Parallels Remote Application Server

Solutions Guide

18.3

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

Contents

CHAPTER 1

Introduction

This guide is intended for system administrators deploying and managing Parallels® Remote Application Server (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

Parallels RAS 18 release history

The following table lists the Parallels RAS 18 release history. Parallels RAS documentation is updated for every release. This guide refers to the latest Parallels RAS 18 release from the table below. If you are using a newer Parallels RAS release or version, please download the current version of the guide from https://www.parallels.com/products/ras/resources/.

Parallels RAS Version	Release	Date
18.0	Initial release	12/14/2020
18.0	Update 1	03/03/2021
18.1	Initial release	07/14/2021
18.2	Initial release	11/03/2021
18.3	Initial release	12/21/2021
18.3	Update 1	02/16/2022

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. In addition, Parallels RAS supports Azure Virtual Desktop. 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. Clientless browser-based access via HTML5 is also available.

For an in-depth information about the rich Parallels RAS features, please read the **Parallels RAS 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 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.

Multi-Tenant architecture and capabilities

Parallels RAS Multi-Tenant architecture with Parallels RAS Tenant Broker allow for sharing of the access layer such as Parallels Secure Client Gateways and front-end High Availability Load Balancers (HALBs) among Tenants, which may be represented as isolated Parallels RAS Farms and/or sites. Tenant Broker is a separate RAS installation that hosts shared RAS Secure Client Gateways and HALB. Tenant farms are deployed just like traditional RAS environments and are joined to the Tenant Broker. Each Tenant farm has its own RAS Publishing Agents and servers hosting published resources (RD Session hosts, VDI, Azure Virtual Desktop, Remote PCs). No local RAS Secure Client Gateways or Load Balancers are needed.

Deployment Flexibility

Parallels RAS offers flexible cloud deployment model support, whether using on-premises, cloud or multi-cloud environments, allowing businesses to leverage different technologies while reducing total cost of ownership.

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 a desktop application for administrators who manage Parallels RAS.

Parallels RAS Management Portal is a modern web-based configuration and administration portal. The Management Portal is designed for administrators using a desktop or laptop computer or a mobile device to carry out configurations and day-to-day activities.

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 a VDI provider through its native API. RAS VDI Agent comes in two varieties. One is built into the RAS Publishing Agent and is available by default. It can be used to control multiple VDI providers in a Parallels RAS Farm. The other is a separate component that can be installed manually on a VDI provider host, in which case it will work with that host only. The built-in RAS VDI Agent can be used with any VDI provider supported by Parallels RAS except **QEmu KVM with libvirt** and **Nutanix Acropolis**. With these two hypervisors, a dedicated RAS Publishing Agent must be manually installed on a VDI provider host. See **RAS VDI Agent dedicated** below for more info.

RAS VDI Agent dedicated is a separate component that can be installed from 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 RAS VDI Agent to control the VDI provider 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 Hyper-V and VMware. Multiple HALB Virtual Servers can be configured, each assigned with different virtual (and floating) IPs to load balance traffic to Secure Client Gateways in the same RAS Site. This enables administrators to configure Virtual Servers for segregated access, for example when using different Secure Client Gateways for internal and external access or different office branches. Multiple HALB deployments can run simultaneously, one acting as the primary and others as secondary. The more HALB deployments a site has, the lower the probability that end users will experience downtime. Primary and secondary HALB deployments share a common or virtual IP address (VIP). Should the primary HALB deployment fail, a secondary is promoted to primary and takes its place.

Parallels Device Manager is a Parallels RAS feature that allows the administrator to manage Windows computers. Windows 7 and new 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.

RAS Enrollment Server is an essential component of the SAML SSO Authentication functionality. It communicates with Microsoft Certificate Authority (CA) to request, enroll, and manage digital certificates on behalf of the user for SSO authentication in the Parallels RAS environment.

Azure Virtual Desktop is a desktop and app virtualization service running on Microsoft Azure, providing access to RD Session Hosts and VDI, including the new offering of Windows 10 and Windows 11 Enterprise multi-session hosts. Parallels RAS 18 provides the ability to integrate, configure, maintain, support and access Azure Virtual Desktop workloads on top of the existing technical capabilities of Parallels RAS.

Microsoft FSLogix Profile Container is the preferred Profile Management solution as the successor of Roaming Profiles and User Profile Disks (UPDs). It is set to maintain user context in non-persistent environments, minimize sign-in times and provide native profile experience eliminating compatibility issues.

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.
Enrollment Server	RAS Enrollment Server (an essential part of SAML SSO Authentication functionality).

Icons

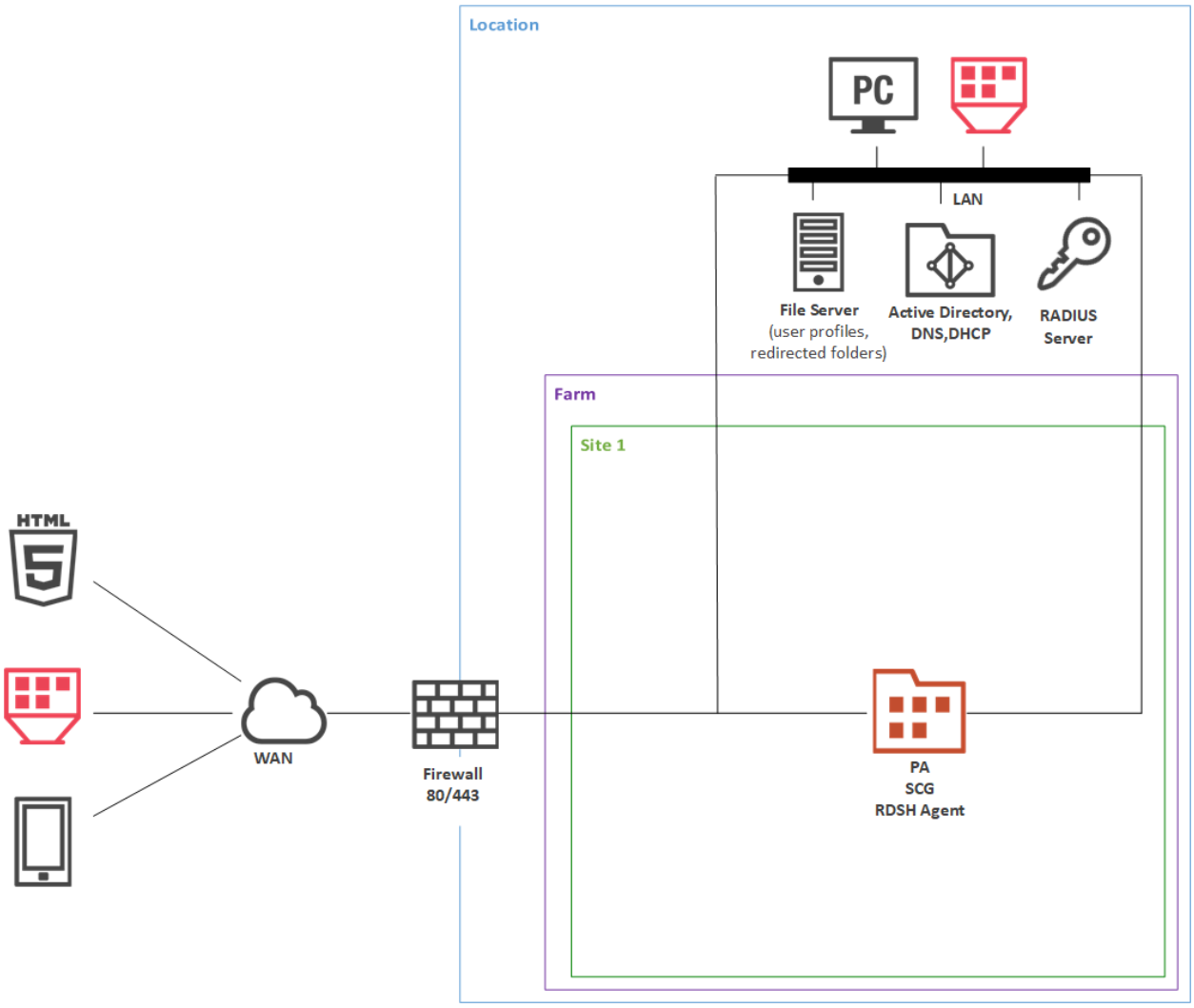
The following table describes the icons used in deployment scenario diagrams.

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).
	Microsoft SQL Server database.
	RAS Reporting and SQL Server Reporting Services (installed on the same server).
	RADIUS server (used for second-level authentication).
	File server for storing user profiles and redirected folders.
	Firewall (ports 80 and 443 are open).
	On-premises VPN gateway.
	RAS Enrollment Server.
	Azure Load Balancer and/or Azure VPN Gateway.

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.

Firewall, represented by a brick wall, is responsible for network protection. Please note that if the scenario description doesn't include any specifics about DMZ or firewall(s), it is up to the administrator or network security officer to decide how network protection should be implemented.

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

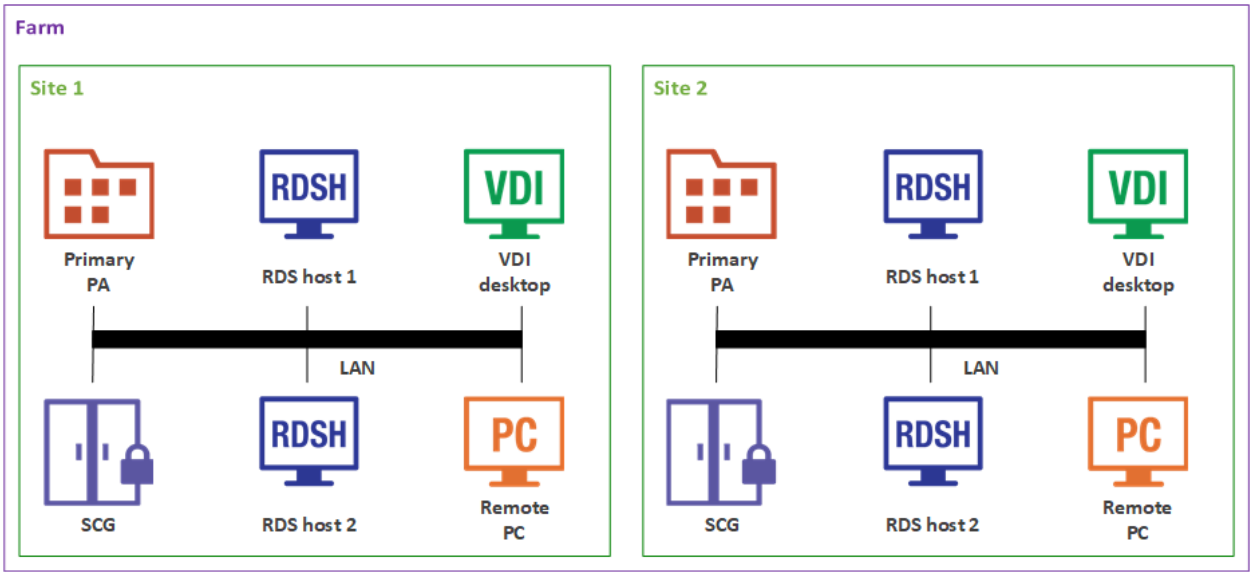
When a user connects to Parallels RAS from Parallels Client, they are presented with published resources (applications, desktops, documents, etc). The user selects a resource and launches it. The system load-balances user requests automatically and launches the resource from a least-loaded host. The user is then presented with the resource seamlessly via RDP protocol.

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

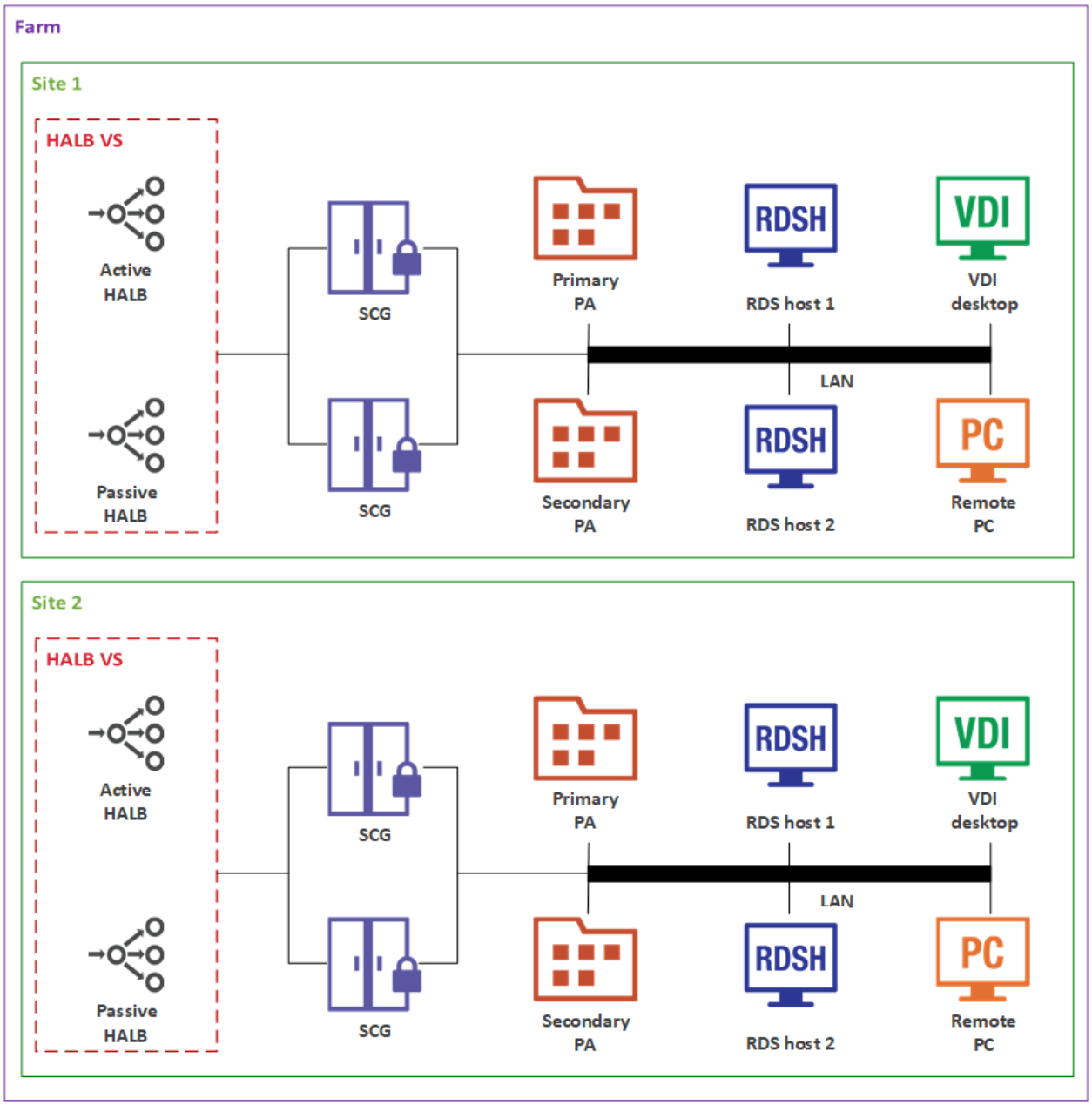
- Farm
- Site
- Agents

The first server added to a farm creates a new site and becomes the primary 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 primary Publishing Agent (Primary 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 Virtual Server (VS) is a virtual representation of the HALB appliances (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 VS is configured, the primary HALB appliance forwards the Parallels Client to the Secure Client Gateway according to load balancing rules.
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

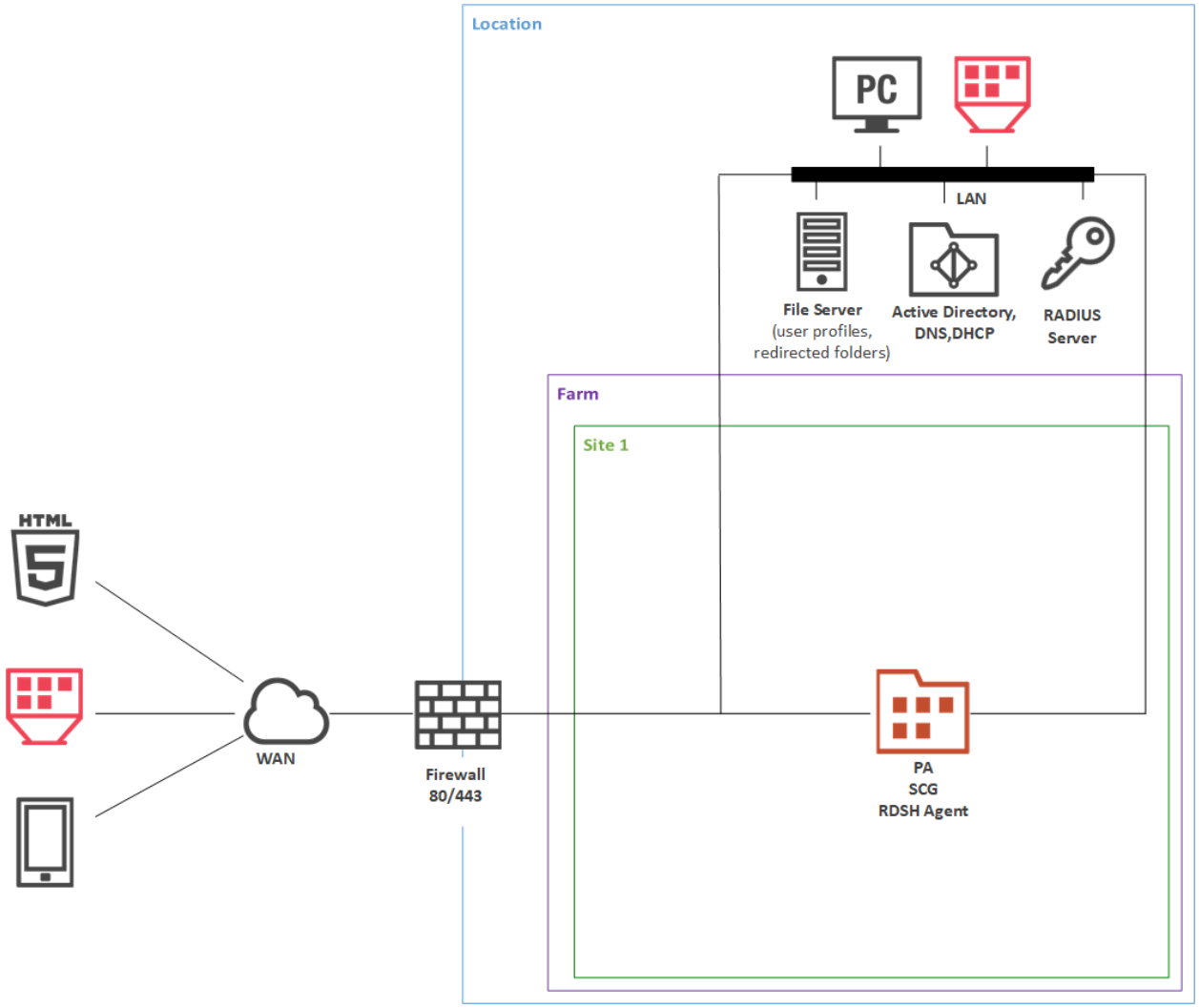
Regardless of the size of a Parallels RAS installation, redundancy among core components of your setup is recommended to ensure the greatest possible uptime. For small deployments, all roles can be installed on a single server, whereas role segregation is recommended for large setups.

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 trusted by 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. 65)).



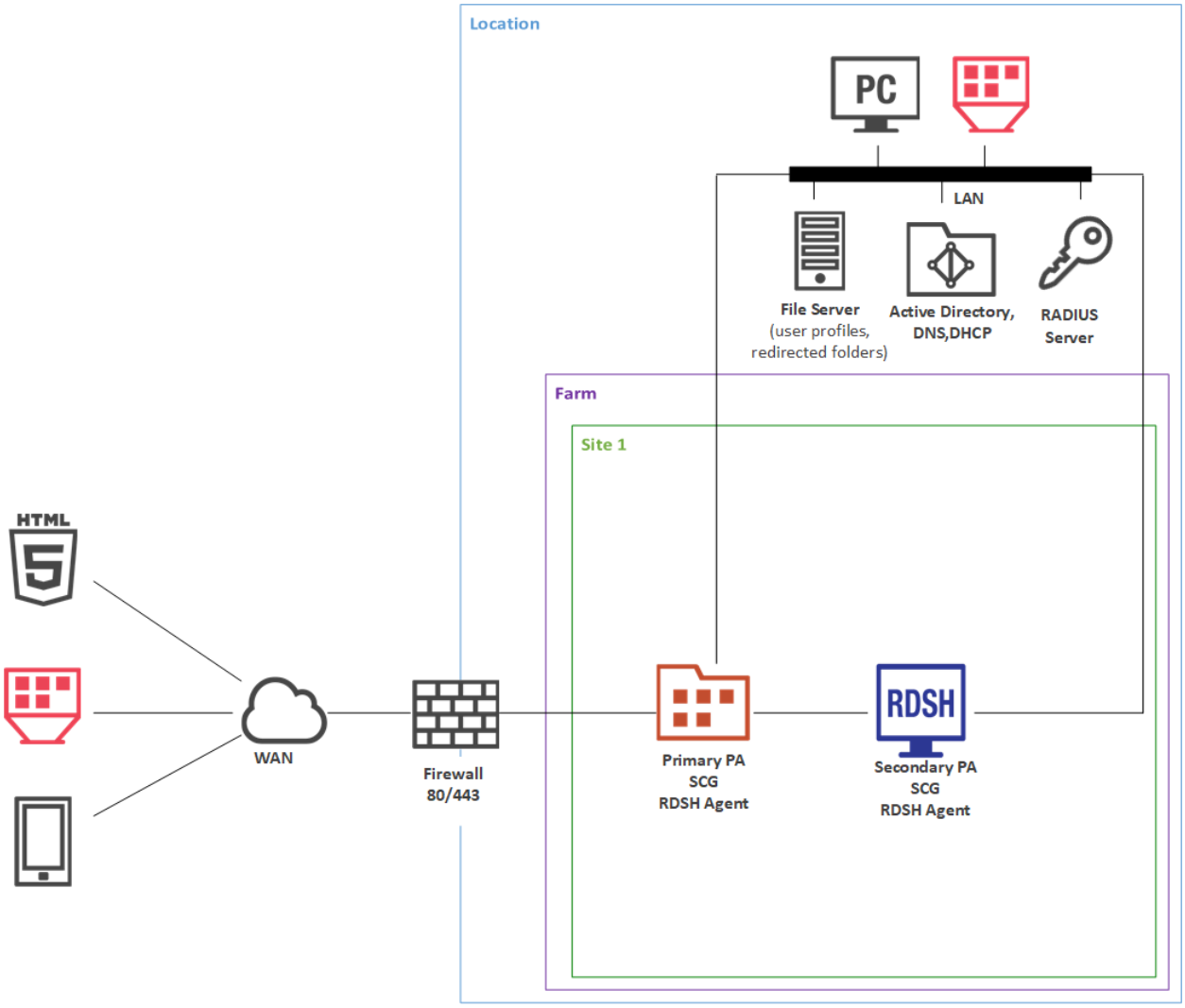
Installation Notes

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

Single server deployment is not recommended for production environments, as it does not provide high availability of service. Such deployment should be used for test or developer environments.

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

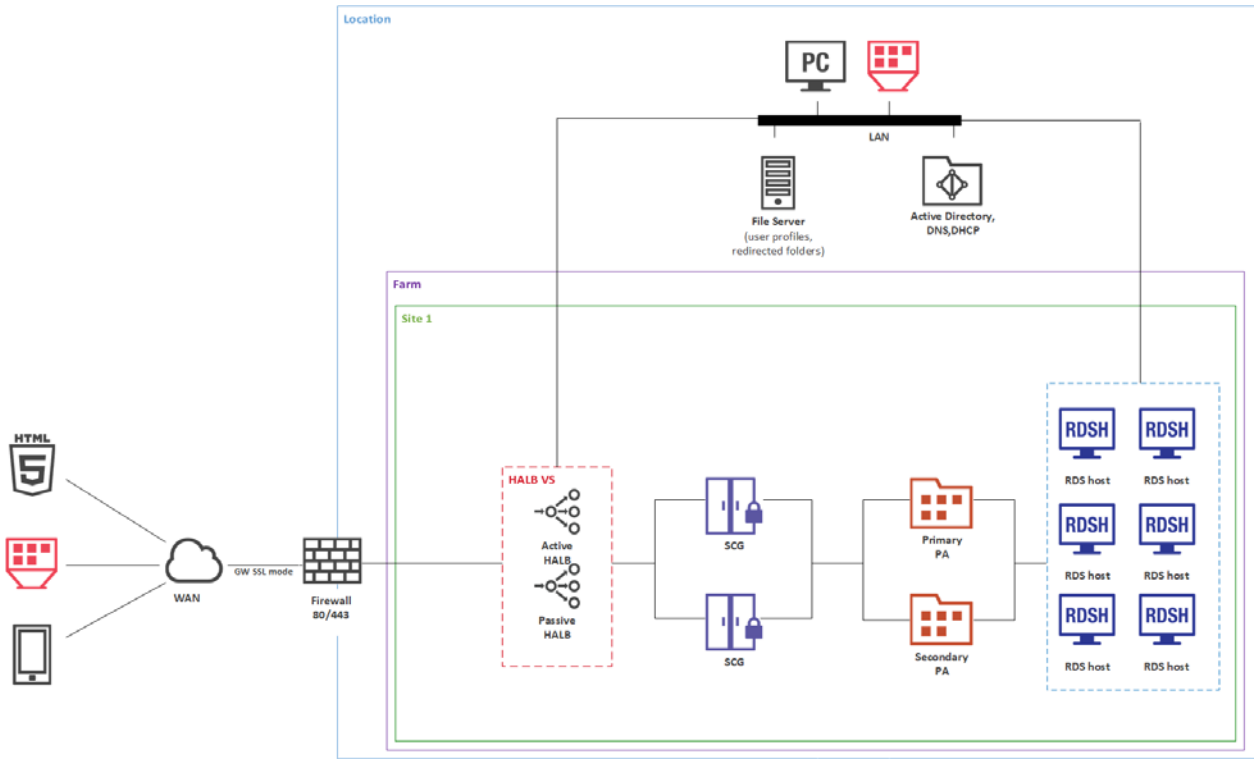
The components on the primary RD Session Host (where the primary RAS Publishing Agent is installed) are installed using the Parallels RAS installer (standard installation).

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, HALB Virtual Server (VS) should have a secondary HALB appliance, additional RAS Publishing Agent and RAS Secure Client Gateway should be deployed. HALB Virtual Server (VS) is a virtual representation of the HALB appliances.



Installation Notes

The components on the primary 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.

HALB Virtual Server (VS) is configured with two HALB appliances.

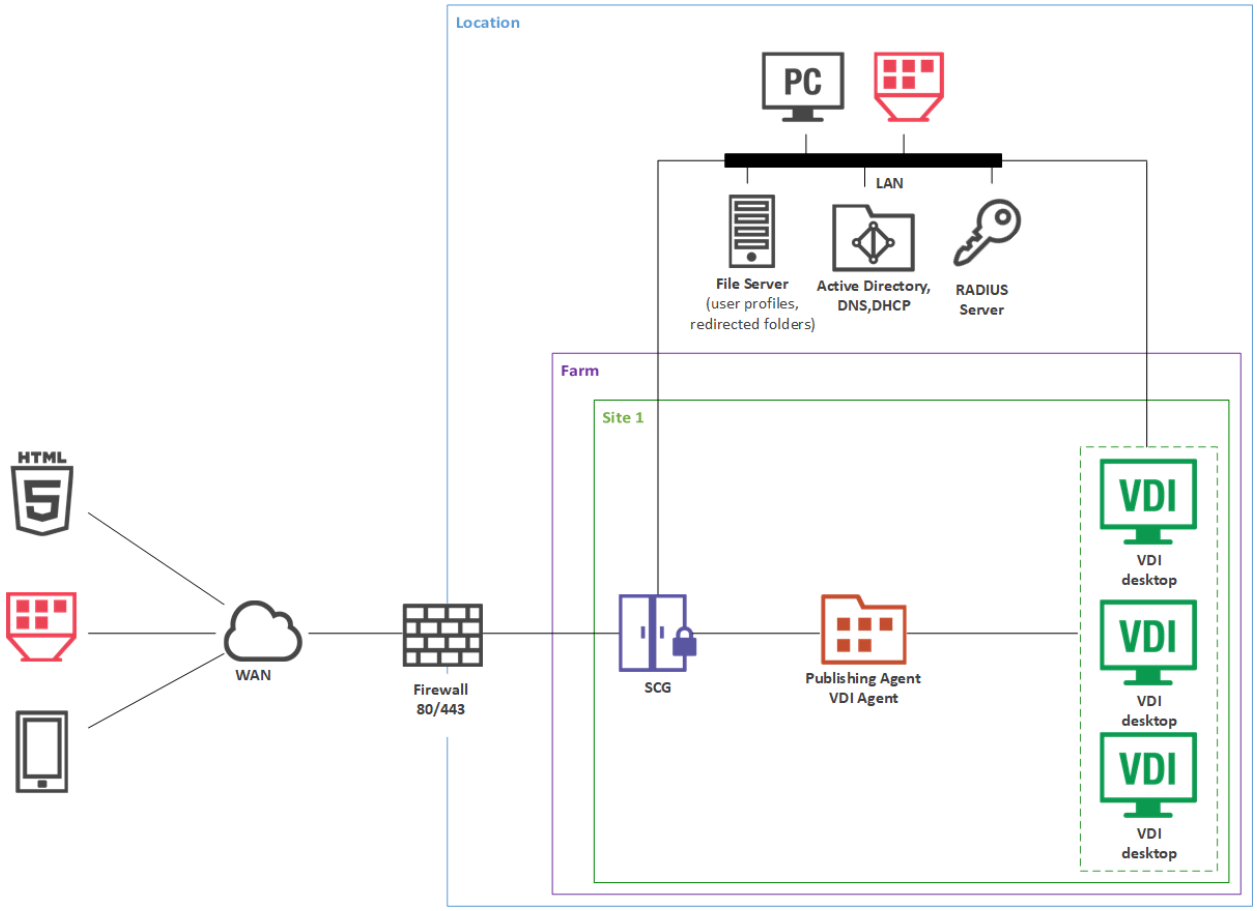
Single Farm with VDI Desktops

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.

- Increased data security provides organizations with an extra layer of protection with dynamic security permissions. This is a security feature which prevents access to VDI without using Parallels RAS Client. After the session is established, Parallels RAS dynamically adds the user to the "Remote Desktop Users" group, granting permissions on logon and removing permissions on logoff. Even if a VDI virtual machine (VM) hostname or IP address is noted, users will not be able to connect to the VDI VM unless connection is setup from the Parallels Client.



Installation Notes

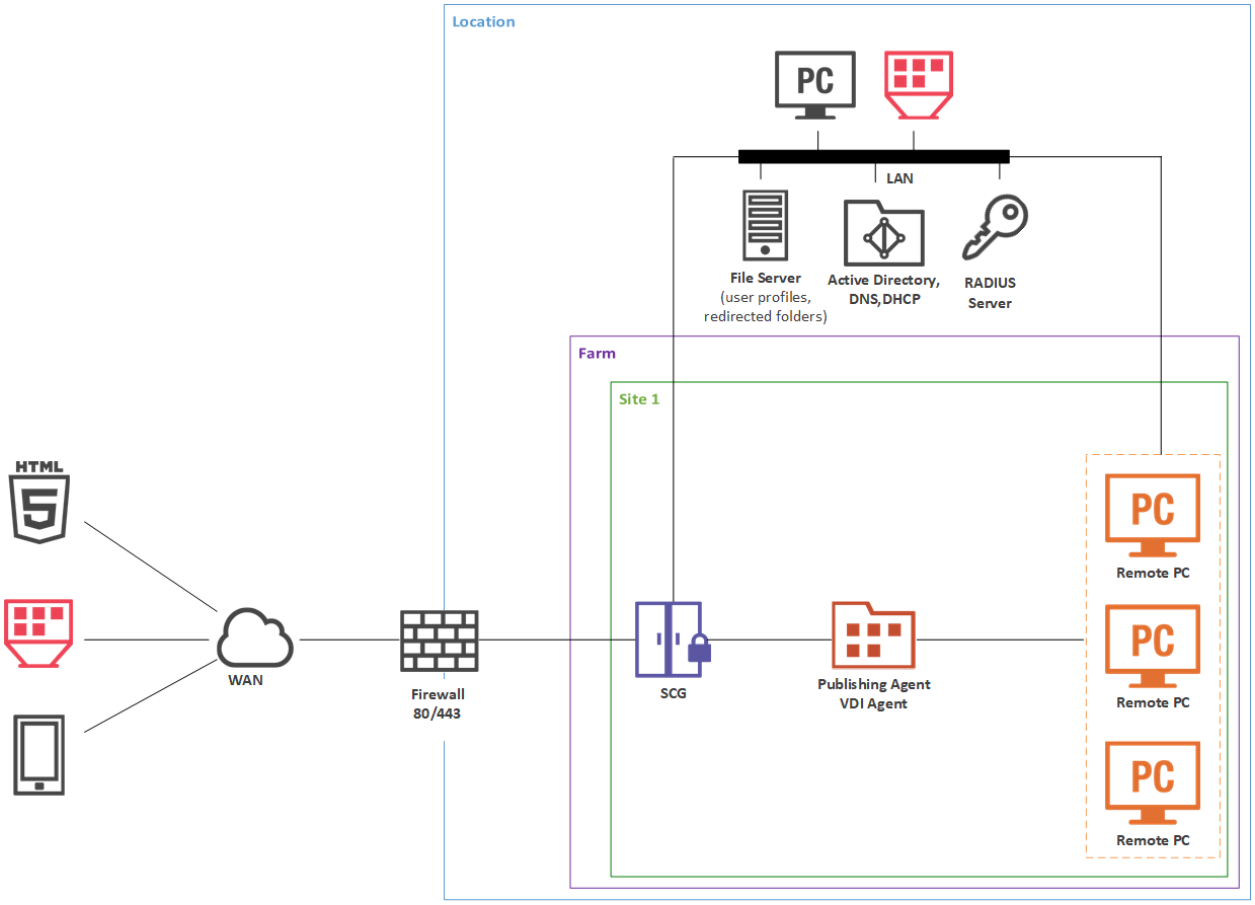
RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

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

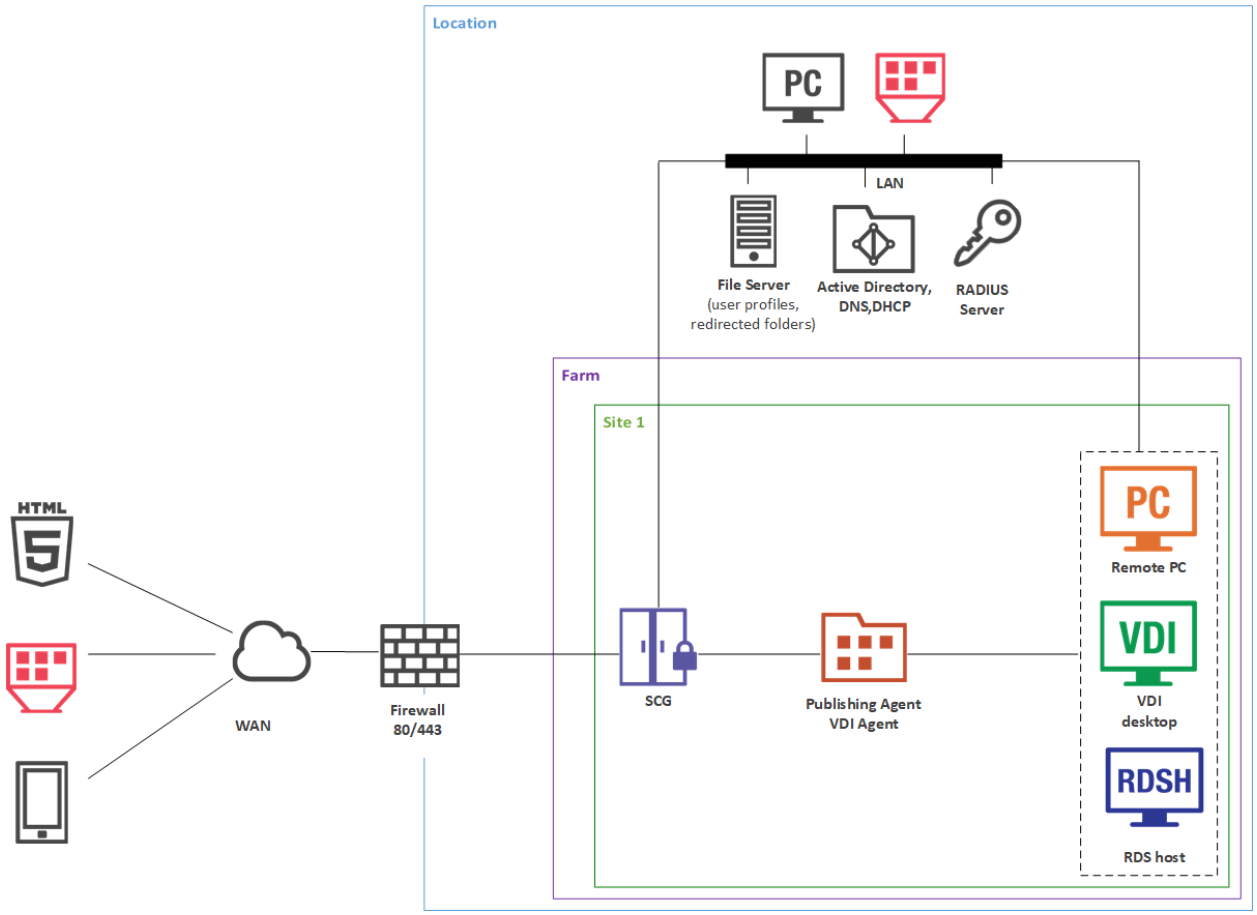
The RAS Guest Agent is used with Remote PC pools instead of the Remote PC Agent. Pool membership is built from either a PC list (manually adding individual PCs or importing the list from a CSV file) or based on an Active Directory OU location (the list is refreshed by the RAS Publishing Agent every 5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

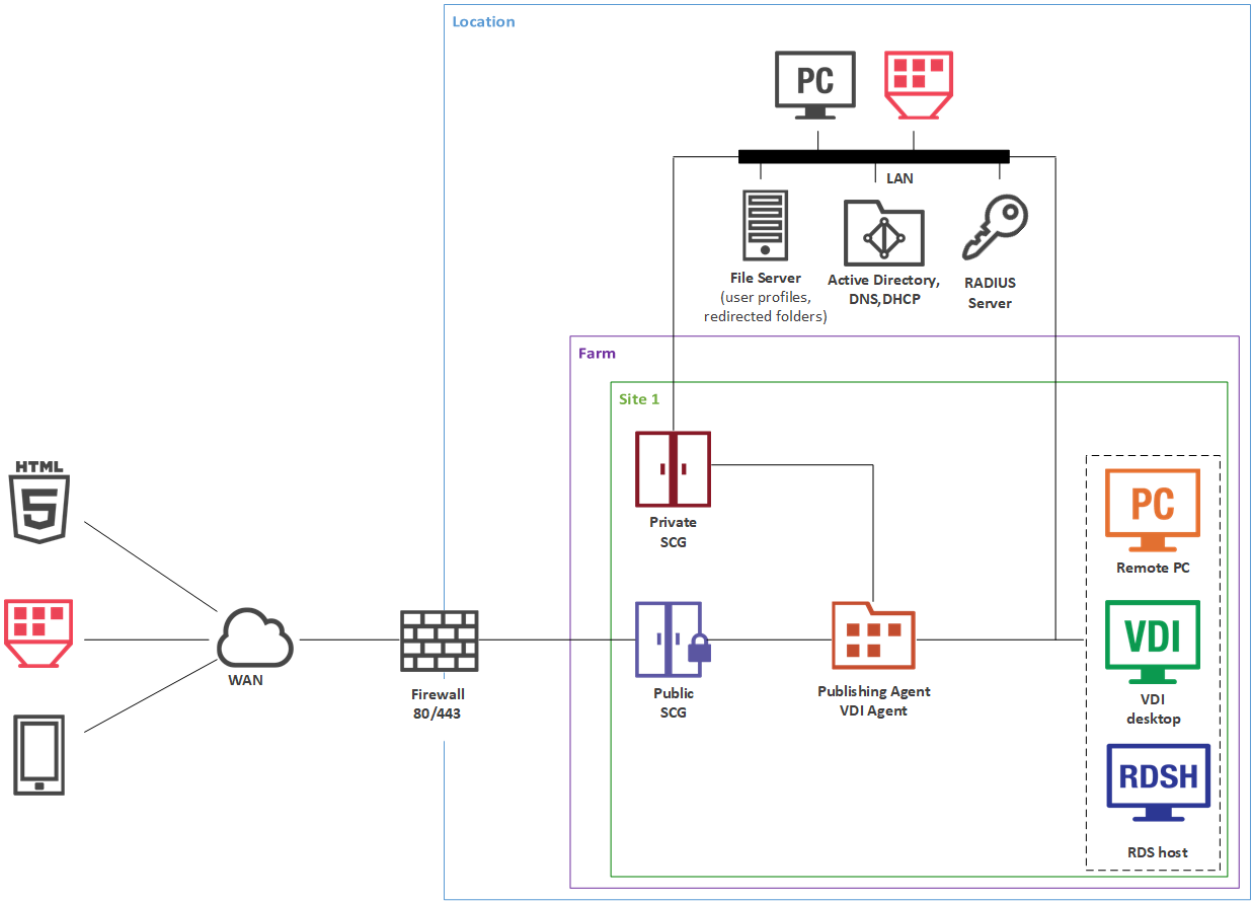
All other components are push-installed from the RAS console.

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

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

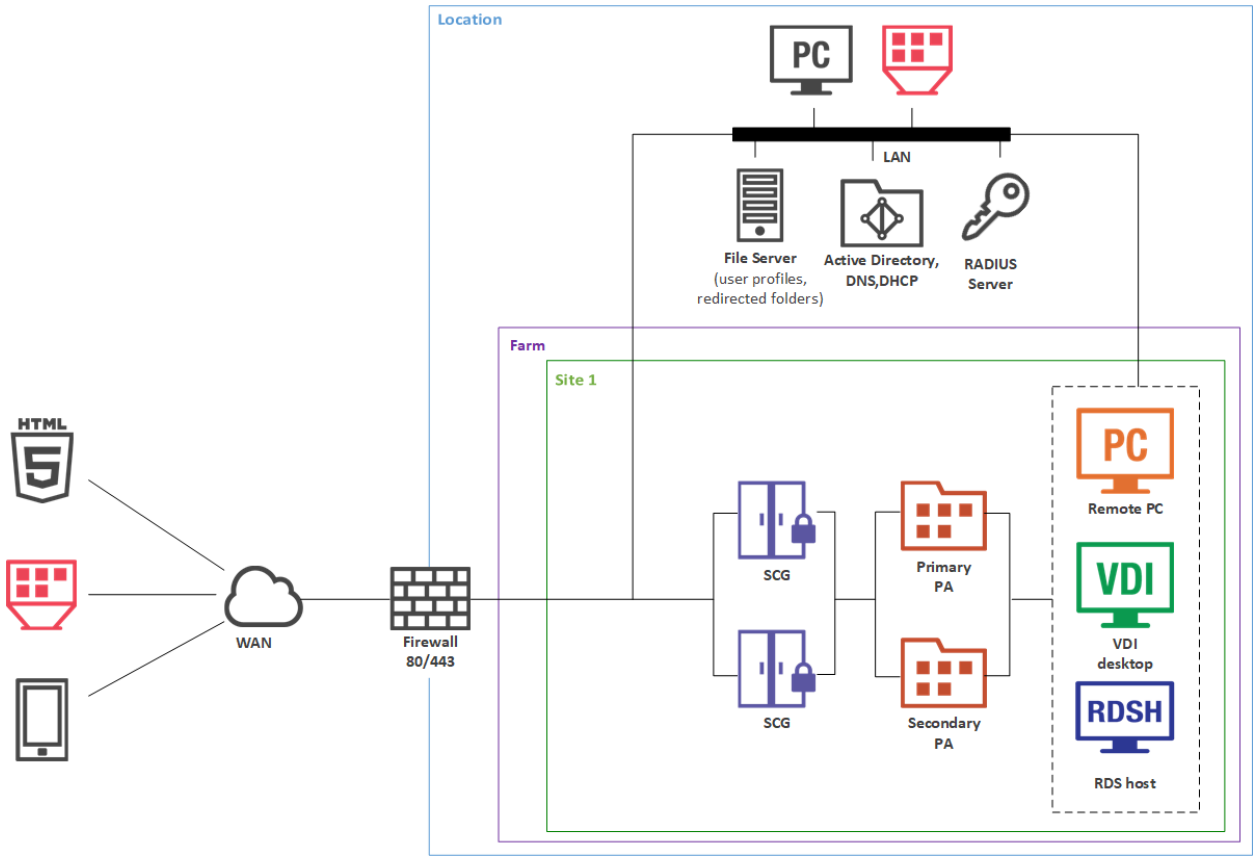
Single Farm with Dual RAS Secure Client Gateways

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 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 RAS 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.

Note: Round-robin DNS load balancing between two Secure Client Gateways works for the TCP protocol only. UDP load balancing may not work properly.



Installation Notes

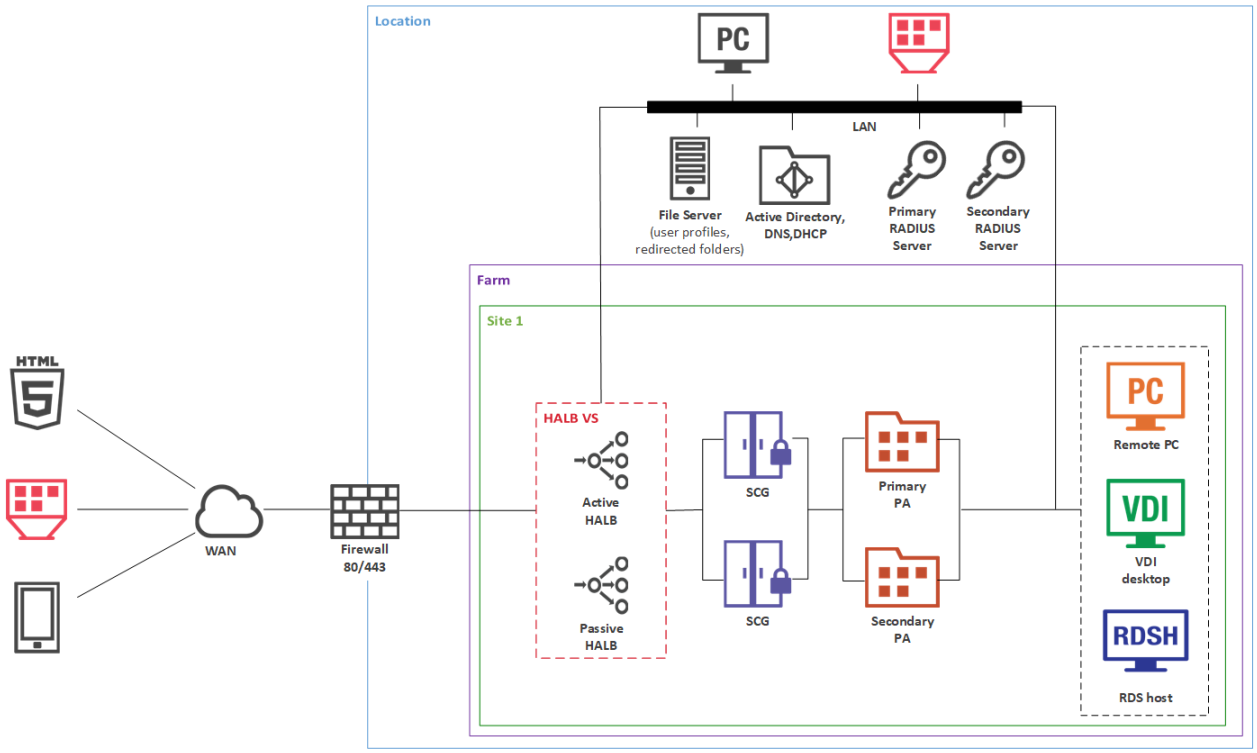
RAS Publishing Agent is installed using the Parallels RAS installer (standard installation).

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 IP address of the HALB VS which represents the HALB virtual appliances in the internal network.



Please note that the diagram above includes an optional secondary RADIUS server which can be used as active/active or active/passive to provide high availability.

See also **Capacity Considerations** (p. 49).

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 and configured in HALB VS properties.

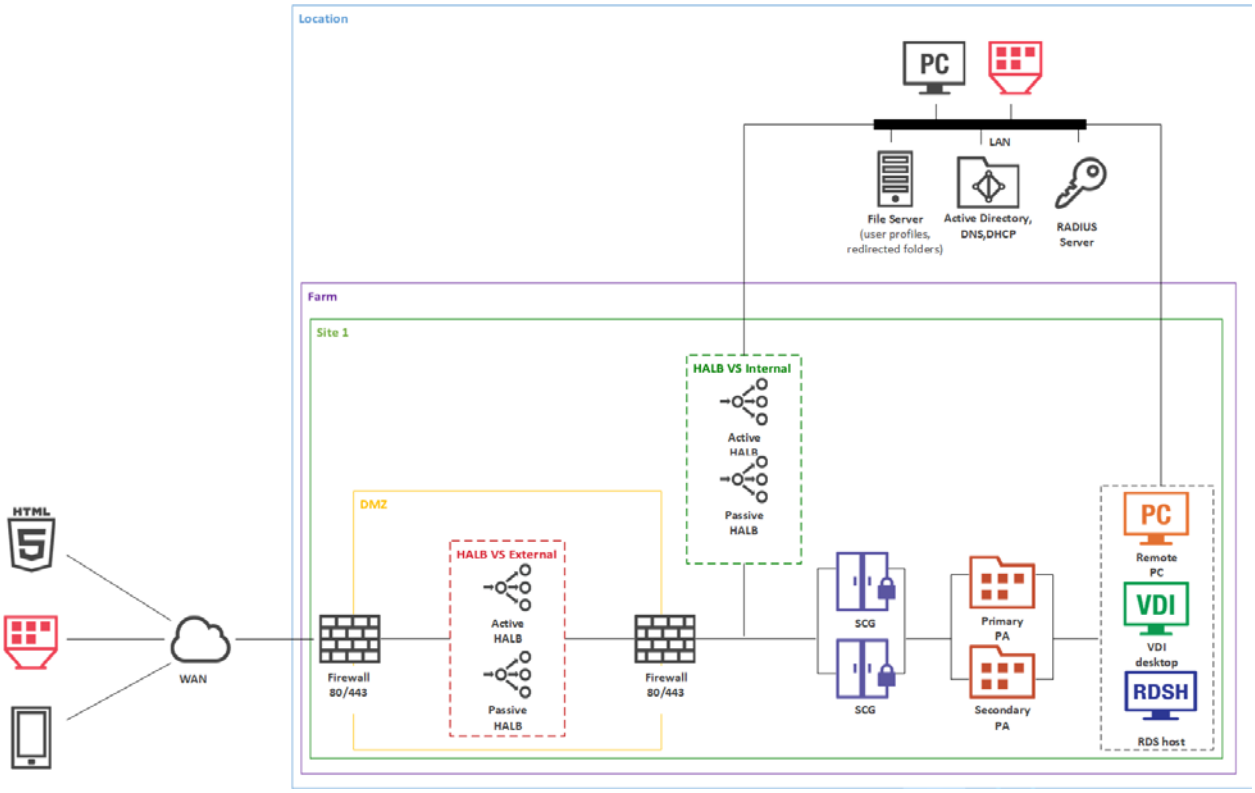
All other components are push-installed from the RAS console.

High Availability with Single-hop or Double-hop DMZ

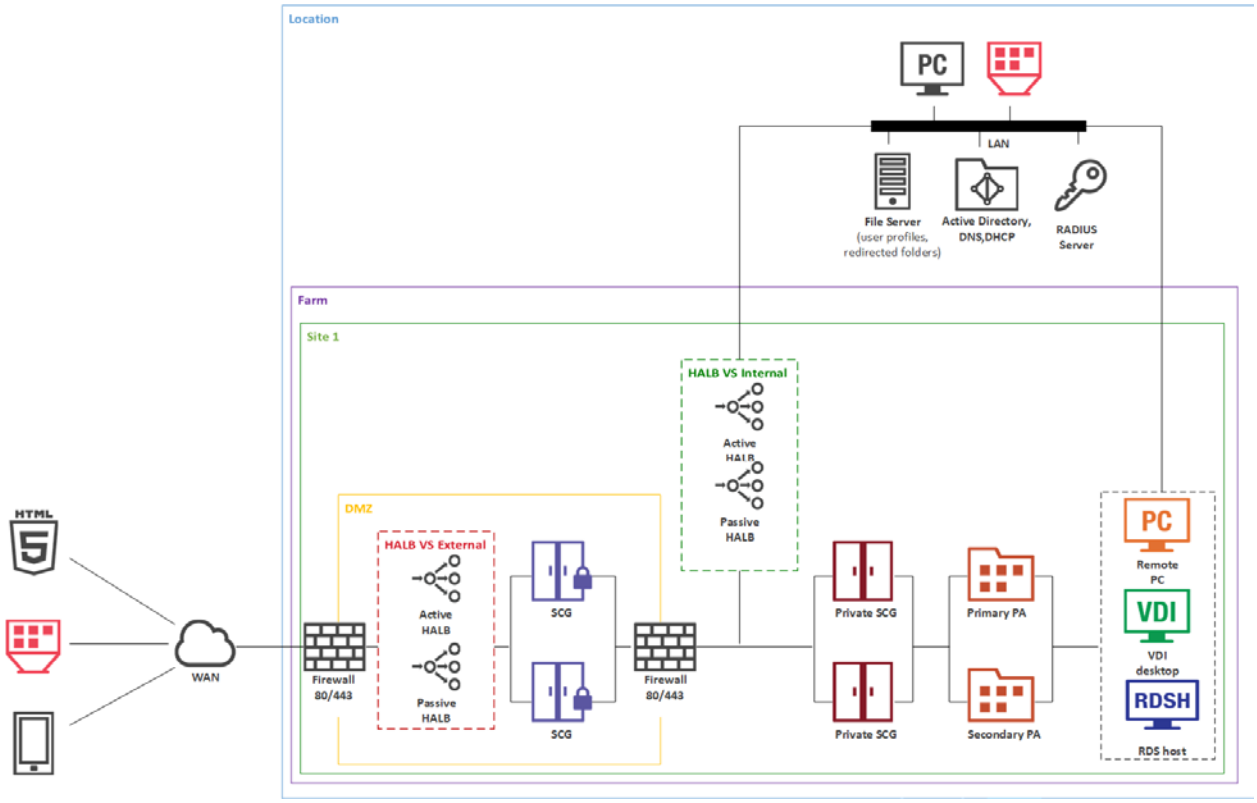
Many companies use the perimeter network (DMZ) to separate the public network with servers that handle exposed services and the internal network with servers that handle internal services. There are two types of DMZ: single-hop and double-hop, with the latter using three firewalls and therefore being more expensive, but more secure (with three firewalls, using different firewall technologies, you can avoid one weakness or one type of attack breaking all firewalls). A firewall between RAS Secure Client Gateways and the intranet must allow gateways and systems to connect to a RAS Publishing Agent using the standard port.

Single-hop DMZ (two firewalls)

In a single-hop 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 of a HALB Virtual Server (HALB VS) representing HALB virtual appliance(s) or other generic protocol load balancing scenarios. Note that in this case two HALB Virtual Servers are used for internal and external traffic load balancing to internal Secure Client Gateways.



To differentiate traffic between internal and external network, you can use public and private gateways (both are equal from the RAS perspective):



In a configuration of this type, HALB appliances installed in front of RAS Secure Client Gateways in the internal perimeter network (DMZ). The WAN users connect to the IP address of external HALBS VS, while LAN users use IP address of the internal HALB VS, which use HALB appliances installed in front of the gateways located in internal network. 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 VS, the second appliance can be deployed for external internal and HALB VS.

Installation Notes

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

HALB is installed as a ready-to-use virtual appliance and configured in HALB VS properties.

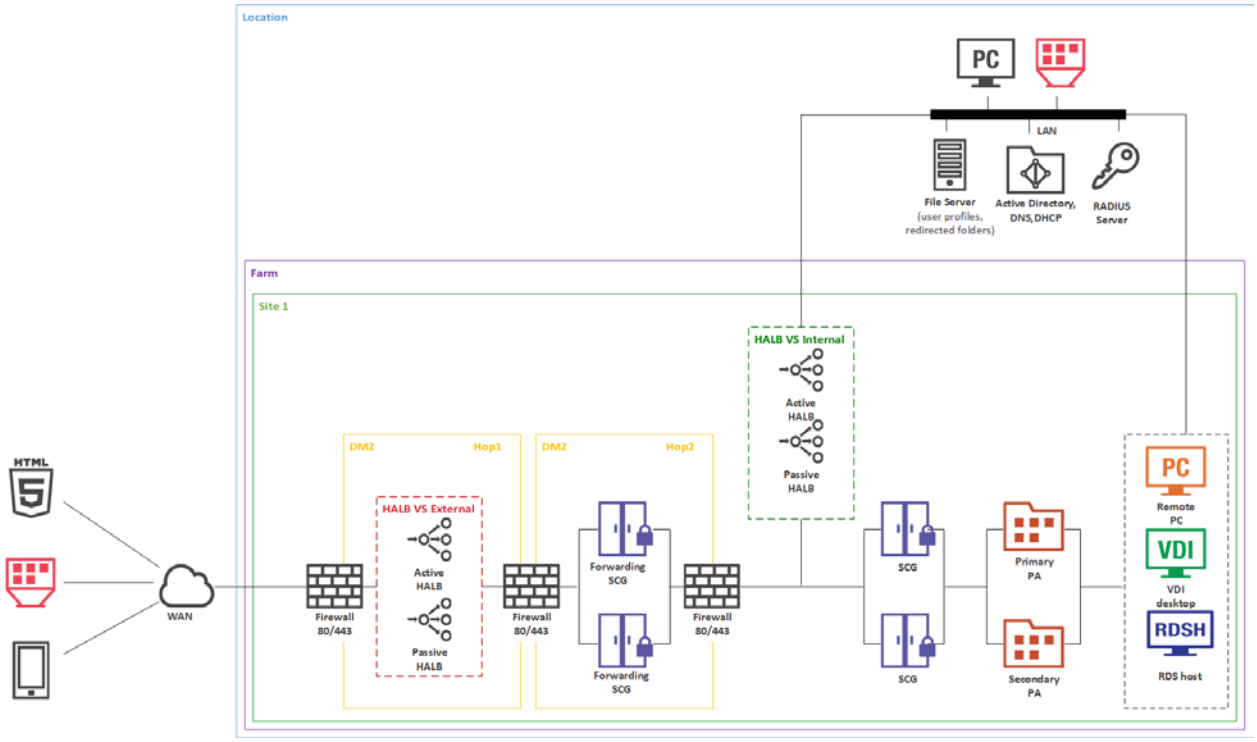
All other components are push-installed from the RAS console.

Double-hop DMZ (three firewalls)

In a double-hop DMZ scenario, settings are simpler and the protection from external malicious agents is higher. Double-hop DMZ requires Forwarding RAS Secure Client Gateways installed in the perimeter network to pass client connections to RAS Secure Client Gateways residing in the internal second perimeter network (the second hop).

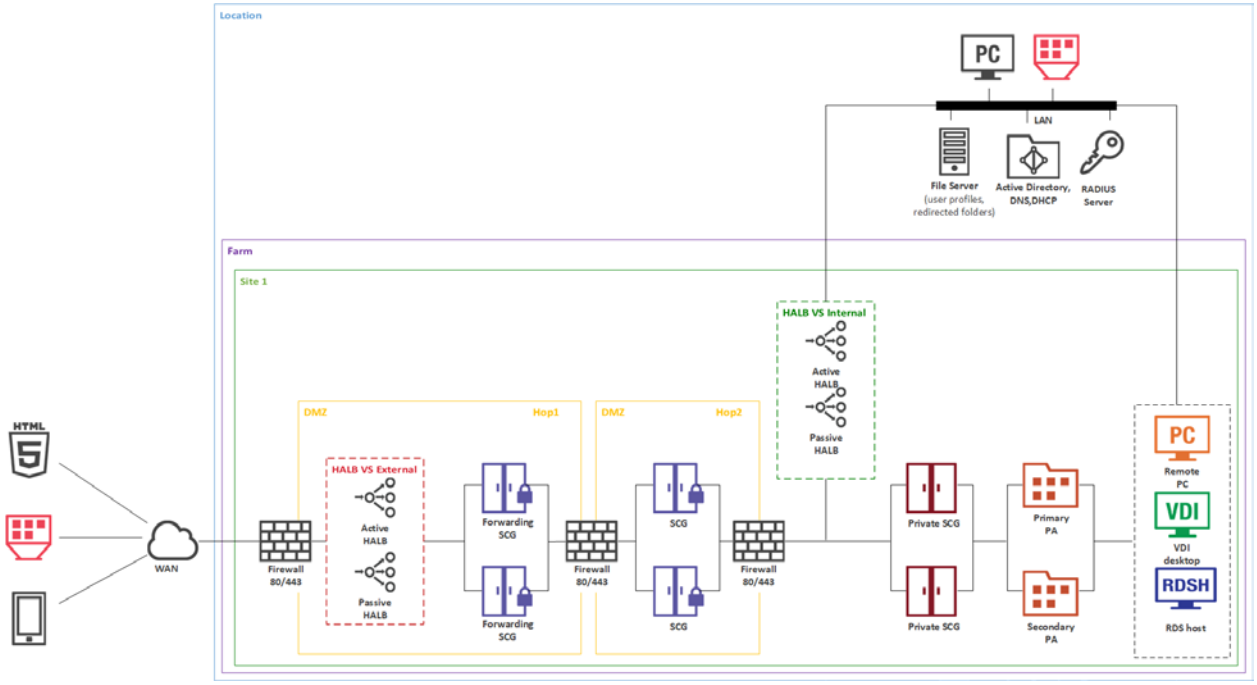
In such configuration, the HALB VS with a HALB pair (primary and secondary) is installed in front of Forwarding RAS Secure Client Gateways in DMZ. WAN users connect to Parallels RAS using the IP address of the HALB VS, while LAN users use IP address of the internal HALB VS, which use HALB appliance installed in front of the gateways located in internal network. 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.



Parallels recommends using Forwarding RAS Secure Client Gateways in double hop DMZ deployments only.

To differentiate traffic between internal and external network, you can use public and private gateways (both are equal from the RAS perspective):



Installation Notes

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

HALB is installed as a ready-to-use virtual appliance and configured in HALB VS properties.

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.

RAS on Microsoft Azure

Please plan your deployment using the following information:

- **Azure regions** — An Azure region is a set of data centers deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Azure gives customers the flexibility to deploy applications where they need to: https://azure.microsoft.com/en-us/global-infrastructure/regions/.

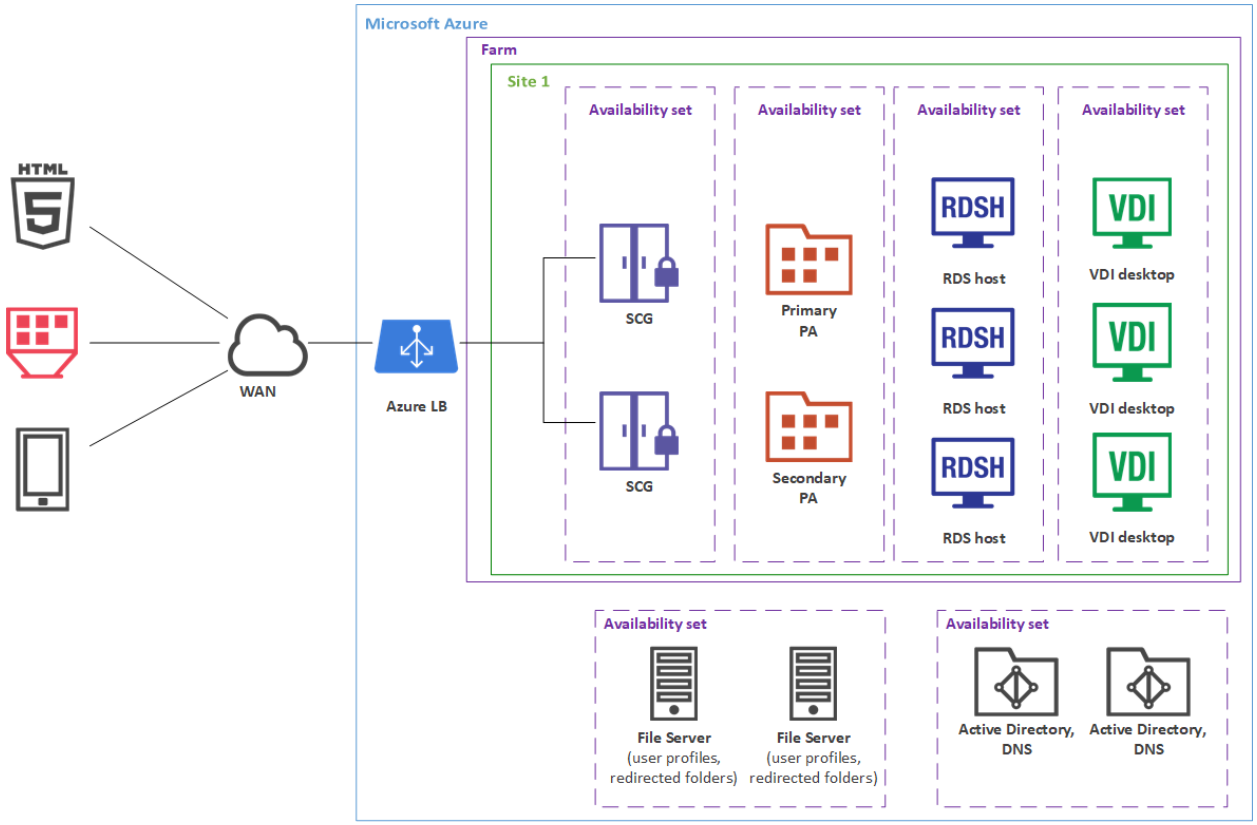
- **Availability Zones** — Availability Zones are physically separate locations within an Azure region. Each Availability Zone is made up of one or more data centers equipped with independent power, cooling and networking. Availability Zones allow customers to run mission-critical applications with high availability and low-latency replication. To ensure resiliency, there's a minimum of three separate zones in all enabled regions: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview .
- **Availability Sets** — An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets .

Please note that Microsoft Azure design is out of scope of this guide.

Parallels RAS provides the two most common scenarios for delivering applications and desktops on Azure. These scenarios are described below.

Parallels RAS infrastructure in the cloud

Parallels RAS infrastructure servers, including RAS Publishing Agents, RAS Secure Client Gateways, RAS Enrollment Servers etc. are located on Azure. Each component of a RAS deployment should be in its own Availability Set to maximize overall availability. For example, a separate Availability Set should be used for Publishing Agents, Secure Client Gateways, Enrollment Servers etc.

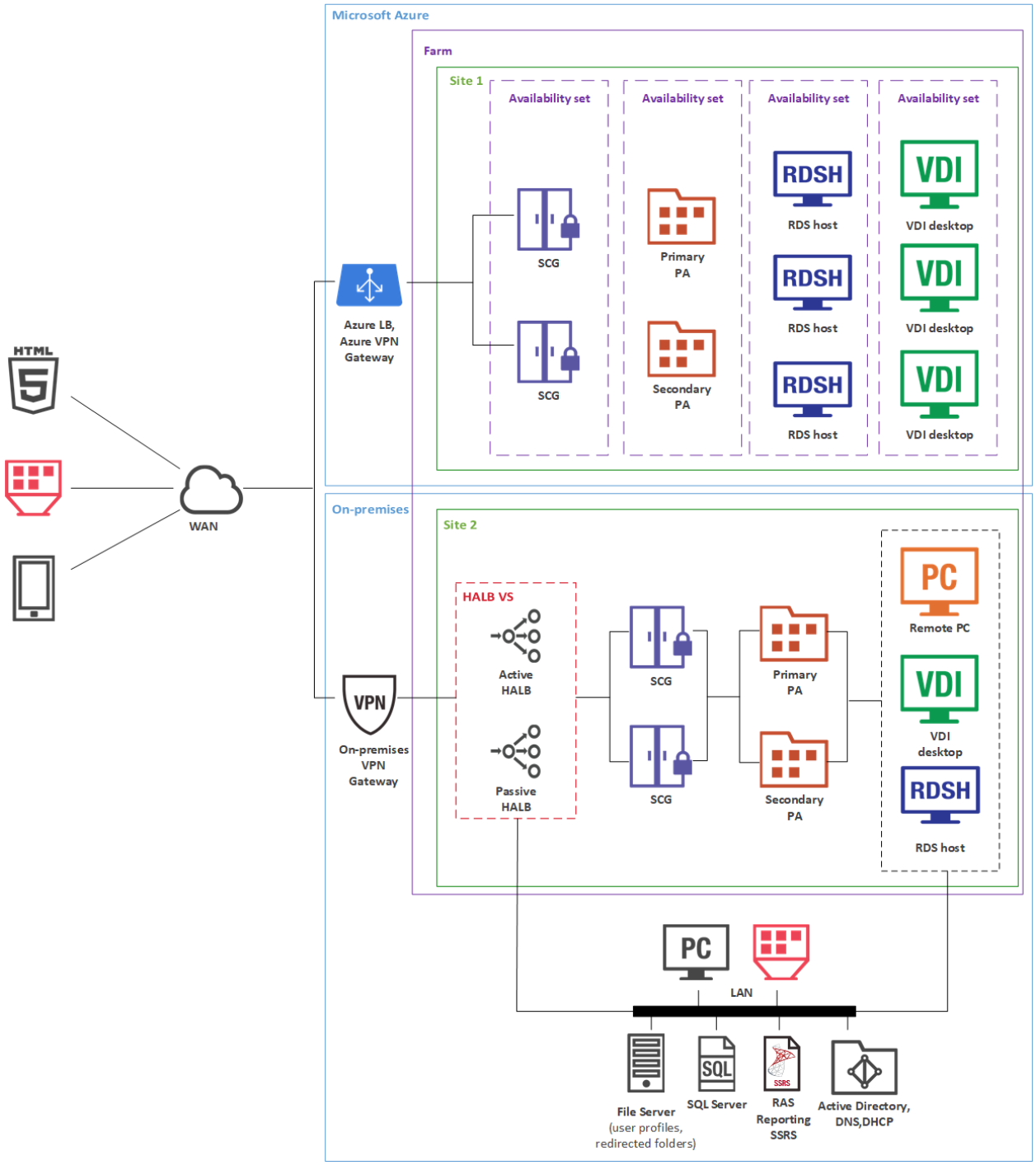


You can also use Azure as a SAML IdP provider and as cloud computing platform for VDI/RDS resource hosts to deliver applications and desktops.

On-premises with backup Site using site-to-site VPN (or Express Route)

Parallels RAS infrastructure servers, including RAS Publishing Agents, RAS Secure Client Gateways, RAS Enrollment Servers etc. are located on premises, whereas VDI/RDSH resource hosts are deployed on Azure in Availability Sets. This can be practical when you need to support burst growth of the usage or business continuity.

Note: A single Farm is used with two Sites.

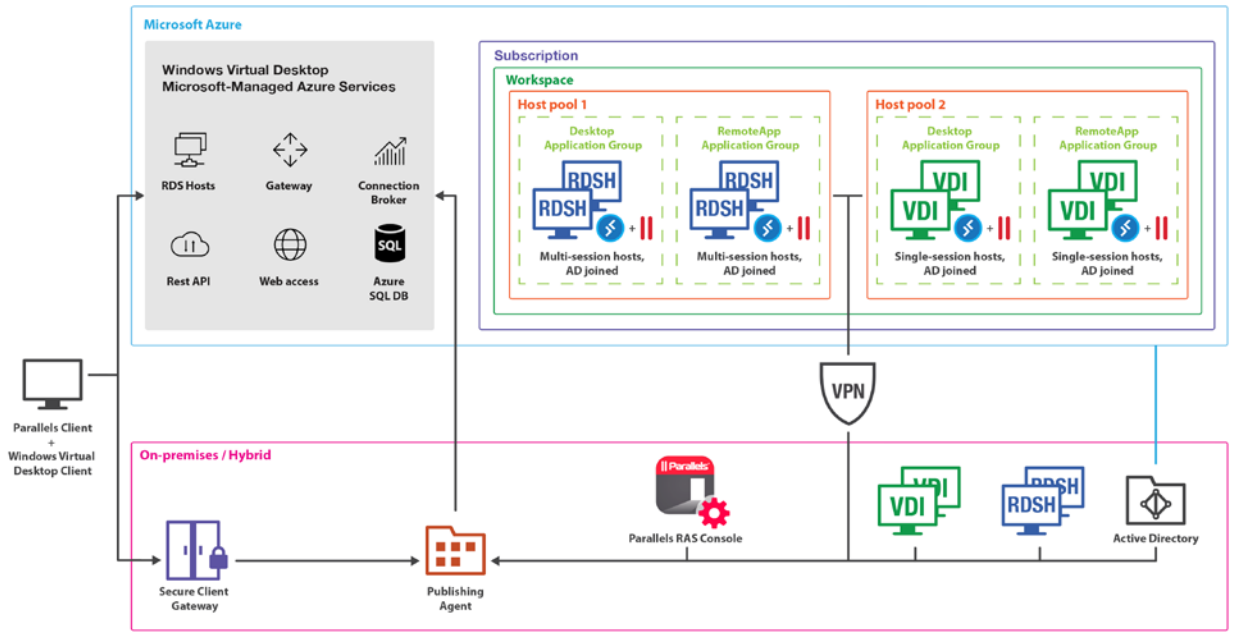


Azure Virtual Desktop integration

Azure Virtual Desktop is a desktop and app virtualization service running on Microsoft Azure, providing access to RD Session Hosts and VDI, including the new offering of Windows 10 and Windows 11 Enterprise multi-session hosts. Parallels RAS provides the ability to integrate, configure, maintain, support and access Azure Virtual Desktop workloads on top of the existing technical capabilities of Parallels RAS.

The diagram below illustrates a hybrid deployment of Parallels RAS and Azure Virtual Desktop with the following characteristics:

- Workload hosts are available both on-premises through standard Parallels RAS deployment and on Microsoft Azure through the service.
- Azure Virtual Desktop objects such as workspaces, host pools, desktop and RemoteApp groups are created and configured from the Parallels RAS Console.
- Azure Virtual Desktop hosts (multi-session or single-session) contain both Azure Virtual Desktop Agent and RAS Agent for management and configuration purposes.
- Parallels Client for Windows is connecting to both Parallels RAS Secure Client Gateway and Azure Virtual Desktop service providing resource availability to end-users from a single interface.



As highlighted earlier, the complete Parallels RAS environment can also reside on Microsoft Azure for a full cloud deployment with Azure Virtual Desktop.

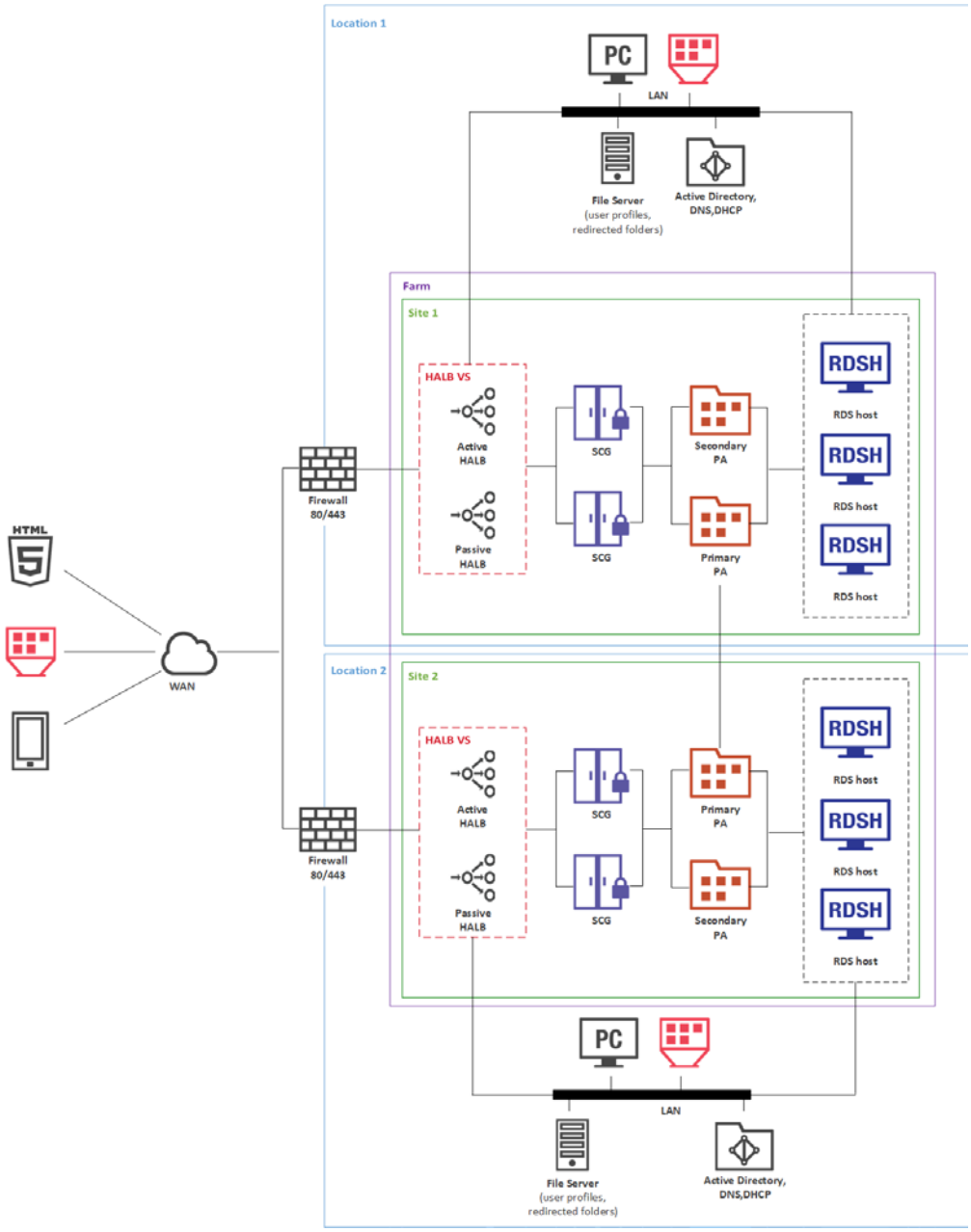
Extended values and capabilities

- Simplify and enhance Azure Virtual Desktop deployment and management.
- Unify administration and UX – single pane of glass – Parallels Clients and Parallels RAS Console.
- Extend reach with flexibility to use hybrid and multi-cloud deployments.
- Automate and streamline administrative routines, provisioning, and management of Azure Virtual Desktop workloads.
- Built in Auto-scale capability on Microsoft Azure and/or on-premises.
- Management of users, sessions, and processes.
- Utilize RAS Universal Printing and Scanning.
- Utilize AI based session prelaunch for ultra-fast logons.
- Accelerated file redirection with the use of the **Enable drive cache redirection** option.
- Integrated automatic image optimizations and FSLogix Profile Containers.
- Client management.
- Security policies for clients.
- Leverage RAS Reporting and Monitoring from the RAS Console.

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 VS IP address of Site2.

LAN users of Site2

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

WAN users

- Primary connection - HALB VS IP address of Site1
- Secondary connections - HALB VS IP 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 and configured in HALB VS properties.

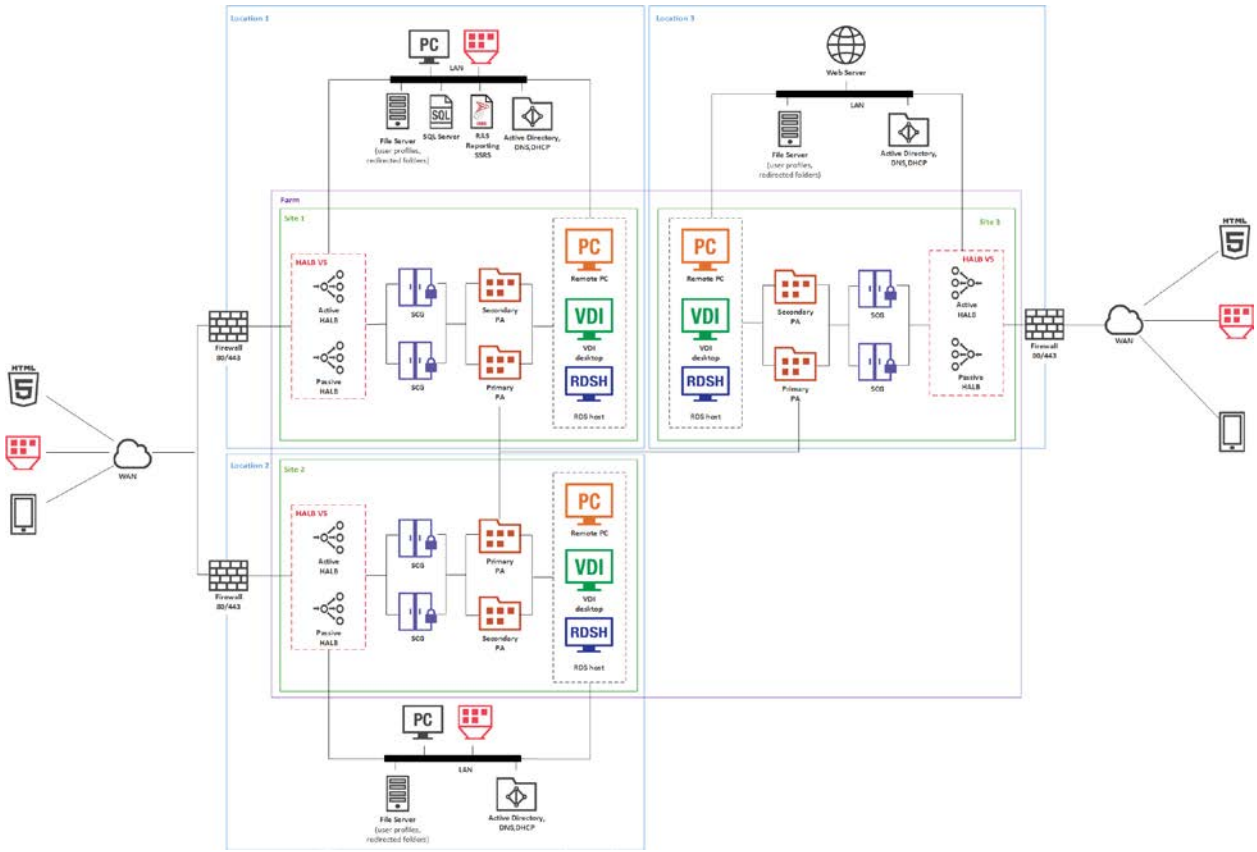
All other components are push-installed from the RAS console.

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 all sites and setup HALB VS IP address of the first site as Server Address and HALB VS IP address of the second and third sites 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

Primary 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 and configured in HALB VS properties.

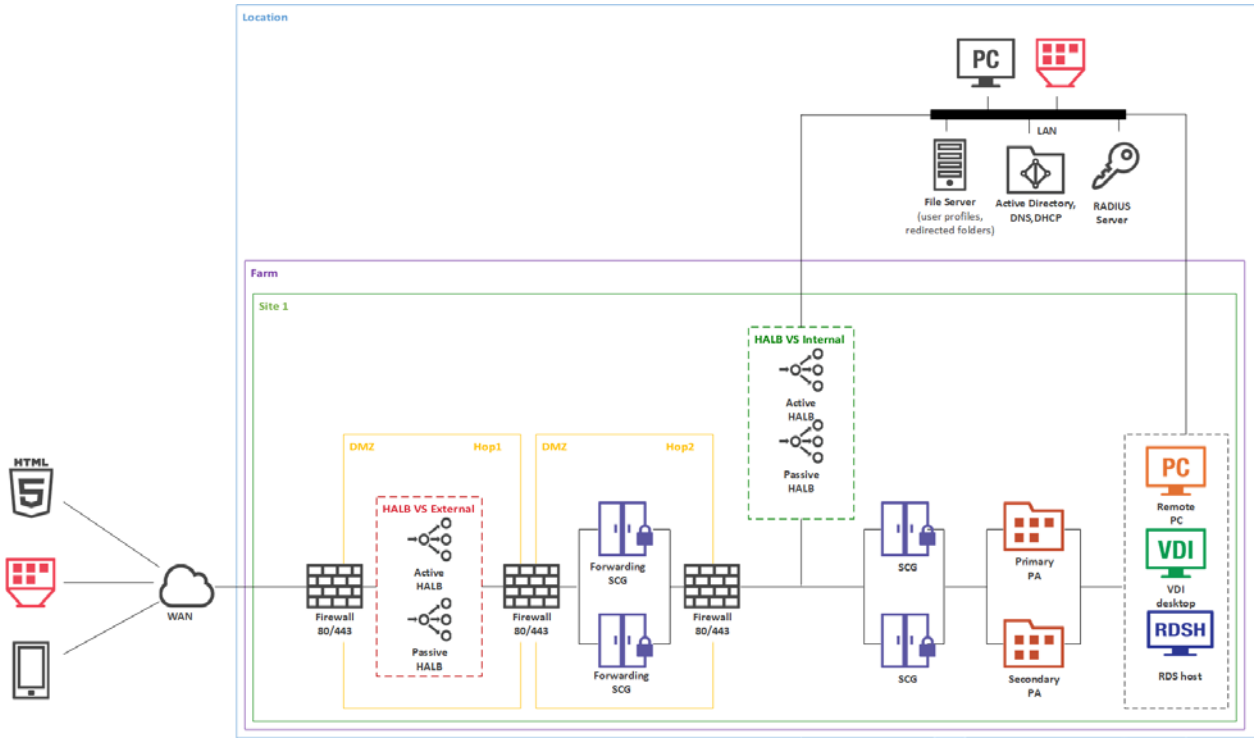
All other components are push-installed from the RAS console.

Secure Setup with Double-hop 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, RADIUS, or Google authenticator.

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.

It is recommended to specify Access Control Lists to only allow the IP addresses and protocols/ports necessary for the Wireless Access Points and other devices to communicate with the RADIUS server. No other devices should have a pathway to the RADIUS server.



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 the username and password or a smart card.

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.

HALB is installed as a ready-to-use virtual appliance and configured in HALB VS properties.

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

SAML SSO authentication

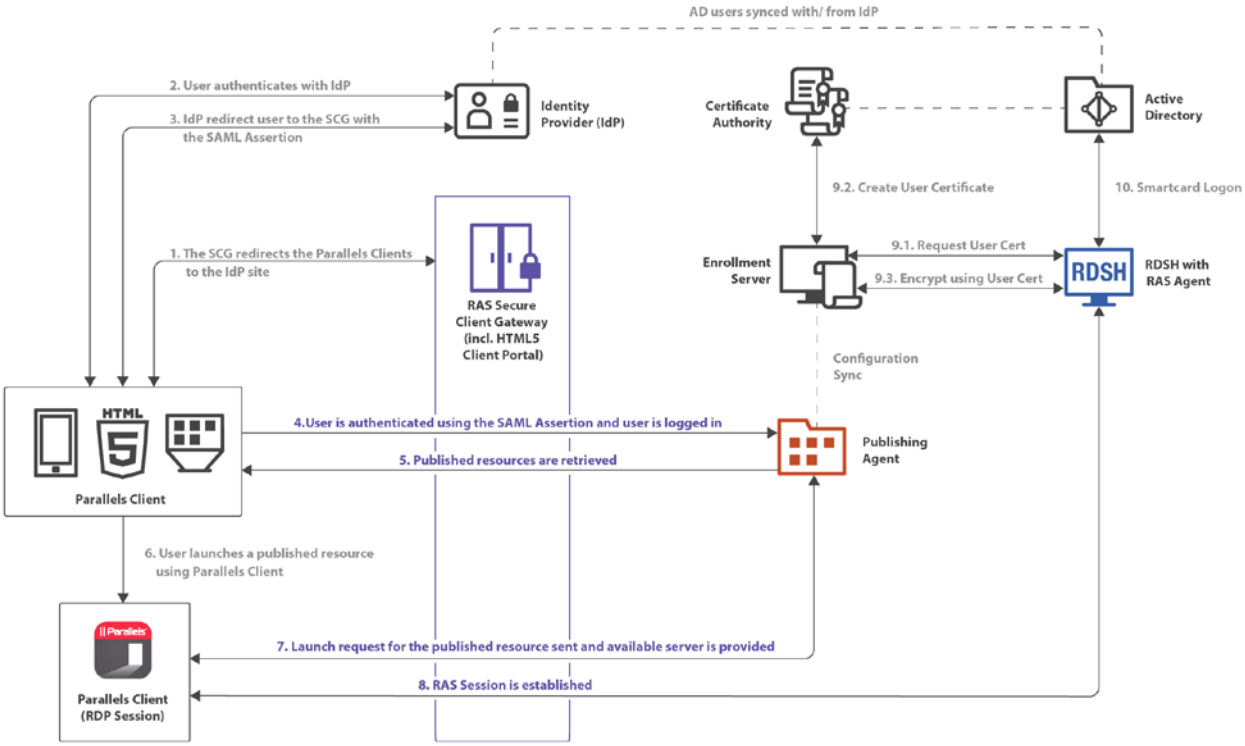
SAML authentication allows Service providers and enterprises with multiple subsidiaries to reduce costs by offload the Identity Management burden to the identity providers. Integrating with third party Identity Providers allows customers and partners to provide end users with a true SSO experience.

Comparing to previously described scenarios, the new server role needs to be added the Farm. As part of the SAML SSO process, the new host with RAS Enrollment Server component communicates with Microsoft Certificate Authority (CA) to request, enroll, and manage digital certificates on behalf of the user to complete authentication without requiring the users to put in their Active Directory credentials.

Parallels RAS supports the following delivery options:

- HTML5 Client
- HTML5 Client portal initiated SAML for Windows
- HTML5 Client Portal initiated SAML for Mac and Linux
- HTML5 Client Portal initiated SAML for Android and iOS
- Parallels Client for Windows initiated SAML Authentication
- Parallels Client for Mac initiated SAML Authentication

The below high-level logical diagram depicts SAML authentication and login process within a Parallels RAS environment:



The SAML authentication and login steps on the diagram above are:

1 RAS Secure Client Gateway redirects the Parallels Client login request to the IdP site.

2 The user authenticates with IdP.

3 IdP redirects the user to the RAS Secure Client Gateway with the SAML Assertion.

4 The user is authenticated using the SAML Assertion and the user is logged in.

5 The list of the available RAS published resources is retrieved.

6 The user chooses a published resource and launches it from Parallels Client.

7 The launch request from the user is sent to the server side and the resource is started on the available server.

8 A Parallels RAS session is established.

9 User certificate is processed:

- Certificate is requested.
- Certificate is created.
- Encryption is preformed using the certificate.

10 Smartcard logon.

Client Manager and Desktop Replacement

The Client Manager feature allows the administrator to convert Windows devices running Windows 7 and newer 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.

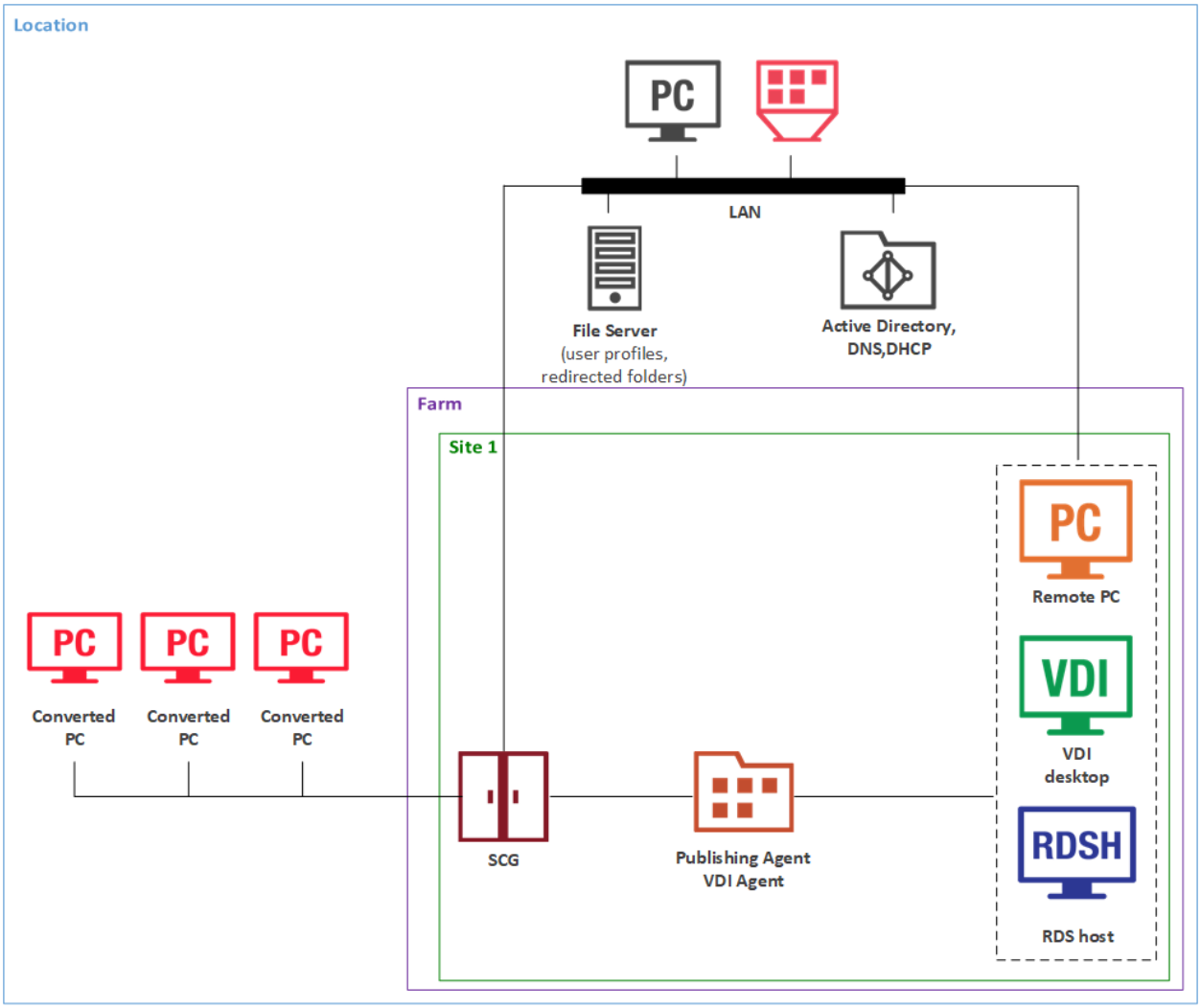
Shadowing

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.

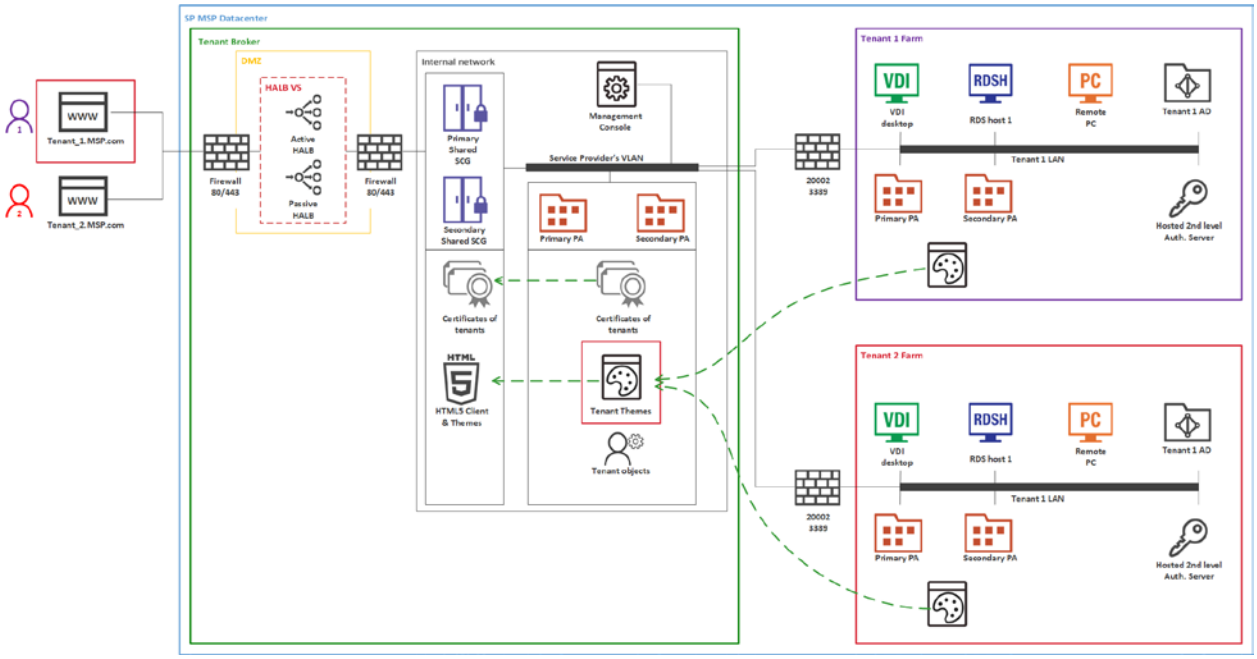
Parallels Client is installed on client desktop computers and converted Windows PCs using the Parallels Client installer.

Multi-Tenant Architecture

This scenario is suited for environments where it is necessary to keep published resources of distinct clients (departments, groups, teams, etc.) isolated. Parallels RAS Multi-Tenant architecture enables organizations to share the RAS infrastructure components among different tenants while keeping client data segregated and reducing costs.

The RAS Multi-Tenant architecture offers the following advantages to Service Providers and organizations:

- Cost savings due to reduction of number of RAS Secure Client Gateways and High Availability Load Balancers (HALBs) while maximizing resource usage and consolidation.
- Faster onboarding of new tenants/customers.
- Simplified centralized management of multi-tenant environments.
- Extended market reach through reduction of operational costs for organizations of any size by allowing cost scaling through shared infrastructure.



- Tenants are deployed as separate individual RAS Farms or Sites.
- A Tenant Farm doesn't need its own RAS Secure Client Gateways and HALB. However, deployments with Gateways and HALB are possible if a Tenant needs them for internal connections.
- All external users connect to a Tenant Farm through the Tenant Broker infrastructure.

- The network configuration of a Tenant requires the Tenant Publishing Agent to Tenant Broker Publishing Agent connectivity. Additionally, shared RAS Secure Client Gateways need to communicate with servers hosting published resources and the Tenant Publishing Agent. These communications require only a limited number of open ports, which are listed below:
  - Tenant Publishing Agent > Tenant Broker Publishing Agent: port 20003
  - Tenant Broker Gateway > Tenant Broker Publishing Agent: port 20002
  - Tenant Broker Gateway > Tenant Publishing Agent: port 20002
  - Tenant Broker Gateway > Servers hosting published resources: port 3389
- Communications with a Tenant domain are always performed from a local Tenant Publishing Agent and never from the Tenant Broker infrastructure.
- Every Tenant must have a unique public domain address. Multiple unique domain addresses, however, can resolve to the same IP address.

Installation Notes

RAS Publishing Agent on the Tenant Broker is installed from the Parallels RAS installer using the Tenant Broker installation option.

RAS Publishing Agent on a Tenant is installed from the Parallels RAS installer using standard installation.

HALB is installed as a ready-to-use virtual appliance and configured in HALB VS properties.

All other components are installed remotely from the RAS console:

- Tenant Broker components are installed from the Tenant Broker console.
- Tenant components are installed from the Tenant console.

CHAPTER 3

Capacity Considerations

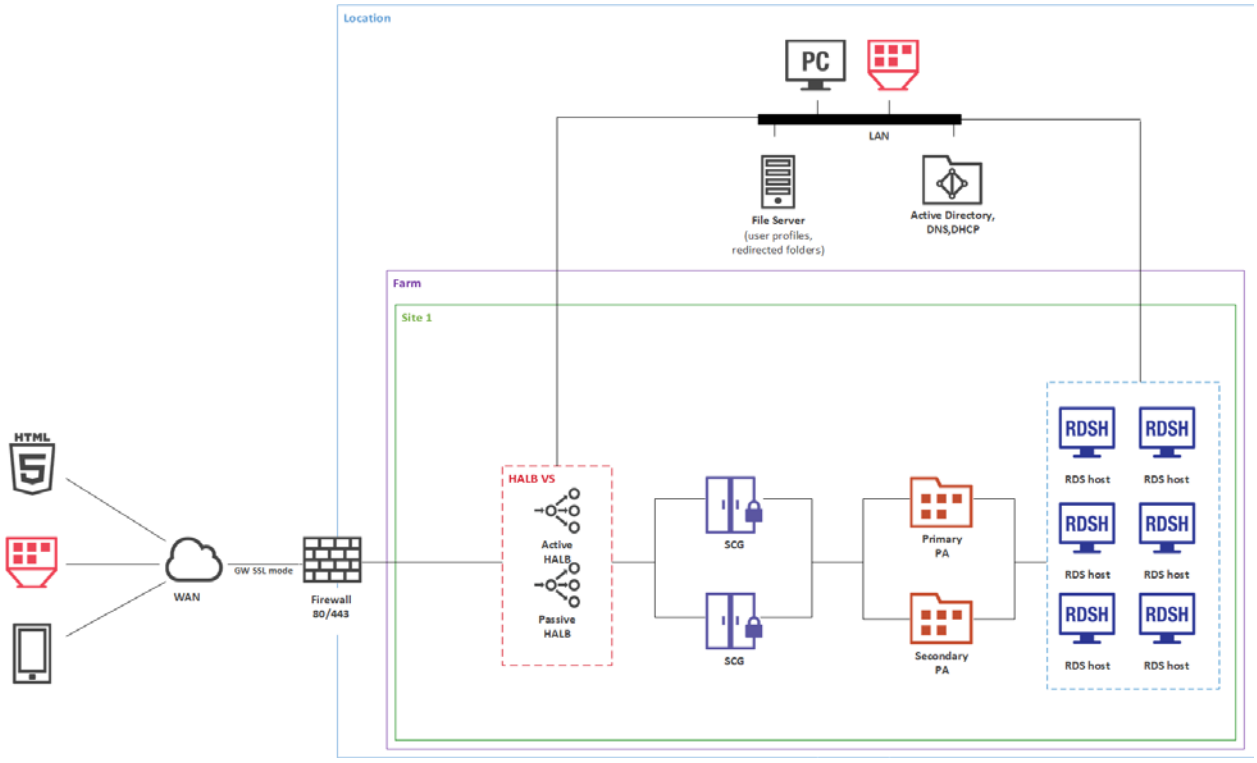
Parallels conducted in-house Parallels RAS scalability testing using a total of two HP DL360 consisting of the following hardware components:

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/v18/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

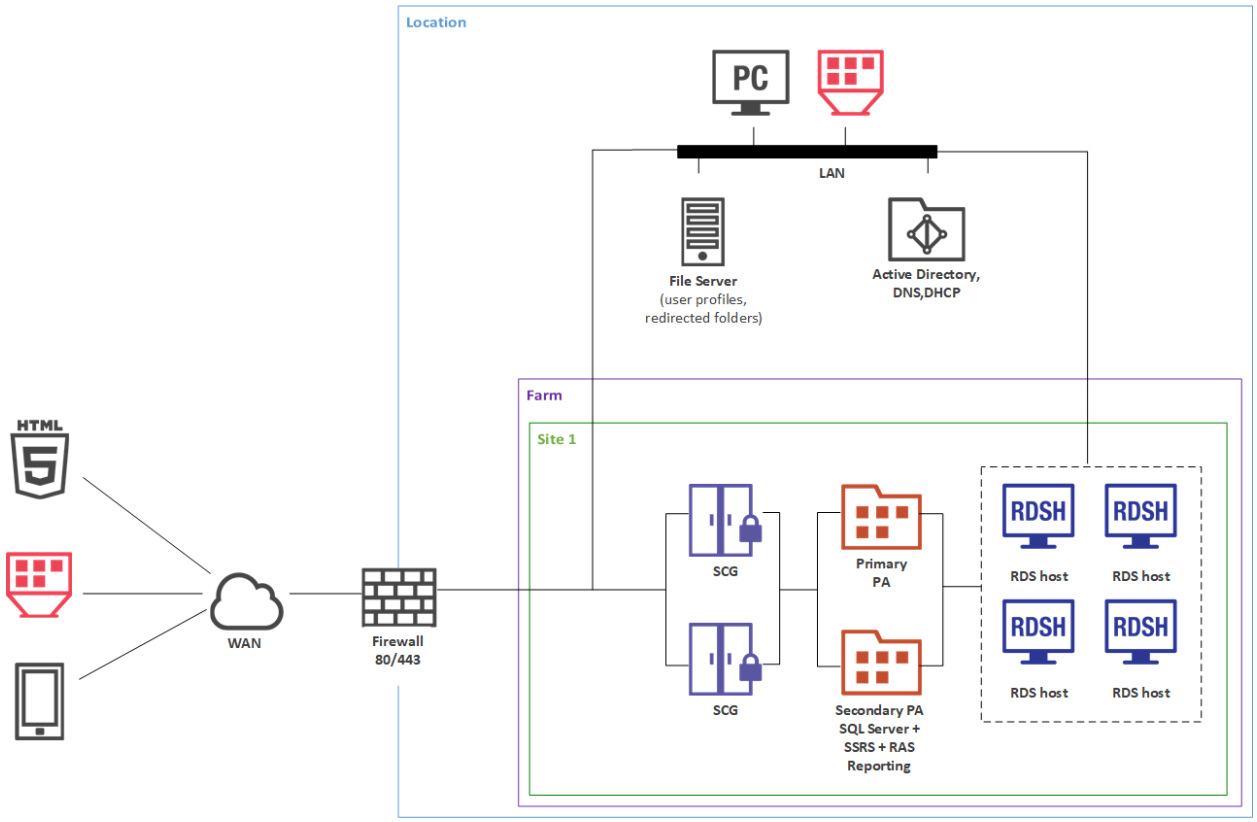
Deploying Parallels RAS Reporting

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

In This Chapter

One Site with Multiple RD Session Hosts

RAS Reporting relies on Microsoft SQL Server and SQL Server Reporting Services (SSRS). In small environments, a SQL Server database instance, SSRS and RAS Reporting can be installed on the same server where primary RAS Publishing Agent is running.



Installation Notes

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

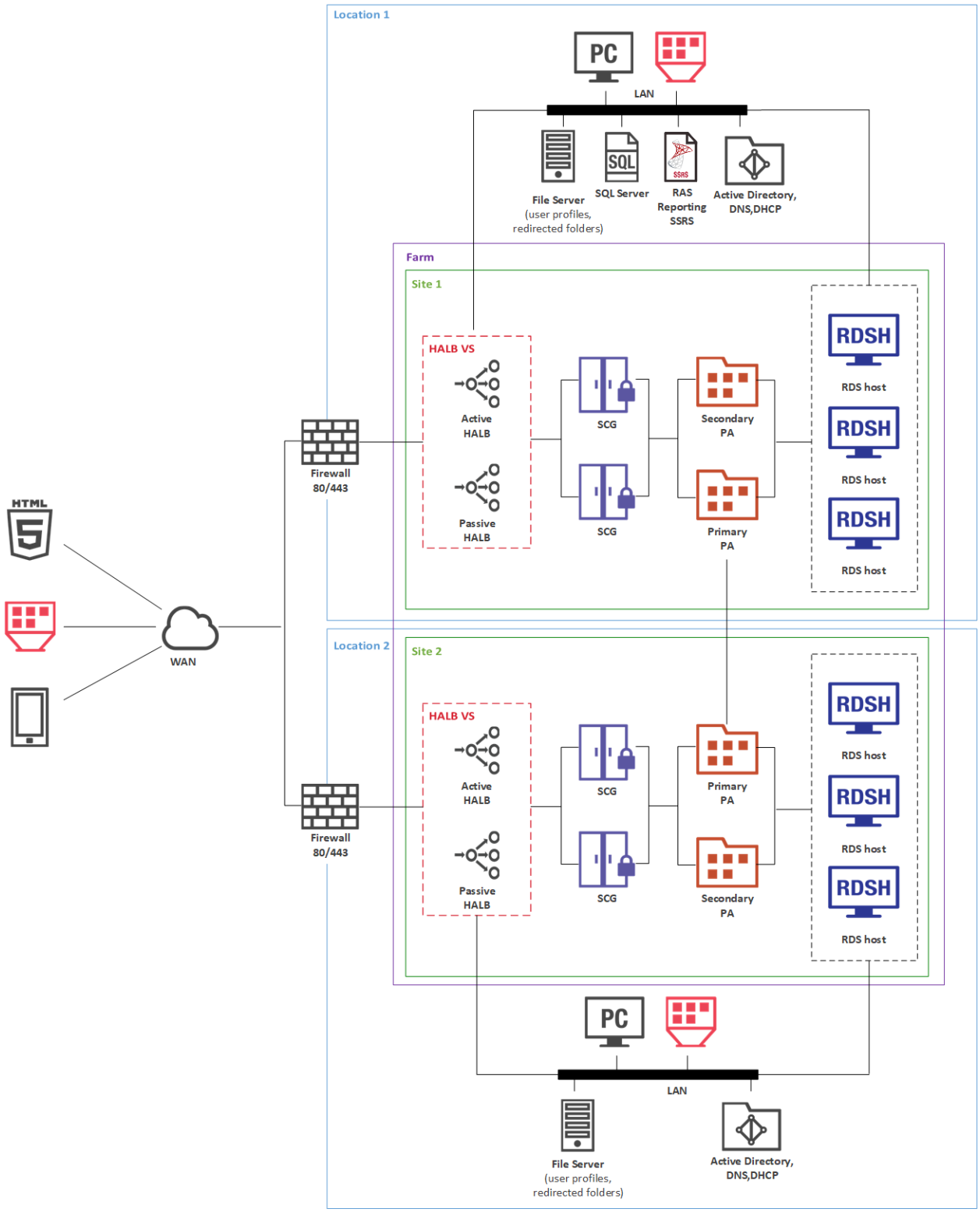
Secondary RAS Publishing Agent is push-installed from the RAS console.

RAS Reporting is installed using Parallels RAS installer.

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

Multiple Sites with Multiple RD Session Hosts and Remote SQL Server

For Parallels RAS installations running in a multi-server environment, it is recommended to install RAS Reporting and SSRS on a dedicated server. SQL Server database engine should also be installed on a dedicated server but can be installed together with SSRS and RAS Reporting.


Location 1
PC
LAN
File Server
(user profiles,
redirected folders)
SQL Server
RAS
Reporting
SSRS
Active Directory,
DNS,DHCP
Farm
Site 1
HALB VS
Active
HALB
Passive
HALB
SCG
SCG
Secondary
PA
Primary
PA
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
HTML
WAN
Location 2
Site 2
HALB VS
Active
HALB
Passive
HALB
SCG
SCG
Primary
PA
Secondary
PA
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
PC
LAN
File Server
(user profiles,
redirected folders)
Active Directory,
DNS,DHCP

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.

HALB is installed as a ready-to-use virtual appliance and configured in HALB VS properties.

RAS Reporting is installed using Windows installer.

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

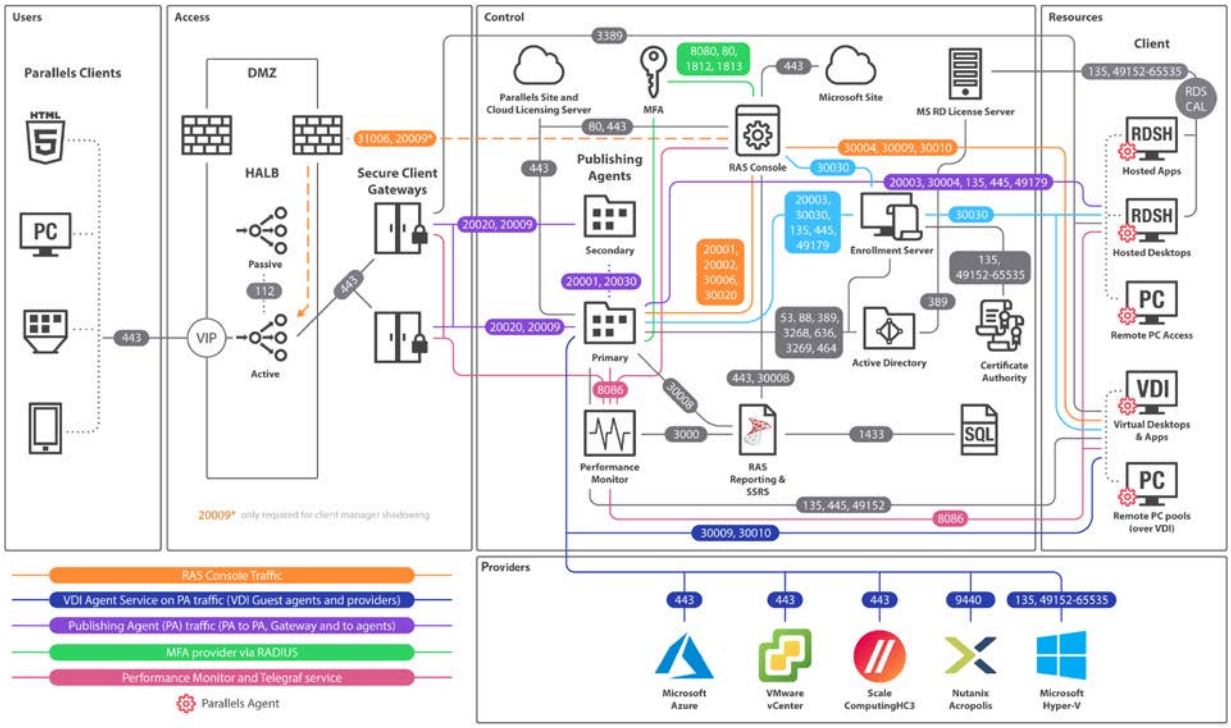
CHAPTER 5

Port Reference and SSL Certificates

In This Chapter

Port reference

The following diagram illustrates communication ports used in Parallels RAS.



The above diagram include SAML SSO components such as RAS Enrollment Server, however it does not include Tenant Broker.

Tip: If you are reading the PDF version of this guide, click the following link to view the full-sized diagram in a web browser: https://download.parallels.com/ras/v18/docs/en_US/Parallels-RAS-18-Administrators-Guide/index.htm#47092.

Parallels Client

Source	Destination	Protocols	Ports	Description
Parallels Client	HALB	TCP, UDP TCP, UDP	80, 443 20009	Management and user session connections. Device Manager shadowing via Firewall (indirect network connection).
	RAS Secure Client Gateway Forwarding mode	TCP, UDP TCP, UDP UDP	80, 443 3389 20000	Management and user session connections. Optional - Used for user session if RDP load balancing is enabled (Standard RDP). Secure Client Gateway lookup broadcast.
	RAS Secure Client Gateway Normal mode	TCP, UDP TCP, UDP TCP, UDP UDP	80, 443, 3389 20009 20000	Management and user session connections. Optional - Used for user session if RDP load balancing is enabled (Standard RDP). Device Manager shadowing via Firewall (indirect network connection) Secure Client Gateway Lookup Broadcast
	Session host (VDI, RDS, RemotePC)	TCP, UDP	3389	Used for user session connections in Direct Mode only. RDP connection is always encrypted.
	Azure Virtual Desktop Services	TCP UDP	443 3390	Azure Virtual Desktop Gateway connection Used for user session connections in ShortPath mode only.
	Microsoft site	TCP	443	Download Microsoft Remote Desktop (MSRDC) client
	Parallels site	TCP	80, 443	Check for updates and download Parallels Client

Web browsers

Source	Destination	Protocols	Ports	Description
Web browser (HTML5)	RAS Web Admin Service [RAS Management Portal]	TCP	20443	Admin access to HTML5 based Management Portal of RAS environment
	HALB	TCP	443	End-user access to Parallels RAS HTML5 Client (on Secure Client Gateway in Normal mode) through the HALB
	RAS Secure Client Gateway	TCP	443	End-user access to Parallels RAS HTML5 Client (on Secure Client Gateway in Normal mode)

HALB

Source	Destination	Protocols	Ports	Description
HALB	HALB	VRRP	112	HALB to HALB communication used for automatic assignment of VIP to active HALB.
	RAS Secure Client Gateway in Forwarding Mode	TCP, UDP	80, 443	Management and user session connections.
	RAS Secure Client Gateway in Normal Mode	TCP, UDP TCP, UDP	80, 443 20009	Management and user session connections. Device Manager shadowing via Firewall (indirect network connection).

RAS Secure Client Gateway

Source	Destination	Protocols	Ports	Description
RAS Secure Client Gateway in Forwarding mode	RAS Secure Client Gateway in Normal mode	TCP, UDP TCP, UDP	80, 443 3389	Management and user session connections. Optional - Used for user session if RDP Load Balancing is enabled.
	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 TCP, UDP	20002 20009	RAS Publishing Agent service port - communications with RAS Secure Client Gateways and the RAS Console (in Normal mode only). Device Manager shadowing via Firewall (indirect network connection) if RAS Console runs on RAS Publishing Agent
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	Localhost	TCP	20020	Communication with HTML5 Gateway web server (NodeJS).

RAS Publishing Agent

Source	Destination	Protocols	Ports	Description
RAS Publishing Agent	AD DS controllers	TCP TCP	389, 3268 636, 3269	LDAP LDAPS

		TCP,UDP UDP	88 53	Kerberos DNS
	RAS Publishing Agent	TCP	20001 20030	Redundancy service. Communication between RAS Publishing Agents running in the same site.
	Parallels Licensing Server	TCP	443	RAS Publishing Agent (primary Publishing Agent in Licensing Site) communicates with Parallels Licensing Server (https://ras.parallels.com). **Note:** Not required for Tenant Broker RAS Publishing Agent (see the **Tenant Broker** section).
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB.
	RAS RD Session Host Agent	TCP, UDP	30004	Server for Publishing Agent requests.
	RAS VDI Agent	TCP, UDP	30006	VDI Agent communication port.
	RAS Remote PC Agent	TCP, UDP	30004	Remote PC Agent Communication Port (agent state, counters and session information)
	2FA Server(s)	TCP, UDP	8080, 80 1812, 1813	Deepnet/ Safenet Radius
	RAS Enrollment Server	TCP	30030	RAS Publishing Agent Sends RAS Enrollment Server connection Request
	RAS Reporting	TCP	30008	Master RAS Publishing Agent communicates with RAS Reporting (installed on the same host as SSRS).
	RAS Remote Installer Service	TCP	30020	Remote agent pushing
	RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Publishing Agent RAS Secure Client Gateway RAS Enrollment Server	TCP	135, 445, 49179	Remote Install Push/Takeover of Software
	SMTP	TCP	587	Notifdispatcher is the service which sends the emails using port specified in the Mailbox settings (+SSL/TLS)

RAS Console

Source	Destination	Protocols	Ports	Description
RAS Console	RAS Reporting	TCP	30008	RAS Console is connected to primary RAS Publishing Agent which communicates with RAS Reporting (installed on the same host as SSRS). SSRS talks to SQL via TCP 1433 (or dynamic if 1433 is not established in the settings).
	SSRS	TCP	443	Reports retrieval.
	HALB	TCP, UDP	31006	Used for configuration.
	Parallels Client	TCP	50005	Shadowing from the RAS Console in case of direct network connection.
	RAS RD Session Host Agent	UDP, TCP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS Guest Agent	TCP UDP	30010 30009	Used for the "Check Agent" task. Used to manage components.
	RAS Remote PC Agent	UDP, TCP	30004	Used for the "Check Agent" task. Used to manage components.
	RAS VDI Agent	UDP, TCP	30006	Used for the "Check Agent" task. Used to manage component.
	MFA Server(s)	TCP, UDP	8080, 80, 1812, 1813	Deepnet / Safenet / Radius
	Microsoft site	TCP	80, 443	Check for updates and download Parallels Client
	Parallels site	TCP	80	Check for updates and download Parallels Client
	RAS Performance Monitor	TCP	20002, 20001	Communication with Publishing Agent and redundancy.
	RAS Publishing Agent	TCP	20002, 20001	Communication with Publishing Agent and redundancy.
	RAS Enrollment Server	TCP, UDP	30030	Used for the "Check Agent" task. Used to manage components and for troubleshooting.
	Wyse Broker	UDP	1234 (outbound only) 68 (inbound only)	Wyse broker discovery request broadcast packet (V_WYSEBCAST). Wyse broker discovery reply packet (V_WYSETEST).
	SMTP	TCP	587	RAS Console can send test emails using port specified in the Mailbox settings (+SSL/TLS)

SSRS

Source	Destination	Protocols	Ports	Description
SSRS	Microsoft SQL Server	TCP	1433	RAS Console is connected to RAS Reporting

RAS Reporting

Source	Destination	Protocols	Ports	Description
RAS Reporting Service	MS SQL	TCP	1433	Store RAS activity information
	SSRS	TCP	8085, 443	Enumeration of reports (incl. custom reports)

RAS Web Administration Service (REST/Management Portal)

Source	Destination	Protocols	Ports	Description
RAS Web Administration Service	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS VDI Agent	TCP	30006	Log retrieval
	RAS Publishing Agent	TCP	20002, 20001 30020	Communication with PA and Redundancy Used during publishing to browse for installed applications or single file/folder browsing. 30020 - remote agent pushing (pre-RAS 18).
	RAS RD Session Host Agent RAS Guest Agent RAS Remote PC Agent RAS Publishing Agent RAS Secure Client Gateway RAS Enrollment Server	TCP	135, 445	Remote Install Push/Takeover of Software (pre-RAS 18).
	RAS Reporting Service	TCP	3000	Integration of RAS Reporting in Management Portal iFrame

RAS PowerShell

Source	Destination	Protocols	Ports	Description
RAS PowerShell	RAS RD Session Host Agent	TCP	30004	Log retrieval
	RAS Guest Agent	TCP	30010	Log retrieval
	RAS Remote PC Agent	TCP	30004	Log retrieval
	RAS VDI Agent	TCP	30006	Log retrieval
	RAS Publishing Agent	TCP	20002, 20001	Communication with PA and Redundancy Used during publishing to browse for installed applications or single file/folder browsing.

RAS VDI Agent

Source	Destination	Protocols	Ports	Description
RAS VDI Agent	RAS Publishing Agent	TCP	20003	Publishing Agent communication port.
	RAS Guest Agent	TCP UDP	30010 30009	TCP is used to send the commands. UDP is used during the initial handshake.
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB - applicable to Hyper-V only.
	Hyper-V	TCP	135, 49152-65535	Used to check if the guest is powered on and send export, import, delete, shutdown, restart or suspend commands.
	Nutanix	TCP	9440	Used to check if the guest is powered on and sends clone, delete, shutdown, restart commands (RestAPI calls, PoSH, remote ncli).
	VMWare	TCP	443	Used to check if the guest is powered on and sends clone, delete, shutdown, restart and suspend commands.
	Microsoft Azure	TCP	443	Used to check if the guest is powered on and sends clone, shutdown, restart commands (via REST).
	Scale	TCP	443	Used to check if the guest is powered on and sends clone, shutdown, restart commands (via REST).
	Remote PC over VDI	TCP	135, 49152-65535	Used to check if the guest is powered on and sends shutdown, restart or suspend commands.

RAS Enrollment Server

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

RAS RD Session Host Agent

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

RAS Guest Agent

Source	Destination	Protocols	Ports	Description
RAS Guest Agent (used by Azure Virtual Desktop)	VDI Agent	TCP, UDP	30006	Communication with VDI Agent Subnet broadcast is sent to find VDI agent Regular UDP heartbeats
	Localhost	TCP	30005	For internal commands - memshell, printer redirector)
	RAS Performance Monitor	TCP	8086	Agent (Telegraf service) sends collected performance data to InfluxDB

	RAS Enrollment Server	TCP	30030	RAS Guest Agent (PrlsSCDriver) connects to get logon credentials
	FSlogix	TCP	443	Download FSlogix installer

RAS Remote PC Agent

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

Tenant Broker

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

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.

Note: For complete information, please also read the **SSL Certificate Management** chapter in the **Parallels RAS Administrator's 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 a Third-Party Trusted Certificate Authority

Generate a CSR

To obtain a certificate from a third-party CA, you need to generate a certificate signing request (CSR) as described below.

In the RAS Console, navigate to **Farm** / **Site** / **Certificates**. Click **Tasks** > **Generate a certificate request**. In the dialog that opens, specify the following options:

- **Name:** Type a name for this certificate. This field is mandatory.
- **Description**: An optional description.
- **Usage**: Specify whether the certificate should be used for RAS Secure Client Gateways or HALB, or both. This selection is mandatory.
- **Key size:** The certificate key size, in bits. Here you can select from the predefine values. The default is 2048 bit, which is the minimum required length according to current industry standards.
- **Country code**: Select your country.
- **Expire in**: The certificate expiration date.
- **Full state or province:** Your state or province info.
- **City:** City name.
- **Organization:** The name of your organization.
- **Organization unit:** Organizational unit.
- **E-mail:** Your email address. This field is mandatory.
- **Common name:** The Common Name (CN), also known as the Fully Qualified Domain Name (FQDN). This field is mandatory.

After entering the information, click **Generate**. Another dialog will open displaying the request. Copy and paste the request into a text editor and save the file for your records. The dialog also allows you to import a public key at this time. You can submit the request to a certificate authority now, obtain the public key, and import it without closing the dialog, or you can do it later. If you close the dialog, the certificate will appear in the RAS Console with the **Status** column indicating **Requested**.

To submit the request to a certificate authority and import a public key:

1. If the certificate request **Properties** dialog is closed, open it by right-clicking a certificate and choosing **Properties**. In the dialog, select the **Request** tab.
2. Copy the request and paste it into the certificate authority web page (or email it, in which case you will need to come back to this dialog later).
3. Obtain the certificate file from the certificate authority.
4. Click the **Import public key** button and finalize the certificate registration by specifying the key file and the certificate file.

Import the certificate

You know need to import the certificate into Parallels RAS. To do so, on the **Certificates** tab, click **Tasks** > **Import certificate**. In the dialog that opens, specify the following:

- **Name:** Type a name for the certificate.
- **Description:** An optional description.
- **Private key file:** Specify a file containing the private key. Click the **[...]** button to browse for the file.
- **Certificate file:** When you specify a private key file (above) and have a matching certificate file, it will be inserted in this field automatically. Otherwise, specify a certificate file.
- **Usage:** Specify whether the certificate will be used for RAS Secure Client Gateways or HALB, or both.

Click **OK** when done. The certificate will appear in the list in the RAS Console with the **Status** column indicating **Imported**.

To view the certificate info, right-click it and choose **Properties**. In the dialog that opens, examine the properties and then click the **View certificate info** button to view the certificate trust information, details, certification path and the certificate status. You can also view the certificate info by right-clicking it and choosing **View certificate info**.

For imported certificates, the **Properties** dialog has an additional tab **Intermediate**. If the original certificate included an intermediate certificate (in addition to the root certificate), it will be displayed here. You can paste a different intermediate certificate here if you wish.

Using Enterprise Certificate Authority

Use IIS to receive a certificate from the Enterprise CA and export the certificate in the PFX format. To install the PFX certificate in Parallels RAS, import it as described in the **Import the certificate** subsection above.

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.

Assign a Certificate to a Gateway

After you add a certificate to a Site, you can assign it to a RAS Secure Client Gateway, HALB, or both depending on the usage type that you specified when you created the certificate (described in the beginning of this chapter). More on the certificate **Usage** option below.

Certificate Usage

Certificate **Usage** is an option that you specify when you create a certificate. It specifies whether the certificate should be available for RAS Secure Client Gateways, HALB, or both. When setting this option, you can choose from the following:

- **Gateway**: If selected, makes the certificate available for RAS Secure Client Gateways.
- **HALB**: If selected, makes the certificate available for HALB.

You can select one of the options above or both, in which case the certificate becomes available for both, Gateways and HALB.

When you configure SSL for a RAS Secure Client Gateway or HALB later, you need to specify an SSL certificate. When you select a certificate, the following options will be available depending on how the **Usage** option is configured for a particular certificate:

- **<All matching usage>**: This is the default option, which is always available. It means that any certificate on which the **Usage** selection matches the object type (Gateway or HALB) will be used. For example, if you are configuring a Gateway and have a certificate that has **Usage** set to "Gateway", it will be used. If a certificate has both, Gateway and HALB usage options selected, it can also be used with the given gateway. This works the same way for HALB when you configure the LB SSL Payload. Please note that if you select this option for a Gateway or HALB, but not a single matching certificate exists, you will see a warning and will have to create a certificate first.

- Other items in the **Certificates** drop-down list are individual certificates, which will or will not be present depending on the certificate's **Usage** settings. For example, if you configure LB SSL Payload for HALB and have a certificate with the **Usage** option set to "HALB", the certificate will appear in the drop-down list. On the other hand, certificates with **Usage** set to "Gateway" will not be listed.

As another example, if you need just one certificate, which you would like to use for all of your Gateways, you need to create a certificate and set the **Usage** option to "Gateways". You can then configure each Gateway to use this specific certificate or you can keep the default **<All matching usage>** selection, in which case the certificate will be picked up by a Gateway automatically. Same exact scenario also works for HALB.

Gateways

To assign a certificate to a RAS Secure Client Gateway:

1. Navigate to **Farm** / **Site** / **Gateways**.
2. Right-click a gateway and choose **Properties**.
3. Select the **SSL/TLS** tab.
4. In the **Certificates** drop-down list, select the certificate that you created.
5. Click **OK**.

Please note that you can also select the **<All matching usage>** option, which will use any certificate that either has the usage set to Gateway or both Gateway and HALB.

Parallels Client Configuration

In case the certificate is self-signed, or the certificate is issued by an Enterprise CA, Parallels Clients should be configured as follows:

1. Export the certificate in Base-64 encoded X.509 (.CER) format.
2. Open the exported certificate with a text editor 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

T

U

W