Radware's AppDirector and Microsoft Windows Terminal Services 2008 Integration Guide

Contents

SOLUTION OVERVIEW **2**

RADWARE APPDIRECTOR OVERVIEW **2**

MICROSOFT WINDOWS TERMINAL SERVICES 2008 ..... **2**

SOLUTION DETAILS **3**

HOW IT WORKS **3**

IMPORTANT NOTES: 3
SOFTWARE AND HARDWARE 4
TESTED NETWORK OVERVIEW 4

CONFIGURATION **5**

RADWARE DEVICES 5
APPDIRECTOR ACTIVE CONFIGURATION *5*
APPDIRECTOR BACKUP CONFIGURATION *9*
WINDOWS 2008 TS SERVER-1 ..... *10*
WINDOWS 2008 TS SERVER-2 ..... *10*
WINDOWS 2008 TS GW SERVER-1 ..... *10*
WINDOWS 2008 TS GW SERVER-2 ..... *11*
CLIENT CONFIGURATION *12*
Technical Support *13*

TECHNICAL SOLUTION GUIDE

AUTHOR: Elad Kurzweil

DATE: Tuesday, November 17, 2009
Version: 1.0

Solution Overview

The Radware and Microsoft Terminal Services 2008 solution ensures Microsoft Terminal Services 2008 customers solution resilience, efficiency and scale. Radware's AppDirector guarantees Terminal Services 2008 maximum availability, scalability, performance and security. AppDirector provides advanced health monitoring to avoid system down time and advanced traffic management to deliver a best of breed subsystem. With a pay as you grow platform licensing model, AppDirector ensures long term investment protection facilitating incremental growth demanded by today's business.

Radware AppDirector Overview

Radware's AppDirector is an intelligent application delivery controller (ADC) which provides scalability and application-level security for service infrastructure optimization, fault tolerance and redundancy. Radware has combined its next-generation, OnDemand Switch multi-gigabit hardware platform with the powerful capabilities of the company's APSolute™ operating system. The result – AppDirector – enables accelerated application performance; local and global server availability; and application security and infrastructure scalability for fast, reliable and secure delivery of applications over IP networks.

AppDirector is powered by the innovative OnDemand Switch platform. This has established a new price/performance standard in the industry, delivering breakthrough performance and superior scalability to meet evolving network and business requirements. Based on its on demand, "pay-as-you-grow" approach, no forklift upgrade is required even when new business requirements arise. This helps companies guarantee short-term and long-term savings on CAPEX and OPEX for full investment protection. Radware's OnDemand Switch enables customers to pay for the exact capacity currently required, while allowing them to scale their ADC throughput capacity and add advanced application-aware services or application acceleration services on demand to meet new or changing application and infrastructure needs. And it does all this without compromising on performance.

AppDirector lets you get the most out of your service investments by maximizing the utilization of service infrastructure resources and enabling seamless consolidation and high scalability. AppDirector's throughput licensing options allows "pay-as-you-grow" investment protection. Make your network adaptive and more responsive to your dynamic services and business needs with AppDirector's fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, application acceleration, bandwidth management, intrusion prevention and DoS protection.
For more information, please visit: http://www.radware.com/

Microsoft Windows Terminal Services 2008

The Terminal Services server role in Windows Server® 2008 provides technologies that enable users to access Windows-based programs installed on a terminal server, or to access the full Windows desktop. With Terminal Services, users can access a terminal server from within a corporate network or from the Internet.

Terminal Services lets you efficiently deploy and maintain software in an enterprise environment. You can easily deploy programs from a central location. Because you install the programs on the terminal server and not on the client computer, programs are easier to upgrade and to maintain.

When a user accesses a program on a terminal server, the program execution occurs on the server. Only keyboard, mouse, and display information is transmitted over the network. Each user sees only their individual session. The session is managed transparently by the server operating system and is independent of any other client session.

Why use Terminal Services?
If you deploy a program on a terminal server instead of on each device, there are many benefits. These include:

- You can quickly deploy Windows-based programs to computing devices across an enterprise. Terminal Services is especially useful when you have programs that are frequently updated, infrequently used, or difficult to manage.
- Terminal Services can significantly reduce the network bandwidth required to access remote applications.
- Terminal Services helps boost user productivity. Users can access programs that are running on a terminal server from devices such as home computers, kiosks, low-powered hardware, and operating systems other than Windows.
- Terminal Services provides better program performance for branch office workers who need access to centralized data stores. Data-intensive programs sometimes do not have client/server protocols that are optimized for low-speed connections. Programs of this kind frequently perform better over a Terminal Services connection than over a typical wide area network.

For more information, please visit:

http://technet.microsoft.com/en-us/library/cc755053%28WS.10%29.aspx

Solution Details

The suggested solution uses 2 Windows 2008 Terminal servers for the Remote Desktop Protocol (RDP) connection. The 2 AppDirectors installed in the front of the Windows 2008 Terminal Servers Gateway and the Windows 2008 Terminal servers are providing availability, acceleration, connection persistency and protection:

- AppDirector continuously monitors the operational availability of the Windows 2008 Terminal servers.
- AppDirector is offloading the SSL traffic processing from the external users (Internet side)
- AppDirector intelligently distributes the application transactions between the Windows 2008 Terminal servers, ensuring that all the transactions that belong to the same application session will reach the same Windows 2008 Terminal server.
- The dual AppDirectors are providing a highly available solution with no single point of failure

How it works

1. The client opens the RDP (RDP over SSL port 443) session to IP 10.1.30.215 (AppDirector TS GW VIP).
2. The AppDirector terminates the SSL connection and connects in the back end over clear HTTP traffic to one of the TS GW servers.
3. The TS GW server peels the RDP from the HTTP and sends it to IP 13.1.2.200 (TS Servers VIP) over TCP port 3389
4. The AppDirector chooses a TS Server and sends the RDP traffic to the TS server (persistency is maintained according to TS Cookie enabled on the AppDirector).

Important Notes:

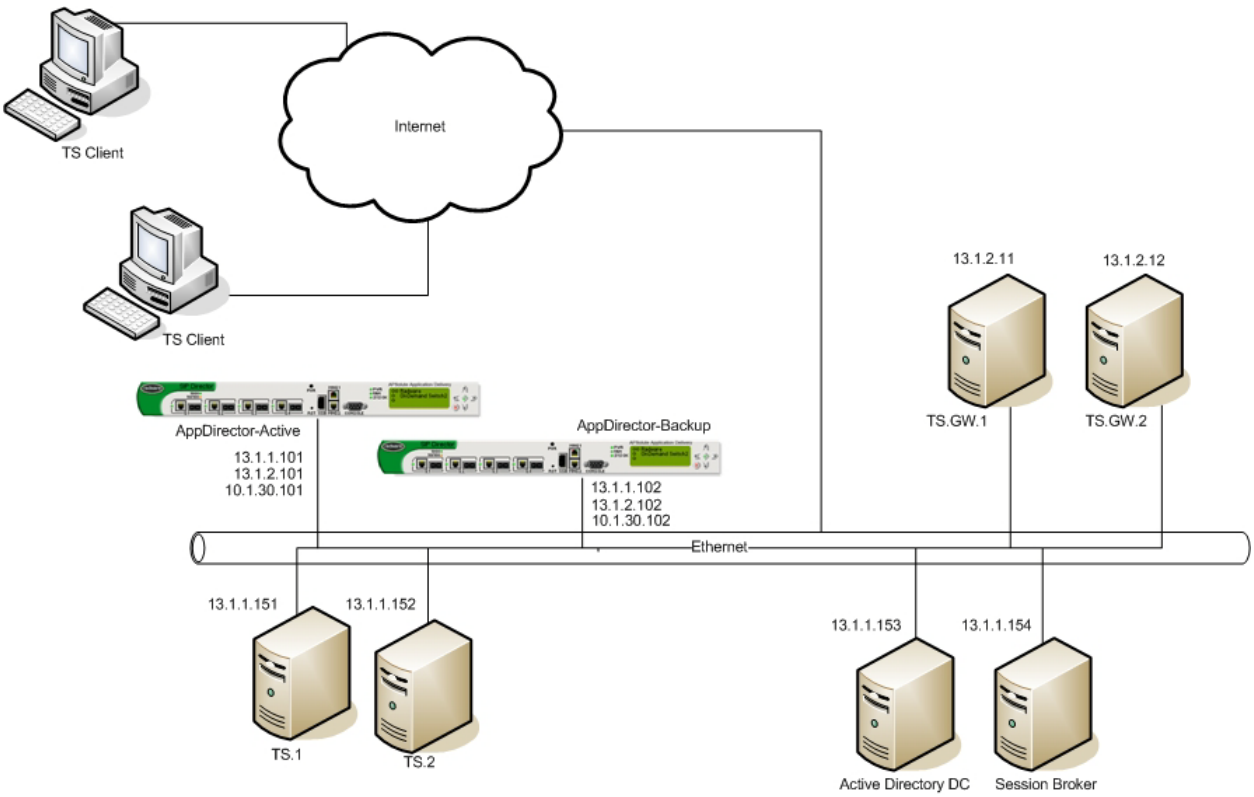
- The solution can be easily extended to support additional Windows 2008 Terminal servers for higher capacity
- Make sure that the L4 for the TS servers are configured with TS COOKIE in the Application field
- Enable the SSL Bridging in the Windows Terminal Gateway servers.

Software and Hardware

The following is a list of hardware and multimedia software tested to verify the interoperabilty of the solution:

- Radware's Appdirector v.2.11
- Video Streaming Server : Windows Terminal services 2008
- Streaming video Client: RDP v6.1, IE8, IE7

Tested network overview



Network Diagram

Configuration

Radware Devices

APPDIRECTOR ACTIVE CONFIGURATION

Network Configuration

- Create IP 10.1.30.101/16 on port 1
- Create IP 13.1.1.101/24 on port 1
- Create IP 13.1.2.101/24 on port 1
- Create default route to 10.1.0.1

Farm Configuration

1. Create Farm named "Win.2008.TS.farm" in **AppDirector -> Farms -> Farm Table** with these parameters:
    - Farm Name – Win.2008.TS.farm
    - Session mode – EntryPerSession
    - Connectivity checks – No Checks
    - Leave all other fields as default

2. Create Farm named "Win.2008.GW.farm" in **AppDirector -> Farms -> Farm Table** with these parameters:
    - Farm Name – Win.2008.GW.farm
    - Session mode – EntryPerSession
    - Connectivity checks – No Checks
    - Leave all other fields as default

Servers Configuration

1. Create Server named "Win.2008.TS.Server.1" and attach it to Farm "Win.2008.TS.farm" in **AppDirector -> Servers -> Server Table** with these parameters:
    - Server Name - Win.2008.TS.Server.1
    - Farm Name – Win.2008.TS.farm
    - Server Address – 13.1.1.151
    - Leave all other fields as default

2. Create Server named "Win.2008.TS.Server.2" and attach it to Farm "Win.2008.TS.farm" in **AppDirector -> Servers -> Server Table** with these parameters:
    - Server Name - Win.2008.TS.Server.2
    - Farm Name – Win.2008.TS.farm
    - Server Address – 13.1.1.152
    - Leave all other fields as default

3. Create Server named "Win.2008.GW.Server.1" and attach it to Farm "Win.2008.GW.farm" in **AppDirector -> Servers -> Server Table** with these parameters:
    - Server Name - Win.2008.GW.Server.1
    - Farm Name – Win.2008.GW.farm
    - Server Address – 13.1.2.11
    - Leave all other fields as default

4. Create Server named "Win.2008.GW.Server.2" and attach it to Farm "Win.2008.GW.farm" in **AppDirector -> Servers -> Server Table** with these parameters:
    - Server Name - Win.2008.GW.Server.2

- Farm Name – Win.2008.GW.farm
- Server Address – 13.1.2.12
- Leave all other fields as default

SSL Policy Configuration

Create an SSL policy in AppDirector -> L4 Traffic Redirection -> SSL Policy with these parameters:

- Policy name – SSL.policy
- Certificate – radware
- Listening Server Port – 80 (AppDirector listens to HTTP port clear traffic)
- Leave all other fields as default

Note: Throughout this guide, reference is made to the "radware" pre-configured certificate, but you can import a certificate or create a new certificate in AppDirector. For more information on exporting, importing, or creating a certificate, see the AppDirector User Guide.

Compression Configuration

Create a compression policy named "compression.policy" in AppDirector -> Servers -> Layer4 Traffic configuration -> Compression Policy with these parameters:

- Policy Name – compression.policy
- Algorithm – GZIP
- Compression lever - 1
- Leave all other fields as default

HTTP Policies

Create HTTP Policy named "TS.policy" in AppDirector -> Servers -> HTTP Policies with these parameters:

- L7 Persistent Switching Mode – First
- Leave all other fields as default

Layer 4 Configuration

1. Create L4 Policy for RDP Traffic named "Terminal.Server.2008.TS.Flow" in **AppDirector -> Servers -> Server Table** with these parameters:
   - L4 Policy Name – Terminal.Server.2008.TS.Flow
   - Virtual IP – 13.1.2.200
   - L4 Protocol – TCP
   - L4 Port – 3389
   - Application – TS COOKIE
   - Farm Name – Win.2008.TS.farm
   - HTTP Policy - TS.policy
   - Leave all other fields as default

2. Create L4 Policy for RDP Traffic named "Terminal.Server.2008.GW.Flow" in **AppDirector -> Servers -> Server Table** with these parameters
   - L4 Policy Name – Terminal.Server.2008.GW.Flow
   - Virtual IP – 10.1.30.215
   - L4 Protocol – TCP
   - L4 Port – 443
   - Application – HTTPS
   - Compression Policy - compression.policy
   - Farm Name – Win.2008.GW.farm
   - HTTP Policy - TS.policy
   - SSL Policy – SSL.policy

- Leave all other fields as default

AppDirector Health Monitoring

1. Enable Health Monitoring in **Health Monitoring -> Global Parameters**

2. Create a Check for RDP on server 13.1.1.151 in **Health Monitoring -> Check Table**
   - Check name – WTS.2008.TS.Server.1
   - Method – TCP Port
   - Dest IP – 13.1.1.151
   - Dest Port – 3389

3. Create a Check for RDP on server 13.1.1.152 in **Health Monitoring -> Check Table**
   - Check name – WTS.2008.TS.Server.2
   - Method – TCP Port
   - Dest IP – 13.1.1.152
   - Dest Port – 3389

4. Create a Check for port 80 on server 13.1.2.11 in **Health Monitoring -> Check Table**
   - Check name – WTS.2008.GW.Server.1
   - Method – TCP Port
   - Dest IP – 13.1.2.11
   - Dest Port – 80

5. Create a Check for port 80 on server 13.1.2.12 in **Health Monitoring -> Check Table**
   - Check name – WTS.2008.GW.Server.2
   - Method – TCP Port
   - Dest IP – 13.1.2.12
   - Dest Port – 80

6. Bind the RDP check WTS.2008.TS.Server.1 to Server Farm Win.2008.TS.farm - 13.1.1.151 in **Health Monitoring -> Binding Table**

7. Bind the RDP check WTS.2008.TS.Server.2 to Server Farm Win.2008.TS.farm - 13.1.1.152 in **Health Monitoring -> Binding Table**

8. Bind the TCP 80 check WTS.2008.GW.Server.1 to Server Farm Win.2008.GW.farm - 13.1.2.11 in **Health Monitoring -> Binding Table**

9. Bind the TCP 80 check WTS.2008.GW.Server.2 to Server Farm Win.2008.GW.farm - 13.1.2.12 in **Health Monitoring -> Binding Table**

VRRP Configuration

1. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
    - IP Redundancy Admin Status – VRRP
    - Interface Grouping – Enable
    - ARP with interface grouping – Send
    - VLAN Redundancy – Active
    - Backup Fake ARP – Enable
    - Backup Interface Grouping – Enable

2. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
    - IF Index – 1
    - VR ID – 1
    - Priority – 255 (Highest number is Active device)
    - Primary IP – 10.1.30.101
    - Leave all other options as default

3. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
    - IF Index – 1
    - VR ID – 1
    - Priority – 255 (Highest number is Active device)
    - Primary IP – 13.1.1.101
    - Leave all other options as default

4. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
    - IF Index – 1
    - VR ID – 1
    - Priority – 255 (Highest number is Active device)
    - Primary IP – 13.1.2.101
    - Leave all other options as default

5. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**

    - IF Index – 1, VR ID – 1, Associated IP 10.1.30.101
    - IF Index – 1, VR ID – 1, Associated IP 10.1.30.215
    - IF Index – 1, VR ID – 1, Associated IP 13.1.1.101
    - IF Index – 1, VR ID – 1, Associated IP 13.1.2.101
    - IF Index – 1, VR ID – 1, Associated IP 13.1.2.200

APPDIRECTOR BACKUP CONFIGURATION

Network Configuration

- Create IP 10.1.30.102/16 on port 1
- Create IP 13.1.1.102/24 on port 1
- Create IP 13.1.2.102/24 on port 1
- Create default route to 10.1.0.1
- Copy the configuration from the Active AppDirector device

Auto Generating the Backup Configuration from the Primary AppDirector

1. From the web interface menu of the Primary AppDirector, select **File -> Configuration -> Receive from Device** and choose Backup (Active-Backup) save the file on your computer and call it AppDirector.backup.txt.
2. Open the browser on the AppDirector backup device and upload the saved configuration (AppDirector.backup.txt) in **File -> Configuration -> Send to Device**
3. Reboot the AppDirector Backup device

VRRP Configuration

1. Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
   - IP Redundancy Admin Status – VRRP
   - Interface Grouping – Enable
   - ARP with interface grouping – Send
   - VLAN Redundancy – Active
   - Backup Fake ARP – Enable
   - Backup Interface Grouping – Enable

2. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
   - IF Index – 1
   - VR ID – 1
   - Priority – 100 (Highest number is Active device)
   - Primary IP – 10.1.30.102
   - Leave all other options as default

3. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
   - IF Index – 1
   - VR ID – 1
   - Priority – 100 (Highest number is Active device)
   - Primary IP – 13.1.1.102
   - Leave all other options as default

4. Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
   - IF Index – 1
   - VR ID – 1
   - Priority – 100 (Highest number is Active device)
   - Primary IP – 13.1.2.102
   - Leave all other options as default

5. Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**
   - IF Index – 1, VR ID – 1, Associated IP 10.1.30.101
   - IF Index – 1, VR ID – 1, Associated IP 10.1.30.215
   - IF Index – 1, VR ID – 1, Associated IP 13.1.1.101

- IF Index – 1, VR ID – 1, Associated IP 13.1.2.101
- IF Index – 1, VR ID – 1, Associated IP 13.1.2.200

WINDOWS 2008 TS SERVER-1

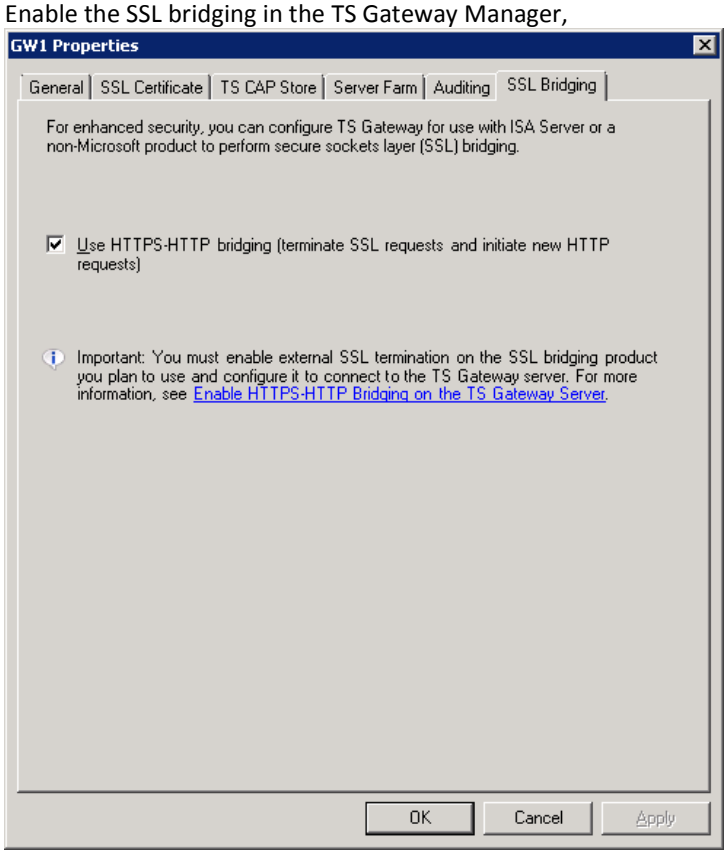
- Create IP 13.1.1.151/24 on network interface
- Create Default GW to 13.1.1.101

WINDOWS 2008 TS SERVER-2

- Create IP 13.1.1.152/24 on network interface
- Create Default GW to 13.1.1.101

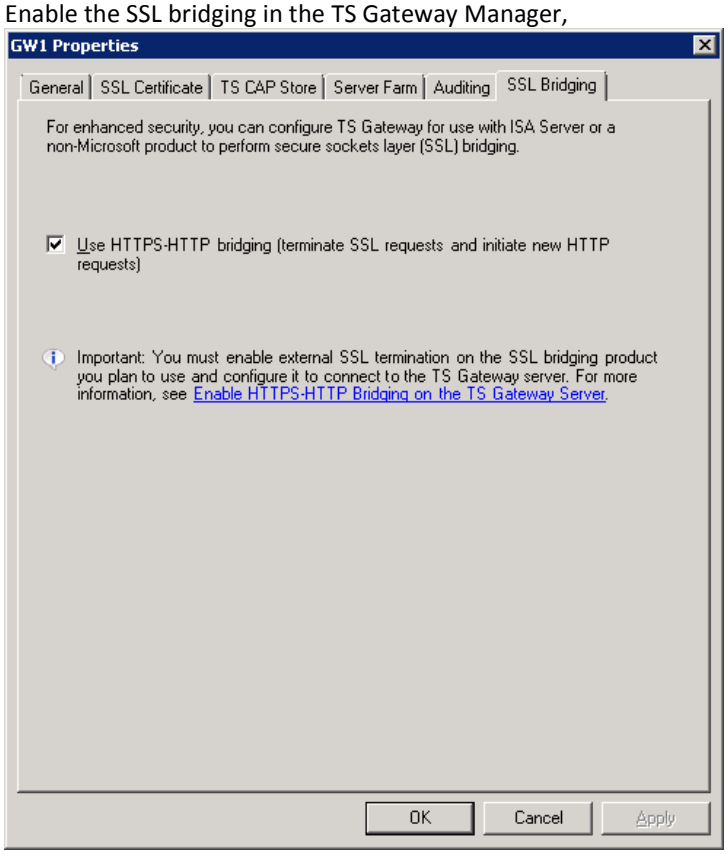
WINDOWS 2008 TS GW SERVER-1

- Create IP 13.1.2.11/24 on network interface
- Create Default GW to 13.1.2.101
- Enable the SSL bridging in the TS Gateway Manager,

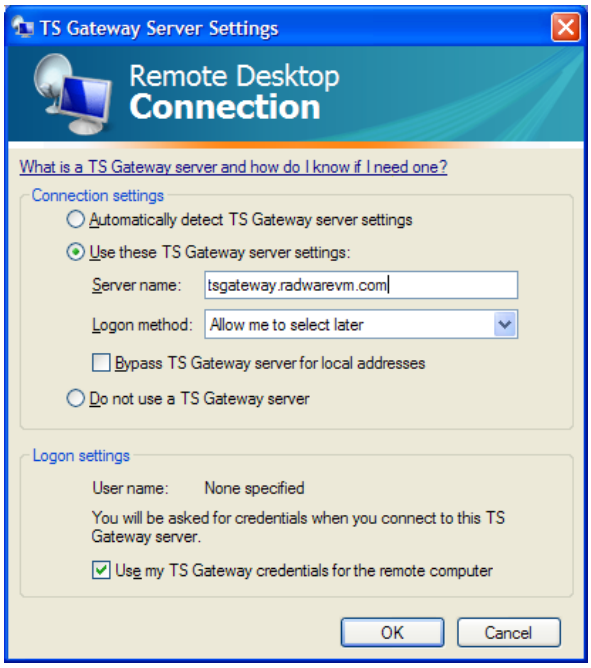


WINDOWS 2008 TS GW SERVER-2

- Create IP 13.1.2.12/24 on network interface
- Create Default GW to 13.1.2.101
- Enable the SSL bridging in the TS Gateway Manager,



CLIENT CONFIGURATION

- In order to work with the RDP client please copy the Certificate from the AppDirector and install it under the computer Root certificates field (Certificate and key).
- RDP Client configuration,
  - Go to Advanced tab
  - Press on Settings button
  - Mark "Use these TS Gateway server settings"
  - In Server Name field add tsgateway.radwarevm.com
  - In Logon settings area mark "Use my TS Gateway credentials for the remote computer"
  - 

Technical Support

Radware offers technical support for all of its products through the Radware Certainty Support Program. Please refer to your Certainty Support contract, or the Radware Certainty Support Guide available at: http://www.radware.com/content/support/supportprogram/default.asp

For more information, please contact your Radware Sales representative or:
U.S. and Americas: (866) 234-5763
International: +972(3) 766-8666