Progress®
Kemp® LoadMaster®

Deployment Guide Parallels Remote Application Server RAS

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Document Purpose 5

Intended Audience 5

Chapter 2: Template 6

Chapter 3: Architecture 7

Parallels RAS Roles 11

Load Balancing the RAS HTML5 Web Portal 11

Load Balancing the Secure Gateway Service 11

Chapter 4: Enable Subnet Originating Requests Globally 12

Chapter 5: Parallels Configuration 14

Secure Gateway Prerequisites 14

Configure the RAS HTML5 Portal 15

Chapter 6: Virtual Service - RAS Secure Gateway 18

Create the RAS Secure Gateway - HTTP Virtual Services 18

Parallels RAS Secure Gateway - HTTP Virtual Service Recommended API Settings (optional) 19

Create the RAS Secure Gateway - HTTPS Virtual Services 20

Parallels RAS Secure Gateway - HTTPS Virtual Service Recommended API Settings

(optional). 21
Create the RAS Secure Gateway - UDP Virtual Services. 21
Parallels RAS Secure Gateway - UDP Virtual Service Recommended API Settings (optional). 22

Chapter 7: Testing 23

1

Introduction

Parallels RAS (Remote Application Server) is a cost-effective application delivery and Virtual Desktop Infrastructure (VDI) solution that allows your employees and customers to access and use applications, desktops, and data from any device. Easy to deploy, configure, and maintain, Parallels RAS provides organizations of any size with a seamless application delivery and VDI experience - while reducing Total Cost of Ownership (TCO) and improving security.

The Progress Kemp Support Team is available to provide solutions for scenarios not explicitly defined in this guide. For further details, refer to the: LoadMaster Support and Learning Hub.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

This document provides the recommended LoadMaster settings used when load balancing Parallels RAS.

Intended Audience

Anyone who is interested in configuring the LoadMaster to optimize Parallels RAS.

2

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

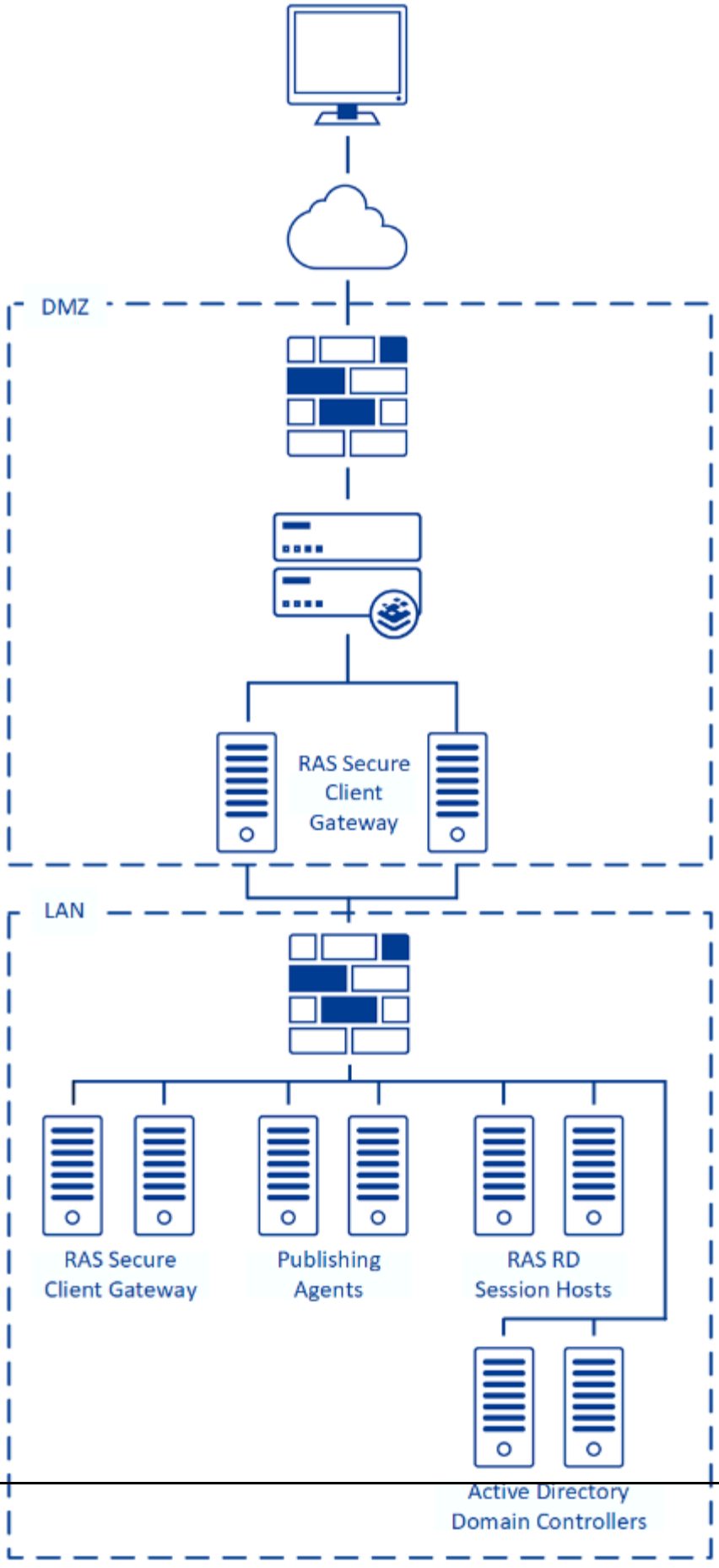
You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

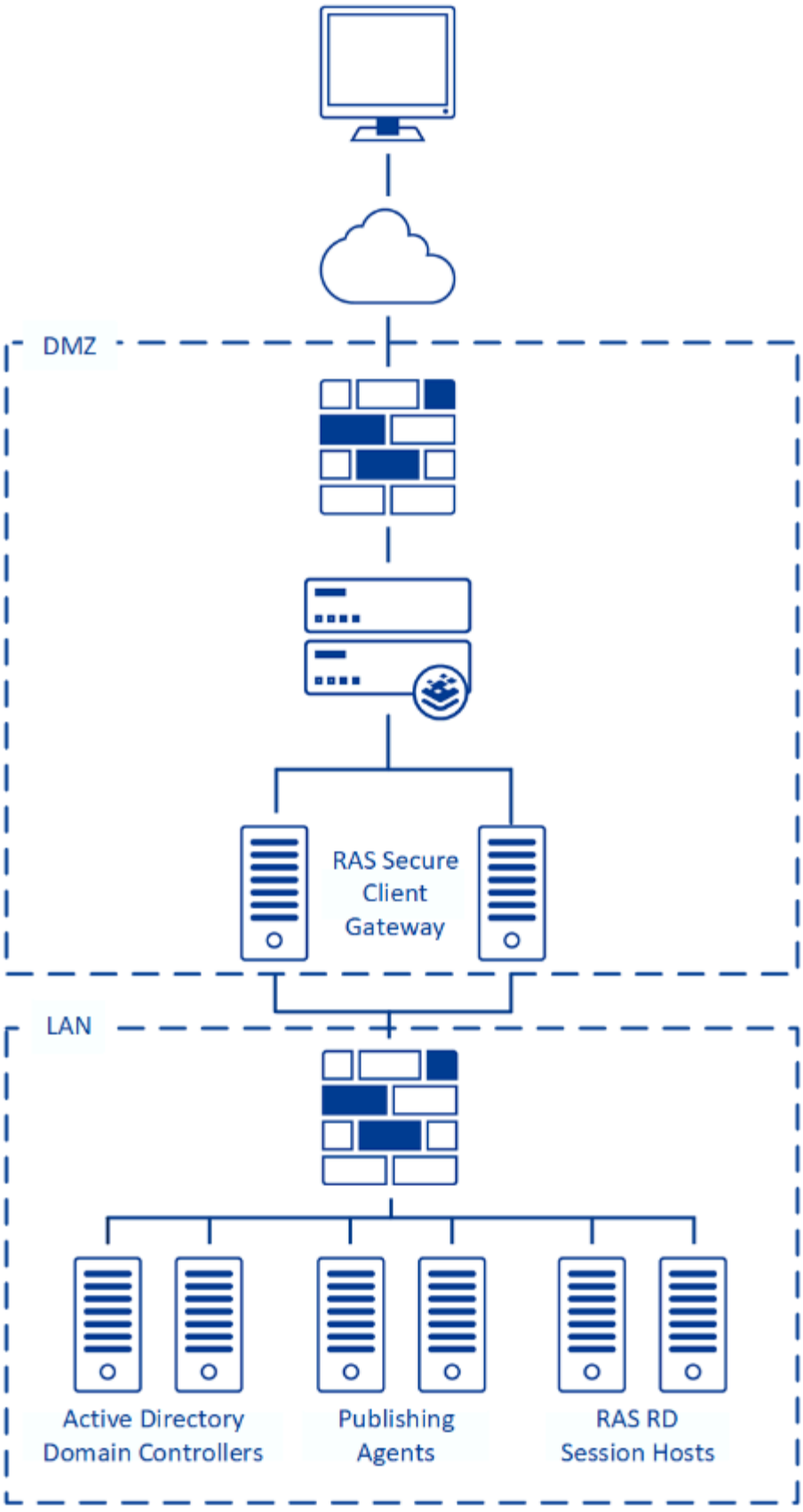
For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

3

Architecture


DMZ
RAS Secure
Client
Gateway
LAN
RAS Secure
Client Gateway
Publishing
Agents
RAS RD
Session Hosts
Active Directory
Domain Controllers

The diagram above shows a scenario where the LoadMaster can be used to load balance the RAS Secure Gateway service in forwarding mode. In this configuration, the Secure Gateway is deployed in the DMZ and is load balanced by the LoadMaster. The RAS Secure Gateways forward to the internal Secure Gateways in a cascaded chain. If your configuration differs from this configuration and there are issues deploying the LoadMaster, contact the local Progress Kemp Support Team for assistance.


DMZ
RAS Secure
Client
Gateway
LAN
Active Directory
Domain Controllers
Publishing
Agents
RAS RD
Session Hosts

The diagram above shows a different scenario where the LoadMaster is used to load balance RAS Secure Gateways. In this configuration, the Secure Gateways (and HTML5 Portal) are deployed in the DMZ with no Secure Gateways in the corporate network. Additional ports such as 3389 must be opened on the internal firewall from the DMZ to the corporate network. If your configuration differs from this configuration and there are issues deploying the LoadMaster, contact the local Progress Kemp Support Team for assistance.

Related Links

For details, see the following topics:

- Parallels RAS Roles

Parallels RAS Roles

Parallels RAS consists of various roles. You can configure the LoadMaster to load balance some of these roles. The sections below discuss the various scenarios in which you can use the LoadMaster to load balance Parallels RAS.

Load Balancing the RAS HTML5 Web Portal

The RAS HTML5 Web Portal is a web application that acts as a web-based portal to an RAS farm. It provides users with a list of available applications and desktops using their web browser.

The RAS HTML5 Web Portal role is part of the Secure Gateway Role. By default, it is enabled when configuring a Secure Gateway Sever.

Load Balancing the Secure Gateway Service

The RAS Secure Gateway Service is an SSL gateway that simplifies the deployment of applications over the Internet. The Secure Gateway Service allows access to published applications and desktops securely through SSL connections.

The RAS Secure Gateway Service provides a proxy connection to RAS components such as RDP Sessions and the HTML5 Web Portal.

4

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If

the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

5

Parallels Configuration

This document covers an example of the settings required for Parallels RAS. The RAS administrator should follow the Deployment Guide provided by Parallels to complete the configuration based on their unique topology.

The Parallels Administrators Guide can be found here: https://download.parallels.com/ras/v17/docs/en_US/Parallels-RAS-v17-Administrators-Guide/39932.htm

Related Links

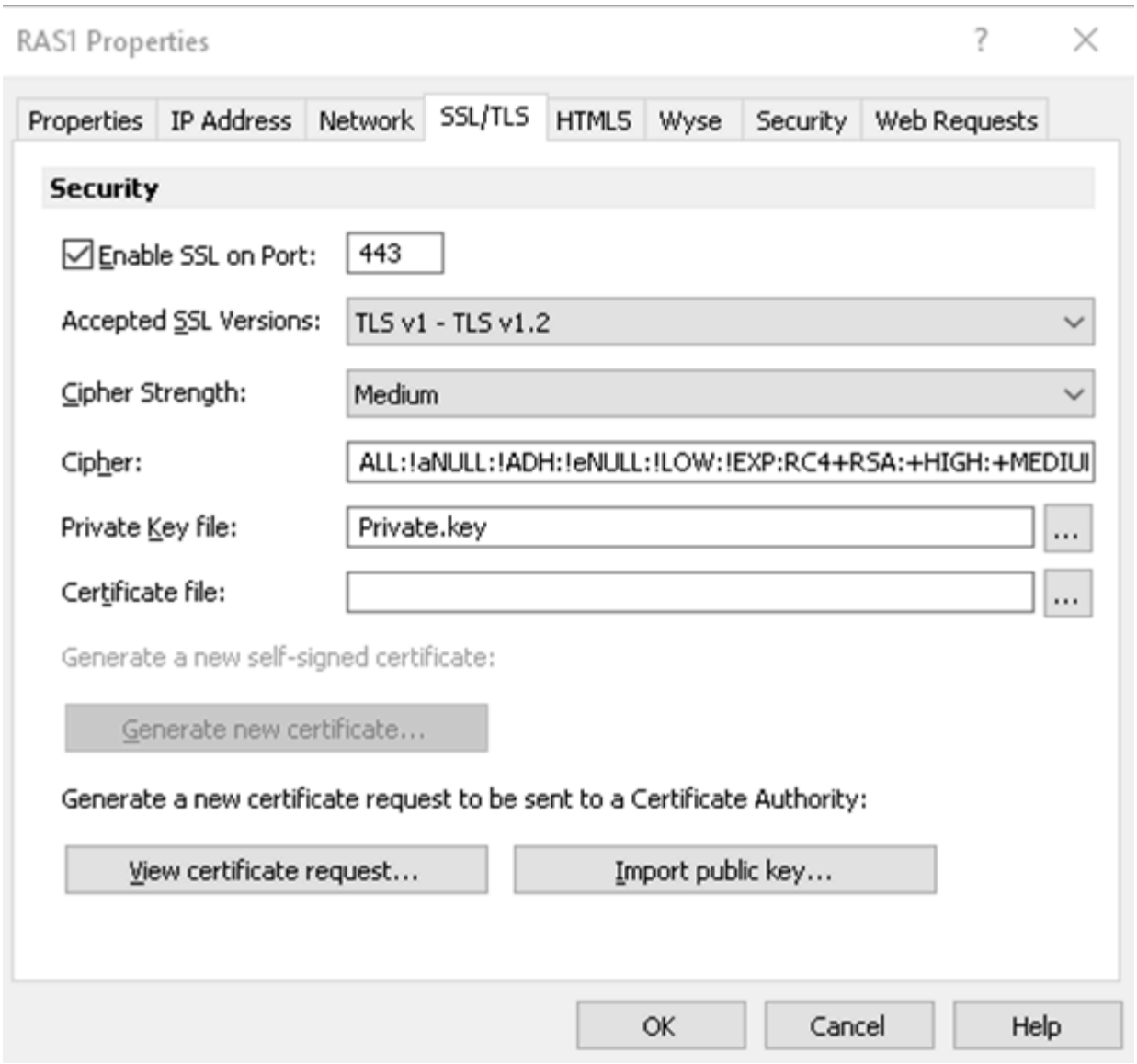
For details, see the following topics:

- Secure Gateway Prerequisites
- Configure the RAS HTML5 Portal

Secure Gateway Prerequisites

Before adding Virtual Services to the LoadMaster, ensure to have the DNS names and IP addresses available for all Secure Access Service roles in your deployment. The DNS Names used must be included in the certificate that will be used to secure the traffic.

1. On each of the Secure Gateway Servers, right click and choose properties.

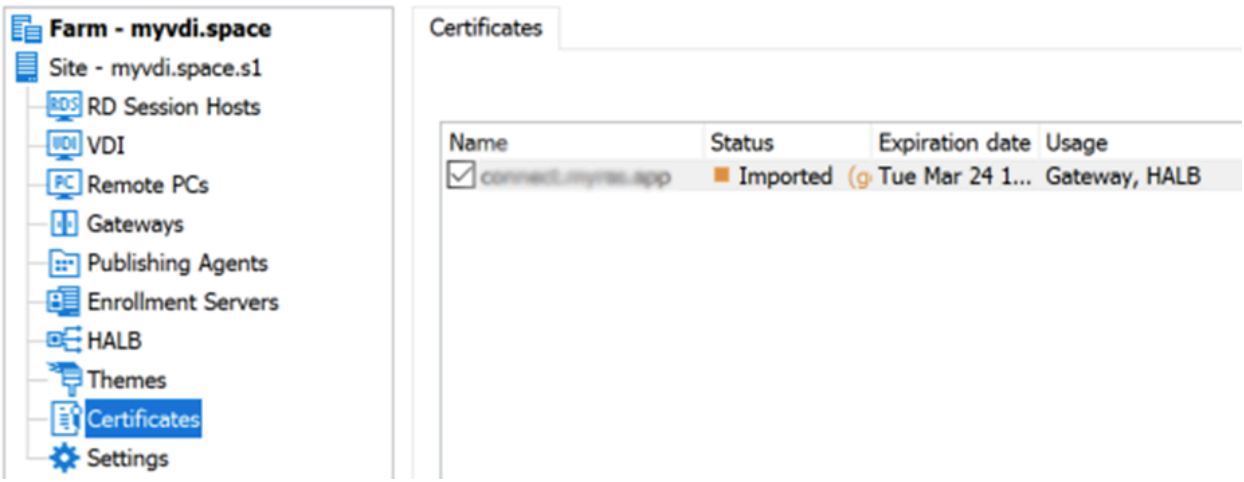


2. Under the properties of the Secure Gateway, configure the following settings:
   1. In the **SSL/TLS** tab, select the **Enable SSL on Port** check box.
   2. Enter **443** as the port.
   3. Import or generate the SSL certificate to be used to encrypt traffic.

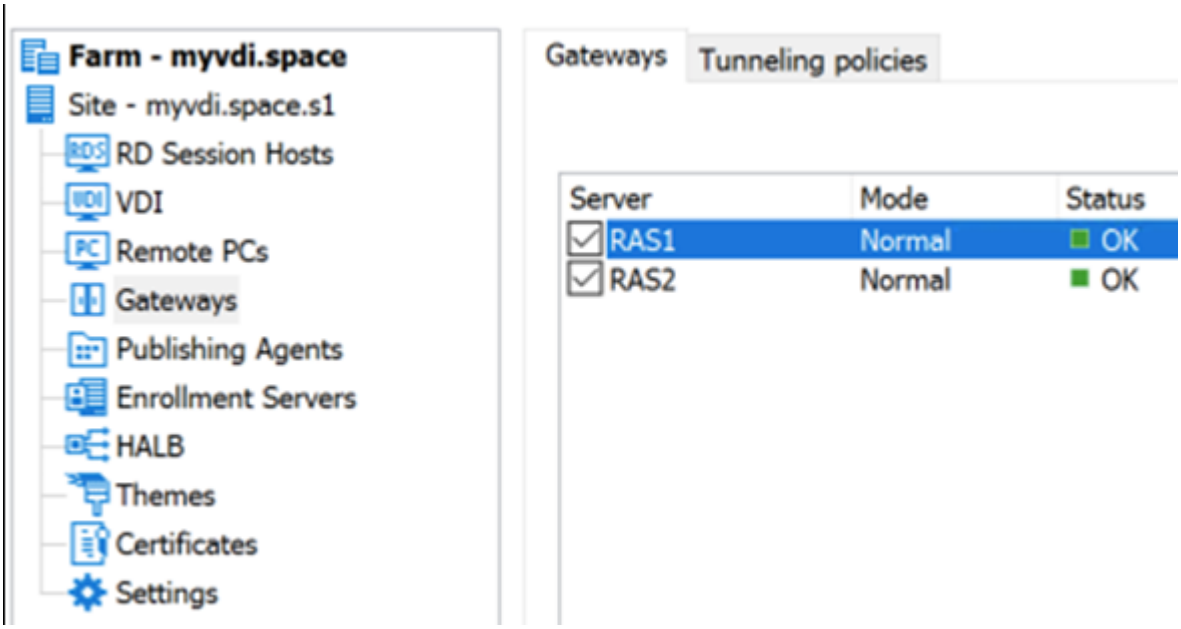
Configure the RAS HTML5 Portal

The RAS HTML5 Portal is part of the Secure Gateway service and is enabled by default. To check that it is enabled and view the properties, go to the gateways section in the RAS console.

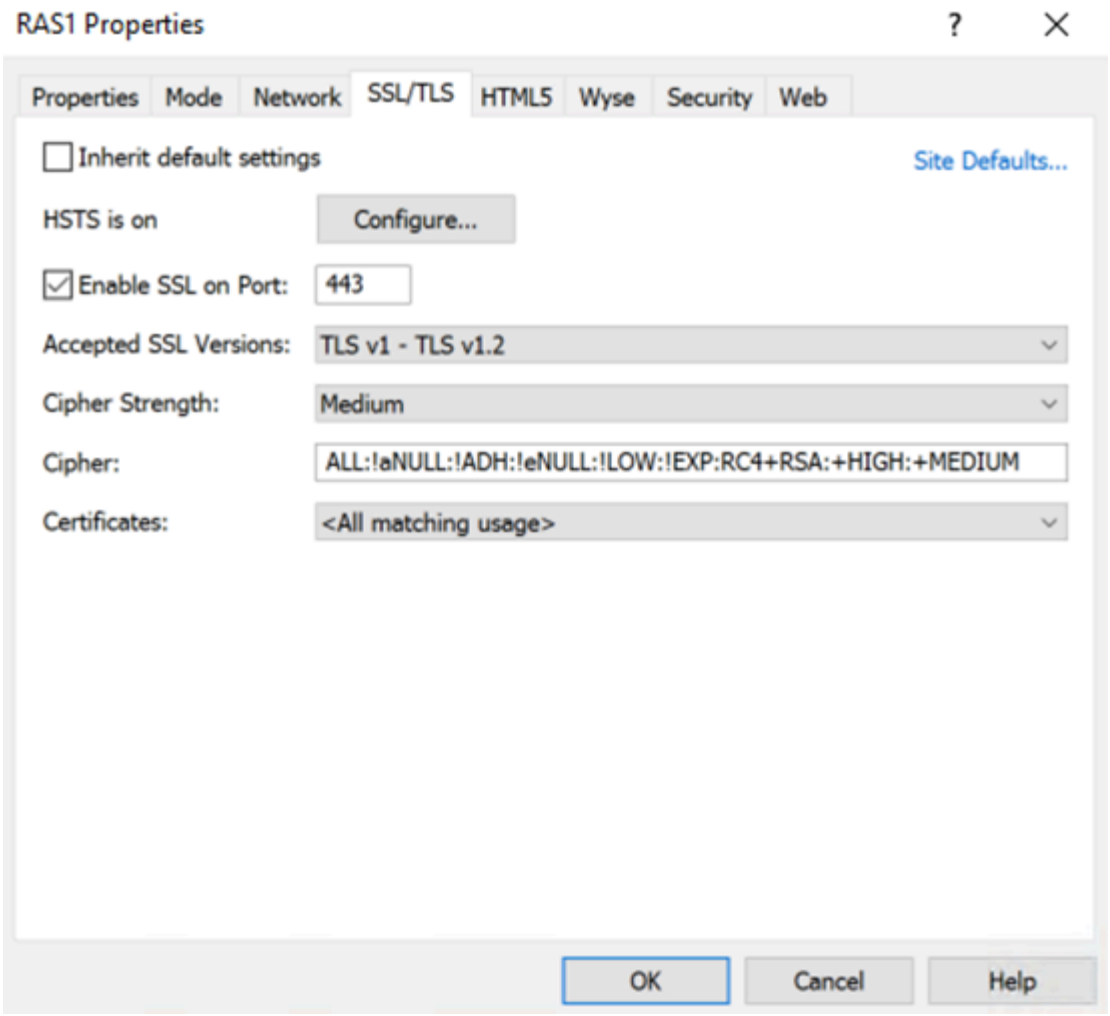
1. Log in to the RAS console and go to **Farm > Gateways**.



2. On each of the Secure Gateway Servers, right-click and choose **Properties**.



3. On the **HTML5** tab, select the **Enable HTML5 Client** check box.



4. Then on the **SSL/TLS** tab, select **<All matching usage>** or the certificate name.
5. Click **OK** to confirm.

6

Virtual Service - RAS Secure Gateway

Refer to the sections below for details on the RAS Secure Gateway Virtual Service.

Related Links

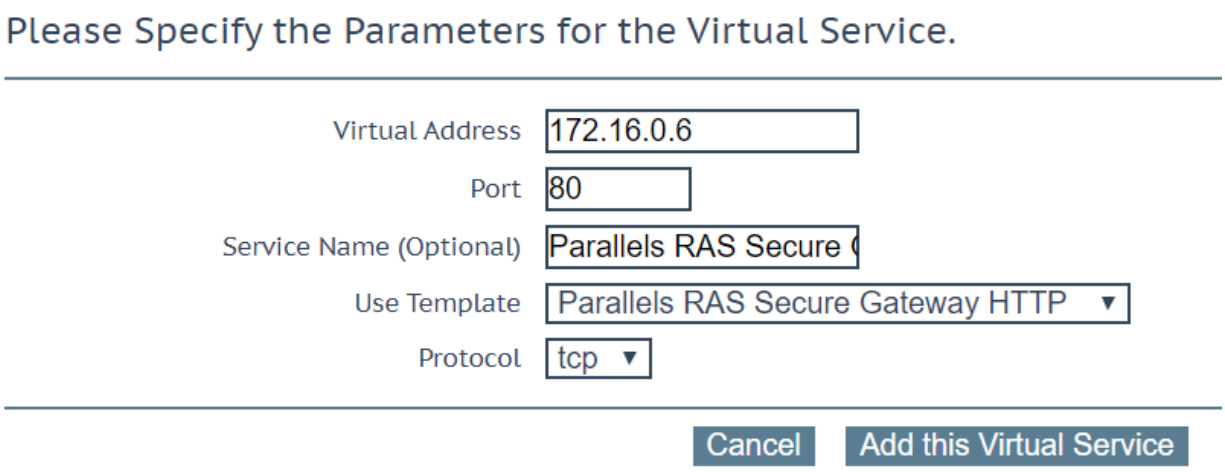
For details, see the following topics:

- Create the RAS Secure Gateway - HTTP Virtual Services
- Create the RAS Secure Gateway - HTTPS Virtual Services
- Create the RAS Secure Gateway - UDP Virtual Services

Create the RAS Secure Gateway - HTTP Virtual Services

The following are the steps and recommended settings to configure the Parallels RAS Secure Gateway HTTP Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Select the **Parallels RAS Secure Gateway - HTTP** template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Type the **Real Server Address**.
8. Confirm that port **80** is entered.
9. Click **Add This Real Server**.
10. Repeat the steps above to add more Real Servers as needed.

Parallels RAS Secure Gateway - HTTP Virtual Service Recommended API Settings (optional)

This table outlines the Application Programming Interface (API) parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

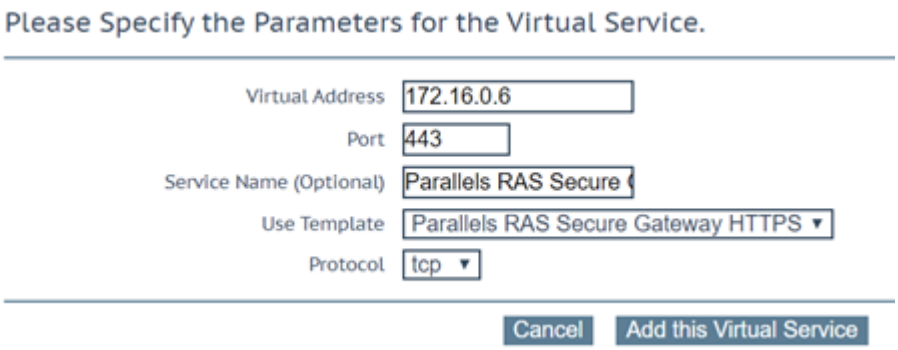
API Parameter	API Value
port	80
prot	tcp
VStype	http
SubnetOriginating	1
Forcel7	1
Transparent	0

API Parameter	API Value
Schedule	lc
Persist	src
PersistTimeout	360
CheckType	tcp
CheckPort	80

Create the RAS Secure Gateway - HTTPS Virtual Services

The following are the steps involved and the recommended settings to configure the Parallels RAS Secure Gateway HTTPS Virtual Service:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Select the **Parallels RAS Secure Gateway - HTTPS** template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Type the **Real Server Address**.
8. Confirm that port **443** is entered.
9. Click **Add This Real Server**.
10. Repeat the steps above to add more Real Servers as needed.

Parallels RAS Secure Gateway - HTTPS Virtual Service Recommended API Settings (optional)

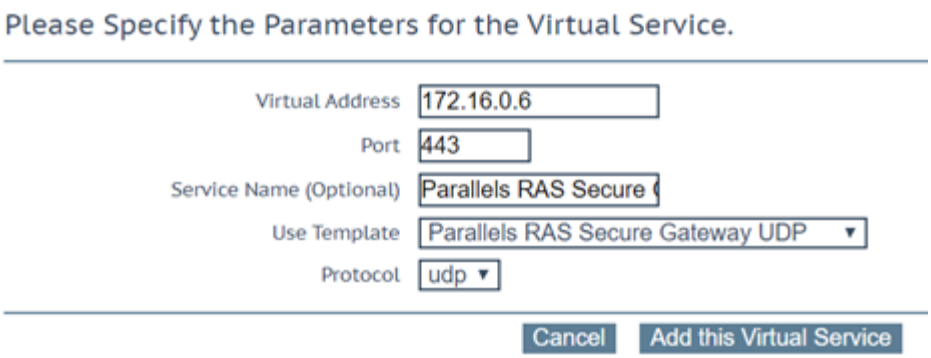
This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Forcel7	1
Transparent	0
Schedule	lc
Persist	src
PersistTimeout	360
CheckType	tcp
CheckPort	443

Create the RAS Secure Gateway - UDP Virtual Services

The following are the steps involved and the recommended settings to configure the Parallels RAS Secure Gateway UDP (RAS RDP Proxy) Virtual Service:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Select the **Parallels RAS Secure Gateway - UDP** template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Type the **Real Server Address**.
8. Confirm that port **443** is entered.
9. Click **Add This Real Server**.
10. Repeat the steps above to add more Real Servers as needed.

Parallels RAS Secure Gateway - UDP Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	udp
SubnetOriginating	1
Forcel7	1
Transparent	0
Schedule	lc
Persist	src
PersistTimeout	360
CheckType	icmp

7

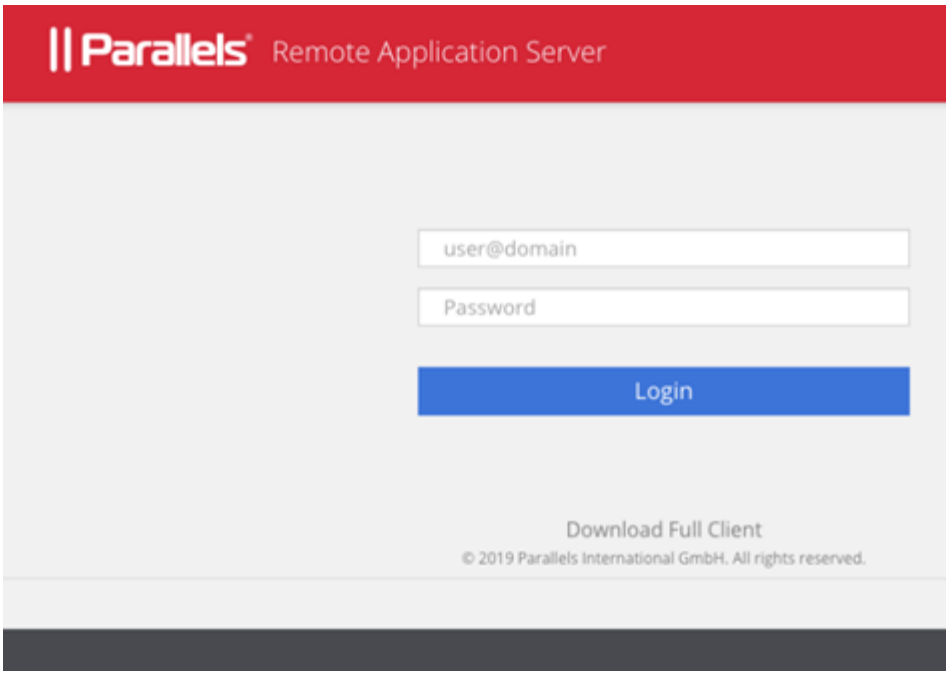
Testing

After following the implementation steps in the previous section, follow the steps below to test the load-balanced Parallels RAS environment:

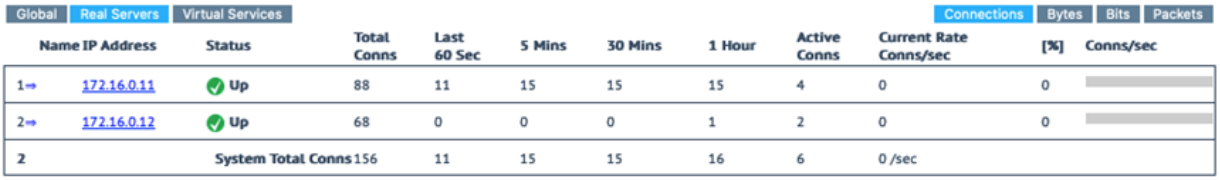
1. Configure your DNS to resolve to the Virtual Service Virtual IP address. In this example, **connect.kempdemo.com** would resolve to **172.16.0.6**.

   Note: This DNS entry would also match your SSL certificate common name.

2. Open a web browser that can reach the load-balanced IP.
3. Browse to the configured DNS name for the load-balanced service, for example **http://connect.kempdemo.com/** which will redirect to **https://connect.kempdemo.com/RASHTML5Gateway/** . A web page should be presented with the RAS login page. This indicates that the LoadMaster has redirected the session to a Real Server.



4. Enter a username and password with permissions to access the Parallels RAS environment.
5. In the LoadMaster WUI, go to **Statistics > Real Time Statistics**.
6. Click **Real Servers**.

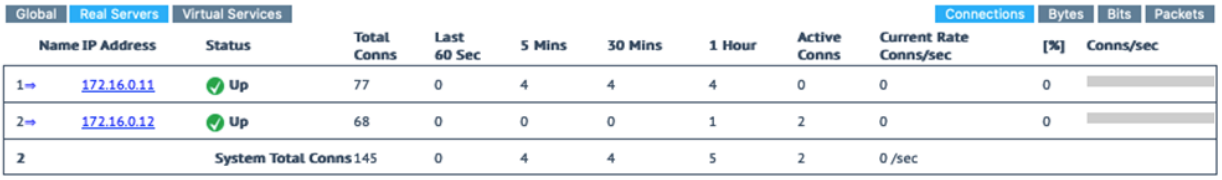


Global | Real Servers | Virtual Services — Connections | Bytes | Bits | Packets

	Name	IP Address	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/sec	[%]	Conns/sec
1		172.16.0.11	Up	88	11	15	15	15	4	0	0	
2		172.16.0.12	Up	68	0	0	0	1	2	0	0	
2			System Total Conns	156	11	15	15	16	6	0 /sec		

7. Open another web browser on a different client and perform the first three steps above.

Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled.



Global | Real Servers | Virtual Services — Connections | Bytes | Bits | Packets

	Name	IP Address	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/sec	[%]	Conns/sec
1		172.16.0.11	Up	77	0	4	4	4	0	0	0	
2		172.16.0.12	Up	68	0	0	0	1	2	0	0	
2			System Total Conns	145	0	4	4	5	2	0 /sec		

8. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method we chose, load is spread over both Secure Access Servers (172.16.0.11 and 172.16.0.12).