

TESTING & INTEGRATION GROUP

SOLUTION GUIDE

AppDirector Load balancing IBM Websphere and AppXcel

INTRODUCTION	2
RADWARE APPDIRECTOR	3
RADWARE APPXCEL	3
IBM WEBSHERE	4
SOLUTION DETAILS	4
HOW IT WORKS	5
SOFTWARE AND HARDWARE	5
TESTED NETWORK OVERVIEW	6
CONFIGURATION	7
RADWARE DEVICES	7
<i>APPDIRECTOR ACTIVE CONFIGURATION</i>	<i>7</i>
<i>APPDIRECTOR BACKUP CONFIGURATION</i>	<i>10</i>
<i>APPXCEL APPLIANCE - 1</i>	<i>12</i>
<i>APPXCEL APPLIANCE - 2</i>	<i>13</i>
<i>IBM WEBSHERE SERVER-1</i>	<i>13</i>
<i>IBM WEBSHERE SERVER-2</i>	<i>13</i>
TECHNICAL SUPPORT	14

Introduction

Business success relies mainly on its ability to provide efficient, reliable and secure services to its customers and employees. Most of these services are provided online by utilizing the business IT infrastructure. Therefore, optimizing IT infrastructure and application servers is a business imperative.

IBM's WebSphere Application Server (WebSphere) conveys a flexible and secure infrastructure to the service architecture of any business application. Such abilities make WebSphere a smart choice to any service oriented industry, particularly in the banking and electronic trading industries.

Radware's AppXcel and AppDirector Application Front End (AFE solution) optimize network performance in front of an IBM WebSphere cluster and add crucial Application Intelligent to the network. The AFE Solution offers high availability, accelerated response time, security and scalability to IBM WebSphere applications servers and IT infrastructure, effectively lowering costs and enabling new revenues.

Reduction of cost includes savings in Capital expenses (CAPEX) as well as operational expenses (OPEX). Radware's AFE HW acceleration capabilities will result in off-loading workload from the WebSphere server, thereby reducing the equipment and development costs of new application services. In addition, Radware's AFE virtualization enablement will result in consolidating server resources and sharing them by all applications.

In addition, Radware's solution is comprised with the capability of automatically identifying server performance failures and bypassing the problem without human intervention. Thereby, it allows easier management and automatic failover capability in handling IT malfunctions.

In summary, by Utilizing the IBM WebSphere and Radware's AFE solution, large scale service oriented enterprises (such as, finance and banking, Insurance, E-com and Service Portals) will be able to provide a wider variety of services and online applications, introduce plenty of new services which will increase their revenue stream, all the while maintaining a friendly user experience and lowering expenses.

Radware AppDirector

Radware AppDirector is an intelligent application delivery controller for the data center that provides scalability and application-level security for IT infrastructure optimization, fault tolerance and redundancy.

AppDirector combines the power of Radware's Multi-Gigabit Application Switching hardware with APSolute OS Application-Smart Networking to ensure local and global server availability, accelerated application performance and safeguard applications with integrated intrusion prevention and denial of service protection for fast, reliable, secure application delivery.

AppDirector uses advanced Layer 4-7 policies and granular application intelligence for end-to-end application-smart networking, aligning server infrastructure operations with application front end requirements to eliminate traffic surges, server bottlenecks, connectivity disconnects and downtime for assured application access, full application continuity and redundancy. AppDirector enables fine tuning of network behavior at all critical points, end-to-end, based on granular application-specific classification of packets to optimize traffic flows for a wide range of enterprise applications such as SAP, Oracle, BEA, Citrix, and other web-based applications including support for VoIP, streaming media, and secure LDAP applications.

With AppDirector's fully integrated intrusion prevention and Denial of Service protection data center applications and server resources are insulated against application level attacks. The ability to control multi-step SSL processing provides enhanced security of HTTP, FTP, SMTP and SIP over SSL.

AppDirector lets you get the most out of your IT investments by maximizing the utilization of server infrastructure resources and enabling seamless consolidation and high scalability. Make your network adaptive and more responsive to your dynamic application and business needs with AppDirector's fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, bandwidth management, intrusion prevention and DoS protection.

For more information, please visit: <http://www.radware.com>

Radware AppXcel

AppXcel provides end-to-end application acceleration for web-based, SSL-based FTP applications, and all types of clients such as desktops, PDAs and smart-phones, enabling complete transaction reliability, accelerated transaction response time and cost effective scalability.

AppXcel is a high yield application accelerator, driving application performance using a comprehensive set of AoIP acceleration technologies including compression, caching, connection pooling, TCP optimization, SSL offloading and wireless acceleration for fastest application and transaction response times and the best end user experience across the LAN, WAN and the Internet. AppXcel allows for economical and transparent scaling of server resources and delivers immediate ROI by optimizing server resources and boosting web-based application speeds by up to 500%.

AppXcel dramatically reduces transaction response times by compressing web content, optimizing images, HTTP connection multiplexing and controlling bandwidth utilization. By offloading SSL and persistent functions (processor and server intensive operations) from servers, AppXcel frees the CPU to handle additional requests, thus eliminating the need to buy additional hardware in order to support application processing requirements. AppXcel

clustering enables further transaction scalability delivering up to 35,000 TPS, for unlimited transaction growth.

AppXcel uses a high throughput, dedicated and specialized acceleration platform that enables fastest SSL transactions per second and supports concurrent connections managing certificates. Featuring client and server side SSL sniffing, AppXcel provides complete transaction visibility and security of encrypted traffic, preventing SSL virus tunneling while guaranteeing end-to-end application-smart performance tuning for web-enabled, SSL-based applications on all types of clients including desktops, PDAs, and smart-phones.

For more information, please visit: <http://www.radware.com>

IBM WebSphere

WebSphere Application Server offers a world-class infrastructure for the next chapter in open e-business platforms. As the foundation of the WebSphere software platform, WebSphere Application Server provides a rich, e-business application deployment environment with a complete set of application services including capabilities for transaction management, security, clustering, performance, availability, connectivity and scalability.

For more information, please visit: <http://www-306.ibm.com/software/websphere/>

Solution Details

The suggested solution uses 2 IBM WebSphere servers for the application logic processing. Radware 2 AppDirectors and 2 AppXcels are installed in the front end of the IBM WebSphere in order to provide availability, acceleration and protection:

- AppDirector continuously monitor the operational of the IBM WebSphere application
- AppDirector intelligently distributes the application transactions between the IBM WebSphere servers, making sure that all the transactions that belong to the same application session will reach the same IBM WebSphere server
- AppDirector intercepts HTTP/HTTPS traffic and forwards it to the AppXcel devices
- AppXcel terminates HTTPS connections and connects to the server using HTTP
- AppXcel compresses HTTP objects to accelerate the response time for the clients
- The dual AppDirector and AppXcel are providing a highly available solution with no single point of failure

How it works

The client opens HTTP or HTTPS session to IP 192.168.1.50 (AppDirector VIP). The AppDirector chooses one of the AppXcel appliances and forwards the connection to that AppXcel. The AppXcel establishes the connection to get the request from the client. The AppXcel terminates the SSL connection (if encrypted). Then, the AppXcel forwards the decrypted request back to the AppDirector. The AppDirector recognizes whether the request belongs to an existing application session or not (by the session ID), selects a server and forwards the request to the server.

On the response, the AppDirector receives the response from the server. If the response includes a new session ID the AppDirector learns it. The response goes back through the AppXcel device, that compresses the object and then encrypts it. It goes back to the client through the AppDirector.

Note that the whole process is transparent to the servers that communicate with the client IP and the client who makes the whole communication with the Virtual service IP address.

Important Notes:

- **SSL with Select Server mode - remember enabling the SSL session ID Tracking on the AppDirector.**
- **The setup can be installed as a global solution with many sites.**
- **If Hardware card install in the AppXcel please use Hardware based compression in the Compression filed.**
- **If client IP transparency is not required, the AppXcel offers TCP multiplexing capability that hides the client IPs and greatly reduces the TCP connections on the server to free all the resources for Application logic processing**

Software and Hardware

The following is a list of hardware and Multimedia software tested to verify the interoperability of the presented solution:

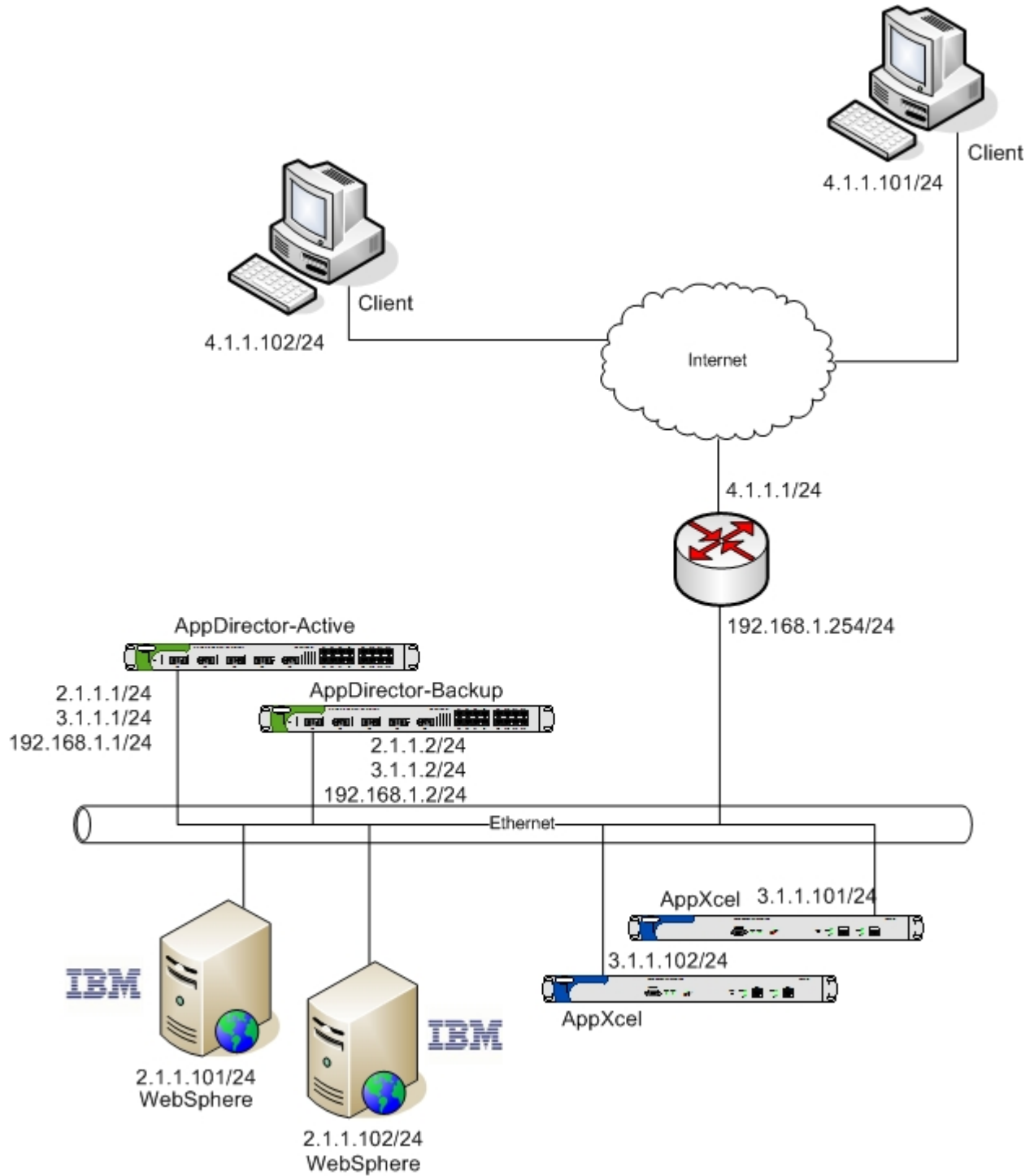
Radware's Appdirector v.1.00.2

Radware's AppXcel v.1.00

Web Client: Windows MS Explorer 6.0

Application Server : IBM WebSphere 6.1

Tested network overview



Network Diagram

Configuration

Radware Devices

APPDIRECTOR ACTIVE CONFIGURATION

Network Configuration

- Create IP 2.1.1.1 on port 17
- Create IP 3.1.1.1 on port 17
- Create IP 192.168.1.1 on port 17
- Create default route to 192.168.1.254

Farm Configuration

- Create Farm named "AppXcel.Farm" in **AppDirector -> Farms -> Farm Table** with these parameters (for the AppXcel appliances using HTTPS mode)
 - o Farm Name – AppXcel.Farm
 - o Session mode – Server per session
 - o Connectivity checks – No Checks
 - o Leave all other fields as default
- Create Farm named "WebSphere.Server.Farm" in **AppDirector -> Farms -> Farm Table** with these parameters (for the WebSphere Servers)
 - o Farm Name – WebSphere.Server.Farm
 - o Session mode – Server per session
 - o Connectivity checks – No Checks
 - o Leave all other fields as default
- Enable SSL ID Tracking in **AppDirector -> Farms -> Additional Parameters**

Servers Configuration

- Create Server named "AppXcel.Server.1" and attach it to Farm "AppXcel.Farm" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – AppXcel.Farm
 - o Server Address – 3.1.1.101
 - o Leave all other fields as default
- Create Server named "AppXcel.Server.2" and attach it to Farm "AppXcel.Farm" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – AppXcel.Farm
 - o Server Address – 3.1.1.102
 - o Leave all other fields as default
- Create Server named "WebSphere.1" and attach it to Farm "WebSphere.Server.Farm" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – WebSphere.Server.Farm
 - o Server Address – 2.1.1.101
 - o Leave all other fields as default
- Create Server named "WebSphere.2" and attach it to Farm "WebSphere.Server.Farm" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – WebSphere.Server.Farm
 - o Server Address – 2.1.1.102
 - o Leave all other fields as default

Layer 4 Configuration

- Create L4 Policy for HTTPS Traffic named "HTTPS.to.AppXcel" in **AppDirector** -> **Servers** -> **Server Table** with these parameters
 - o Virtual IP – 192.168.1.50
 - o L4 Protocol – TCP
 - o L4 Port – 443
 - o Application - HTTPS
 - o L4 Policy Name – HTTPS.to.AppXcel
 - o Farm Name – AppXcel.Farm
 - o Leave all other fields as default

- Create L4 Policy for HTTP Traffic named "HTTP.to.AppXcel" in **AppDirector** -> **Servers** -> **Server Table** with these parameters
 - o Virtual IP – 192.168.1.50
 - o L4 Protocol – TCP
 - o L4 Port – 80
 - o Application - HTTP
 - o L4 Policy Name – HTTP.to.AppXcel
 - o Farm Name – AppXcel.Farm
 - o Leave all other fields as default

- Create L4 Policy for HTTP Traffic named "HTTP.to.WebSphere" in **AppDirector** -> **Servers** -> **Server Table** with these parameters
 - o Virtual IP – 192.168.1.51
 - o L4 Protocol – TCP
 - o L4 Port – 80
 - o Application - HTTP
 - o L4 Policy Name – HTTP.to.WebSphere
 - o Farm Name – WebSphere.Server.Farm
 - o Leave all other fields as default

Layer 7 Configuration

- Create L7 Text match session ID persistency (cookie) in **AppDirector** -> **L7 Server Persistency** -> **Text Match** with these parameters
 - o Farm Name – WebSphere.Server.Farm
 - o Persistency Identifier - JSESSIONID
 - o Lookup mode – Cookie
 - o Persistent L7 Switching mode – Complete and Maintain Connection
 - o Leave all other fields as default

AppDirector Health Monitoring

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

- Create a Check for HTTPS on server 3.1.1.101 in **Health Monitoring** -> **Check Table**
 - o Check name – AppXcel.1.HTTPS.Check
 - o Method – SSL
 - o Dest IP – 3.1.1.101
 - o Dest Port – 443

- Create a Check for HTTPS on server 3.1.1.102 in **Health Monitoring** -> **Check Table**

- Check name – AppXcel.2.HTTPS.Check
 - Method – SSL
 - Dest IP - 3.1.1.102
 - Dest Port – 443
- Create a Check for HTTP on server 2.1.1.101 in **Health Monitoring -> Check Table**
 - Check name – Web.Server.1.HTTP.Check
 - Method – HTTP
 - Dest IP – 2.1.1.101
 - Dest Port – 80
- Create a Check for HTTP on server 2.1.1.102 in **Health Monitoring -> Check Table**
 - Check name – Web.Server.2.HTTP.Check
 - Method – HTTP
 - Dest IP - 2.1.1.102
 - Dest Port – 80
- Bind the SSL check AppXcel.1.HTTPS.Check to Server 3.1.1.101 in **Health Monitoring -> Binding Table**
- Bind the SSL check AppXcel.2.HTTPS.Check to Server 3.1.1.102 in **Health Monitoring -> Binding Table**
- Bind the SSL check Web.Server.1.HTTP.Check to Server 2.1.1.101 in **Health Monitoring -> Binding Table**
- Bind the SSL check Web.Server.2.HTTP.Check to Server 2.1.1.102 in **Health Monitoring -> Binding Table**

VRRP Configuration

- 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
- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - IF Index – 17
 - VR ID – 1
 - Priority – 255 (Highest number is Active device)
 - Primary IP – 2.1.1.1
 - Leave all other options as default
- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - IF Index – 17
 - VR ID – 2
 - Priority – 255 (Highest number is Active device)
 - Primary IP – 3.1.1.1
 - Leave all other options as default

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 3
 - o Priority – 255 (Highest number is Active device)
 - o Primary IP – 192.168.1.1
 - o Leave all other options as default

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

- o IF Index – 17, VR ID – 1, Associated IP 2.1.1.1
- o IF Index – 17, VR ID – 2, Associated IP 3.1.1.1
- o IF Index – 17, VR ID – 3, Associated IP 192.168.1.1
- o IF Index – 17, VR ID – 3, Associated IP 192.168.1.50
- o IF Index – 17, VR ID – 3, Associated IP 192.168.1.51

APPDIRECTOR BACKUP CONFIGURATION

Network Configuration

- Create IP 2.1.1.2 on port 17
- Create IP 3.1.1.2 on port 17
- Create IP 192.168.1.2 on port 17
- Create default route to 192.168.1.254

- Copy all configuration from the Active AppDirector device

Redundancy

- Work with the ConfigwareInsite wizard to copy and convert the Active AppDirector configuration choosing the redundancy mode VRRP or Proprietary.

VRRP Configuration

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

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 1
 - o Priority – 100 (Highest number is Active device)
 - o Primary IP – 2.1.1.1
 - o Leave all other options as default

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 2
 - o Priority – 100 (Highest number is Active device)
 - o Primary IP – 3.1.1.1
 - o Leave all other options as default

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 3
 - o Priority – 100 (Highest number is Active device)
 - o Primary IP – 192.168.1.1
 - o Leave all other options as default

- Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP –> IP Addresses**
 - o IF Index – 17, VR ID – 1, Associated IP 2.1.1.1
 - o IF Index – 17, VR ID – 2, Associated IP 3.1.1.1
 - o IF Index – 17, VR ID – 3, Associated IP 192.168.1.1
 - o IF Index – 17, VR ID – 3, Associated IP 192.168.1.50
 - o IF Index – 17, VR ID – 3, Associated IP 192.168.1.51

Redundancy

- Work with the ConfigwareInsite wizard to copy and convert the Active WSD configuration choosing the redundancy mode VRRP or Proprietary.

APPXCEL APPLIANCE - 1**SSL configuration**

- Create a Key in **SSL -> KEY**
 - o Index – 1
 - o Size – 1024
 - o Password – 123456
 - o Verify Password – 123456
- Create a Certificate in SSL -> Certificate

Tunneling

- Create Tunnel for HTTPS Traffic in **Tunnel -> Table**
 - o Listening interface - LAN1
 - o Listen port - 443 (SSL mode)
 - o Key ID – 1
 - o Virtual Host IP – 3.1.1.101 (IP of the Interface LAN1)
 - o NetMask – 255.255.255.0
 - o Remote IP – 192.168.1.51
 - o Remote Port - 80
 - o Compression Engine – Software based (If Hardware card installed please used Hardware based)
 - o Compression level – 9 (9 is the highest compression)
 - o Transparency - Enable
 - o Leave all other fields as default.
- Create Tunnel for HTTP Traffic in **Tunnel -> Table**
 - o Listening interface - LAN1
 - o Listen port - 80 (HTTP mode)
 - o Virtual Host IP – 3.1.1.101 (IP of the Interface LAN1)
 - o NetMask – 255.255.255.0
 - o Remote IP – 192.168.1.51
 - o Remote Port - 80
 - o Compression Engine – Software based (If Hardware card installed please used Hardware based)
 - o Compression level – 9 (9 is the highest compression)
 - o Transparency - Enable
 - o Leave all other fields as default.

APPXCEL APPLIANCE - 2**SSL configuration**

- Create a Key in **SSL -> KEY**
 - o Index – 1
 - o Size – 1024
 - o Password – 123456
 - o Verify Password – 123456
- Create a Certificate in SSL -> Certificate

Tunneling

- Create Tunnel for HTTPS Traffic in **Tunnel -> Table**
 - o Listening interface - LAN1
 - o Listen port - 443 (if using SSL)
 - o Key ID – 1
 - o Virtual Host IP – 3.1.1.102 (IP of the Interface LAN1)
 - o NetMask – 255.255.255.0
 - o Remote IP – 192.168.1.50
 - o Remote Port - 80
 - o Compression Engine – Software based
 - o Compression level – 9 (9 is the highest compression)
 - o Transparency - Enable
 - o Leave all other fields as default.
- Create Tunnel for HTTP Traffic in **Tunnel -> Table**
 - o Listening interface - LAN1
 - o Listen port - 80 (HTTP mode)
 - o Virtual Host IP – 3.1.1.102 (IP of the Interface LAN1)
 - o NetMask – 255.255.255.0
 - o Remote IP – 192.168.1.51
 - o Remote Port - 80
 - o Compression Engine – Software based
 - o Compression level – 9 (9 is the highest compression)
 - o Transparency - Enable
 - o Leave all other fields as default.

IBM WEBSHERE SERVER-1

- Create IP 2.1.1.101 on network interface
- Create Default GW to 2.1.1.1

IBM WEBSHERE SERVER-2

- Create IP 2.1.1.102 on network interface
- Create Default GW to 2.1.1.1

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