Brocade Virtual Traffic Manager and Parallels® Remote Application Server

Deployment Guide

Contents

Preface

Welcome to the Brocade Virtual Traffic Manager and Parallels Remote Application Server Deployment Guide. Read this preface for an overview of the information provided in this guide and for contact information. This preface includes the following sections:

- About This Guide
- Contacting Brocade

About This Guide

The Brocade Virtual Traffic Manager and Parallels Remote Application Server Deployment Guide describes the different ways of load-balancing different Parallels Remote Application Server (RAS) components. The guide also details the reference architecture of the Parallels RAS solution.

Audience

This guide is written for network operations professionals, server administrators, and DevOps professionals familiar with administering and managing application delivery controllers (ADCs), servers, and applications.

You must also be familiar with:

- Parallels Remote Application Server components
- Brocade Virtual Traffic Manager (vTM)

For more details on the Brocade vADC product family, see brocade.com/vADC.

Contacting Brocade

This section describes how to contact departments within Brocade.

Internet

You can learn about Brocade products through the company website: brocade.com.

Technical Support

If you have problems installing, using, or replacing Brocade products, contact Brocade Support or your channel partner who provides support. To contact Brocade Support, see brocade.com/en/support.html.

Professional Services

Brocade Global Services has the expertise to help organizations build scalable and efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Brocade Global Services delivers world-c lass professional services, technical support, and education services, enabling organizations to maximize their Brocade investments, accelerate new technology deployments, and optimize the performance of networking infrastructures.

Chapter 1: Solution Overview

This chapter includes the following sections:

- Virtual Traffic Manager Overview
- Parallels Remote Application Server Overview

Virtual Traffic Manager Overview

Brocade Virtual Traffic Manager (vTM) is a software-based application delivery controller (ADC) that is designed to deliver faster and more reliable access to public websites and private applications. vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables applications to run on any physic al, virtual, or c loud environment. With vADC products from Brocade, organizations can:

- Make applications more reliable with local and global load balancing.
- Scale application servers by up to 3x by offloading TCP and SSL connection overhead.
- Accelerate applications by up to 4x by using web content optimization (WCO).
- Secure applications from the latest application attacks, including SQL injection, XSS, and CSRF.
- Control applications effectively with built-in application intelligence and a full-featured scripting engine. Virtual Traffic Manager offers much more than basic load balancing. It controls and optimizes end user services by inspecting, transforming, prioritizing, and routing application traffic .The powerful Traffic Script® engine facilitates the implementation of traffic management policies that are unique to an application by allowing organizations to build custom functionality or leverage existing features in Virtual Traffic Manager in a specialized way. With vTM, organizations can deliver the following.

Performance

Improve application performance for users by offloading encryption and compression from the web server by dynamic caching and reducing the number of TCP sessions on the application.

Reliability and Scalability

Increase application reliability by load-balancing traffic across web and application servers, balancing load across multiple data c enters (private or public c louds), monitoring the response time of servers in real time to decide the fastest way to deliver a service, protecting against traffic surges, and managing the bandwidth and rate of requests used by different classes of traffic.

Application Acceleration

Dramatic ally accelerate web-based applications and websites in real time with optional web content optimization (WCO) functionality. WCO dynamic ally groups activities for fewer long distance round trips, resamples and uses image sprites to reduce bandwidth, and minifies JavaScript and combines style sheets to give the best possible response time for loading a web page on any browser or device.

Application-layer Security

Enhance application security by filtering errors in web requests and protecting against external threats, with the option of a comprehensive Layer 7 firewall to defend against deliberate attacks.

Chapter 2: Parallels Remote Application Server Architecture

The Parallels Remote Application Server high-level network architecture, as depicted in the following figure, has a few key components relevant to this deployment guide.

Terminology

A category consists of a number of settings related to a specific task or operation. In the Parallels Remote Application Server Console, the following categories are available:

- Start
- Farm
- Load Balancing
- Publishing
- Universal Printing
- Universal Scanning

Connection

- Client Manager
- Policies
- Administration
- Information
- Reporting
- Licensing

Start

The start section consists of three subsections that will easily help in configuring Parallels Remote Application Server, which are “Add Terminal Servers”, “Publish Applications”, and “Invite Users”. The “Add Terminal Servers” section configures and adds terminal servers to Parallels Remote Application Server. The second section, “Publish Applications”, consists of a wizard which easily sets up published applications for users. Finally, the “Invite Users” section sends out invitations via email to specified users to guide them in using and downloading all the necessary applications to use the published applications and desktops as required by the specific user.

Farm

A farm consists of a Parallels Remote Application Server installation on a site or multiple sites.

Licensing Server Site

The site where the main configuration database is stored and manages all other sites in the Parallels Farm. Other servers in a site can be upgraded to Licensing Server status if the main licensing server is not available.

NOTE: Upgrades of the Parallels Remote Application Server MUST be applied to the licensing server site first.

Publishing

The act of making items installed on a Remote Desktop Server, VDI Host, or Remote PC available to the users via the Parallels Remote Application Server.

Publishing Agent

The Publishing Agent provides load balancing of published applications and desktops.

RDS

RDS stands for Remote Desktop Services and is a server role in Windows Server® that provides technologies to enable users to connect to virtual desktops and session-based desktops. RDS replaced Terminal Services beginning in Windows® 2008 R2.

Site

A site consists of a publishing agent, a Secure Client Gateway or multiple gateways, and the agents installed on the Terminal Servers, VDIs, and PCs.

Parallels Remote Application Server Description

Parallels Remote Application Server enables people to work from anywhere with virtually any device. It's a powerful tool that allows businesses to leverage their existing applications on multiple devices with client support for PC, Mac®, Linux, iOS, Android™, HTML5, and Chrome™.

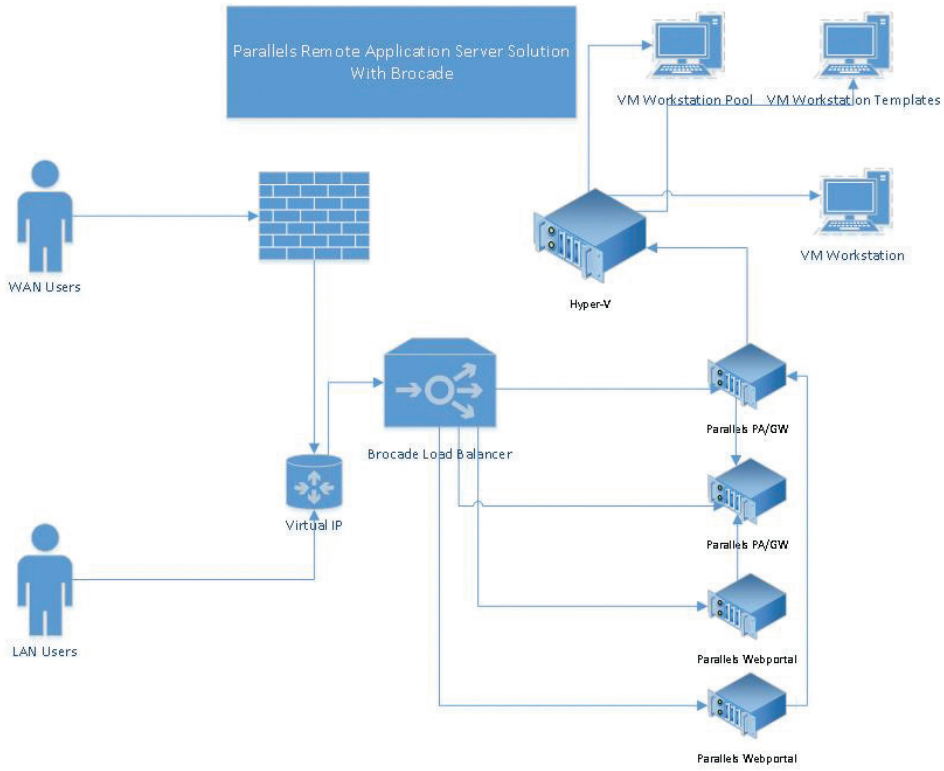
Some of the key benefits of the Parallels Remote Application Server are:

- Centralized resources that can be more effectively managed from both a cost and security perspective.
    - The cost of software updates can be reduced with volume licensed copies that can be shared instead of a full individual copy for every user.
    - Users' terminal server access can be strictly controlled with security groups and group policies i.e., software cannot be installed or downloaded on terminal servers. SSL connections and Second-Level Authentication can be used to create a secure environment.
- Applications can be delivered to users on multiple OS platforms for both desktop and mobile devices.
    - The Parallels client is available for Windows XP, 7, 8, 10, Raspberry Pi, OS X®, and Linux desktop operating systems.
    - The Parallels client is available on iPhone®, iPad®, and both Android tablets and phones.
    - The Parallels HTML5 client provides access from any device with an HTML5 browser.
- Load Balancer
    - The load balancer nodes monitor each other using Keepalived, and if the master fails, a slave becomes the master, which means the users will not notice any disruption of the service.
- Parallels Desktop Replacement
    - Parallels Desktop Replacement allows you to extend the lifespan of your hardware and delay migration to the latest OSes to a time that suits you best.
    - The Parallels solution allows you to be very flexible: you can lock machine configuration on the user side, placing your corporate data in an extremely secure position, or you might decide to allow users to run some local and remote applications.
    - Parallels Client Desktop Replacement is able to reduce the operability of the local machine by disabling the most common local configuration options, while guaranteeing the same level of service and security afforded by thin clients directly from your existing PCs.
- Parallels RAS Reporting Service
    - Parallels Remote Application Server has an inbuilt reporting engine which the administrator can use to understand how the system is functioning. The information provided can help in adjusting the system to perform better and be used in a more efficient way. With it, you can detect bottlenecks that can lead to future problems, thus avoiding them. You can also analyze how your users are using the system and extract important statistics.

- The system provides 13 reports which are grouped into five categories. You can view the available reports in a flat view by clicking the flat view button in the reports header.
- The reports are displayed in two chart types, giving you the ability to toggle between two graphical configurations, either as a bar graph or as a pie chart.

- Business Continuity and Disaster Recovery
  - Application downtime is reduced with redundant systems and quick client build times.
  - Parallels Remote Application Server also has inbuilt backup capabilities.

Figure 2-1: Parallels Remote Application Server Architecture



In order to provide scalability and availability, a load balancer is deployed to load-balance both Secure Gateways and Web Portals.

Chapter 3: Deploying Virtual Traffic Manager for Parallels Remote Application Server

This chapter describes the process of deploying Virtual Traffic Manager in the Parallels Remote Application Server architecture. It includes the following sections:

- Requirements
- Load-balance Connection Servers
- Configure vTM for RAS Gateway Servers
- Load-balance RAS Web Portals
- Configure vTM for SSL Offload for RAS Gateways and Web Portals

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- SSL Certificates
- Parallels RAS Remote Application Servers (Gateways and Web Portals, Version 15 and earlier)
- Parallels RAS Clients (Version 15 or earlier)

Load-balance Parallels Remote Application Server Gateways

The following traffic flow figure shows the Virtual Traffic Manager deployment with Parallels RAS using Gateway Servers only. In this deployment, Virtual Traffic Manager is set up to handle the following Connection Mode Types:

- Direct Mode
    - Direct Mode: Clients first connect to the Parallels Secure Client Gateway for the best available server and then connect directly with that particular server. This is best used when the client and the server are on the same network.
- Direct Mode SSL
    - SSL Mode: This connection is created as in the Direct Mode option, but the connection to the Parallels Secure Client Gateway is encrypted.
- Gateway Mode
    - Gateway Mode: Clients are connected with the Parallels Secure Client Gateway, and the session connection is tunneled through the first available connection. This mode is ideal for servers which are only reachable via the gateway and do not require a high level of security.
- Gateway Mode SSL
    - Gateway SSL Mode: Connection is made as in the regular gateway mode, but the connection is encrypted.

Direct Mode and Gateway Mode Connections

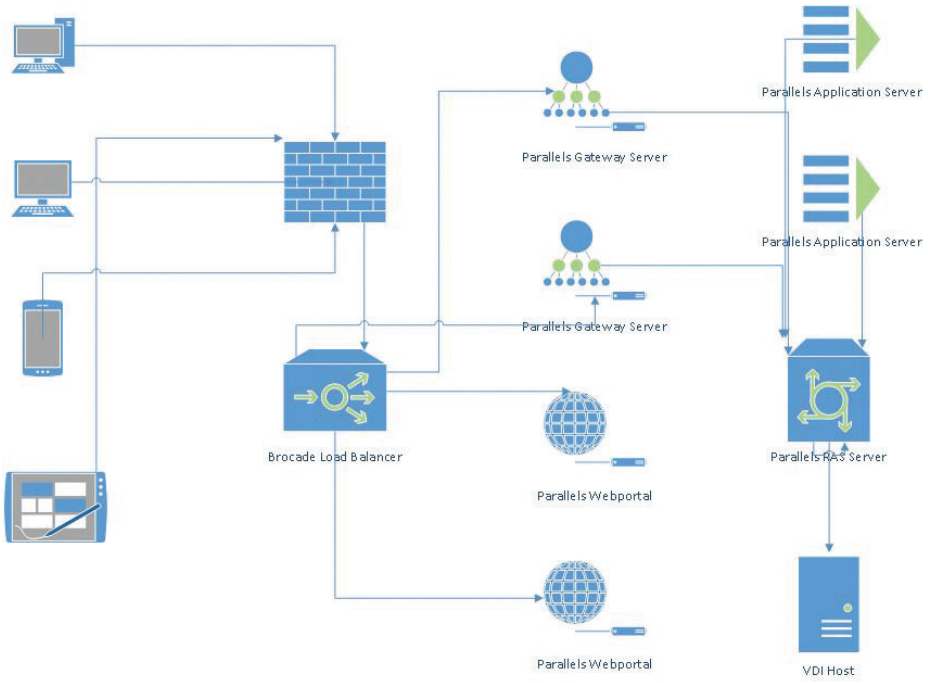
1. The client machine makes a Direct Mode connection to the Virtual Traffic Manager's Traffic IP address for the Parallels RAS Gateway.
2. The Traffic Manager accepts the connection and load-balances the connection among the Parallels RAS Gateways.

Direct Mode SSL and Gateway Mode SSL Connections

1. The Virtual Traffic Manager decrypts the SSL connections and load-balances the connections among the Parallels RAS Gateway Servers. Optionally, Virtual Traffic Manager can be configured to re-encrypt the connection established to the backend Parallels RAS Gateway Server

2. After authentication, the applications or desktops are available for access. The user then proceeds to the appropriate Parallels RAS application or desktop, bypassing Virtual Traffic Manager.

Figure 3-1: Load-balancing Parallels RAS Remote Application Server—TM Deployment with Parallels RAS Gateways



The Installation Guide for Parallels Remote Application Server can be viewed at the following link:

Parallels Installation Guide

Configure Parallels Remote Application Server Access on Virtual Traffic Manager

The following steps allow the Virtual Traffic Manager to load-balance the Parallels Remote Application Server Gateways for Gateway Mode and Direct Mode.

1. Log in to the **Parallels Remote Application Server Console.**

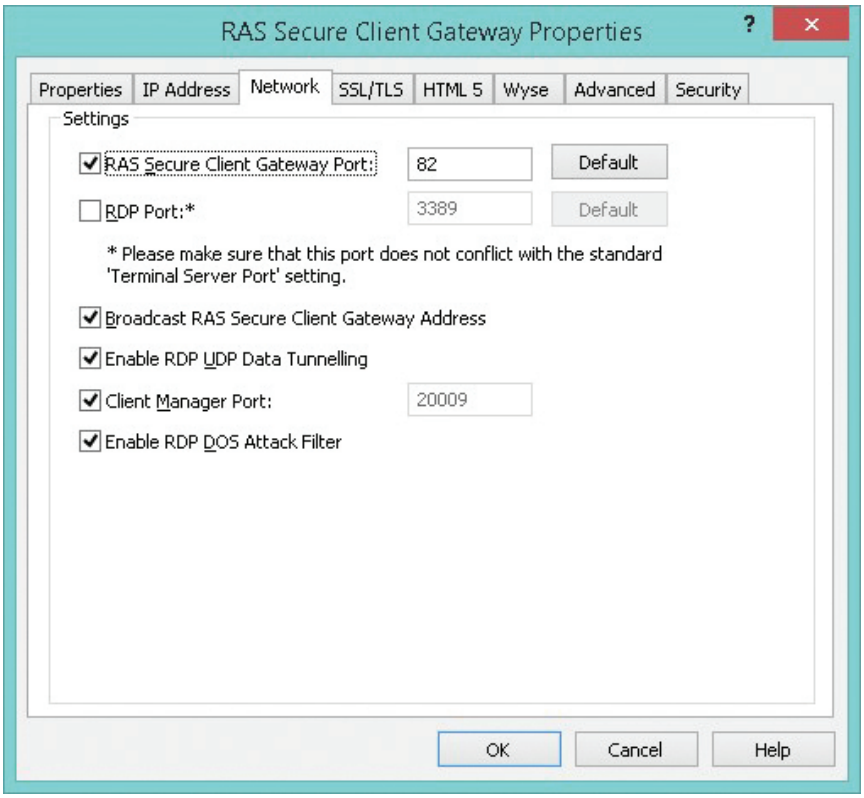
2. Click on the Farm Icon and then click on Gateways.

3. On the Gateway, right-click and click Properties.

4. Click on the Network tab. The port by default is TCP Port 80. You can change this port to any port not being used by the Windows Server.

5. Once you have all Gateways set up that you would like to load-balance, your next step is to configure the Virtual Traffic Manager.

Gateway Mode and Direct Mode Port Example: In the below example, TCP port 82 is used for the RAS Secure Client Gateway. This port is used for Gateway Mode and Direct Mode connections.



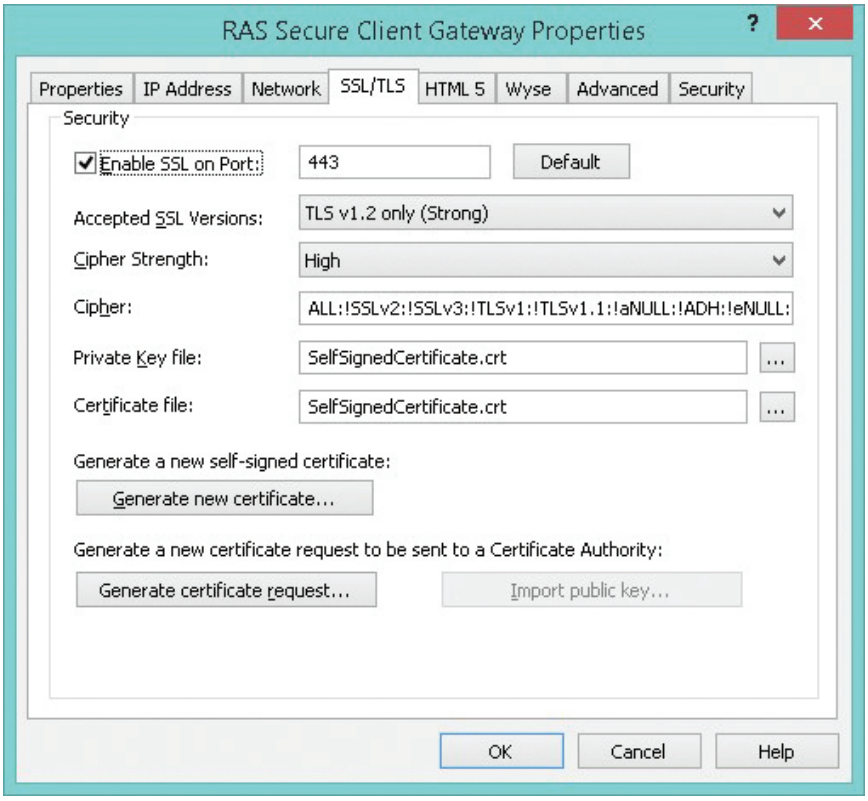
Configure Parallels Remote Application Server for Gateway Mode SSL and Direct Mode

SSL on Virtual Traffic Manager

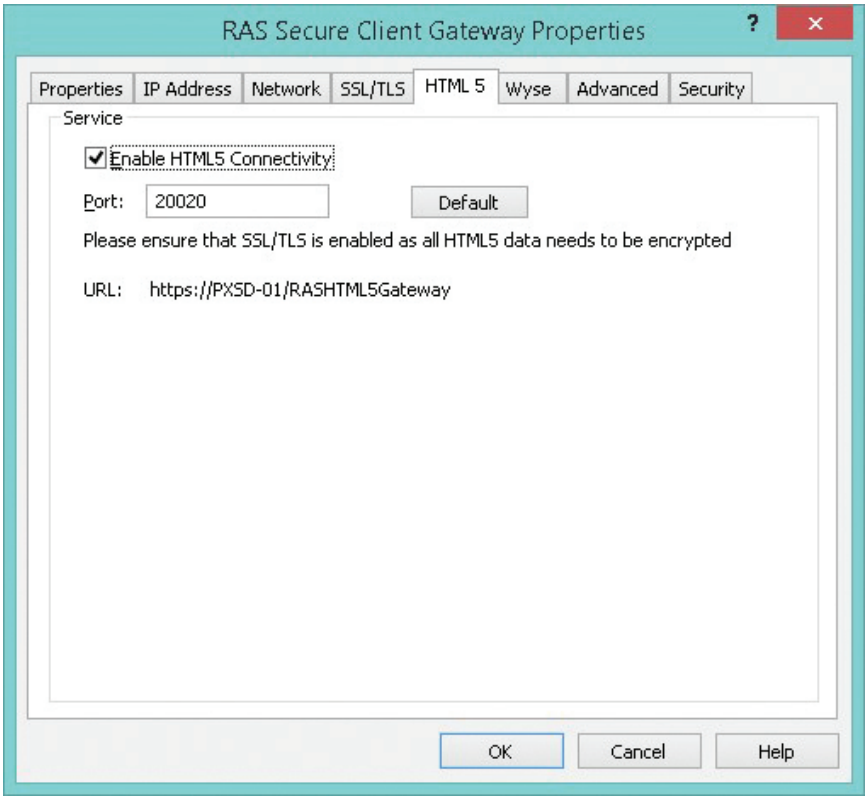
The following steps allow the Virtual Traffic Manager to send encrypted traffic directly to the Parallels Gateway Servers.

1. Log in to the Parallels Remote Application Server Console.
2. Click on the Farm Icon and then click on Gateways.
3. On the Gateway, right-click and click Properties.
4. Click on SSL/TLS.
5. You will need to have an SSL certificate installed on each Gateway. These can be self-signed or actual certificates.
6. The port by default is TCP Port 443. You can change this port to any port not being used by the Windows Server.
7. Once an SSL certificate is in place, you can also enable the HTML5 Gateway. The HTML5 RAS Gateway only works with SSL certificates in place. You will not be able to SSL offload the RAS Gateway with the Brocade Traffic Manager. The SSL certificate is required to be on each gateway in order to enable the Parallels RAS HTML5Gateway.
8. Once you have all Gateways set up that you would like to load-balance, your next step is to configure the Virtual Traffic Manager.

Gateway Mode SSL and Direct Mode SSL Port Example: In the below example, TCP port 443 is used for the RAS SSL/TLS Gateway. This port is used for Gateway Mode SSL, Direct Mode SSL, and HTML5 connections.



Parallels RAS HTML5 Gateway Access Example: In the below example, the Parallels RAS HTML5 Gateway Access is enabled. Note that you must have an SSL certificate in place in order to enable Parallels RAS HTML5Gateway Access.



Configure vTM for View Connection Servers

The following table displays the process for configuring the Virtual Traffic Manager:

Component	Procedure	Description
Virtual Traffic Manager (once)	Create a Traffic IP group.	A single traffic IP group must be created to front the Parallels RAS Gateway Server pool. For details, see the “Create a Traffic IP Group” section.
	Create a pool.	A pool must be created per port. The IP address of each individual Parallels RAS Gateway Server should be added to the pool. For details, see the “Create a Pool” section.
	Configure the Health Monitors for Parallels RAS Gateways and Web Portals	For details, see the “Configure a Health Monitor” section.
	Create a virtual server.	A virtual server must be created per port. For details, see the “Create a Virtual Server” section.
	Configure SSL decryption.	Import the certificate to perform SSL decryption on the vTM. For details, see the “Configure SSL Decryption” section.

Create a Traffic IP Group

A traffic IP group (also known as a virtual IP) must be created on which the virtual server will be listening. To create a new traffic IP group, select **Services > Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**. Fill in the fields as follows:

- Name: A descriptive name for the traffic IP group, i.e., Parallels.RAS for the Parallels RAS Gateways
- IP Addresses: An IP address to be associated to the FQDN of the Parallels RAS Servers.

Create a Pool

A pool must be created for each service managed by the Virtual Traffic Manager. To create a new pool, select **Services > Pools** and scroll down to **Create a new Pool**. Fill in the fields as follows:

- **Pool Name:** A descriptive name for the pool.
- **Nodes:** hostname:80 or ipaddress:80 if SSL decryption is enabled on Virtual Traffic Manager for each of the actual bac kend Connection Servers.

Monitor: Leave as Ping for now.

Configure a Health Monitor

This section details the steps to create a health monitor. The HTTP monitor is used for port 80 on the Parallels Web Portals Connection Servers.

1. Select **Catalogs > Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a name. Set the type to **HTTP** and the scope to **Node**.
4. Click **Create Monitor** to create the monitor.
5. In the subsequent configuration page, scroll down and change the path to /.
6. Change **status regex to ^200$**.
7. Change body regex to **Parallels RAS Webportal**.

Attach the Monitor to a Pool

After the monitor has been created, it must be attached to the appropriate pool.

1. Select **Services > Pools**, and choose the pool that the monitor will be attached to.
2. Scroll down and click **Health Monitoring**.
3. Add the appropriate health monitor.

Create a Virtual Server

Create a virtual server to handle all View Client traffic.

1. Select Services > Virtual Servers, and scroll down to Create a new Virtual Server.
2. Enter the following:
    - **Virtual Server Name:** A descriptive name for the virtual server
    - **Protocol: Generic Client First**
    - **Port:** 443
    - **Default Traffic Pool:** The pool created earlier
4. Click Create **Virtual Server**.
5. In the next screen under **Listening on**, select **Traffic IP Groups**, and c heck the appropriate traffic IP group that was created earlier.

Configure SSL Decryption

Import the Certificate

In order to perform SSL decryption, the certificate and private key used for the Parallels RAS Gateway Virtual Server created earlier must be imported to the Virtual Traffic Manager.

1. Select the **Catalogs > SSL > SSL Certificates** catalog.
2. Click **Import Certificate** to import the appropriate certificate

Enable SSL Decryption on the Virtual Server

After importing the certificate, enable SSL decryption on the virtual server created with the following steps:

1. Select **Services > Virtual Servers**, and choose the virtual server created earlier that will be doing the SSL decryption.
2. Scroll down and click **SSL Decryption**.
3. Set **ssl decrypt** to **Yes**.
4. Select the certificate imported earlier.

Configuration Summary

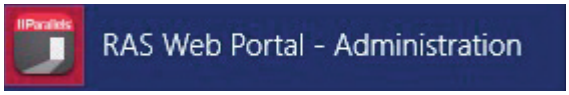
By accessing the **Services > Config Summary** on the webGUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of how the services are configured.

Virtual Servers ▽	Rules	Pools	Nodes
gatewayras *:82	*Use default pool*	**gatewayras**	98.142.5.25:82 98.142.5.5:82
gatewayrassl *:443	*Use default pool*	**gatewayrassl**	98.142.5.25:443 98.142.5.5:443
Webportals *:80	*Use default pool*	**Webportals**	98.142.5.18:80 98.142.5.5:80

Configure Parallels Remote Application Server Web Portal for HTTP and/or HTTPS

The following steps allow the Virtual Traffic Manager to send traffic directly to the Parallels Gateway Servers via the Parallels Web Portal.

1. The Parallels RAS Web Portal must be installed. Note: Web Services ISS is a required role for all Parallels Web Portals.
2. Once ISS is installed on the Web Server, you can run the Parallels Web Portal MSI installer.
3. After the Web Portal is installed, you will see two icons on the Server Desktop.
4. Click on RAS Web Portal – Administration

a. 

b. This will launch the Web Portals Admin Page. This will give you the ability to configure the Parallels RAS Web Portal.

5. Follow the Parallels RAS Web Portal Installation Guide. Parallels Installation Guide
6. Once you have all Parallels Web Portal Servers set up that you would like to load-balance, your next step is to configure the Virtual Traffic Manager.

Preface

Welcome to the Brocade Virtual Traffic Manager (vTM) and Microsoft IIS Deployment Guide. Read this preface for an overview of the information provided in this guide and contact information.
This preface includes the following sections:

- About This Guide
- Contacting Brocade

About This Guide

The Brocade Virtual Traffic Manager and Microsoft IIS Deployment guide describes optimization of Microsoft IIS server farms.

Audience

This guide is written for network operations professionals, server administrators, and DevOps professionals familiar with administering and managing Application Delivery Controllers (ADCs), servers, and applications.

You must also be familiar with:

- Microsoft IIS
- Brocade Virtual Traffic Manager

For more details on the Brocade vADC product family, see: brocade.com/vADC.

Contacting Brocade
This section describes how to contact departments within Brocade.

Internet
You can learn about Brocade products through the company website: brocade.com.

Technical Support
If you have problems installing, using, or replacing Brocade products, contact Brocade Support or your channel partner who provides support. To contact Brocade Support, see brocade.com/en/support.html.

Professional Services
Brocade Global Services has the expertise to help organizations build scalable and efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Brocade Global Services delivers world-class professional services, technical support, and education services, enabling organizations to maximize their Brocade investments, accelerate new technology deployments, and optimize the performance of networking infrastructures

Chapter 4: Solution Overview
This chapter includes the following sections:

- Virtual Traffic Manager Overview
- Microsoft IIS

Virtual Traffic Manager Overview
Brocade Virtual Traffic Manager (vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public websites and private applications. vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run on any physical, virtual, or cloud environment. With vADC products from Brocade, organizations can:

- Make applications more reliable with local and global load balancing.
- Scale application servers by up to 3x by offloading TCP and SSL connection overhead.
- Accelerate applications by up to 4x by using web content optimization (WCO).
- Secure applications from the latest application attacks, including SQL injection, XSS, CSRF, and more.
- Control applications effectively with built-in application intelligence and full-featured scripting engine.

Virtual Traffic Manager offers much more than basic load balancing. It controls and optimizes end- user services by inspecting, transforming, prioritizing, and routing application traffic. The powerful TrafficScript® engine facilitates the implementation of traffic management policies that are unique to an application by allowing organizations to build custom functionality or to leverage existing features in Virtual Traffic Manager in a specialized way. With vTM, organizations can deliver:

Performance
Improve application performance for users by offloading encryption and compression from the web server by dynamic caching and reducing the number of TCP sessions on the application.

Reliability and scalability
Increase application reliability by load balancing traffic across web and application servers, balancing load across multiple data centers (private or public clouds), monitoring the response time of servers in real-time to decide the fastest way to deliver a service, protecting against traffic surges, and by managing the bandwidth and rate of requests used by different classes of traffic.

Advanced scripting and application intelligence

Manage application delivery more easily with fine-grained control of users and services using TrafficScript, an easy-to-use scripting language that can parse any user transaction, and take specific, real-time action based on user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, while operations teams use it to quickly respond to changing business requirements or problems within an application before developers can fix it.

Application acceleration

Dramatically accelerate web-based applications and websites in real-time with optional web content optimization (WCO) functionality. It dynamically groups activities for fewer long distance round trips, resamples and sprites images to reduce bandwidth, and minifies JavaScript and combines style sheets to give the best possible response time for loading a web page on any browser or device.

Application-layer security

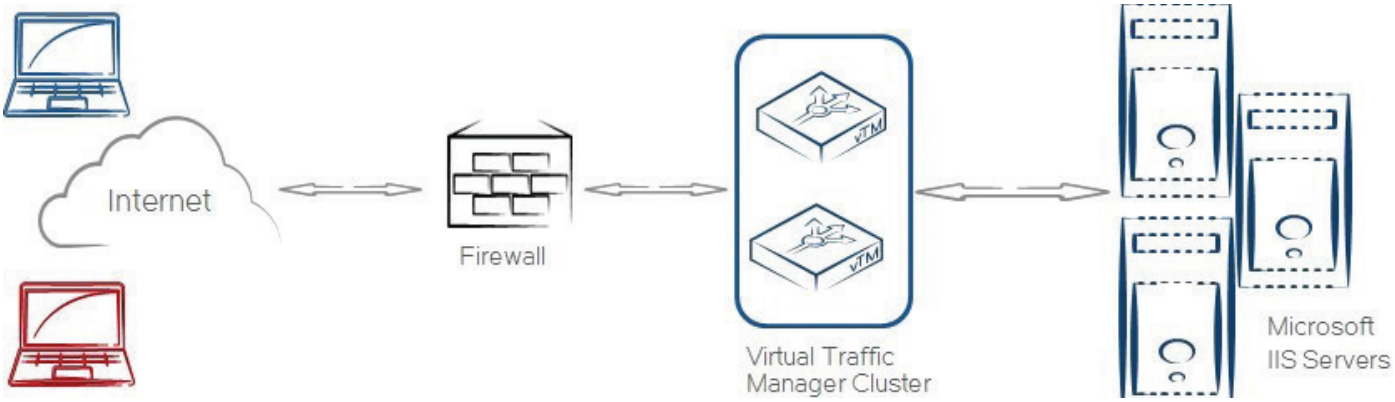
Enhance application security by filtering out errors in web requests, and protecting against external threats, with the option of a comprehensive Layer-7 firewall to defend against deliberate attacks.

Microsoft IIS

Internet Information Services (IIS) for Windows Server is a flexible, secure, and manageable web server for hosting anything on the Web. From media streaming to web applications, IIS's scalable and open architecture is ready to handle the most demanding tasks.

Chapter 5: Microsoft IIS Architecture and Parallels RAS Web Portal

The deployment architecture, including the Traffic Manager and Microsoft IIS servers, is shown in the following topology:



IIS can be quickly, easily, and securely integrated into the Traffic Manager. Because access to IIS is generally secured using HTTPS, it is recommended to do SSL decryption on the Traffic Manager, thereby reducing the CPU load on the IIS server backend. An HTTP protocol server, listening on port 443 and decrypting traffic, should be configured to handle traffic to the IIS server.

Chapter 6: Deploying Traffic Manager for IIS and Parallels RAS Web Portal

This chapter describes the process for deploying Virtual Traffic Manager to optimize the IIS installation. It includes the following sections:

- Requirements
- Configure vTM for Microsoft IIS

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft IIS (6.0 or later)

Note: This deployment guide was certified while the product was with Riverbed and for 9.x or earlier versions of the Traffic Manager.

Configure vTM for Microsoft IIS

This section contains step by step instructions on configuring Traffic Manager for Microsoft IIS suite:

Component	Procedure	Description
Virtual Traffic Manager (once)	Create Traffic IP Group for Microsoft IIS	A single Traffic IP Group must be created For details, see “Create Traffic IP Group”
	Create Pool for the IIS server farms (once for each server farm)	A Pool needs to have a set of servers to load-balance. Enter the hostname or IP address of the node along with the TCP/UDP port For details, see “Create Pool”
	Create Virtual Server for the application servers	Create and associate the Virtual Server to the server pool. For details, see “Create Virtual Server”
	SSL decryption	Configure SSL Decryption to enable SSL offloads. For details, see “SSL Decryption”
	Configure Session Persistence	Configure SSL Decryption to enable SSL offloads. For details, see “Configure Session Persistence”
	Preserve Client IP address	Configure vTM to preserve client IP address For details, see “Configure vTM to preserve client IP”

Create Traffic IP Group

A Traffic IP Group (also known as a Virtual IP) will need to be created on which the virtual server will be listening. To create a new Traffic IP Group:

1. Navigate to Services->Traffic IP Groups and scroll down to Create a new Traffic IP Group.
2. Fill in the fields as follows:
    - Name: A descriptive name for the application server
    - IP Addresses: An IP Address that is mapped to FQDN of the application.
3. Click Create Traffic Group.

Create Pool

A Pool has to be created for the IIS server farm as shown in the topology diagram. To create a new Pool:

1. Navigate to Services->Pools and scroll down to Create a new Pool.
2. Fill in the fields as follows:
    - Pool Name: A descriptive name for the pool

- Nodes: hostname:80 or ipaddress:80
- Leave the monitor on the defaults.
- Select Load balancing algorithm under Services -> Pools -> <pool> -> Load balancing as Least connections.

Create Virtual Server

Create a Virtual Server that will handle all the application traffic. To create a new Virtual Server:

1. Navigate to **Services->Virtual Servers** and scroll down to **Create a new Virtual Server**.
2. Enter the following:
   - **Virtual Server Name:** A descriptive name for the Virtual Server
   - **Protocol:** HTTP
   - **Port:** 443
   - **Default Traffic Pool:** Select the pool created in the step above.
3. Click on **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate Traffic IP Group that was created earlier.
5. Set **Enabled:** to **Yes**.
6. Click on the **Update** button to apply changes.

SSL Decryption

In order to perform SSL decryption, the certificate and the private key used for the Virtual Server created in the previous step must be imported into the Traffic Manager.

1. Navigate to the **Catalogs > SSL > SSL Certificates** catalog.
2. Click on **Import Certificate** to import the appropriate certificate.

After importing the certificate, enable SSL decryption on the Virtual Server created:

1. Navigate to **Services > Virtual Servers** and select the virtual server that will be performing SSL decryption.
2. Scroll down and click on **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in the previous step.
5. Scroll down to the bottom of the page and click **Update**.

Configure Session Persistence

To ensure that clients persist their connections to the load-balanced servers after login, configure the following:

1. Go to **Catalogs > Persistence** and create a new class called **IIS Persistence**.
2. Set this class to use the **Transparent Session Affinity** method and failure mode of **choose a new node to use**.
3. Click **Update** to finish.
4. Go to **Services > Pools > <IIS pool> > Session Persistence**.

5. Select the class from the list and click **Update**.

Configure vTM to preserve client IP

To ensure that the client IP is preserved when it reaches the IIS farm, configure the following:

1. Enable the add_cluster_ip setting in the Traffic Manager under **Services -> Virtual Server -> Connection Settings > HTTP Specific settings**.

2. Use a custom ISAPI filter to change the logging behavior of IIS. The header you need to log is X-Cluster-Client-IP.

Configuration Summary

By accessing the **Services > Config Summary** on the webGUI, a complete snapshot of all the configured services is provided. This is very useful table to glance through to get a good understanding of how the services are configured.