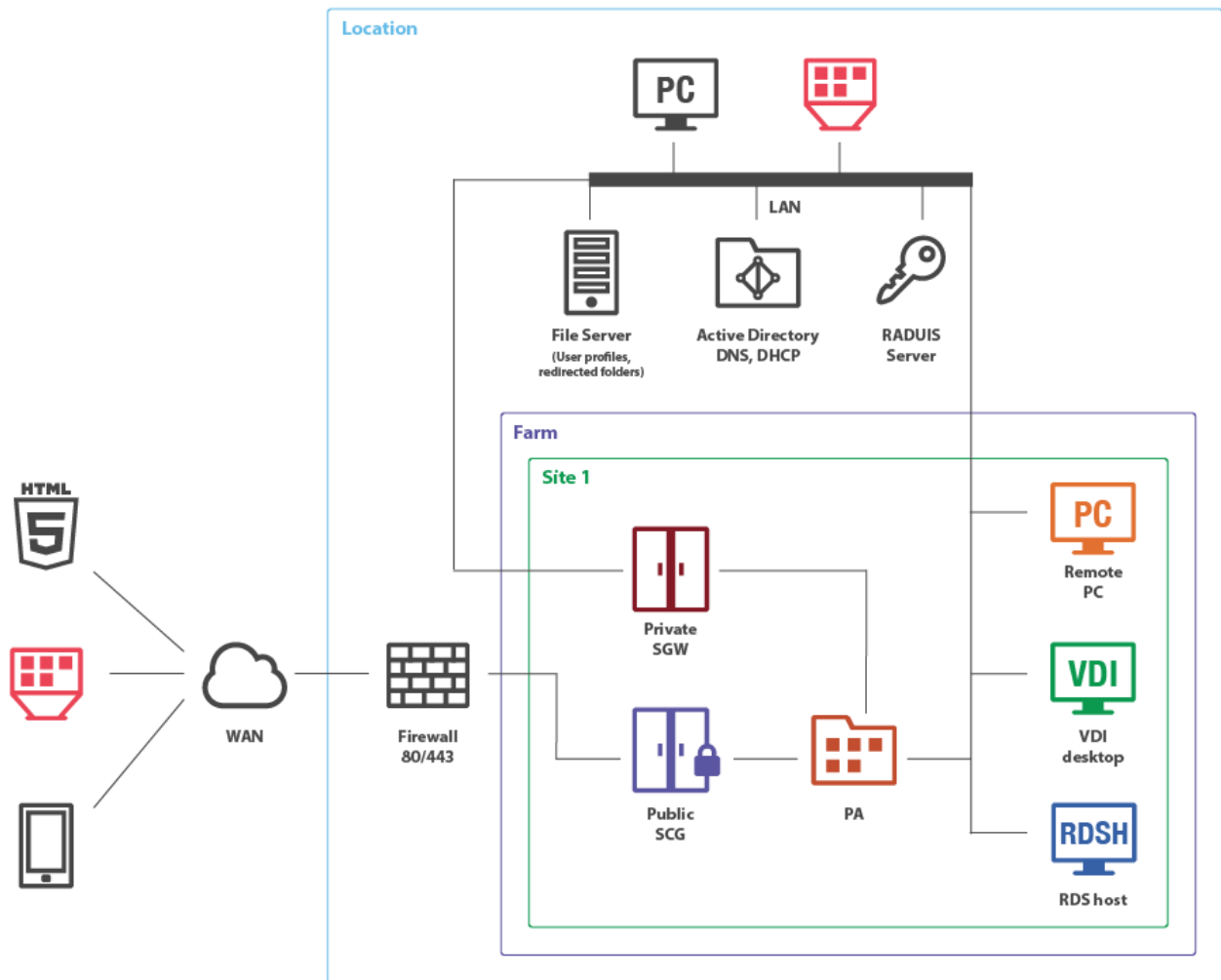
All other components are push-installed from the RAS console.

Single Farm with Public & Private RAS Secure Client Gateways

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

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 RAS Console or manually in the Parallels Client.



Installation Notes

Public RAS Secure Client Gateway and master RAS Publishing Agent are installed using the Parallels RAS installer (standard installation).

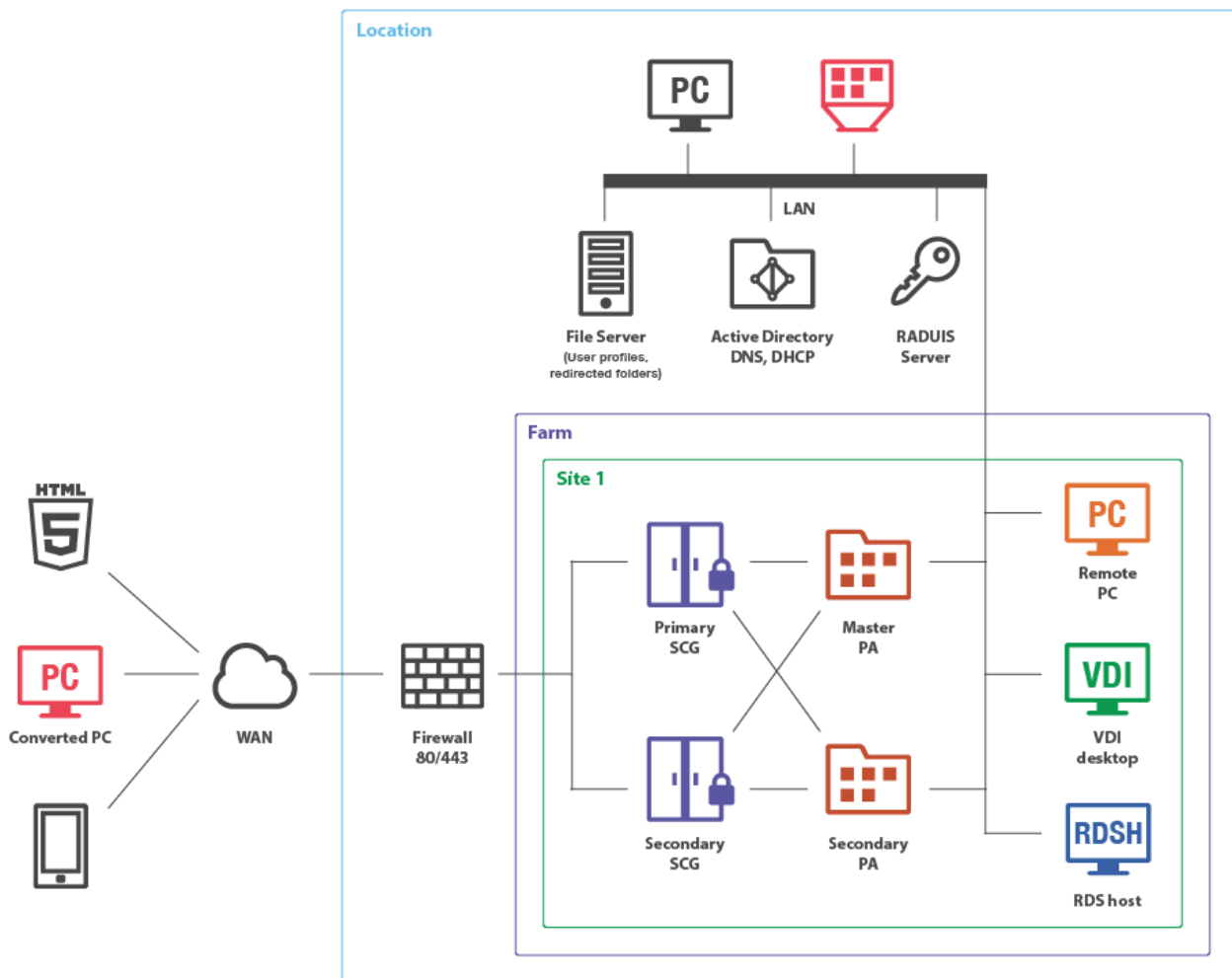
All other components are push-installed from the RAS console.

Single Farm with Dual RAS Secure Client Gateways

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

To enable high availability for client connections using RAS connection settings, the Parallels Client should be configured to connect to primary and secondary Secure Client Gateways using the primary and secondary connection settings in the RAS connection properties. In this case, primary and secondary RAS Secure Client Gateways must be configured to connect to the same RAS Publishing Agents (using the Advanced Client Gateway Settings). When the Primary RAS Secure Client Gateway is not available, Parallels Clients can connect to the farm using the Secondary RAS 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 round-robin DNS, two new host records must be created in the DNS forward lookup zone with the same name (e.g. myhost.example.com) but with two different IP addresses of primary and secondary RAS Secure Client Gateways.



Installation Notes

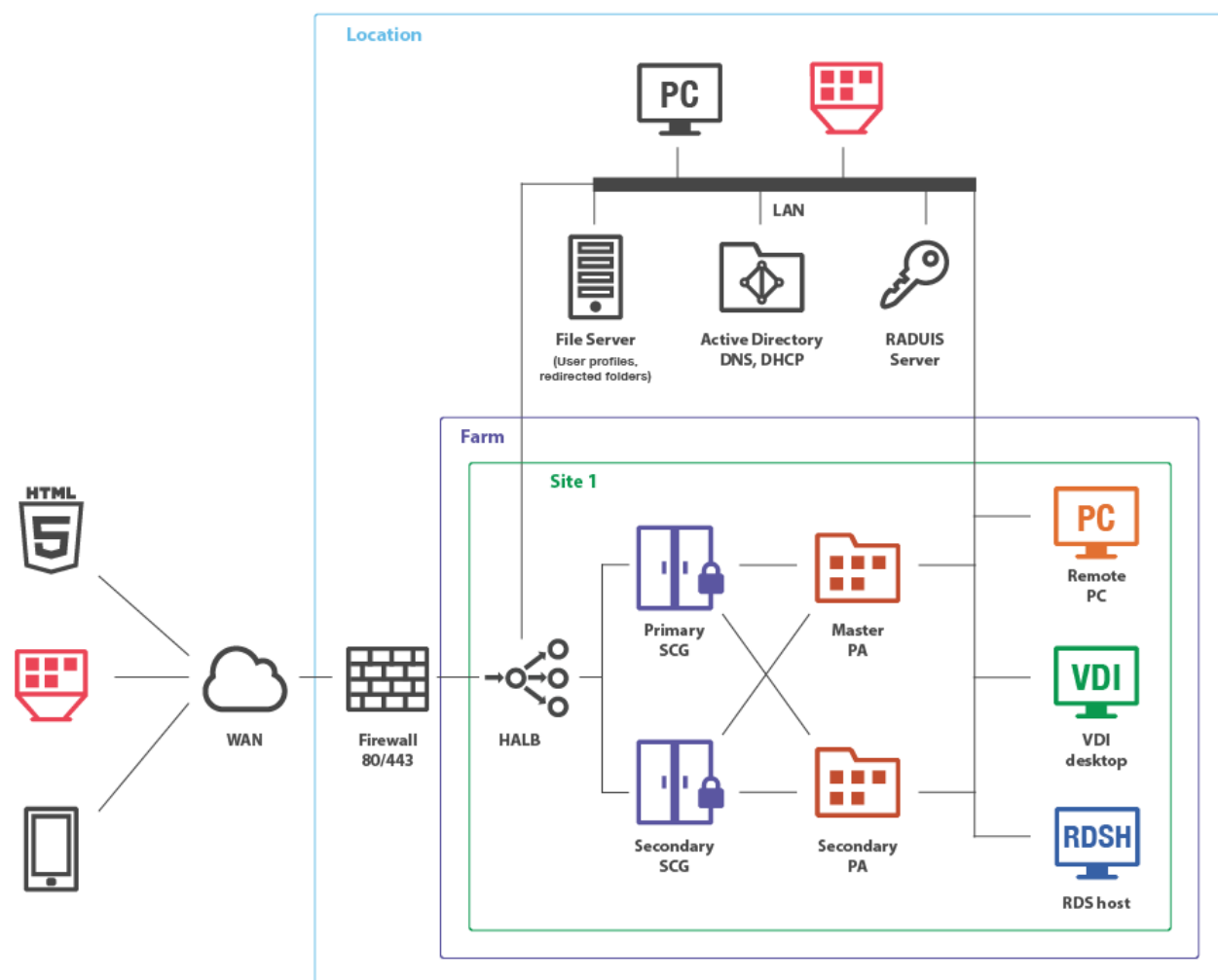
RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

All other components are push-installed from the RAS console.

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.



See also **Capacity Considerations** (p. 39).

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

Installation Notes

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

HALB is installed as a ready-to-use virtual appliance.

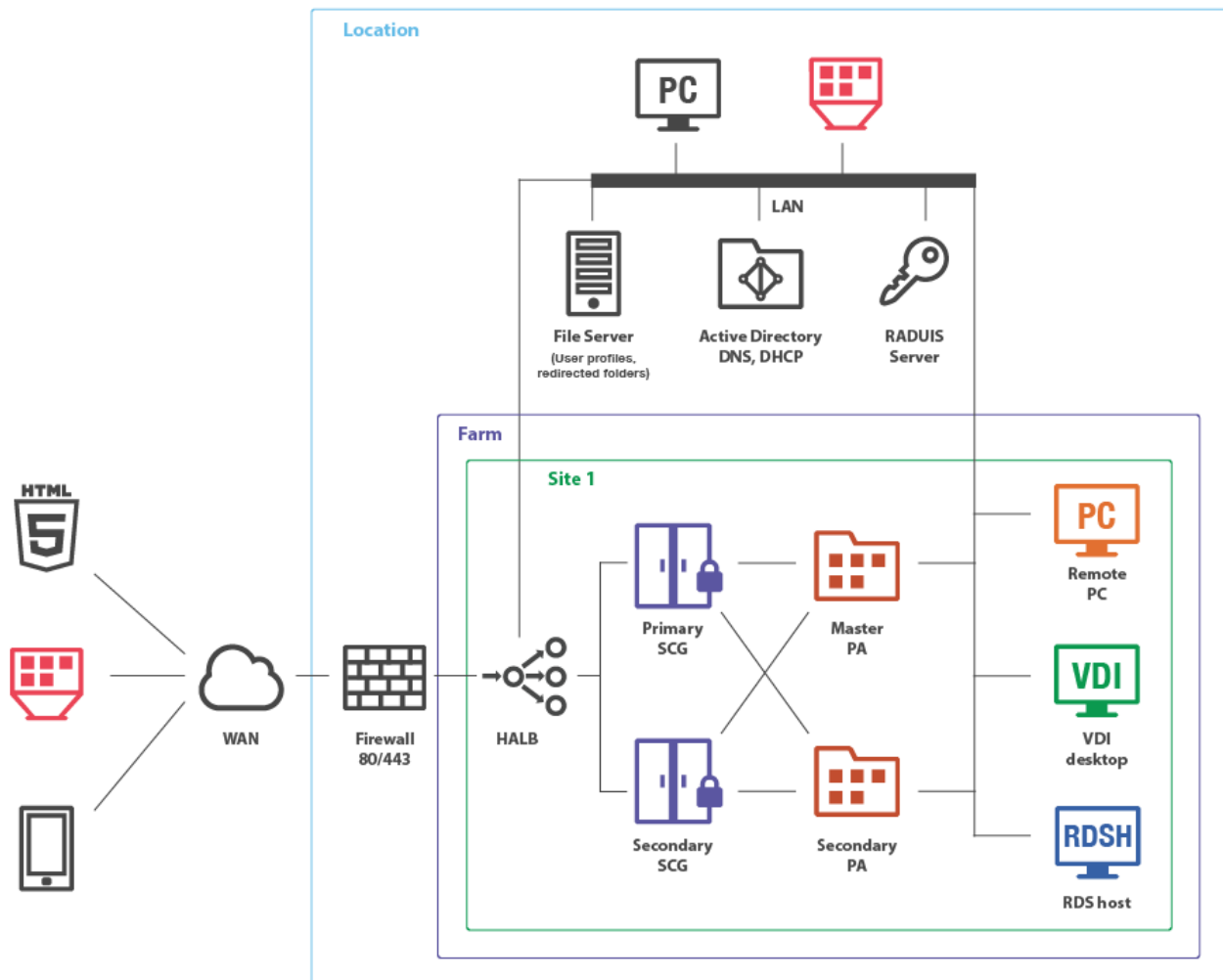
All other components are push-installed from the RAS console.

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 RAS 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 RAS Secure Client Gateways to RAS 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 RAS Secure Client Gateways in the internal network. The WAN users connect to HALB VIP address, 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.

Installation Notes

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

HALB is installed as a ready-to-use virtual appliance.

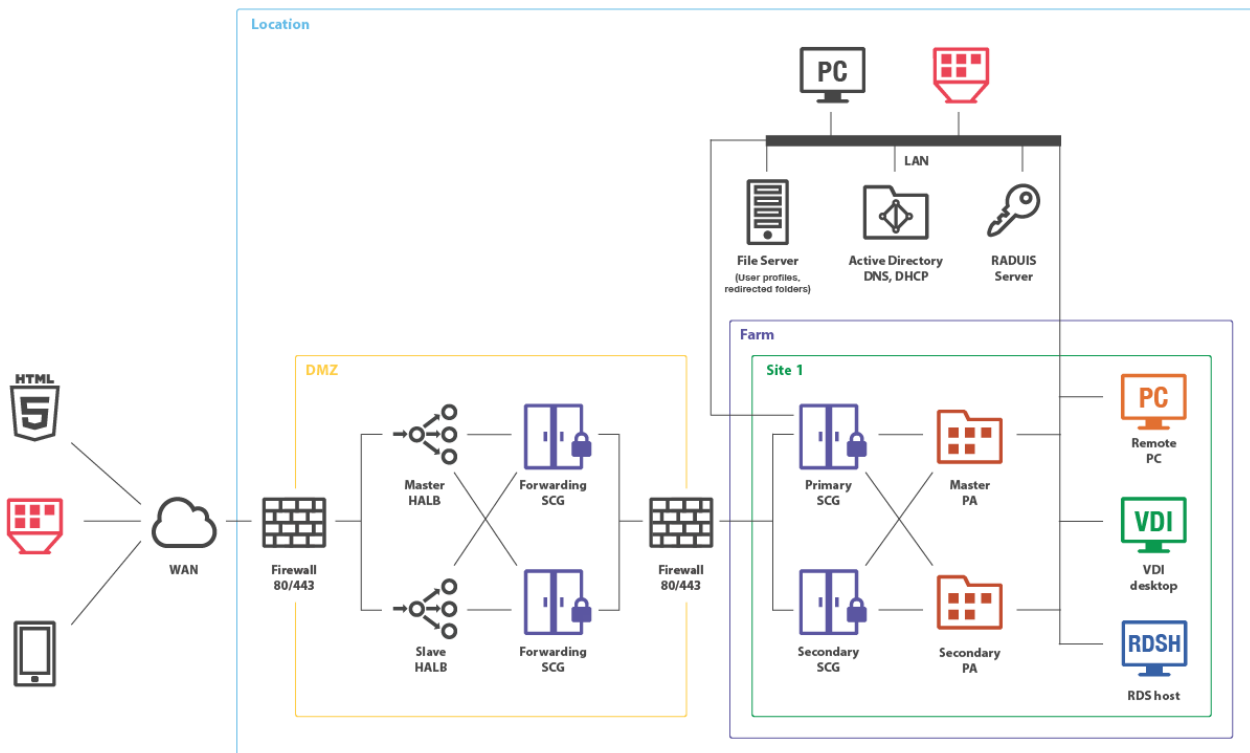
All other components are push-installed from the RAS console.

Dual Firewall DMZ

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

In such a configuration, a HALB pair (master and slave) is installed in front of Forwarding RAS Secure Client Gateways in DMZ. WAN users connect to Parallels RAS using the HALB's VIP address, whereas LAN users connect to Primary and Secondary Gateways (set up as primary and secondary connection options of a RAS connection on the client side). Parallels RAS connection properties can be configured either centrally (using Client Policy in the RAS Console) or manually in Parallels Client.

Forwarding RAS 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.



Installation Notes

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

HALB is installed as a ready-to-use virtual appliance.

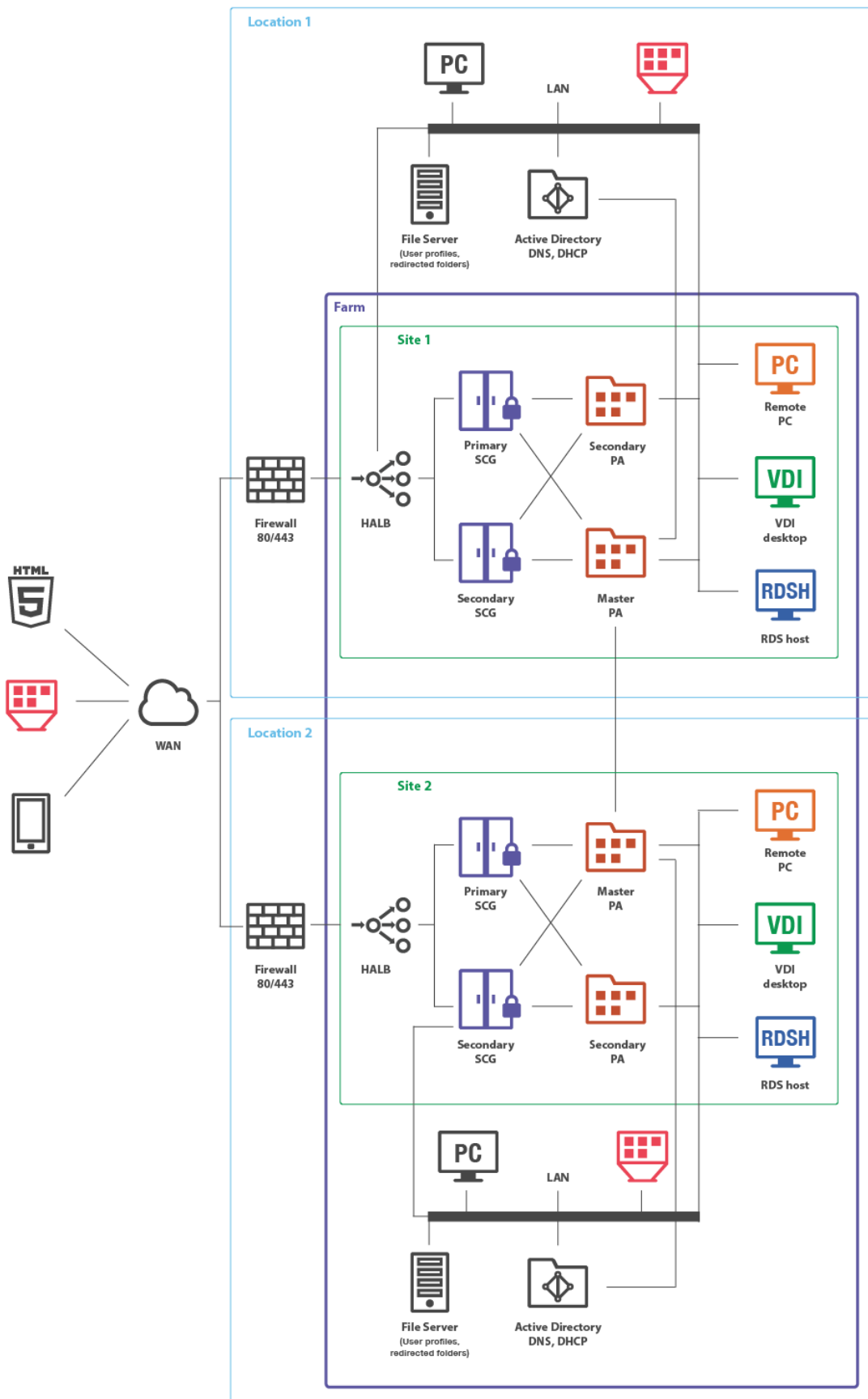
All other components are push-installed from the RAS console.

If the Forwarding RAS Secure Client Gateway cannot be push-installed for any reason, you can run the Parallels RAS installer on the target server. When doing so, select **Custom** installation type and then choose the **RAS Secure Client Gateway** component.

Mixed Scenarios

Multi-Site 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 a RAS Publishing Agent, RAS Secure Client Gateway (or multiple gateways), and agents installed on RD Session Host 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, end users can use both sites via a single RAS connection. The following settings should be used as RAS connection properties in Parallels Client:

LAN users of Site1

- Primary connection: local Primary Secure Client Gateway.
- Secondary connections:
 - Local Secondary Secure Client Gateway.
 - HALB VIP address of Site2.

LAN users of Site2

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

WAN users

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

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

Installation Notes

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

HALB is installed as a ready-to-use virtual appliance.

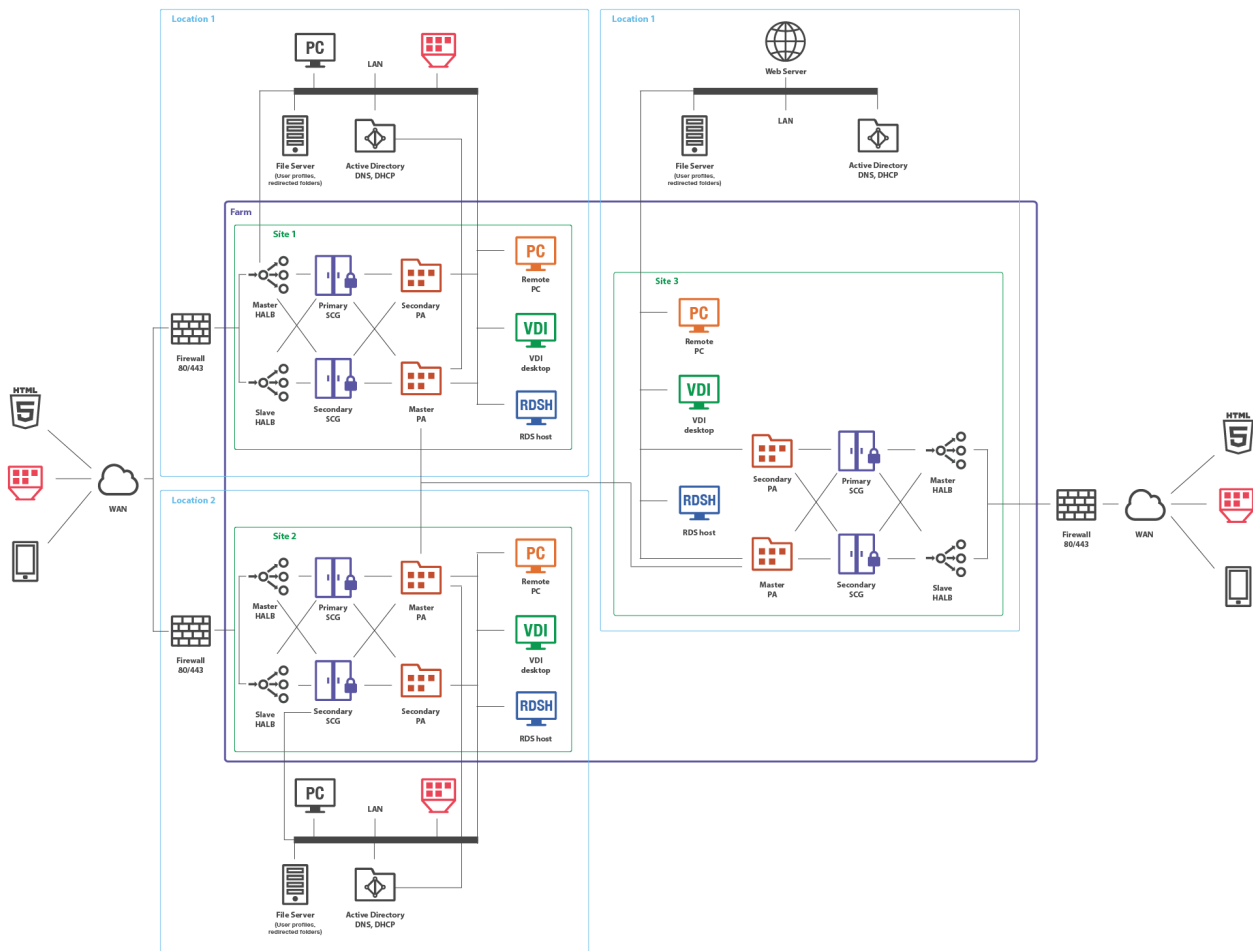
All other components are push-installed from the RAS console.

Business Continuity and Disaster Recovery

A Parallels RAS 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 RAS 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 address of the first site as Server Address and HALB VIP address 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 RAS Console) or manually.



Installation Notes

Master RAS Publishing Agent is installed using the Parallels RAS installer (standard installation). Secondary RAS Publishing Agent is push-installed from the RAS Console.

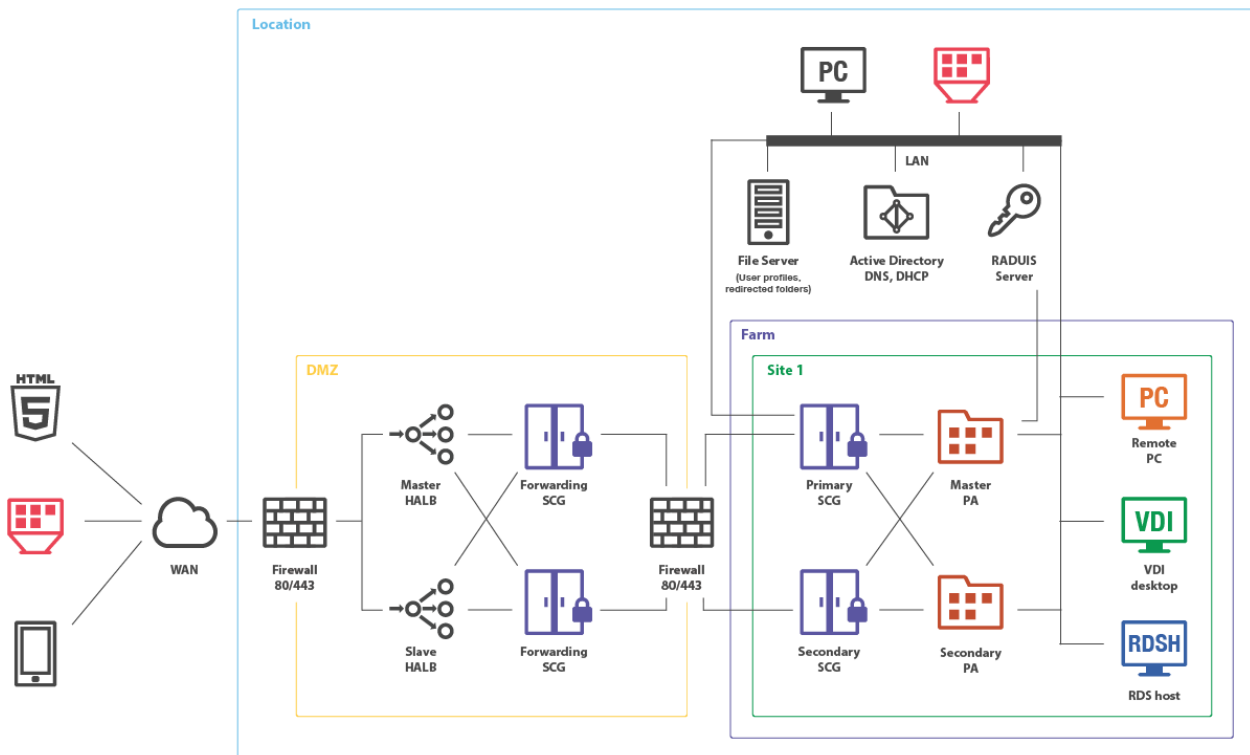
HALB is installed as a ready-to-use virtual appliance.

All other components are push-installed from the RAS console.

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 remote 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 together with the RAS 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 performed first. If the authentication procedure is successful, the next authentication takes place at the Active Directory level using either a user name and password or a smart card.

Installation Notes

Master RAS Publishing Agent is installed using the Parallels RAS installer (standard installation). Secondary RAS Publishing Agent is push-installed from the RAS Console.

Master and slave HALB are installed as ready-to-use virtual appliances.

All other components are push-installed from the RAS console.

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.

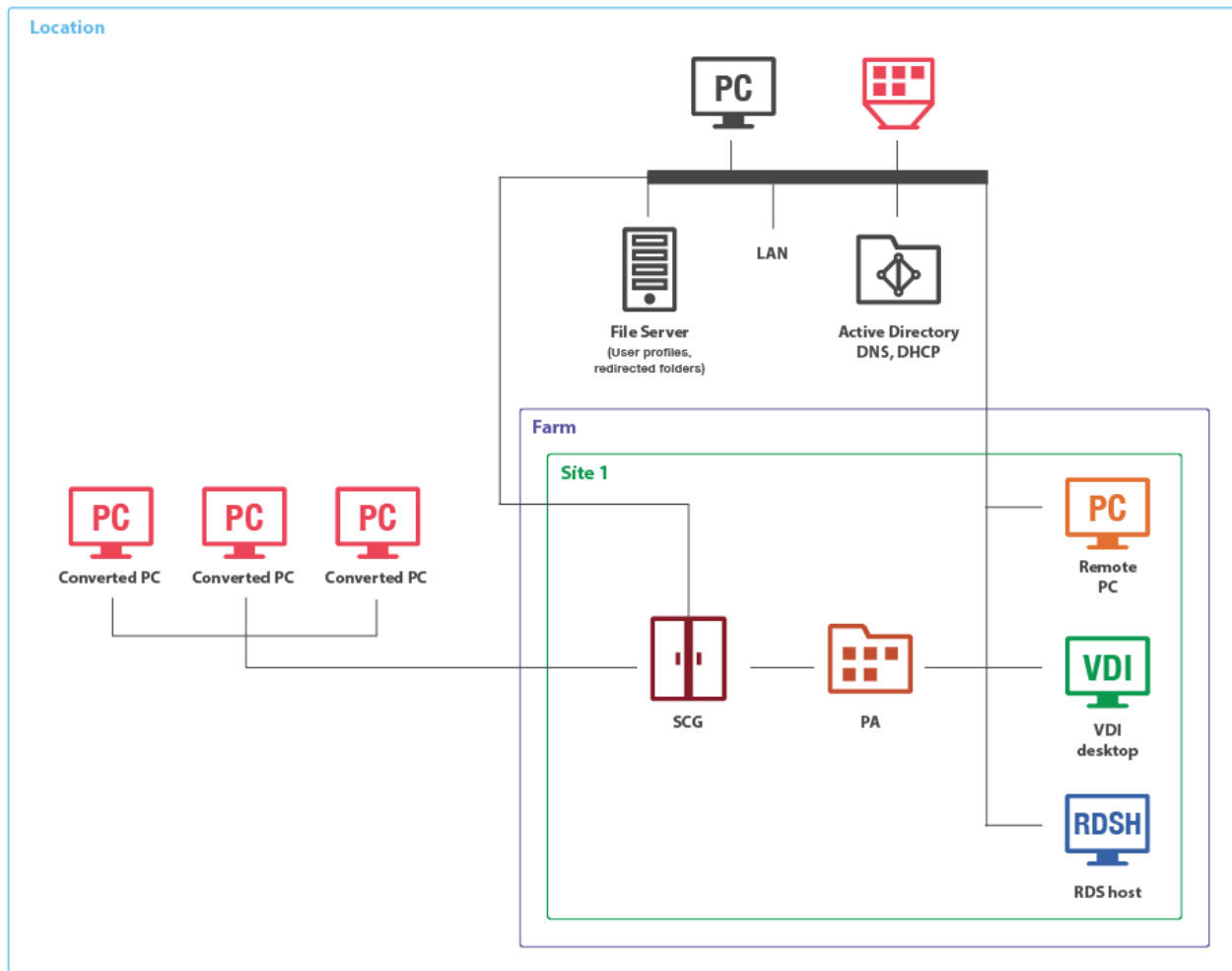
Shadowing

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 RAS. 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.



Installation Notes

RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

All other server-side components are push-installed from the RAS console.

Parallels Client is installed on client desktop computers and converted Windows PCs using the Parallels Client installer.

CHAPTER 3

Capacity Considerations

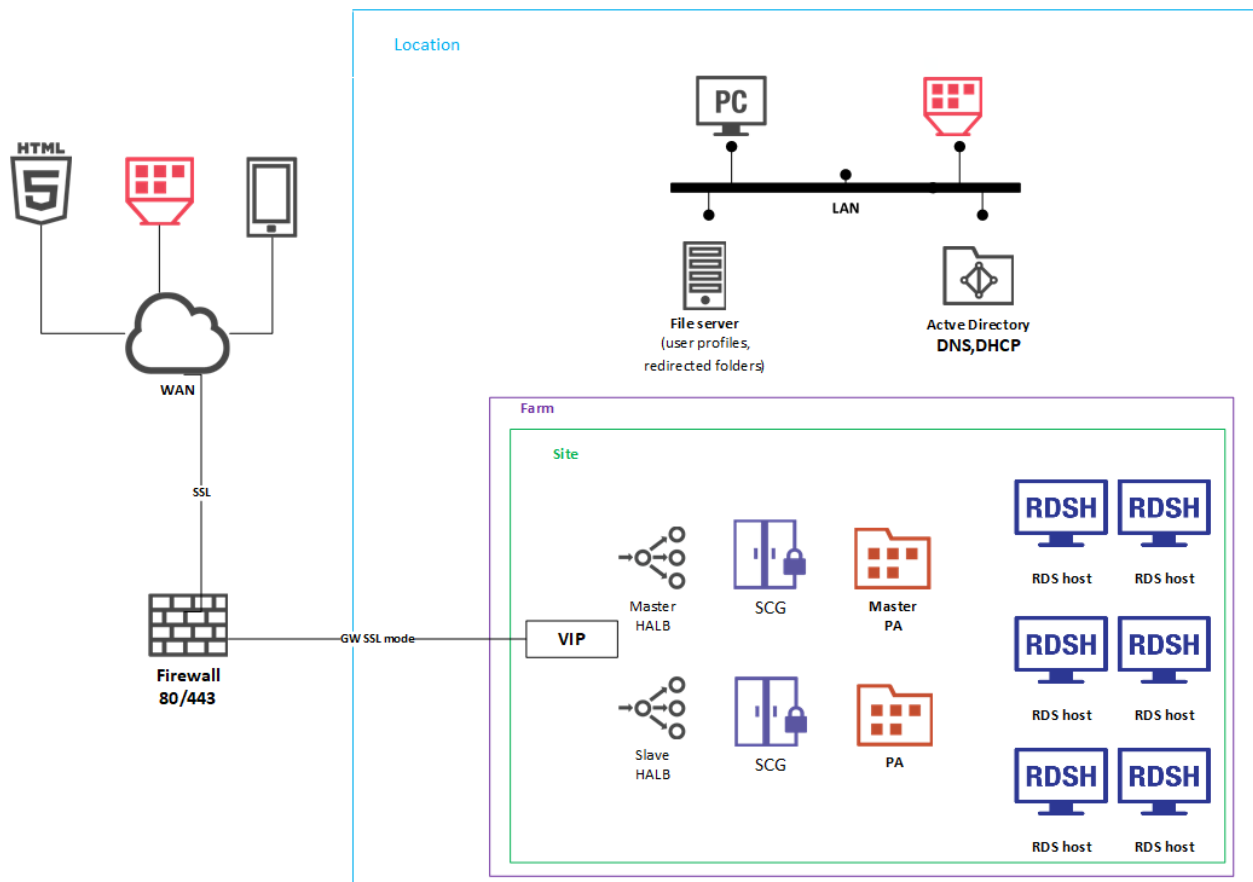
Parallels conducted in-house Parallels RAS scalability testing using a total of two HP DL360 consisting of the following hardware components:

Component	Description
CPU	2x Xeon E5-2670 v1, 2.6GHz, 20 MB L3, 115W TDP
RAM	128 GB, 16x 8 GB Micron DDR-4-2100 at 1600MHz
HDD	Western Digital Blue 1 TB SSD

The following Parallels RAS lab environment was used:

- A farm consists of 1 site.
- Single hop DMZ.
- Each Gateway can host 1200 sessions in Gateway SSL mode (enumeration and proxying RDP session in SSL + HTML5 gateway).
- Each Gateway has an HTML5 Gateway enabled and balanced by HALB using the same port 443 (# Using HTML5 URL <https://HALB-VIP/RASHTML5Gateway/> the incoming connections will be distributed appropriately because SSL session persistence is in a place).

Note: To enable SSL and HTML5 Gateway, a server certificate must be installed.



250 users

Parallels RAS was deployed on VMware vSphere 6.5 on Windows 2016 Server as follows:

Parallels RAS Component	Total VMs	vCPU in Each VM	RAM in Each VM
RAS Publishing Agent	2	2	4 GB
RAS Secure Client Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	6	6	24 GB

- All components doubled for redundancy.
- RDSH N+1 for redundancy.

The above configuration has been tested with both our internal tools and Login VSI. For more details, you could read the **Parallels RAS Scalability Testing with Login VSI** paper, which is available at the following URL: https://download.parallels.com/ras/v16/docs/en_US/Parallels-RAS-Scalability-Testing-Login-VSI.pdf

500 users

Parallels RAS was deployed on VMware vSphere 6.5 on Windows 2016 Server as follows:

Parallels RAS Component	Total VMs	vCPU in Each VM	RAM in Each VM
RAS Publishing Agent	2	2	4 GB
RAS Secure Client Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	12	6	24 GB

- All components doubled for redundancy.
- RDSH N+2 for redundancy.

1000 users

Parallels RAS Component	Total VMs	vCPU in Each VM	RAM in Each VM
RAS Publishing Agent	2	2	4 GB
RAS Secure Client Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	24	6	24 GB

- All components doubled for redundancy.
- RDSH N+4 for redundancy.

CHAPTER 4

Deploying Parallels RAS Reporting Service

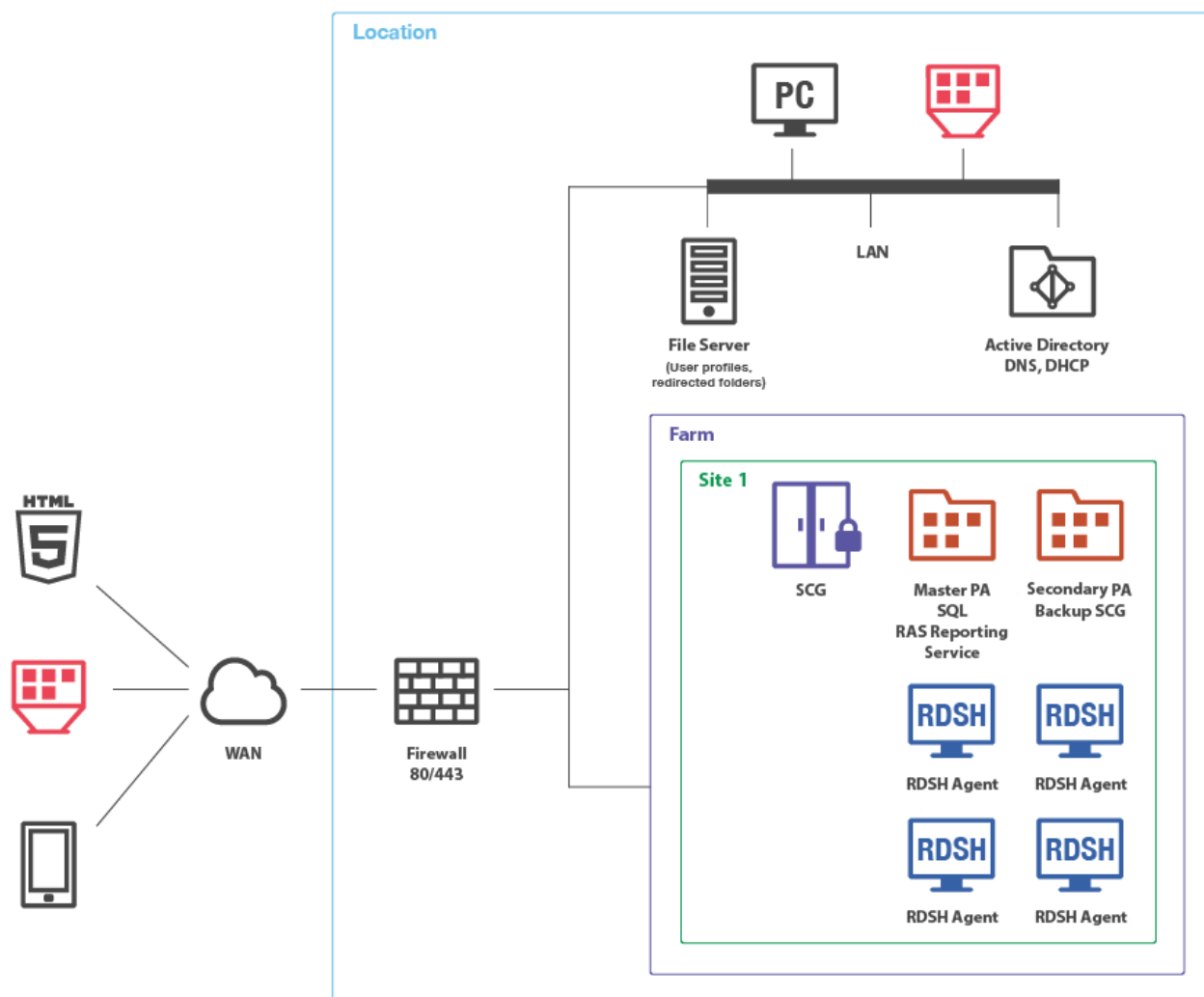
This chapter describes common scenarios for deploying the Parallels RAS Reporting Service.

In This Chapter

One Site with Multiple RD Session Hosts.....	43
Multiple Sites with Multiple RD Session Hosts.....	44

One Site with Multiple RD Session Hosts

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 RAS is running.



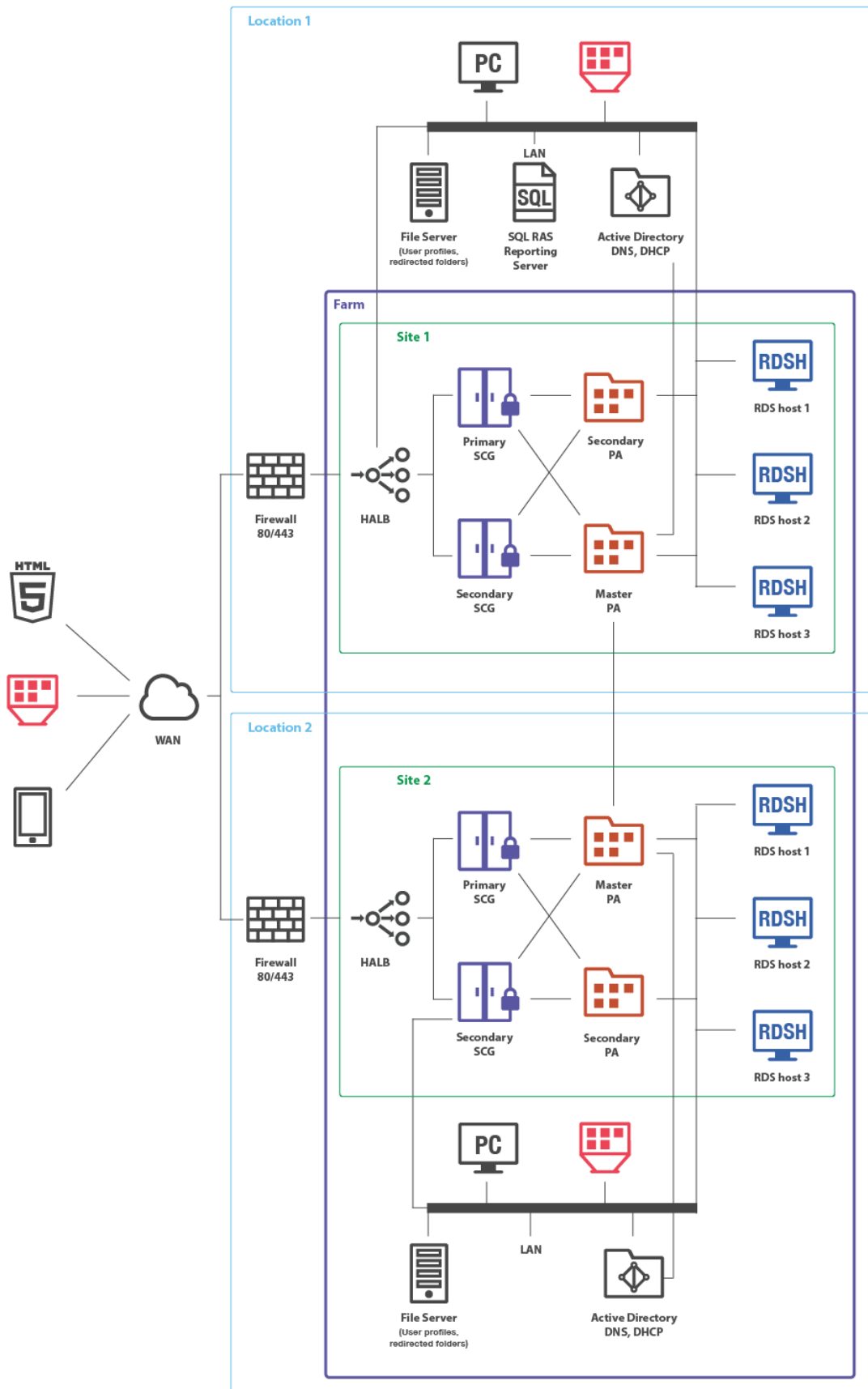
Installation Notes

Primary RAS Publishing Agent is installed using the Parallels RAS installer (standard installation). Secondary RAS Publishing Agent is push-installed from the RAS console.

All other components are push-installed from the RAS console.

Multiple Sites with Multiple RD Session Hosts

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



Installation Notes

Master RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).
Secondary RAS Publishing Agent is push-installed from the RAS Console.

HALB is installed as a ready-to-use virtual appliance.

SQL RAS Reporting Server is installed using the Windows installer.

All other components are push-installed from the RAS console.

CHAPTER 5

Port Reference and SSL Certificates

This chapter provides reference information about ports used by Parallels RAS and describes how SSL certificates are used in Parallels RAS.

In This Chapter

Port Reference	47
SSL Certificates.....	52

Port Reference

Parallels RAS v16.1 and newer

Parallels Client

Source	Destination	Protocols	Ports	Description
Parallels Client	HALB	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used.
		TCP, UDP	20009	Client Manager, shadowing via FW.
	RAS Secure Client Gateway (Normal and Forwarding modes)	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used.
		TCP, UDP	20009	Client Manager, shadowing via FW only for Normal mode. Since RAS v16, forwarding gateways don't support client management.
		UDP	20000	Gateway lookup broadcast.
	RDP Session	TCP, UDP	3389	Connections in Direct mode 3389 is used. RDP connection is always encrypted.

Web Browsers

Source	Destination	Protocols	Ports	Description
HTML5 web browser	RAS Secure Client Gateway	TCP	443	HTML5 (in Normal mode only).
Web browser	Web Portal	TCP	81	Web portal UI. An actual session uses the Parallels Client information.
		TCP	443	If SSL is enabled.
Web Portal	RAS Secure Client Gateway	TCP	80, 443	If SSL is enabled.

RAS Secure Client Gateway

Source	Destination	Protocols	Ports	Description
RAS Secure Client Gateway in Forwarding mode	RAS Secure Client Gateway in Normal mode	TCP	80, 443, 3389	TCP 3389 if RDP load balancing is enabled.
		UDP	80, 443	If RDP-UDP is used. Note: Since RAS v16, forwarding gateways don't support client management.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS Secure Client Gateway in Normal mode	Remote Desktop Services	TCP, UDP	3389	RDP Connections
	RAS Publishing Agent	TCP	20002	TCP 20002 Publishing Agent Service Port - communications with RAS Secure Client Gateways and RAS Console (in Normal mode only).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	Localhost	TCP	20020	Communication with NodeJS web server.

RAS Publishing Agent

Source	Destination	Protocols	Ports	Description
RAS Publishing Agent	RAS Publishing Agent	TCP	20001, 20030	TCP 20001 Redundancy Service. TCP 20030 Communication between Publishing Agents running in the same site.
		UDP	20021	RAS Publishing Agent lookup broadcast.
	Parallels Licensing Server	TCP	443	Outbound TCP 443 - RAS Publishing Agent (Master RAS Publishing Agent in Licensing Site) communicates with Parallels Licensing Server (https://ras.parallels.com)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	RAS RD Session Host Agent	TCP	30004	TCP 30004 Server for RAS Publishing Agent requests.
	RAS VDI Agent	TCP	30006	TCP 30006 - RAS VDI Agent communication port.
	RAS Guest Agent	TCP	30004 (30010 on RAS v16.5 and later) 30005	TCP 30004 (30010 on RAS v16.5 and later) is used by RAS Console during RAS Template creation. TCP 30005 is used by components on the destination RDS/Guest/Remote PC for internal communication. Client does not use it.
	RAS Remote PC Agent	TCP	30004	RAS Remote PC Agent communication port (Agent status, counters and session information).
	2FA Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.

RAS Console

Source	Destination	Protocols	Ports	Description
RAS Console	SQL host with SSRS and Reporting component	TCP	30008	RAS Publishing Agent (RAS Console and reporting).
	HALB	TCP, UDP	31006	TCP, UDP 31006 configuration.
	Parallels Client	TCP	50005	Shadowing from RAS Console in case of direct network connection.
	RAS Guest Agent RAS RD Session Host Agent RAS Remote PC Agent RAS Publishing Agent RAS Secure Client Gateway	TCP	135, 445, 49179	Remote install push/takeover of software.
	RAS Guest Agent	TCP	30004 (30010 on RAS v16.5 and later)	Used for the "Check Agent" task.
		UDP	30004 (30009 on RAS v16.5 and later)	Used to manage components.
	RAS Remote PC Agent RAS RD Sessions Host Agent	TCP, UDP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS VDI Agent	TCP, UDP	30006	Used for the "Check Agent" task. Used to manage component.
	2FA Server/s	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.
	www.turbo.net	TCP	80, 443	When Turbo containerized apps publishing is enabled and used. Used to obtain app categories and available apps metadata for further publishing.
	RAS Performance Monitor	TCP	3000	Performance Dashboard in the Monitoring category (Grafana connection).
	RAS Publishing Agent	TCP	20002, 20001	Communication with RAS Publishing Agent and Redundancy.

RAS Agents: RD Session Host, VDI, Guest, Remote PC

Source	Destination	Protocols	Ports	Description
RAS RD Session Host Agent	RAS Publishing Agent	TCP	20003	TCP, UDP 20003 Communications with RAS Publishing Agents.
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	www.turbo.net	TCP	80, 443	When Turbo support is enabled and used. Used to download Turbo installation package and install / update application containers.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS VDI Agent	RAS Publishing Agent	TCP	20003	RAS Publishing Agent communication port.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB - applicable to Hyper-V only.
RAS Guest Agent	RAS VDI Agent	TCP	30006	Communication with RAS VDI Agent
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
RAS Remote PC Agent	RAS Publishing Agent	TCP	20003	RAS Publishing Agent communication.
	Localhost	TCP	30005	For internal commands - memshell, printer redirector).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.

HALB

Source	Destination	Protocols	Ports	Description
HALB	HALB	VRRP	112	RAW

Common Communication Ports

Source	Destination	Protocols	Ports	Description
RAS Console	Any host to which Agents are pushed	TCP	135, 445, 49179	Remote install push/takeover of software.
Master RAS Publishing Agent	AD DS controllers	TCP	389, 3268	LDAP
		TCP	636, 3269	LDAPS
		TCP	88	Kerberos
		UDP	53	DNS
	2FA Server/s	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius.

Active Directory and Domain Services Ports

For Active Directory and Active Directory Domain Services port requirements, please see the following article: <https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx>

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 TLS 1.2 as the SSL settings option.

- 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 CSR request.

Using Enterprise Certificate Authority

Use IIS to receive a certificate from Enterprise CA and export the certificate in the PFX format.

Install the PFX certificate on RAS Secure Client Gateway as follows:

- 1 Launch the Parallels RAS Console.
- 2 Select a RAS Secure Client Gateway, open its properties and switch to the SSL tab page.
- 3 Click [...] next to **Private Key** or **Public Key** fields.
- 4 Browse for the `.pfx` file and click **OK**.
- 5 Click **Apply**.

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 the `Program Files\Parallels` or `Program Files(x86)\ Parallels` on the client side.

Enable SSL on RAS 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

Active Directory and Domain Services Ports - 51
Advantages of Parallels RAS Solution - 5

B

Business Continuity and Disaster Recovery - 34

C

Capacity Considerations - 39
Client Connection Modes - 15
Client Manager and Desktop Replacement - 37
Common Communication Ports - 51

D

Deploying Parallels RAS Reporting Service - 42
Deployment Scenarios - 17
Dual Firewall DMZ - 30

G

General Considerations - 17

H

HALB - 51
High Availability with Multiple Gateways - 27
High Availability with Single or Dual F/W DMZ - 29

M

Mixed Scenarios - 32
Multiple Sites with Multiple RD Session Hosts - 44
Multi-Site Scenario - 32

O

One Site with Multiple RD Session Hosts - 43

P

Parallels Client - 47
Parallels Client Connection Flow - 14
Parallels RAS Basic Concepts - 11
Parallels RAS Components - 6
Parallels RAS Deployment Scenarios - 17
Port Reference - 47
Port Reference and SSL Certificates - 47

R

RAS Agents
 RD Session Host, VDI, Guest, Remote PC - 50
RAS Console - 49
RAS Publishing Agent - 48
RAS Secure Client Gateway - 48

S

Secure Setup with Dual Firewall DMZ and Second-Level Authentication - 36
Single Farm with Dual RAS Secure Client Gateways - 26
Single Farm with Mixed Desktops - 24
Single Farm with One RD Session Host - 17
Single Farm with Public & Private RAS Secure Client Gateways - 25
Single Farm with RD Session Host Auto Scaling - 20
Single Farm with Remote PC Desktops - 22
Single Farm with Two RD Session Hosts - 19
Single Farm with VDI Desktops - 21
Single Firewall DMZ - 29
SSL Certificates - 51

U

Understanding Deployment Scenario Diagrams - 8

W

Web Browsers - 47

What is Parallels RAS - 5