



TESTING & INTEGRATION GROUP
SOLUTION GUIDE

Alteon Application Switch Optimizing the Delivery of VMware Horizon 6.2 with Security Servers

TECHNICAL SOLUTION GUIDE
DATE: Wednesday, January 13, 2016
Version: 1.0
Author – Elad Kurzweil

Contents

INTRODUCTION.....	3
RADWARE ALTEON	3
VMWARE HORIZON	5
RADWARE ALTEON AND VMWARE HORIZON SERVER ARCHITECTURE.....	6
PREREQUISITES	7
IMPORTANT IMPLEMENTATION NOTES	7
CONFIGURATION.....	8
ALTEON ACTIVE CONFIGURATION	8
<i>Network Configuration</i>	8
<i>Sync Configuration</i>	8
<i>PIP Configuration</i>	8
<i>Alteon Process Directions</i>	8
<i>SLB Configuration</i>	9
<i>SSL Configuration</i>	10
<i>VRRP Configuration</i>	11
ALTEON STANDBY CONFIGURATION.....	13
<i>Network Configuration</i>	13
<i>Sync Configuration</i>	13
<i>VRRP Configuration</i>	13
VMWARE HORIZON CONNECTION SERVERS (CONNECTION 1).....	14
VMWARE HORIZON CONNECTION SERVERS (CONNECTION 2).....	14
VMWARE HORIZON SECURITY SERVERS (CONNECTION 1).....	14
VMWARE HORIZON SECURITY SERVERS (CONNECTION 2).....	14
VMWARE VIEW CONNECTION SERVERS	15
<i>Configure VMware View Connection global settings</i>	15
VMWARE VIEW SECURITY SERVERS	16
<i>Configure VMware View Connection global settings</i>	16
TECHNICAL SUPPORT.....	17

Introduction

Implementing VMware View in an organization introduces a new set of challenges for IT, pushing its infrastructure to the limit and challenging its current administration policies. VMware View requires that an organization meet SLA commitments and provide QoE assurances. The inability to comply with these requirements will result in user frustration and loss of user productivity.

This Solution Guide describes a standardized integration solution in which Radware's load balancing and acceleration product, Alteon, is set up in front of a VMware View environment to ensure its availability and performance in order to meet SLA and QoE requirements.

Radware Alteon

Radware's Alteon ADC solution provides advanced and comprehensive application delivery capabilities needed to effectively meet the challenges of application deployment and application delivery in today's data centers. Equipped with advanced application acceleration capabilities, a global server load balancing solution and a comprehensive Layer 7 modification tool, Alteon ADC is well-positioned as the leading ADC in the industry. Alteon ADC also spearheads the ADC virtualization trend with ADC-VX™, the industry's first ADC virtualization and consolidation platform based on a specialized ADC hypervisor, and Alteon virtual appliance (Alteon VA).

Integrated Application Acceleration Capabilities with FastView™

Radware's Alteon ADC delivers a wide set of advanced application acceleration capabilities, designed to accelerate application response time while offloading server processing. By offloading processor intensive operations, such as SSL, Web compression, caching, HTTP multiplexing, and TCP optimization, it frees the servers' CPUs to handle additional requests, which results in reduced application server hardware and lower CAPEX.

Radware's FastView™ result-driven acceleration technology adds Web Performance Optimization (WPO) capabilities on top of the standard ADC application acceleration features to deliver the fastest Web application response time and ensure best application SLA. The result is best business impact for increased revenues, more page views, higher customer loyalty as well as improved employee productivity when using enterprise Web applications for all browsers and all end-user device types – starting from the first page visit.

Shaped to Deliver Applications

With Radware's AppShape™ technology, Alteon ADC benefits from reduced deployment time of application delivery services by 85%, while guaranteeing maximum value for each business critical application in terms of availability, performance and security. AppShape offers configuration templates and wizards for leading business applications. AppShape allows application delivery services to be

fully managed and operated from an application-centric view, including operational screens, logs and compliance – resulting in simplified and efficient application management in the ADC. Furthermore, AppShape’s reporting capabilities help organizations with capacity planning tasks by providing per application trends analysis and resources utilization reports.

VMware Horizon

VMware View delivers rich, personalized virtual desktops as a managed service from a virtualization platform, built to deliver the entire desktop, including the operating system, applications, and data. With VMware View, desktop administrators virtualize the operating system, applications, and user data and deliver modern desktops to end-users. VMware View provides centralized automated management of these components for increased control and cost savings. It improves business agility while providing a flexible high performance desktop experience for end-users across a variety of network conditions.

VMware View brings the agility and availability of cloud computing to the desktop and applications. Built on VMware vSphere, View delivers desktops from a single integrated platform as part of your cloud services. You can dynamically allocate resources to enable highly responsive and available environment to end-users. You can scale up and down desktop services on demand to quickly meet changing business needs and proactively protect against planned and unplanned downtime. You can run your desktops as business critical services for your workforce.

VMware View increases control of desktops, applications and data by delivering and managing them as centralized services. A single, powerful administrative console provides oversight of desktop services while enabling IT to execute previously cumbersome tasks such as provisioning, updates, and patches, with a few mouse clicks. You can manage desktop components separately for greater flexibility in provisioning, updates, and delivery. You can easily apply policies and quickly enable and disable users, all from a centralized console for optimal business response. View frees up time from maintenance for technology innovation.

Radware Alteon and VMware Horizon Server Architecture

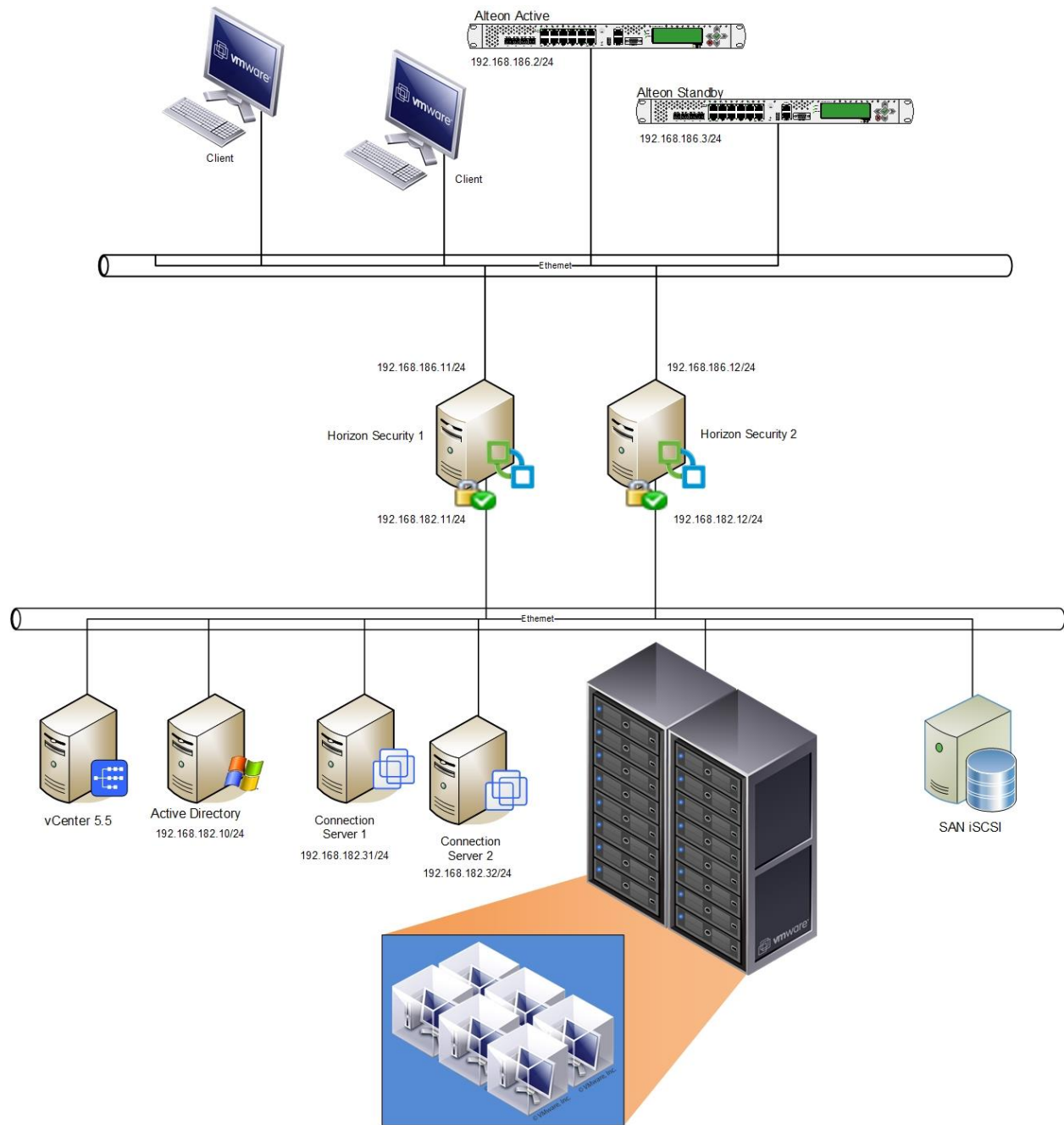


FIGURE 1 – TESTED EXAMPLE CONFIGURATION

Prerequisites

Important Implementation Notes

1. Throughout this guide, reference is made to the "Radware" pre-configured certificate, but you can import a certificate or create a new certificate in Alteon. For more information on exporting, importing, or creating a certificate, see the *Alteon Application Switch Operating System Application Guide*.
2. A VMware Horizon SSL Certificate must be installed on all connection servers and on the Alteons.
 - The certificate must include inside the server's certificate (DNS field), connection servers names, and VIP name. For example:
VIP - view.vradware.com and connection servers con1.vradware.com, con2.vradware.com, con1 and con2. If you have Wildcard certificate use *.vradware.com
 - A common name should be the VIP name. For example: view.vradware.com
3. VMware Horizon can work using the following different methods:
 - **Blast Secure Gateway** - This means that all traffic (PCoIP and login) on port 443 (secure) go through the connection servers (proxy mode).
 - **PCoIP Secure Gateway mode** - All PCoIP traffic goes on port 4172 through the connection servers (proxy mode).
 - If you select only **use Secure Tunnel Connection**, logins go through the connection servers (443 secure) and PCoIP traffic goes directly from the client to the selected VM.
4. **VERY IMPORTANT** - If you are using **PCoIP Secure Gateway mode** - change all load balancing on ports 4172,443 and 8443 to use source IP persistency (the Layer 7 configuration does not work).
5. Persistency is performed using Layer 4.
6. The Default Aging time for a session is 600 minutes. This can be changed inside the connection servers and inside the Alteon AppShapes script.

Software and Hardware

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

- Microsoft Windows 2008 R2 x64bits
- Radware Alteon version 30.0.2
- VMware Horizon Connection, Agent, Composer, Security and client v.6.2
- VMware vCenter 5.5

Configuration

Alteon Active Configuration

Network Configuration

```
/c/port 1
    pvid 101
/c/l2/vlan 1
    learn ena
    def 0
/c/l2/vlan 101
    ena
    name "Client.net"
    learn ena
    def 1
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 2 101
/c/sys/access/sshd/sshv1 dis
/c/sys/access/sshd/on
/c/l3/if 1
    ena
    ipver v4
    addr 192.168.186.2
    vlan 101
/c/l3/gw 1
    ena
    ipver v4
    addr 192.168.186.254
```

Sync Configuration

```
/c/slb/sync
    pips e
    certs e
/c/slb/sync/peer 1
    ena
    addr 192.168.186.3
```

PIP Configuration

```
/c/slb/pip/type port
/c/slb/pip/add 192.168.186.201 1
```

Alteon Process Directions

```
/c/slb/port 1
    client ena
    server ena
    proxy ena
```

SLB Configuration

```
/c/slb
  on
/c/slb/adv
  direct ena
  vstat ena
  submac "ena"
/c/slb/real 1
  ena
  ipver v4
  rip 192.168.186.11
  name "Security.Server.1"
/c/slb/real 2
  ena
  ipver v4
  rip 192.168.186.12
  name "Security.Server.2"
/c/slb/group 1
  ipver v4
  metric roundrobin
  add 1
  add 2
  name "Horizon.group"
/c/slb/group 2
  ipver v4
  add 1
  add 2
  name "UDP.4172"
/c/slb/pip/type port
/c/slb/pip/add 192.168.186.201 1
/c/slb/port "1"
  client ena
  server ena
  proxy ena
/c/slb/port "2"
  client ena
  server ena
  proxy ena
/c/slb/virt 1
  ena
  ipver v4
  vip 192.168.186.200
  vname "Horzion.VIP"
/c/slb/virt 1/service 4172 basic-slb
  group 1
  rport 4172
  pbind clientip norport
  ptmout 600
/c/slb/virt 1/service 443 https
  group 1
  rport 443
  pbind clientip norport
  dbind forceproxy
```

```

    ptmout 600
/c/slb/virt 1/service 443 https/ssl
    srvrcert cert 1
    sslpol 1
/c/slb/virt 2
    ena
    ipver v4
    vip 192.168.186.200
    vname "VIP.4172.UDP"
/c/slb/virt 2/service 4172 basic-slb
    group 2
    rport 4172
    protocol udp
    pbind clientip norport
    ptmout 600
/c/slb/gslb
    off
    hostlk ena
/c/sys/access/https/cert WebManagementCert
/c/sys/access/https/https e

```

SSL Configuration

```

/c/slb/ssl/certs/key 1
/c/slb/ssl/certs/import key "1" text
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9A8E4E794457FC6A

```

```

1um8rxpX+2OrWwltlEC/2j6aHcBesDl2NUoWTR9osQuWbsrUrDOUgvss7jVw2vkJ
OVALV2eK0L00Xb8Kth5ApZlar4s421gQnKfnQToKuHm6c2LVbEblzx2v9+17fK0o
LumvIfsajwKiVmsgCxfENNyWujoIflpbKycN65GbGiWws+8r1SUQICoyZOMCDte
m9YX6dX4GSBbhonLQHgn6yxooqFmRDzrVm5aAtws/fINyFABFWE1NeJ3fDCmEGk4
2L6f2vO/3oSYSltwP20m0S2wK3LN4MnjuXR3byy+FwFAM4u1lzp5A7PbDQ4ZjB9U
PZsLaguvxjIo7i9IPt0rloMo4wiUF9t35ECP4i1TqrpHln5fzmJ1TFKft3f1fmXP
tSpfZH3QjI8CCjidsq+efSZb15uxTQNaK724B8SUD8vYL69OAMya4WN2/t3YvAnE
Mj66t7Fekdxfy4jb+L6pHoA29ACoIgKE3PA0wShbIr8oYDcsxaGG/Jv4LVH9Zv3D
W87lX0mU5NQecw8vsv/c/6rhe6ihZPVq9kEDXTcLd+ZyuzmKeZA90t06vvex9hf
NQb+sSluUAHOPxEFLs8i6MGr262+2UdB46Wco0l0Rs2GEiS0WnCIIO43GLnn+Bis
q7pUnu/ehmDq4dOq4P8euMt/tlHul0yLaCuRGgqqmVZ77/z1Qo7Em77yml/hItNl
m31lZNiN96NPK4JyzH6n+4viIgeYU/2i08q9LSmLXKS2t5kftxrTugLG6ZBfGOWi
sMrOMhipc3SwlFY/ht7Jh9Za+0xenmQhLSvgF8u+23/wM7ZYAPkTKD3AyO006kRN
DzkdxUwREaswyUONB8NV8vgA7onekQ+dcMdb5nFC7wsX/7LZT5r5LF0bvtShDE5K
1HuoRZYh7h0cnRlLE/p6H4IsQUuitf/QFDBM7+7MxzXPIU8BaAsawy07I9cf7N2/
5YqawAMEuYlTQE19JIwtaeoJyNy0EkL/4xocWJwQJ1mNz0986ma9FURDMWCJ4LSX
zmrnuC+a3cg2q2/ZFoZtzoaOPzCsbqdD69agTJUcu+ZsBHR8voHUWf5l8upYjr2J
E2f2AkGLRYS3CZzh+rTNTt41IQSPMCoVmmN44L8zIruilYYcwurAK1ivozZHEQc
Wn3AQqpSMJ0HHxIOGS9QzE/8pUj7UDZczaV/8vxqKHVIqVV1XkdCjjoy2WLqOq4d
w33z3yQanboBQV5VoQfuec+rNHfpSa6oZuy7YwWkKzPwQvqdB0BpWdatNdpZ4xy3
aBYA+M9C37+yYZlWVJv0CthejDHKyFZuK6wnWRVzZMCqXE+fkMd3MeDlpP+E5VF3
8DeGUoGyPKnHWdecT6A7ZdrzyeV2JlTfojdFh/qbqYuncjdUnBxf6qgY8vO+teuW
/XHG32woqeMnUhkE+/MojG2y7UwloiduOBHAeizfZ6ilAACTYKRL9R7I+VjR4H5/
a1tpSYAE4pf+tZN2mvpt6U3FoBxnXuTVuAbUI2NBpwgvVh+h0FfBSrp0VF5eAGyq
75S0S+Gw69YPvPEB7mX50dy7sD4c40jlgEF7Tk5qINZFXk5jppzU3Q==

```



```
    ipver v4
    vrid 102
    if 1
    prio 250
    addr 192.168.186.1
/c/13/vrrp/vr 103
    ena
    ipver v4
    vrid 103
    if 1
    prio 250
    addr 192.168.186.201
/c/13/vrrp/vr 104
    ena
    ipver v4
    vrid 104
    if 1
    prio 250
    addr 192.168.186.200
/c/13/vrrp/group
    ena
    ipver v4
    vrid 254
    if 1
    share dis
```

Alteon Standby Configuration

Network Configuration

```
/c/port 1
  pvid 102
/c/l2/vlan 1
  learn ena
  def 0
/c/l2/vlan 102
  ena
  name "LAN"
  learn ena
  def 1
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 2 102
/c/sys/access/sshd/ena
/c/sys/access/sshd/sshdv1 dis
/c/sys/access/sshd/on
/c/l3/if 1
  ena
  ipver v4
  addr 192.168.186.3
  vlan 102
/c/l3/gw 1
  ena
  ipver v4
  addr 192.168.186.254
```

Sync Configuration

```
/c/slb/sync
  pips e
  certs e
/c/slb/sync/peer 1
  ena
  addr 192.168.186.2
```

VRRP Configuration

```
/c/l3/vrrp/vr 102
  ena
  ipver v4
  vrid 102
  if 1
  prio 250
  addr 192.168.186.1
/c/l3/vrrp/vr 103
  ena
  ipver v4
  vrid 103
  if 1
  prio 250
```

```
    addr 192.168.186.201
/c/l3/vrrp/vr 104
    ena
    ipver v4
    vrid 104
    if 1
    prio 250
    addr 192.168.186.200
/c/l3/vrrp/group
    ena
    ipver v4
    vrid 254
    if 1
    share dis
```

VMware Horizon Connection servers (connection 1)

- IP Address - 192.168.182.31/24
- DG - 192.168.182.254

VMware Horizon Connection servers (connection 2)

- IP Address - 192.168.182.32/24
- DG - 192.168.182.254

VMware Horizon Security servers (connection 1)

- Out Leg - 192.168.186.11/24
- In Leg - 192.168.182.11/24
- DG - 192.168.186.254

VMware Horizon Security servers (connection 2)

- Out Leg - 192.168.186.12/24
- In Leg - 192.168.182.12/24
- DG - 192.168.186.254

VMware View Connection Servers

Configure VMware View Connection global settings

1. Go to the **View Configuration > Servers > Connection servers** tab.
2. Edit each connection server, and add the External URL name **https://view.mycomapny.com:443** (this is the name that the clients point to).

The screenshot shows the 'Edit Connection Server Settings' dialog box with the following configuration:

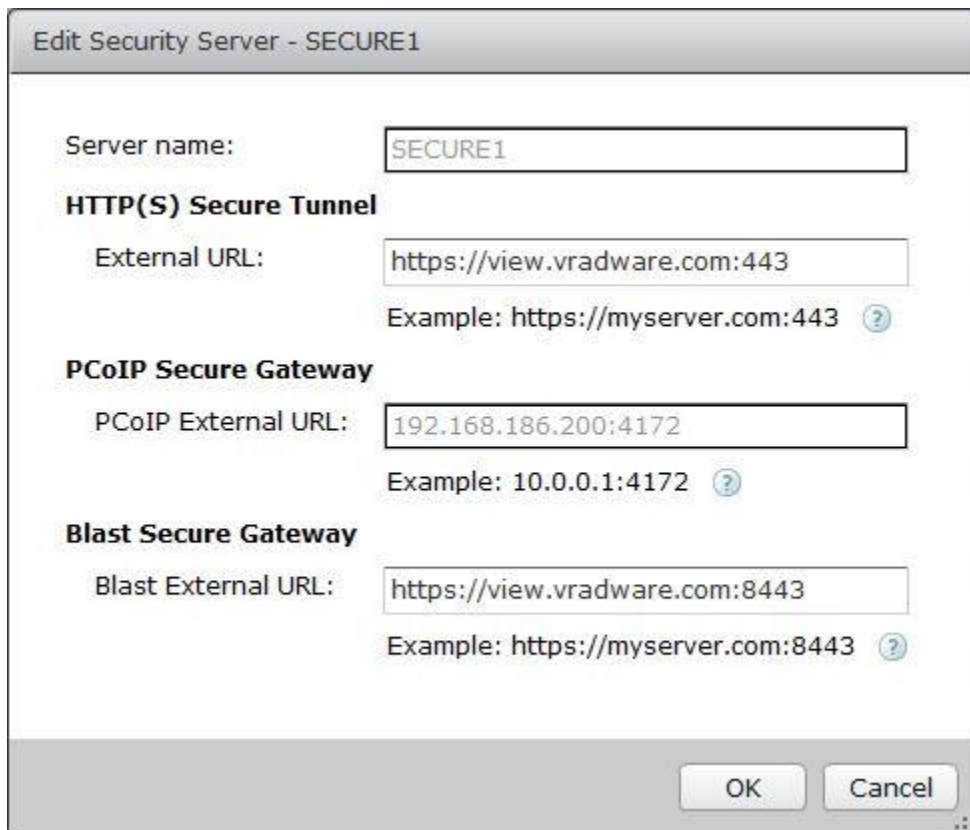
- General** tab is selected.
- Tags:** An empty text box with the instruction 'Separate tags with ; or ,'.
- HTTP(S) Secure Tunnel:** Use Secure Tunnel connection to machine. External URL: Example: https://myserver.com:443
- PCoIP Secure Gateway:** Use PCoIP Secure Gateway for PCoIP connections to machine. PCoIP External URL: Example: 10.0.0.1:4172
- Blast Secure Gateway:** Use Blast Secure Gateway for HTML access to machine. Blast External URL: Example: https://myserver.com:8443

Buttons: OK, Cancel

VMware View Security Servers

Configure VMware View Connection global settings

1. Go to the **View Configuration > Servers > Security Servers** tab.
2. Edit each connection server, and add the External URL name **https://view.mycomapny.com:443** (this is the name that the clients point to).



Edit Security Server - SECURE1

Server name:

HTTP(S) Secure Tunnel

External URL:
Example: https://myserver.com:443 ?

PCoIP Secure Gateway

PCoIP External URL:
Example: 10.0.0.1:4172 ?

Blast Secure Gateway

Blast External URL:
Example: https://myserver.com:8443 ?

OK Cancel

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