CONFIGURATION GUIDE

Ruckus Virtual SmartZone Data Plane (vSZ-D) Configuration Guide for SmartZone 3.6

Supporting 3.6

Part Number: 800-71558-001 Rev A
Publication Date: November 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

Preface....5
Document Conventions....5
Notes, Cautions, and Warnings....5
Command syntax conventions....5
Document feedback....6
Ruckus resources....6
Online Training Resources....6
Contacting Ruckus Customer Services and Support....7
What Support Do I Need?....7
Open a Case....7
Self-Service Resources....7
About This Guide....9
About this Guide....9
Virtual SmartZone Data Plane Features....11
Virtual SmartZone Data Plane Overview....11
Features and Benefits....13
Tunneled WLANs and Flexible Traffic Redirection....14
Architecture and Deployment Flexibility....14
IPv6 Address Support....15
vSZ-D Zone Affinity....15
DHCP Server and NAT Service on the vSZ-D....16
DHCP/NAT....17
AP-based DHCP/NAT....17
Profile-based DHCP....17
Profile-based NAT....17
L3 Roaming....17
Editing L3 Roaming for a vDP....18
Lawful Intercept....19
Enabling Flexi VPN....20
Enabling Tunnel Encryption....21
Network Architecture....23
Communication Workflow....25
NAT Deployment Topologies....27
AP Behind NAT and vSZ-D Behind NAT....27
vSZ and vSZ-D at Data Center Behind NAT....27
vSZ-D at Access Side with NAT....28
vSZ-D Behind NAT....29
DHCP Relay with NATDHCP Option 82 and Bridge Profile....30
Hardware Requirements....35
Important Notes About Hardware Requirements....35
Supported Modes of Operation....36
vSZ-D with DirectI/O....38
vSZ-D with Hypervisor vSwitch Installed....38

vSZ-D and vSZ with Hypervisor vSwitch Installed....39
Recommended NICs and Operation Modes....41
Hypervisor Configuration....43
Supported Hypervisors....43
General Configuration....43
VMware Specific Configuration....43
KVM Specific Configuration....48
CPU Type....48
Disk Configuration....49
NIC Configuration in Direct IO Mode....51
NIC Configuration in vSwitch Mode....51
Upgrade Procedure....55
Upgrade Procedure....55
vSZ-D Performance Recommendations....59

Preface

- Document Conventions....5
- Command syntax conventions....5
- Document feedback....6
- Ruckus resources....6
- Online Training Resources....6
- Contacting Ruckus Customer Services and Support....7

Document Conventions

The following tables list the text and notice conventions that are used throughout this guide.

TABLE 1 Text conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples.	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.

Convention	Description
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - SmartCell Gateway 200 S2a Interface Reference Guide for SmartZone 3.5.1
  - Part number: 800-71306-001
  - Page 88

Ruckus resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate documentation by product or perform a text search.

White papers, data sheets, and other product documentation are available at www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Request for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

The Support Portal at https://support.ruckuswireless.com/contact-us offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/software
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management

About This Guide

- About this Guide..... 9

About this Guide

This document describes the features and configuration required for setting up the Ruckus Wireless Virtual SmartZone Data Plane (vSZ-D) on the network.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

> NOTE
> If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at https://support.ruckuswireless.com/contact-us.

Virtual SmartZone Data Plane Features

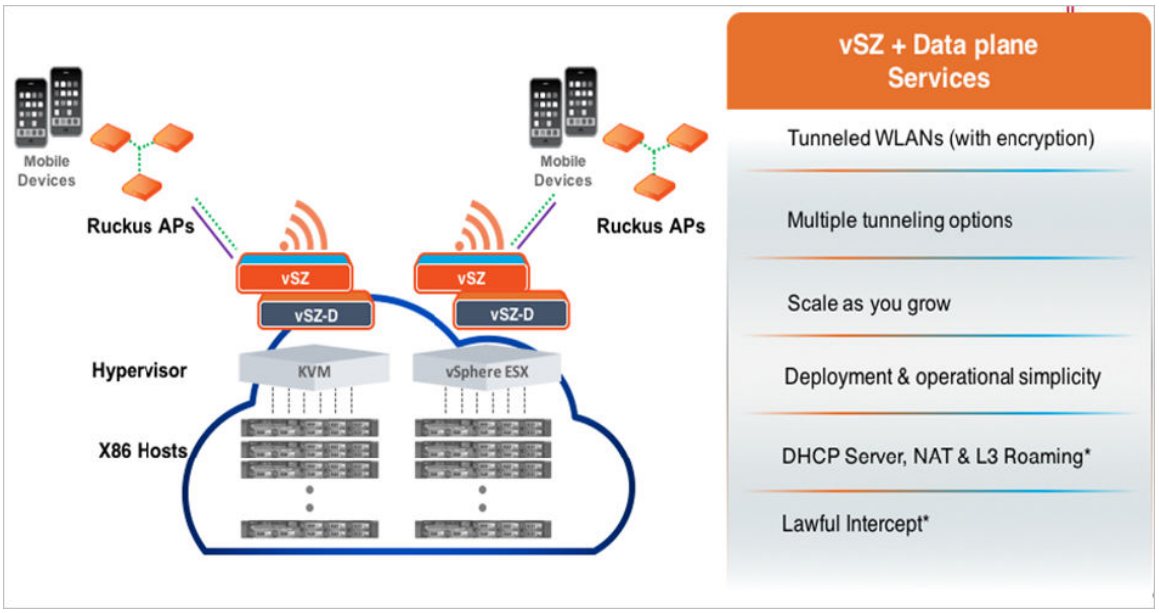
- Virtual SmartZone Data Plane Overview.....11

Virtual SmartZone Data Plane Overview

The Ruckus Wireless Virtual SmartZone controller platform is the industry's most scalable Wi-Fi controller platform that enables service providers and enterprises to leverage virtualization technologies to deploy superior Wi-Fi management systems.

With the introduction of the Virtual Data Plane (vSZ-D) in SZ 3.2 release, the Virtual SmartZone platform launched sophisticated data plane capabilities in a virtualized form factor. This is truly differentiated and distinguished offering that provides compelling business benefits for varied deployment scenarios.

FIGURE 1 vSZ-D services



Features and Benefits

- Tunneled WLANs and Flexible Traffic Redirection....14
- Architecture and Deployment Flexibility....14
- IPv6 Address Support....15
- vSZ-D Zone Affinity....15
- DHCP Server and NAT Service on the vSZ-D....16
- DHCP/NAT....17
- L3 Roaming....17
- Lawful Intercept....19
- Enabling Flexi VPN....20
- Enabling Tunnel Encryption....21

vSZ-D is a virtualized service to segregate and securely tunnel user data traffic.

Some of the key use cases for the vSZ-D are:

FIGURE 2 Use cases

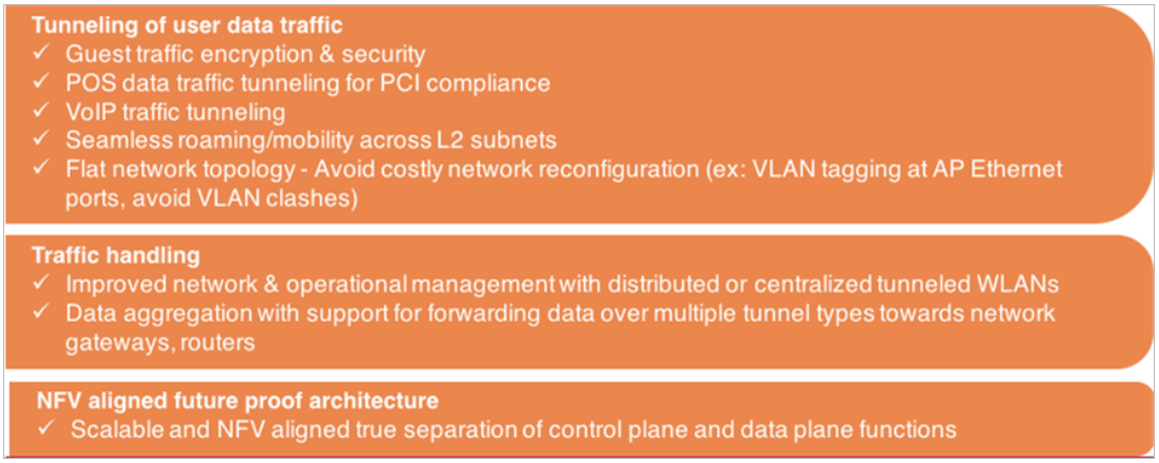


TABLE 2 Feature and Benefits

Feature	Benefit
Secure data plane tunneling	Manages the creation of aggregated user data streams through secure tunnel
Multiple Hypervisor Support	Supports the most widely deployed VMware and KVM hypervisors
Dynamic data plane scaling	Supports 1Gbps, 10Gbps or even higher throughput capacities to support all types of enterprise and carrier deployments that can be dynamically tuned without needing software updates
Seamless integration with vSZ controller	• Simple integration and management with vSZ controller clustering architecture enables support for multiple vSZ-D instances • 10 vSZ-D instances per vSZ instance • 40 vSZ-D instances per vSZ cluster of 4 instances • The controller runs in Active/Active (3+1) mode for extremely high availability. • Each vSZ-D runs as an independent virtual machine instance that is managed by the controller.

TABLE 2 Feature and Benefits (continued)

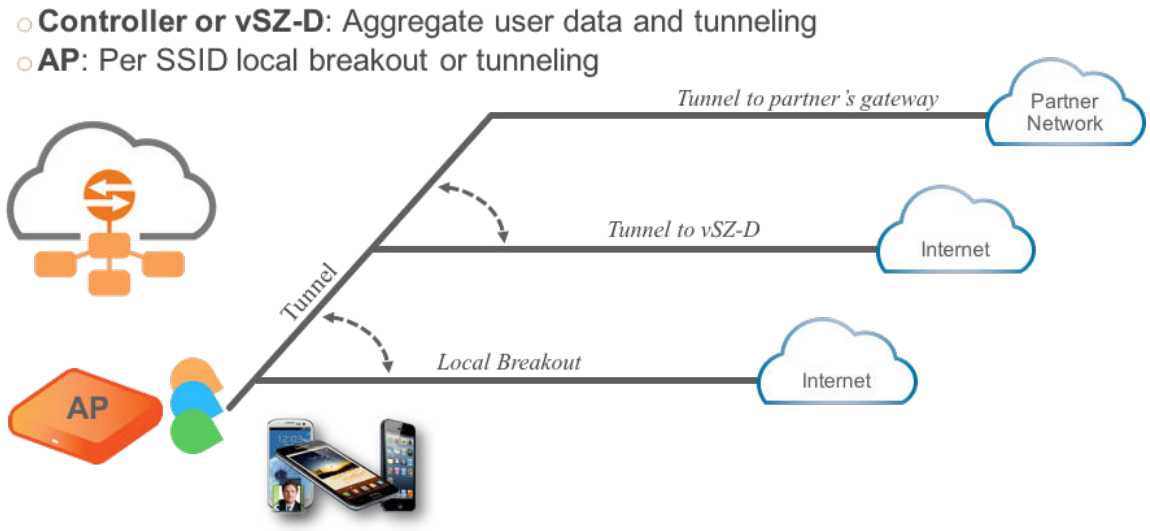
Feature	Benefit
	• With vSZ-D Zone Affinity enabled, it is possible to support a distributed vSZ-D instance on a per vSZ Zone basis.
Superior data plane functions	Encrypted tunnel aggregation from all types of WLANs (Captive portal, 802.1x, HS2.0), VLANs, DHCP Relay, DHCP Server, NAT, L3 Roaming, Lawful Intercept, IPv6 Support and NAT traversal between AP and vSZ-D.
Scalable Deployment Architectures	Provides the ability to service distributed and centralized network configurations
Deployment and operational simplicity	Simple integration and management with vSZ-E and vSZ-H installations
Site level QoS and policy control	Service policy management and data stream (will be supported in a later release)

Tunneled WLANs and Flexible Traffic Redirection

Many WiFi deployments have requirements to support tunneled WLANs for guest isolation and encryption, POS data security, VoIP traffic management, and seamless roaming across L2 subnets. One of the most deployed and easily managed way to meet these requirements is to enable a flat network topology by tunneling traffic to a controller.

With the vSZ-D, it is now possible to support tunneled WLANs on Ruckus Wireless APs that are managed by a vSZ controller. In addition, both the Ruckus Wireless AP and the vSZ-D support encryption capabilities on tunnels for data protection. This is especially important when tunneling guest traffic and in use cases where the service provider or enterprise operator does not have control on the backhaul links.

FIGURE 3 Traffic redirection flexibility with the Virtual SmartZone platform

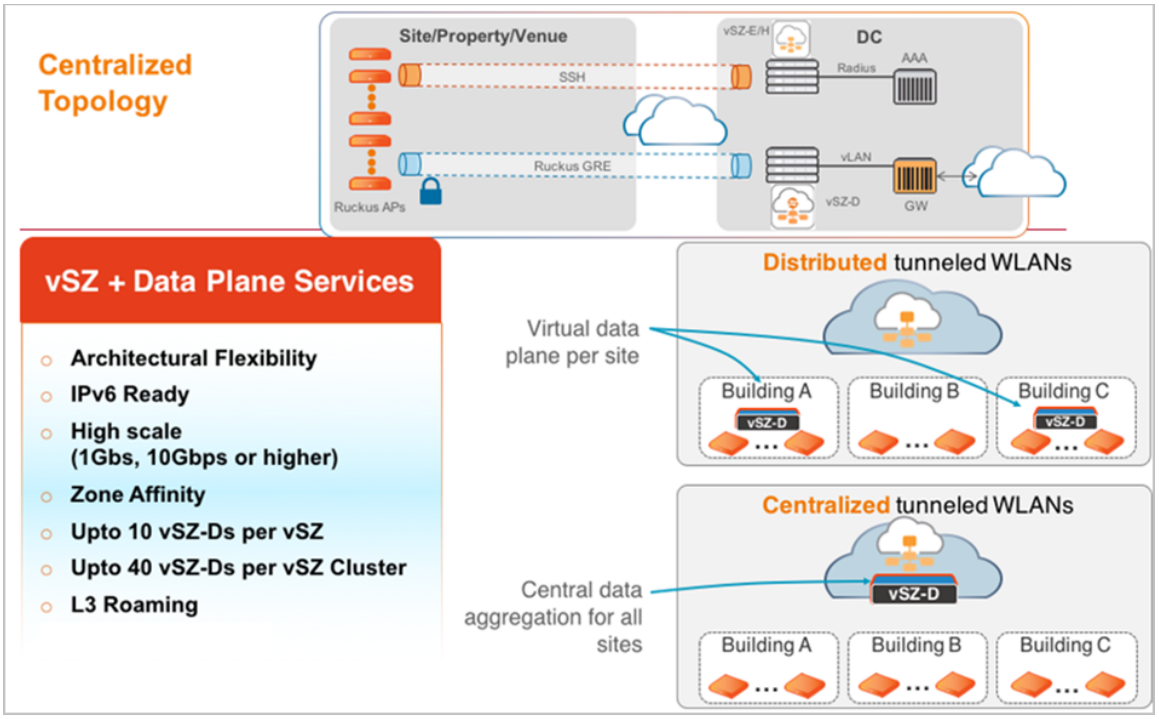


Architecture and Deployment Flexibility

Existing architectures for supporting tunneled WLANs involve tunneling data back into controllers. This results in architectures where a complete controller needs to be deployed on each site or all the tunneled WLAN traffic being backhauled into a centralized data center. This also results in dependencies on choices for controller platforms with different capacity profiles, which increase the capital and operating expenses of the entire solution without actually solving the real problem.

With the vSZ-D, it is now possible to deploy the same software either on-premise (on cheaper COTS hardware) when needed, as well as deploy it at the data center (on higher end COTS hardware) and the entire Wi-Fi management controller by the vSZ controller.

FIGURE 4 Unmatched architecture flexibility



IPv6 Address Support

The vSZ-D supports IPv6 addresses for the data and control/management plane interfaces. The vSZ-D also supports client IPv6 addressess for DHCP Relay only.

NOTE
vSZ-D does not support IPv6 addresses for northbound soft-GRE tunnels.

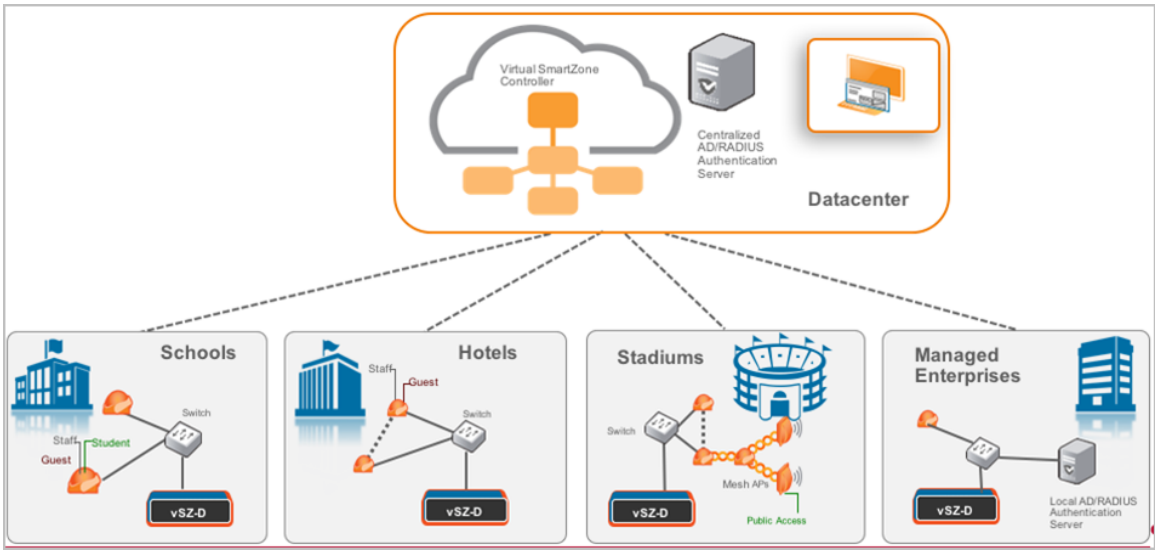
vSZ-D Zone Affinity

vSZ-D Zone Affinity is a new feature introduced in this release. It is now possible to dedicate vSZ-D instance on a per distributed site basis.

This is especially useful for managed service providers and ISPs who manage remote distributed sites through a central or regional data center. In this architecture, the vSZ is in the provider's data center managing APs across all remote distributed sites.

On sites where there is a need for tunneling, they can introduce the vSZ-D and bind those vSZ-Ds to that particular site so that all APs on that site shall tunnel traffic locally to the vSZ-D on that site.

FIGURE 5 vSZ-D Zone Affinity



DHCP Server and NAT Service on the vSZ-D

3.5 Release introduces a highly scalable and optimized DHCP Server on the vSZ-D that is designed from the ground up for WiFi networks. It also introduces NAT capability.

> **NOTE**
> DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

> **NOTE**
> DHCP Server and NAT service configuration is supported using AP and web user interface. Refer to Administrator Guide for configuring DHCP server and NAT service on the web interface.

DHCP Server

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D provides high scale IP assignment and management with minimal impact on forwarding latency. DHCP Server supports 440K IP addresses and 64 pools with profile support.

> **NOTE**
> The default maximum allowed IP assignment for DHCP server should not be more than 50K IPs. If you need to increase the IP assignment, you would need to buy additional licenses.

NAT Service

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D before being forwarded to the core network. Each vSZ-D supports up to 990K ports and 16 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

> **NOTE**
> Only single subnet is supported.

DHCP/NAT

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery you can choose appropriate user profile for DHCP and NAT services on vDP.

AP-based DHCP/NAT

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vDP will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vDP.

Profile-based DHCP

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D provides high scale IP assignment and management with minimal impact on forwarding latency. By default, the maximum allowed IP assignment for the DHCP server is 50K IP addresses in a vSZ cluster managing multiple vDP. Additional IP assignment requires additional licensing.

NOTE
DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

Profile-based NAT

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D before being forwarded to the core network. Each vSZ-D supports up to 900K NAT ports (traffic sessions) and 128 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

L3 Roaming

Ruckus vSZ and vSZ-D architecture now supports L3 Roaming without the need for additional mobility controllers.

The key use cases for L3 Roaming are well-understood,. Typically, a large WLAN network where APs are separated on different VLAN segments and there is a need for IP address preservation and potentially session persistence. Most common deployments are large campus networks designed with multiple switches and VLANs and there is a need to support L3 Roaming.

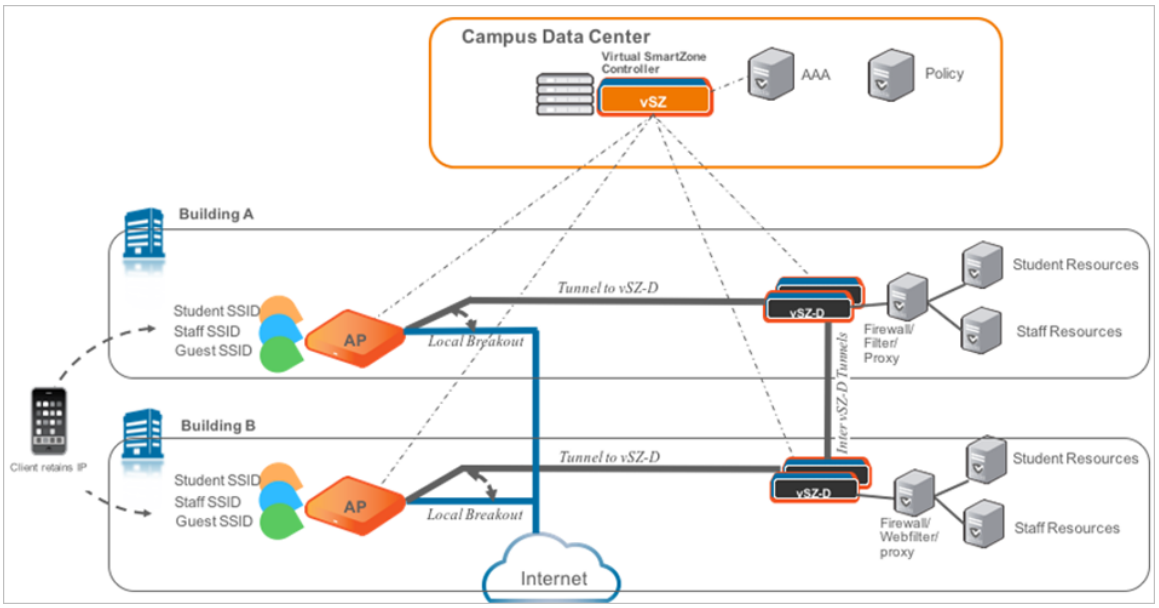
With the 3.5 release and on the vSZ-D, Ruckus Wi-Fi can now support L3 Roaming with IP Address preservation. Below is the high level use case that describes the feature functions. A large network that is broken up into various campuses and there is a need to support L3 Roaming. Below figure depicts 2 campuses, which are L2 separated but need L3 Roaming.

The APs in campus A setup a tunneled WLAN to the vSZ-D (Using Zone Affinity) and APs in building B setup a tunneled WLAN to the vSZ-D in their building.

Each vSZ-D in the building can be configured to run a DHCP Server and NAT the traffic or be setup as a DHCP Relay. When a client roams from an AP in building A to an AP in building B, the vSZ-D in building B detects the roaming event and forwards the traffic (or assigns the same IP back to the client) to the vSZ-D in building A (home vSZ-D or anchor vSZ-D) to ensure that service to the client is not interrupted.

One additional unique benefit of this architecture over other L3 Roaming solutions is that with this architecture, the roamer client can still have access to his home network resources (this is similar to mobile roaming on 3G/4G networks).

FIGURE 6 Usage of L3 roaming



Editing L3 Roaming for a vDP

For L3 roaming to work without session break, the vDPs between which the roaming happens must both be enabled with the L3 Roaming feature.

> **NOTE**
> If the IP address of the UE changes, then the session breaks.

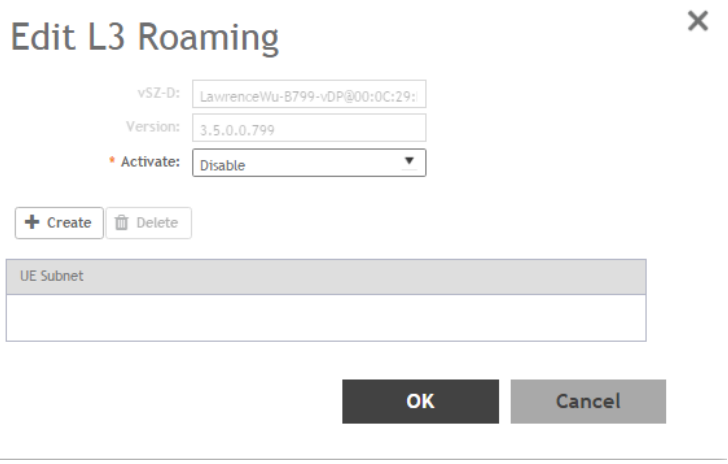
1. Go to **Services & Profiles** > **Tunnels and Ports**.
2. Select the **Forwarding Rule (vSZ-D)** tab.

   The page with Flexi-VPN and L3 Roaming settings appears.

3. In L3 Roaming Profiles, select a virtual data plane for which you want to enable the L3 roaming feature, and then click **Configure**.

   The **Edit L3 Roaming** page appears.

FIGURE 7 Configuring the L3 Roaming setting for a vDP



4. In **Activate**, select Enable or Disable as appropriate.
5. Based on the *Roaming Criteria* that you set, you will be able to add a UE subnet or a VLAN ID to the selected vDP. Click **Create** to add a UE Subnet or VLAN ID to the vDP. The **UE Subnet** or **Add VLAN ID** page appears, respectively, depending on the roaming criteria you chose.
6. Type the **UE Subnet** IP address or the **VLAN ID** as appropriate.
7. Click **OK**.
8. Click **OK** again.

   In L3 Roaming Profiles, the following information about the vDP is displayed:

   - vSZ-D: Displays the name of the virtual data plane.
   - Version: Displays the version of the vDP.
   - Activate: Displays whether L3 roaming is enabled or disabled.
   - UE Subnet or VLAN ID: Depending on the global settings you choose for the roaming criteria, the UE subnet IP address or the VLAN ID is displayed.

You have enabled L3 roaming in the selected vDP.

Lawful Intercept

An important carrier class feature that is being introduced on the vSZ-D with the 3.5 release is to support Lawful Intercept requirements.

These are slowly becoming mandatory and stringent on SP-WiFi deployments where Service Providers need to meet the CALEA standard requirements.

Ruckus vSZ-D now supports the ability to identify a device that has a LI warrant issued against it and mirror the client data traffic to a LIG (Lawful Intercept Gateway) that is hosted in the SP's data center over L2oGRE.

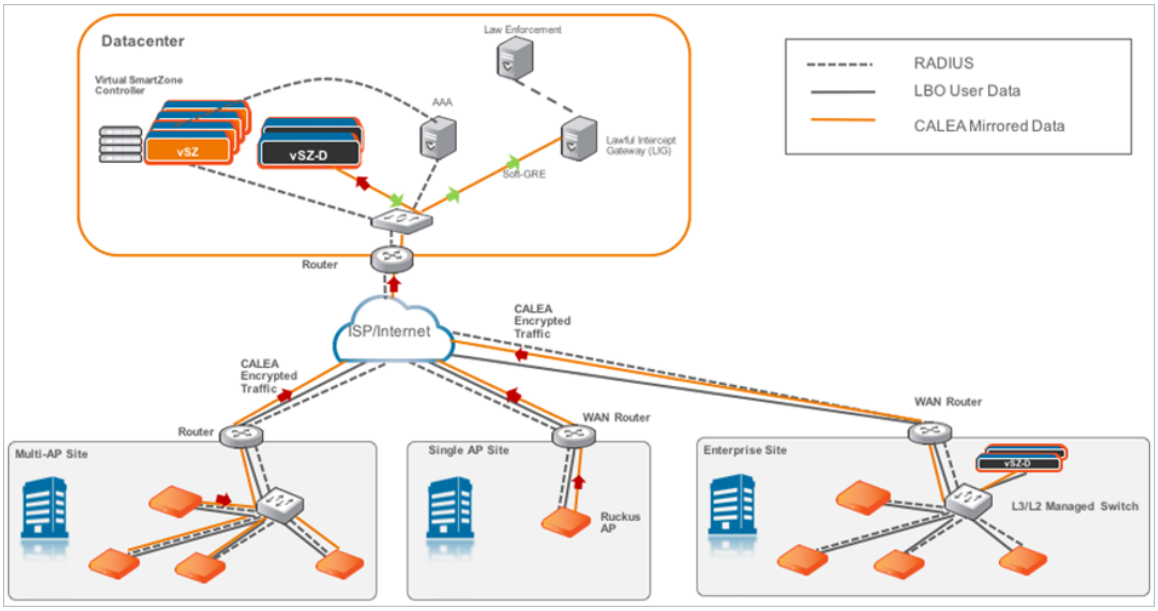
The figure below illustrates the high level architecture that is supported for Lawful Intercept capabilities. It aslo depicts an architecture where smaller sites (with lesser number of APs) that do not need data tunneling to vSZ-D (depicted as Multi-AP and Single AP sites) but need

Lawful Intercept. On the other side is a large enterprise site with large number of APs and need tunneling (depicted as Enterprise site with vSZ-D on premise) with Lawful intercept.

> **NOTE**
> As mentioned in this document, the flexibility of the Ruckus vSZ/vSZ-D architecture is that WiFi service providers can deploy the vSZ-D only on premises where there is a need (typically larger venues) for tunneling.

The Ruckus architecture simply involves spinning up a vSZ-D instance at the central data center and designate that vSZ-D instance as a CALEA mirroring agent. All of this configuration is centrally managed through the vSZ. Once the network is setup appropriately, when a client device with a matching MAC address that has a warrant is detected on any of the access sites, the APs (or the vSZ-D) will mirror the packets to the vSZ-D (CALEA Mirroring agent) in the DC which will then forward the traffic to the LIG (Lawful Intercept Gateway) either in the DC or SP DC.

FIGURE 8 Usage of Lawful Intercept



Enabling Flexi VPN

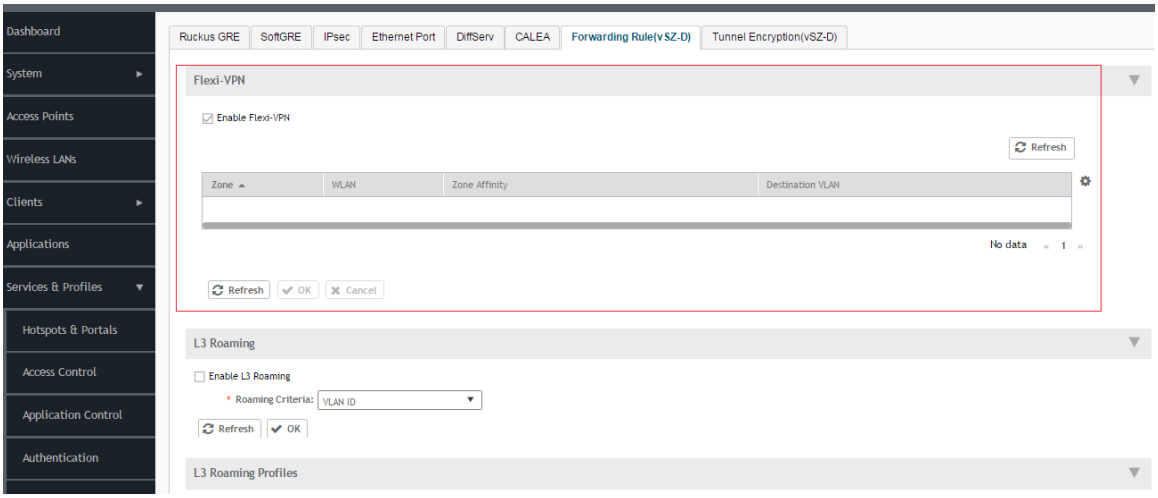
You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

1. Go to **Services & Profiles** > **Tunnels and Ports**> **Forwarding rule**.

2. Select the **Forwarding Rule (vSZ-D)** tab.

   The page with Flexi-VPN and L3 Roaming settings appears.

FIGURE 9 Enabling Flexi-VPN



NOTE

The Flexi-VPN option is only available if the Access VLAN ID is 1, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options are disabled.

NOTE

You can only apply 1024 WLAN IDs to a Flexi-VPN profile.

Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

3. Select a virtual data plane for which you want to enable the Flexi-VPN feature, and then select the **Enable Flexi-VPN** check-box.
4. Click **OK**.

You have successfully enabled the Flexi-VPN feature on the selected vDP.

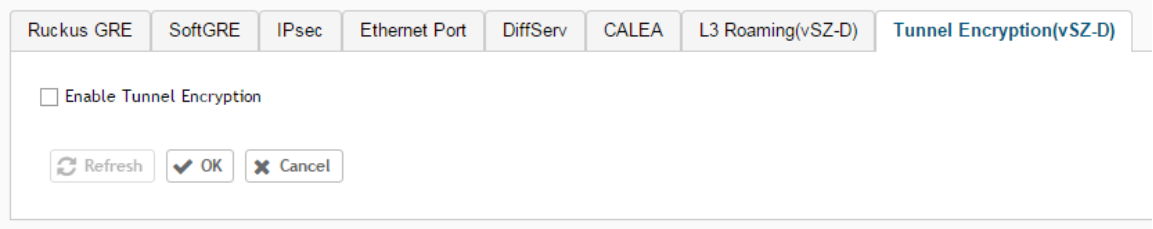
Enabling Tunnel Encryption

You can use the tunnel encryption feature to encrypt data for a private network, through a public network. This feature is ava ilable in vSZ-H and vSZ-E.

1. Go to **Services & Profiles** > **Tunnels and Ports**.

2. Select the **Tunnel Encryption (vSZ-D)** tab, and then select the zone for which you want to create the profile.
   The **Tunnel Encryption (vSZ-D)** page appears.

FIGURE 10 Tunnel Encryption (vSZ-D)



3. Select the **Enable Tunnel Encryption** check-box.
4. Click **OK**.

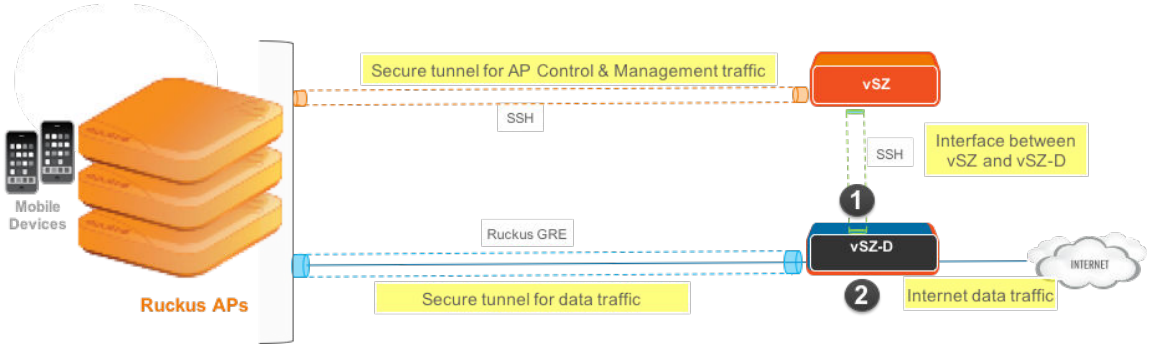
You have successfully enabled tunnel encryption.

Network Architecture

vSZ-D requires at least two physical interfaces: one for control/management and another for data plane.

The control/management interface is used for communication with the vSZ controller, as well as the command line interface. The data plane interface is used to tunnel user data traffic from the APs.

FIGURE 11 vSZ-D logical interfaces



The access layer (southbound) is used to tunnel traffic to and from managed APs. The following connections exist on the access layer.

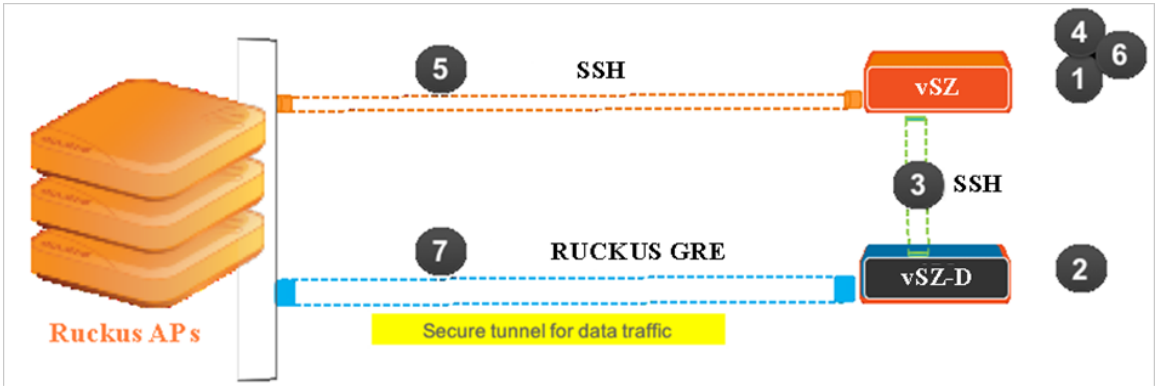
1. AP to and from vSZ-D: Data plane, secured by Ruckus GRE tunnel.
2. vSZ to and from vSZ-D: Control plane, for vSZ to manage vSZ-D
3. AP to and from vSZ: Control plane, for vSZ to manage the AP

The core layer (northbound) is used by vSZ-D to forward traffic to and from the core network.

Communication Workflow

The figure below captures a high level end-to-end communication flow between Ruckus Wireless APs, vSZ and vSZ-D.

FIGURE 12 Communication workflow between Ruckus Wireless APs, vSZ, and vSZ-D



The following are the steps seen in the above figure.

1. Update the vSZ controller to the latest 3.x release or perform a fresh install of the vSZ controller with the latest release

   NOTE
   If you are upgrading the vSZ controller and the vSZ-D, Ruckus Wireless recommends the update of vSZ controller before the update of vSZ-D

2. Install vSZ-D and point it to the vSZ-E or vSZ-H controller by using the following options:
   - Set vSZ-E or vSZ-H control interface IP address or FQDN or configure the controller IP address via DHCP option 43.
   - For vSZ-E or vSZ-H configured with three (3) IP interfaces, the IP address to use is the vSZ control interface IP address.
3. The vSZ-D management interface connects with the vSZ-E or vSZ-H controller control interface
4. The vSZ-E or vSZ-H controller administrator approves the vSZ-D connection request
5. The vSZ informs the AP of the vSZ-D data interface
6. The vSZ-D is displayed as active and managed on vSZ-E or vSZ-H
7. AP establishes a Ruckus GRE tunnel with the vSZ-D data interface when a tunnelling WLAN is configured

Figure 12 depicts logical network architecture. In real-world deployments, there may be network routers, gateways, firewalls and other devices; these typical network devices are not shown in the figure to focus on the vSZ-D interfaces and communication protocol aspects between the various entities.

It is also important to note that support for distributed or centralized deployment topologies introduce NAT routers/gateway devices. The communication interfaces between Ruckus Wireless APs, vSZ and vSZ-D are designed to support NAT traversal so as to support such NAT Deployment Topologies on page 27.

NAT Deployment Topologies

vSZ-D supports several deployment topologies.

AP Behind NAT and vSZ-D Behind NAT

When an AP is behind NAT, it is assumed that AP is sitting in the private world and wants to talk to vSZ-D in the public world through NAT. The AP obtains its private IP address and communicate with the vSZ-D through NAT. During communication with vSZ-D, the NAT router will intercept the packet and change the source IP address (which is the AP IP address) to a public IP address and add a new source port number before forwarding the packet to vSZ-D. vSZ-D, in this case, is insensitive to the NAT router's operation. When the packet comes back from vSZ-D to the AP, the NAT router will intercept the packet and translate the destination IP address and port number back to the appropriate (original) AP IP address and port number.

When vSZ-D is behind NAT, it is assumed that vSZ-D is sitting in the private world and wants to talk to the AP in the public world through NAT. In this case, it is needed to setup the NAT IP (public IP) and a port number pair in vSZ-D "setup" process. vSZ picks up this public address and the associated port number and informs the AP that this is the vSZ-D address/port (public-IP, port) pair to connect to.

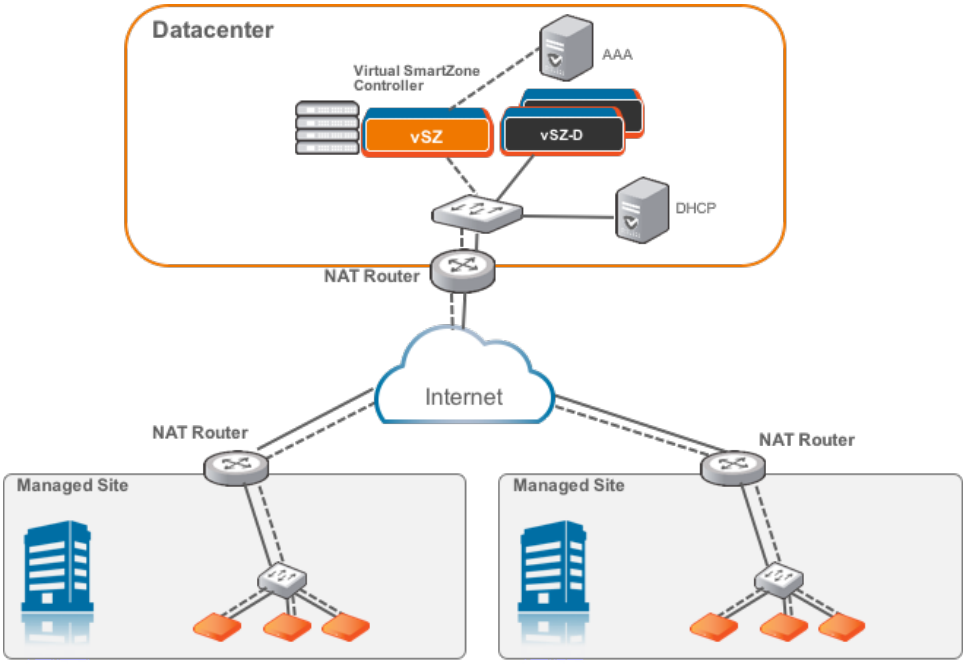
It is also needed to configure the NAT device and enter the port mapping, basically, (public-IP, port) <-> (private-IP, 23233) into NAT's rule table. Thus, when NAT receives the packet bound for vSZ-D (sent to public-IP/port) from the AP, it will translate it to (private-IP, 23233) based on the rule table before sending it to vSZ-D, and conversely, for packet from vSZ-D, NAT router will look at the srcIP/srcPort (IP, 23233), and convert it to public IP address or port based on the rule table before sending it to AP.

> NOTE
> Both TCP and UDP protocols on port 23233 need to be forwarded as both are used (TCP is used for tunnel establishment and UDP for client data)

vSZ and vSZ-D at Data Center Behind NAT

In this deployment topology, vSZ-D and vSZ are co-located at the data center behind NAT, while Ruckus Wireless APs are on the access network behind NAT.

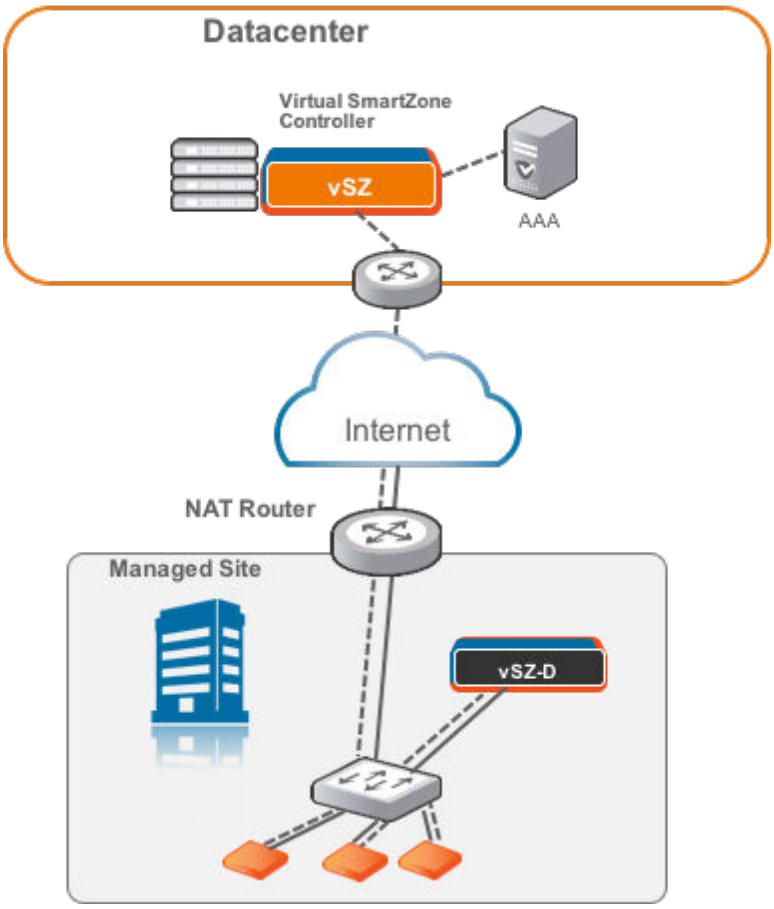
FIGURE 13 vSZ and vSZ-D at data center behind NAT



vSZ-D at Access Side with NAT

In this deployment topology, vSZ is at the data center and vSZ-D is co-located with the Ruckus Wireless APs on the access network. In this scenario, there are NAT routers between vSZ and vSZ-D/Ruckus APs.

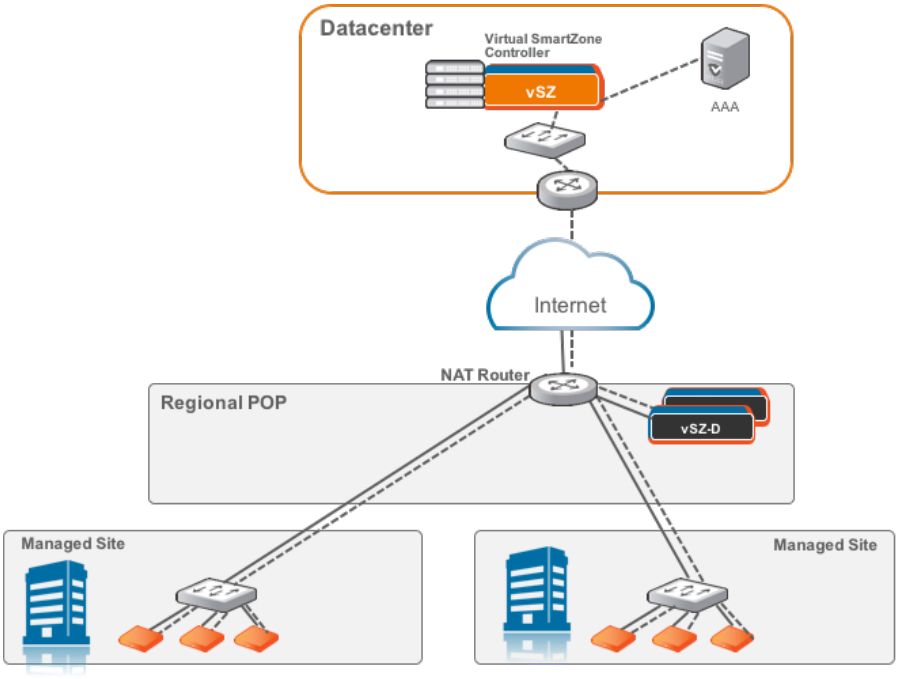
FIGURE 14 vSZ-D at access side with a NAT router



vSZ-D Behind NAT

In this deployment topology, vSZ is at the data center and vSZ-D is in a distributed site but not co-located with the Ruckus Wireless APs within the access network. There are NAT routers between vSZ and vSZ-D, and between vSZ-D and Ruckus Wireless APs. The vSZ-D port to communicate with vSZ control plane is port 22.

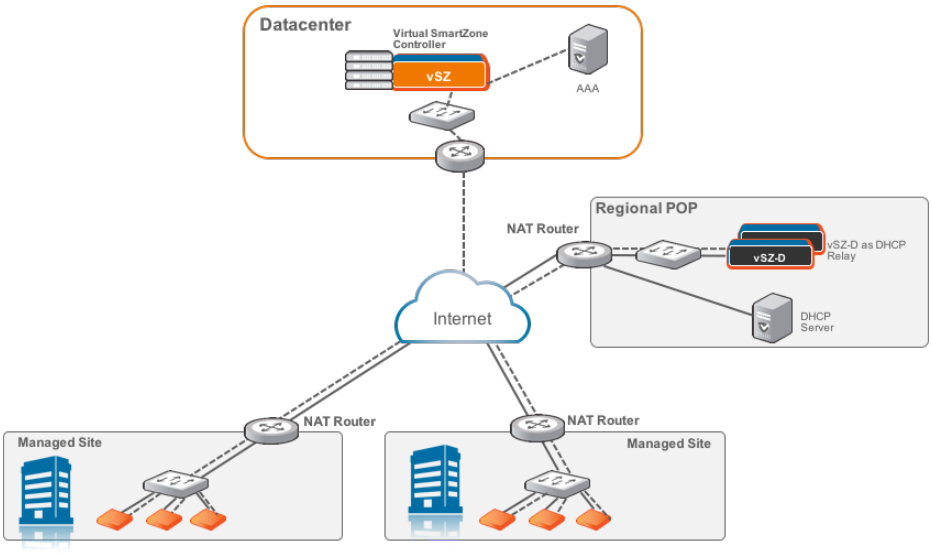
FIGURE 15 vSZ-D behind a NAT router



DHCP Relay with NAT

Similar to the *vSZ-D Behind NAT*, in this deployment topology, vSZ is at the data center and vSZ-D is in a distributed site but not co-located with the Ruckus Wireless APs within the access network. There are NAT routers between vSZ and vSZ-D, and between vSZ-D and Ruckus Wireless APs. However, in this topology, the DHCP server assigning client IP addresses is on its own separate subnet. vSZ-D provides the DHCP relay function to support such a network configuration.

FIGURE 16 DHCP relay with a NAT router

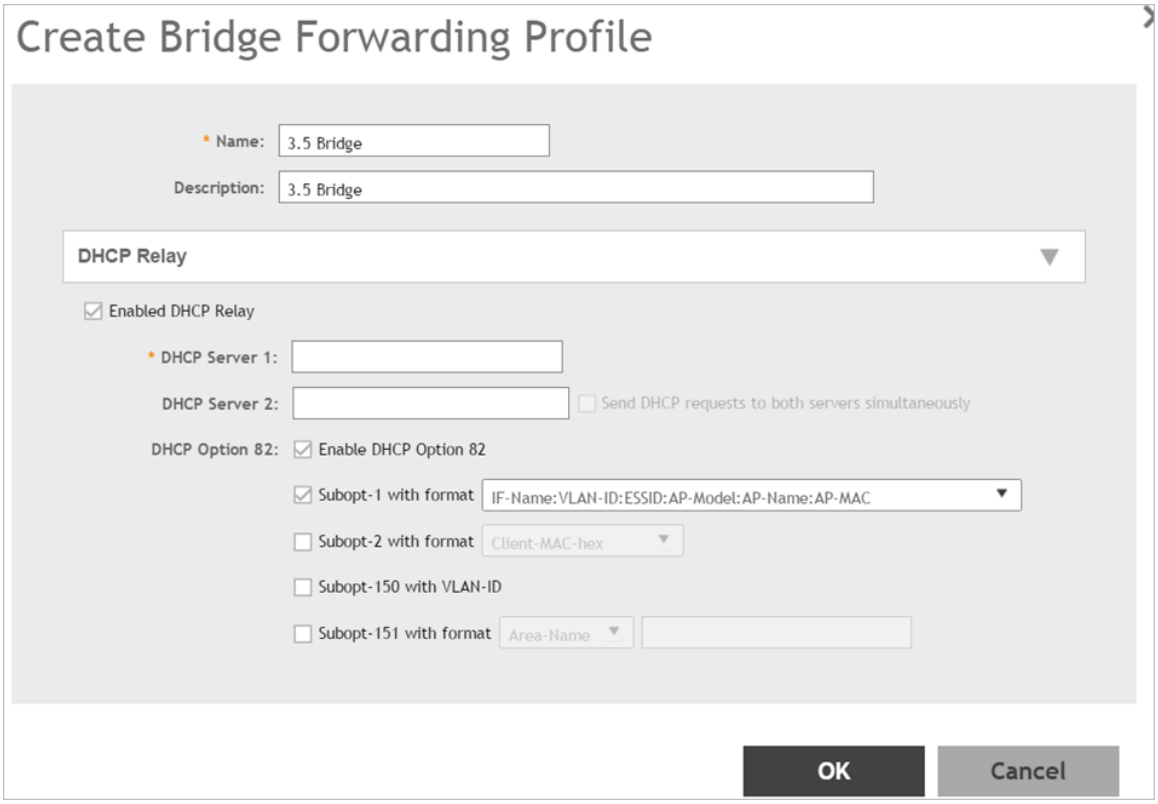


DHCP Option 82 and Bridge Profile

If you are enabling the DHCP Option 82 in WLAN configuration in the controller vSZ, it means that the AP is going to put DHCP Option 82 in the DHCP server and will send it to vSZ-D. This is in the format `IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC`. If you want to give the users the option to choose what needs to be included in DHCP Option 82, you would need to create a *Bridge Service Profile* in the vSZ controller web interface. Follow the steps to create a *Bridge Service Profile*.

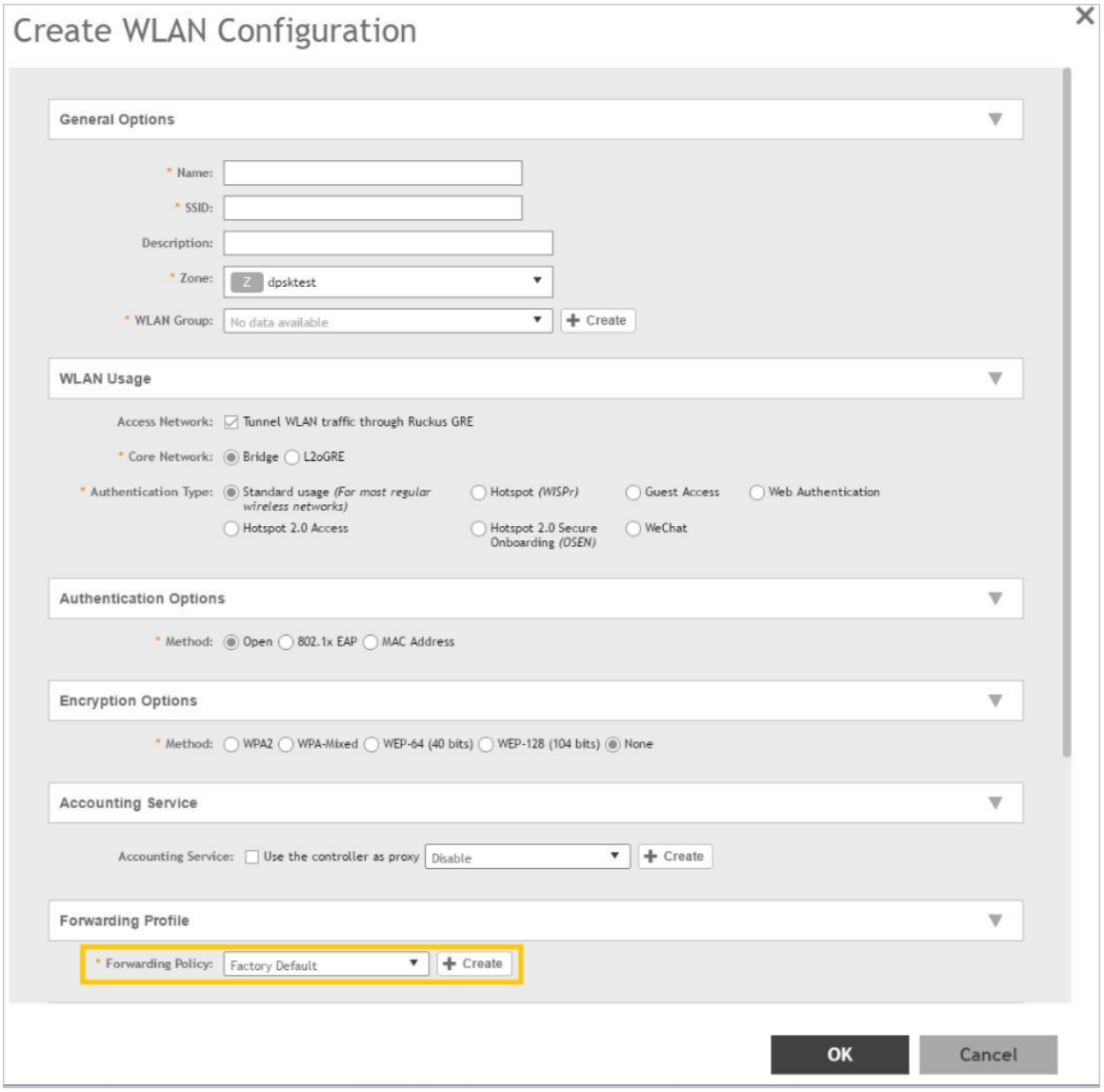
- Go to **vSZ controller web interface** > **Services & Profiles** > **Core Network Tunnel**
- Click on **Create** to add a **Bridge Forwarding Profile**
- Verify if the **DHCP Relay** is enabled.
- Add the **DHCP server** IP address
- Enable **DHCP Option 82** and choose the sub options based on your requirement or of the user. This will be taken care by vSZ-D during DHCP packet relay to the DHCP server.

FIGURE 17 Creating Bridge Profile



- Go to **vSZ controller web interface** > **Wireless LANs**
- Click on **Create** to add the following new WLAN configuration:
  - **Access Network** as **Tunnel WLAN traffic through Ruckus GRE**
  - **Core Network** as **Bridge**
  - **Authentication Options** > **Method**as **Open**
  - **Encryption Options** > **Method**as **None**
  - **Forwarding Policy** as **Factory Default** . Choose the forwarding policy as the bridge profile.
- Click **OK** to complete and save the configuration.

FIGURE 18 Creating a WLAN Configuration



Hardware Requirements

- Important Notes About Hardware Requirements..... 35
- Supported Modes of Operation..... 36

vSZ-D supports auto scaling, which means the number of CPU cores can be expanded without needing a software update. Ruckus Wireless has tested from three to six CPU core allocations for the vSZ-D in release 3.2 and above.

> **NOTE**
> The minimum memory and CPU requirements for vSZ have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to the Release Notes or the vSZ Getting Started Guide.

The following table lists the minimum hardware requirements recommended for running an instance of vSZ-D.

TABLE 3 vSZ-D hardware requirements

Hardware Component	Requirement
Hypervisor support required by Management Interface	VMWare Esxi 5.5 and later OR KVM (CentOS 7.0 64bit)
Processor	Intel Xeon E55xx and above. Recent Intel E5-2xxx chips are recommended
CPU cores	• Minimum 3 to 6 cores per instance dedicated for data plane processing. • DirectIO mode for best data plane performance. **NOTE** Actual throughput numbers will vary depending on infrastructure and traffic type. • vSwitch mode for flexibility and service chaining
Memory	Minimum 6 Gb memory per instance
Disk space	10GB per instance
Ethernet interfaces	2
NICs that support Intel DPDK requiredby Data Interface	• Intel NICs iab, ixabe • 82576, I350 • 82599EB, 82599, X520

Important Notes About Hardware Requirements

- If you change the number of CPU cores, you must reboot vSZ-D for the changes to take effect.
- The first core is always shared between Linux and NPE. Other cores are dedicated to NPE.
- vSZ-D requires two interfaces and these interfaces must be deployed on different subnets.
- The management interface of the vSZ-D can be any model as long as the NIC is supported by the hypervisor.
- The data interface needs to be Intel DPDK based.

Supported Modes of Operation

vSZ-D supports two modes of operation: direct IO mode and vSwitch mode.

For best performance, Ruckus Wireless recommends using the direct IO mode. SR-IOV mode is unsupported. Refer to the table below for mode of operation

> **NOTE**
> NICs assigned to direct IO cannot be shared. Moreover, VMware features such as vMotion, DRS, and HA are unsupported.

The hardware configuration for a single vSZ-D instance specified in the guide will scale to handle 10K tunnels (10K APs) and up to 10Gbps of throughput (unencrypted) with appropriate underlying Intel NIC cards (10G interfaces) in directIO mode of operation. This aligns with the number of Ruckus AP that a vSZ controller supports. Refer to the dimensioning table below.

TABLE 4 Hardware Dimensioning

Number of vSZ Instances	Number of vSZ-D Instances	Number of Ruckus APs	Number of Tunnels on vSZ-D	Maximum Throughput (Unencrypted)	Notes
1	1	10000	10000	10 Gbps	It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
1	2	10000	5000 (10K maximum in case of failover)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. This is useful when data plane redundancy is required. It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
2	2	10000	5000 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
2	4	10000	2500 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
3	6	20000	3300 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
4	8	30000	3750 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.

TABLE 5 Mode of Operation

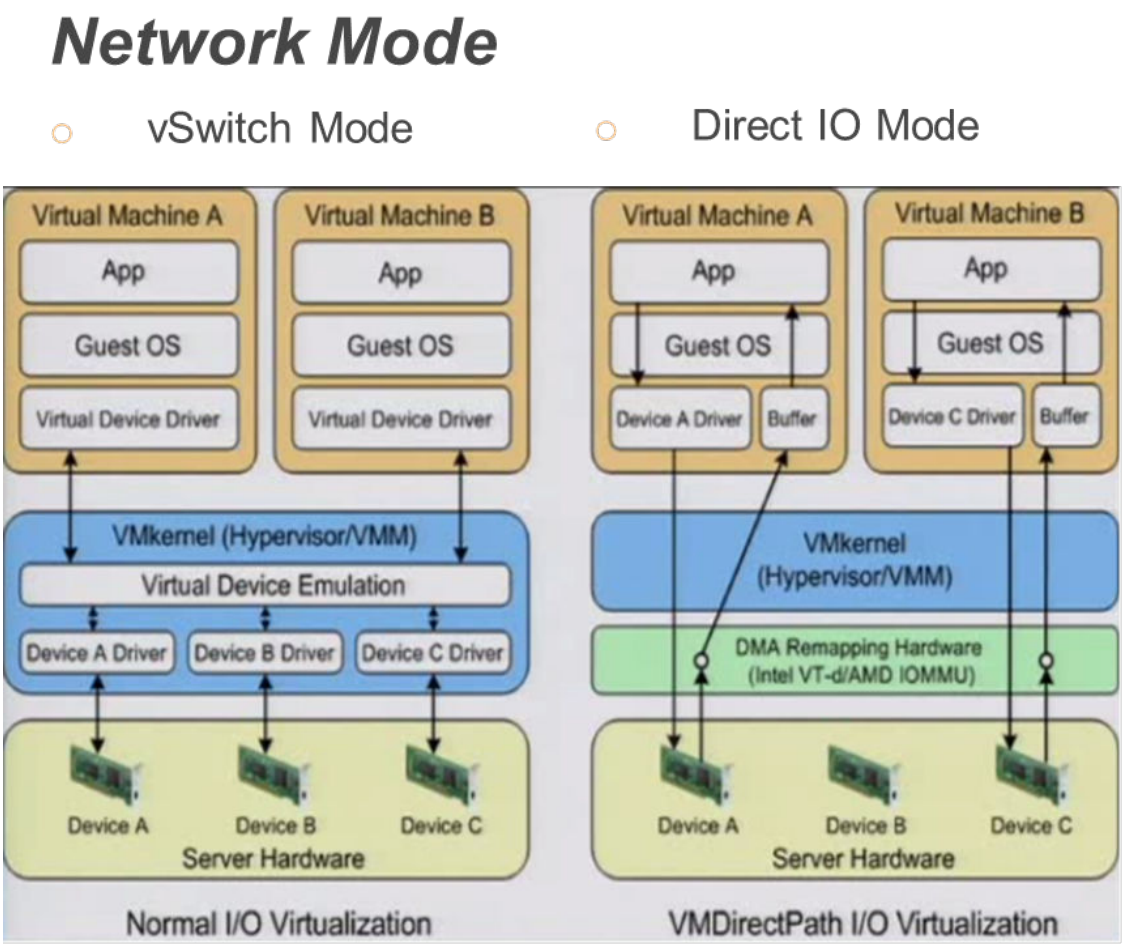
Hypervisor	Number of CPUs	Memory (GB)	Hard Disk (GB)	Number of Tunnels	Tunnel Bandwidth (Intel NIC-10 G) (Unencrypted)	Packet Size (Bytes)
Vmware (DirectIO)	3	6	10	1000	17.6 Gbps	1400
Vmware (DirectIO)	6*	6	10	10000	6.3 Gbps	Random
Vmware (DirectIO)	3	6	10	10000	4.5 Gbps	Random

NOTE

Refer to the vSZ-D Performance Recommendations on page 59 chapter for encryption and vSwitch impacts.

NOTE

* vDP needs to increase the CPUs to 6 for sustaining the 10GB line rate in random-byte traffic when the encryption is enabled. Encrypted requires 6 cores and unencrypted requires 3 cores



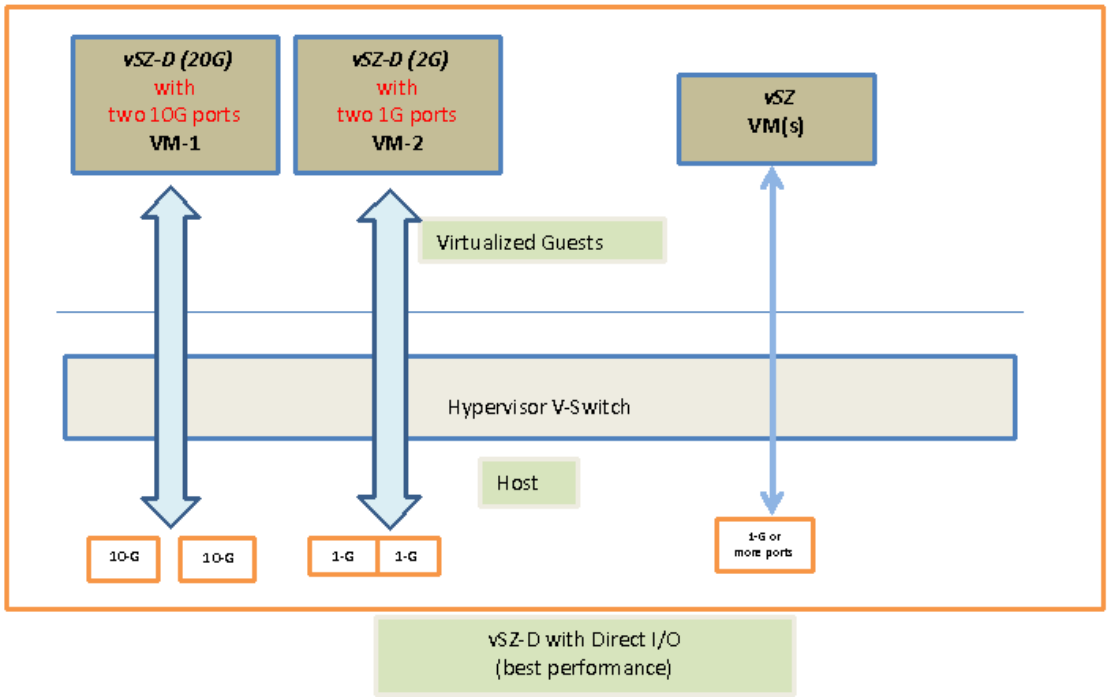
The figure below depicts a sample configuration in DirectIO mode. This is the recommended deployment model for the vSZ-D for best performance benefits. In this setup, cores as well as the NICs are dedicated to the vSZ-D VM only for best performance.

NOTE
In this setup, the vSZ-D data plane interfaces directly with the DPDK NIC, completely bypassing the vSwitch

vSZ-D with DirectI/O

NOTE
The figure below depicts multiple virtual data plane instances for reference purposes only.

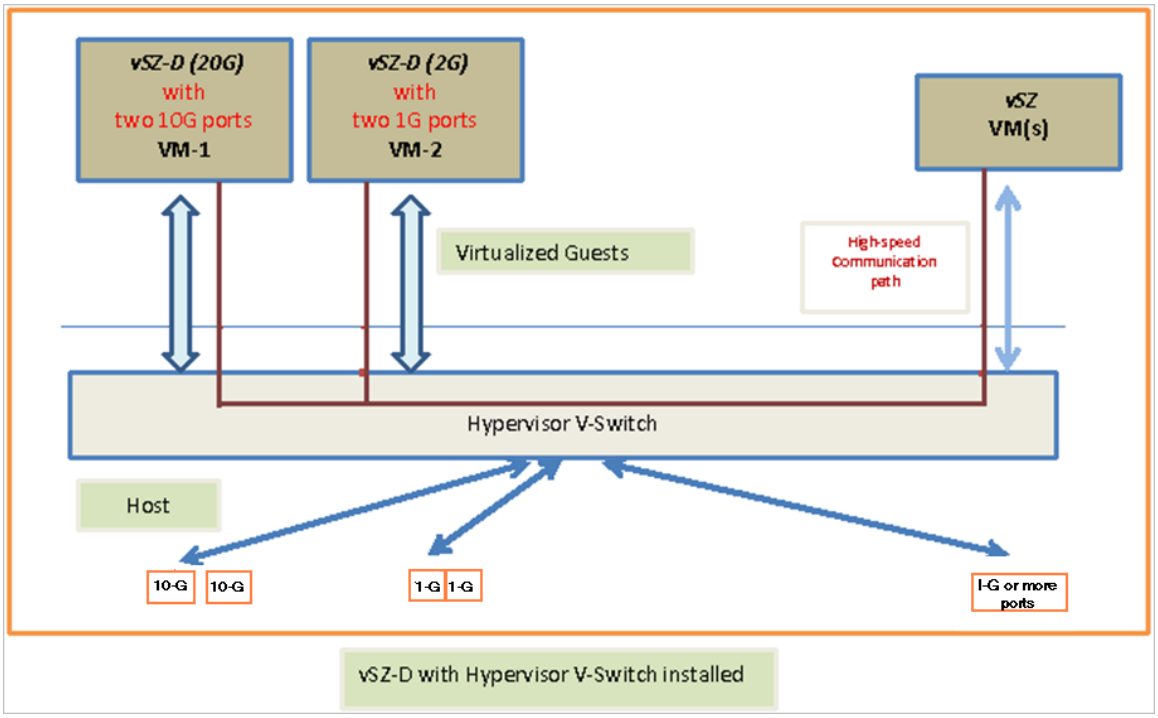
It also depicts a vSZ controller instance running as a separate VM. These VMs can be running on the same underlying host or potentially different hosts.



vSZ-D with Hypervisor vSwitch Installed

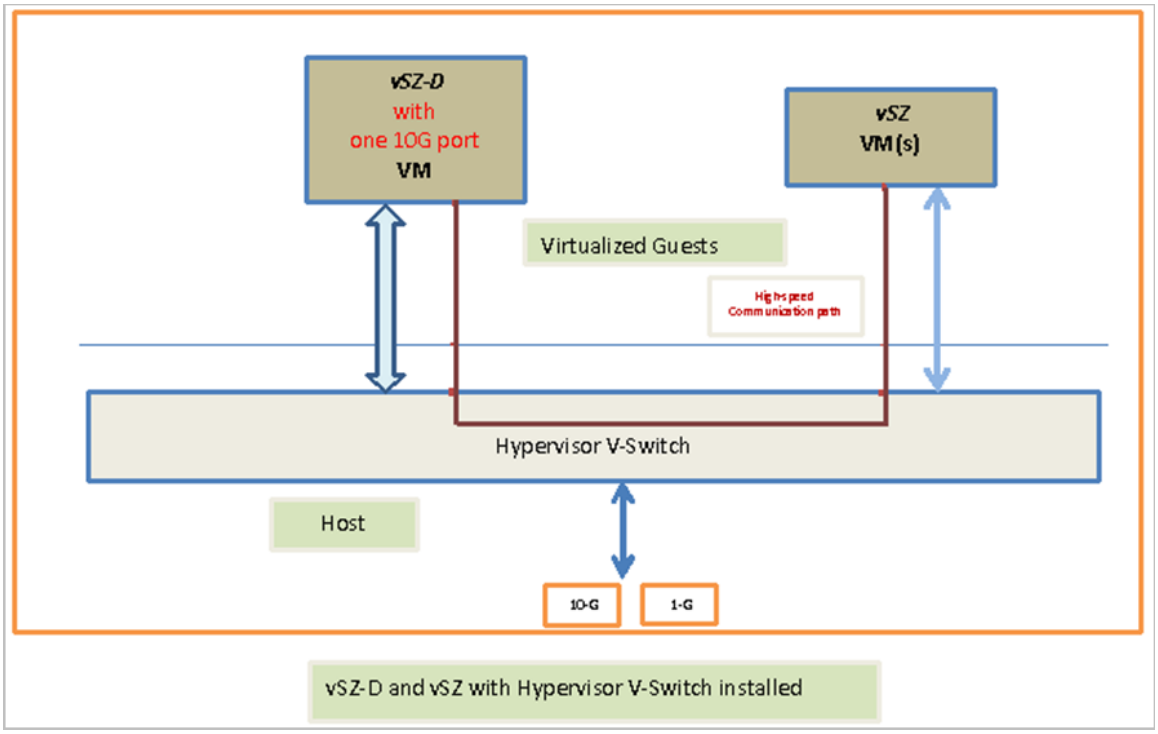
The figure below depicts a sample setup via the vSwitch.

NOTE
The figure below depicts multiple virtual data plane instances for reference. It also depicts a vSZ controller instance running as a separate VM.



vSZ-D and vSZ with Hypervisor vSwitch Installed

The figure below depicts an architecture where vSZ and vSZ-D are running on the same underlying host.



Recommended NICs and Operation Modes

The following table lists the modes of operation and network interface cards (NICs) that have been tested by Ruckus Wireless. Other NICs that support Intel DPDK architectures may or may not work.

TABLE 6 Recommended NICs and operation modes

Interface	Mode	Supported NIC Driver		NIC Model
Control / management	vSwitch	E1000		82574
Data	Direct IO	1GB	igb	I350
				82576
				Intel 82571EB
				Broadcom BCM5720
		10GB	ixgbe	82599EB
				82598
				X540 (T1 and T2, for RJ-45 twist-pair)
				X520
	vSwitch	VMware	VMXNET3	--
		KVM	Virtio	--

Hypervisor Configuration

- Supported Hypervisors....43
- General Configuration....43
- VMware Specific Configuration....43
- KVM Specific Configuration....48

This section covers hypervisor-specific configurations that Ruckus Wireless recommends and other settings that you may need to fine tune.

Supported Hypervisors

Unlike the vSZ controller, vSZ-D can only be installed on specific versions of VMware and KVM.

The tables below list the hypervisors and versions on which vSZ and vSZ-D can and cannot be installed.

TABLE 7 vSZ and vSZ-D supported hypervisors

	vSZ	vSZ-D
VMware 5.1	Supported from 2.5	
VMware 5.5 and later	Supported from 3.0	Supported from 3.2
KVM CentOS 6.5 64-bit	Supported from 2.5	
KVM CentOS 7.0 64-bit	Supported from 3.0	Supported from 3.2
Hyper-V	Supported from 3.2	
Azure	Supported from 3.2	
GCE	Supported from 3.2	

General Configuration

Ruckus Wireless offers the following general configuration recommendations.

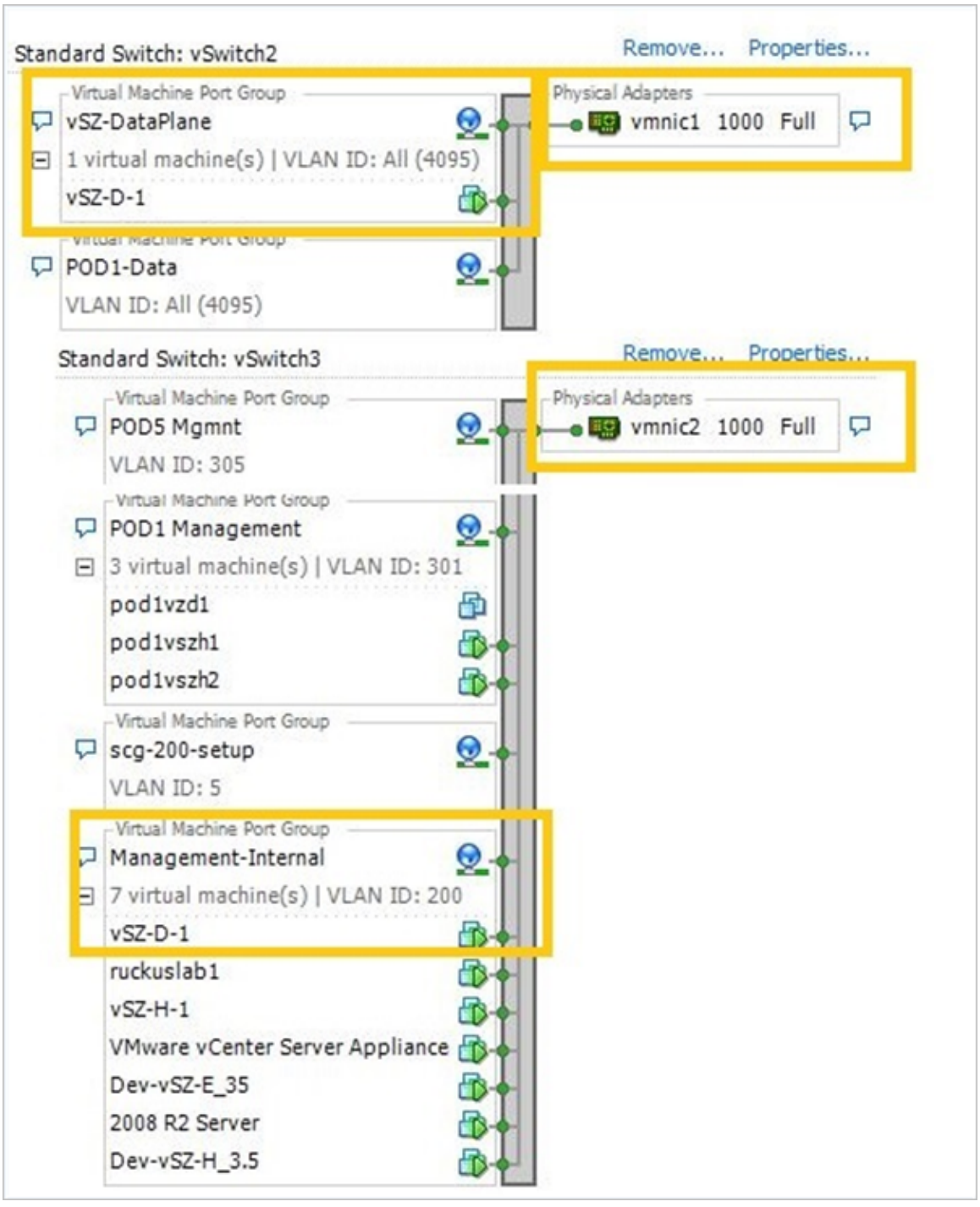
TABLE 8 General vSZ-D configuration recommendations

Component	Minimum Recommendation
Recommended reserved memory	Minimum 6144MB
Recommended number of CPU cores	Minimum three CPU cores. For improved performance in a large-scale deployment, allocate six CPU cores.
Configuration via DirectIO or through vSwitch	To enable passthrough on NIC devices, configure DirectIO mode in ESXi in **Advanced Settings**.

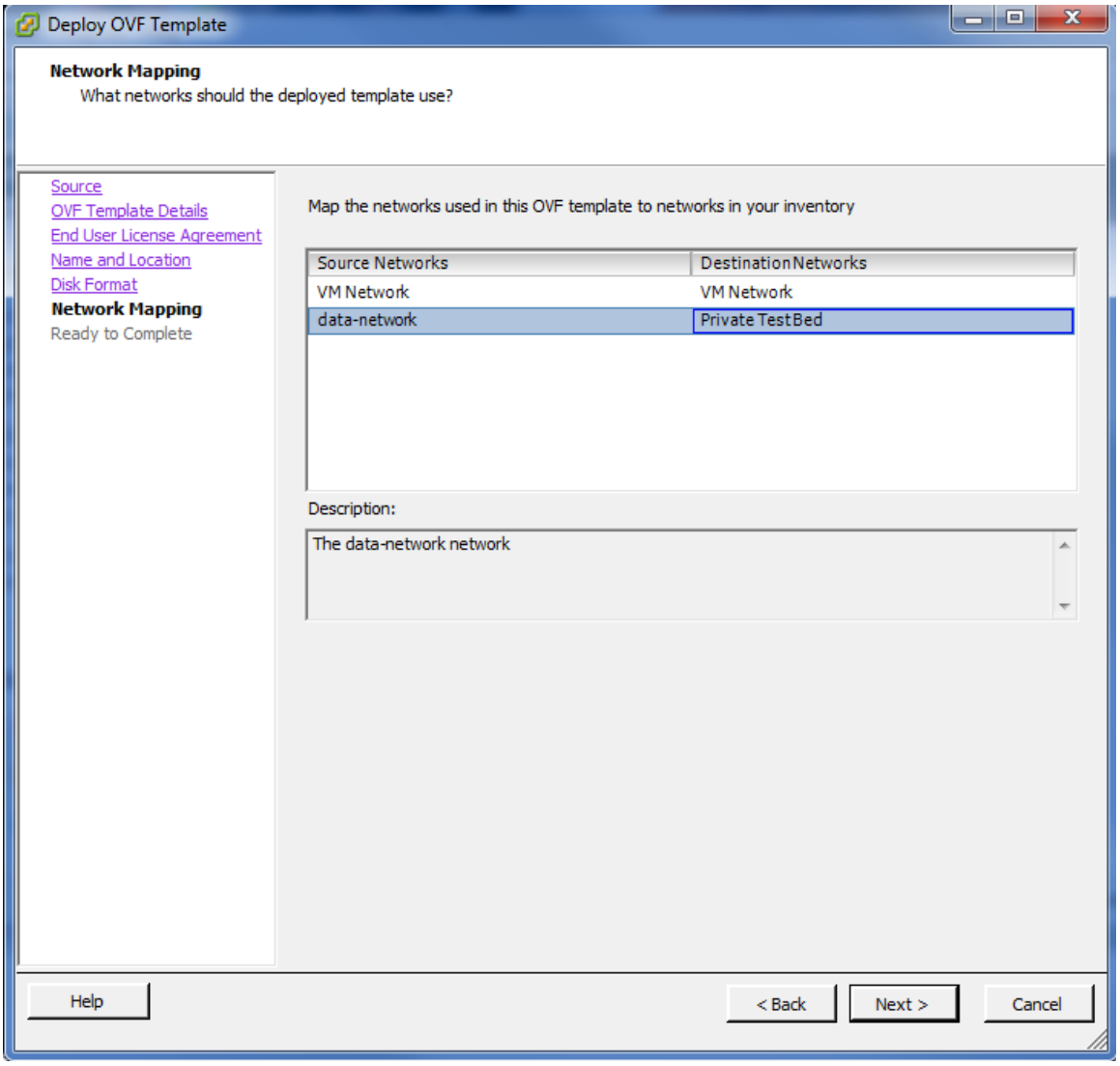
VMware Specific Configuration

If you are installing vSZ-D on VMware, read these VMware specific configuration recommendations from Ruckus Wireless.

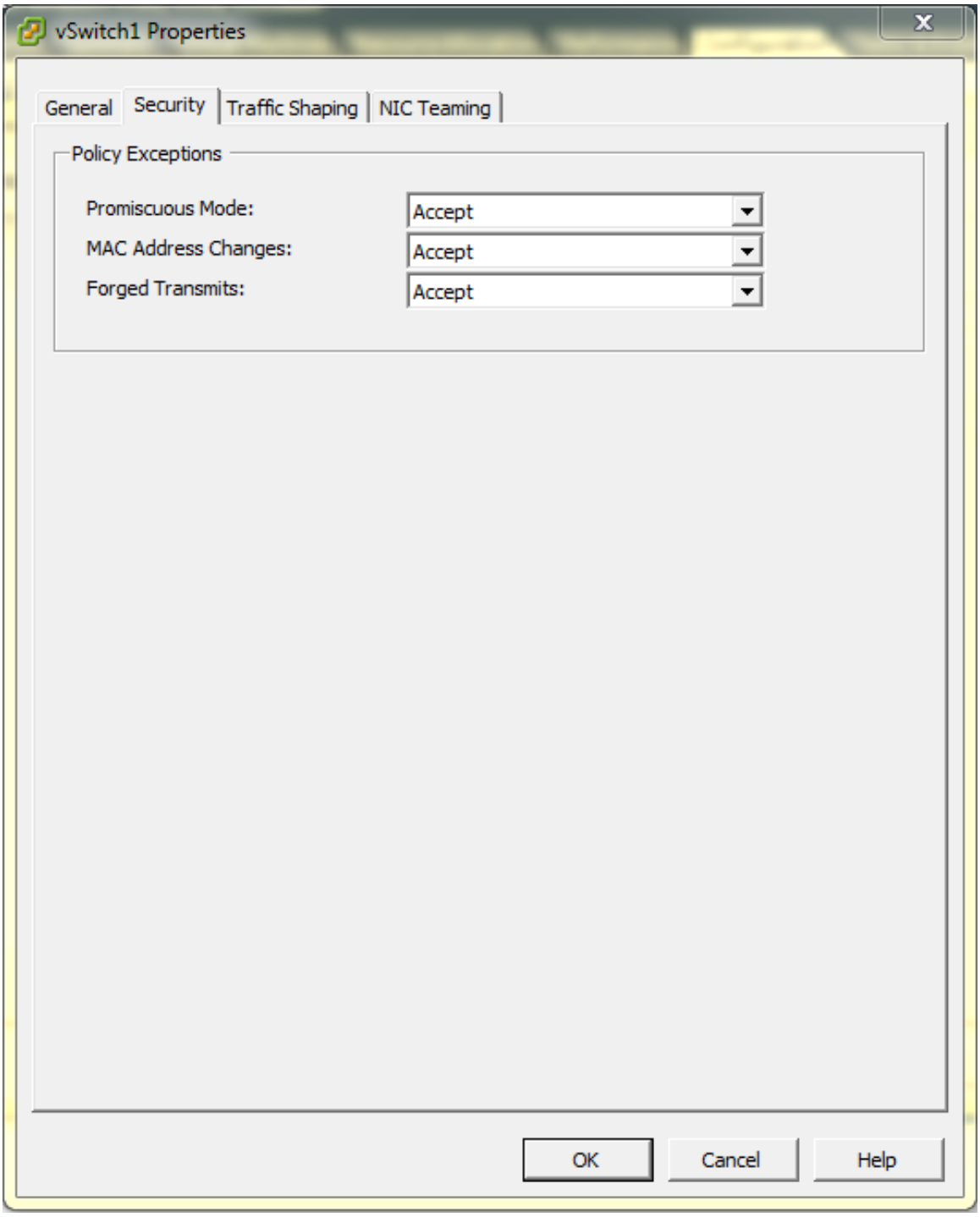
- Deploy vSZ-D on a machine that has at least two physical NICs. Alternatively, deploy to two vSwitch instances with dedicated physical NICs.



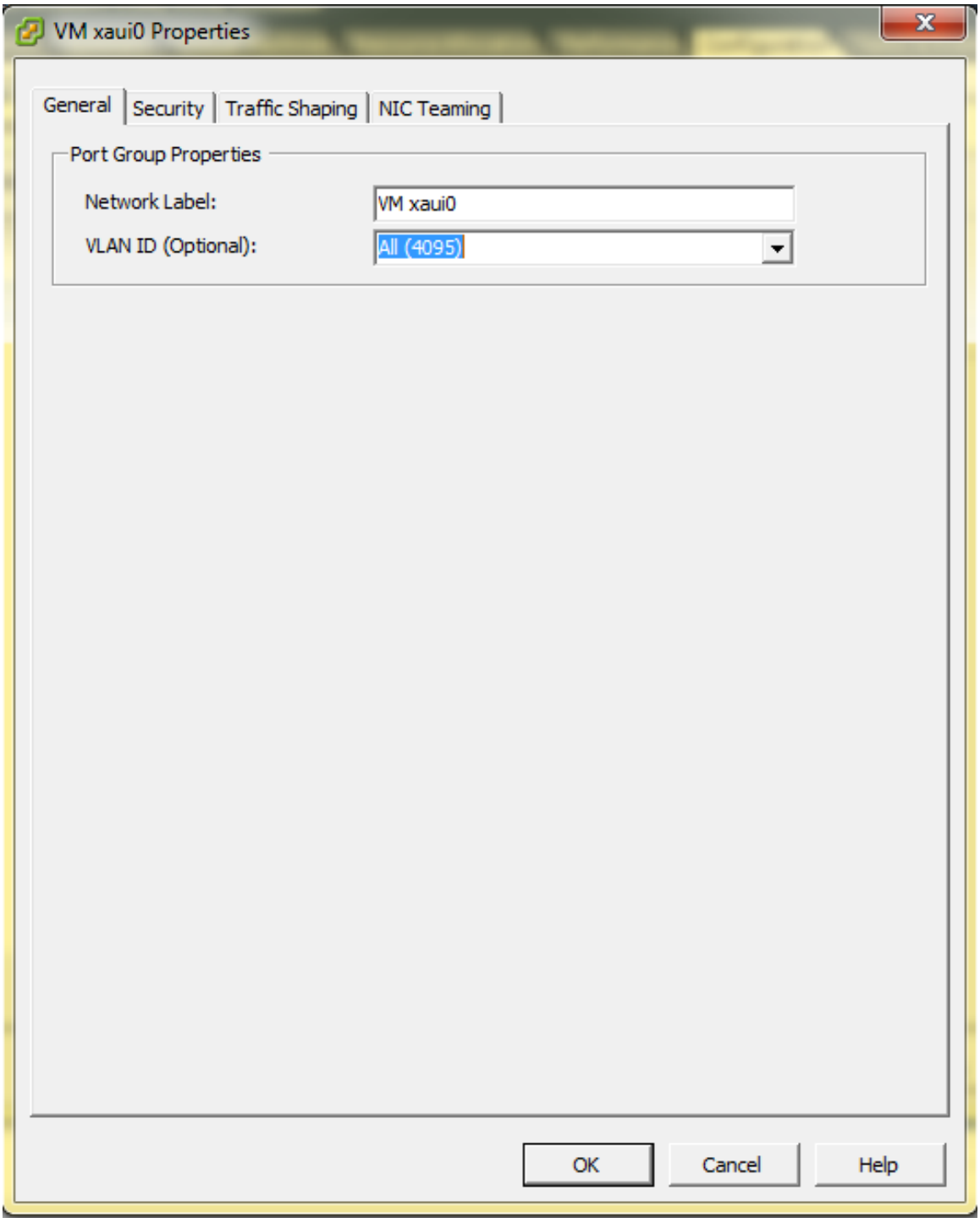
- When deploying an instance of vSZ-D using an OVA file, you must assign the management and data interfaces to two different network groups (vSwitch) on different subnets.



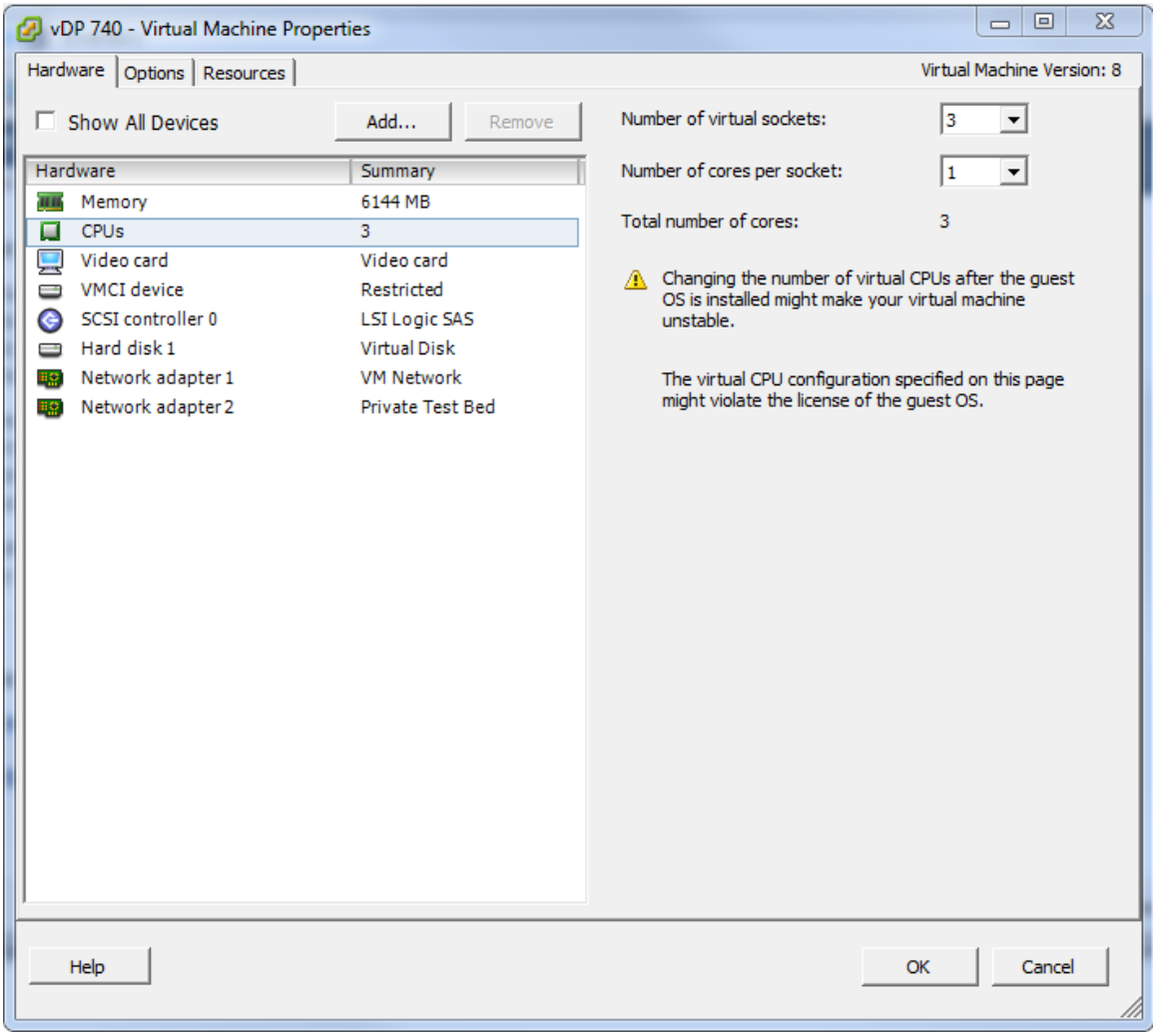
- Enable **Promiscuous** mode in vSwitch Config.



- In **vSwitch Config**, enable VLAN ID for **All**.



- After the vSZ-D instance is ready, modify the number of CPU cores (if needed) before powering on vSZ-D.



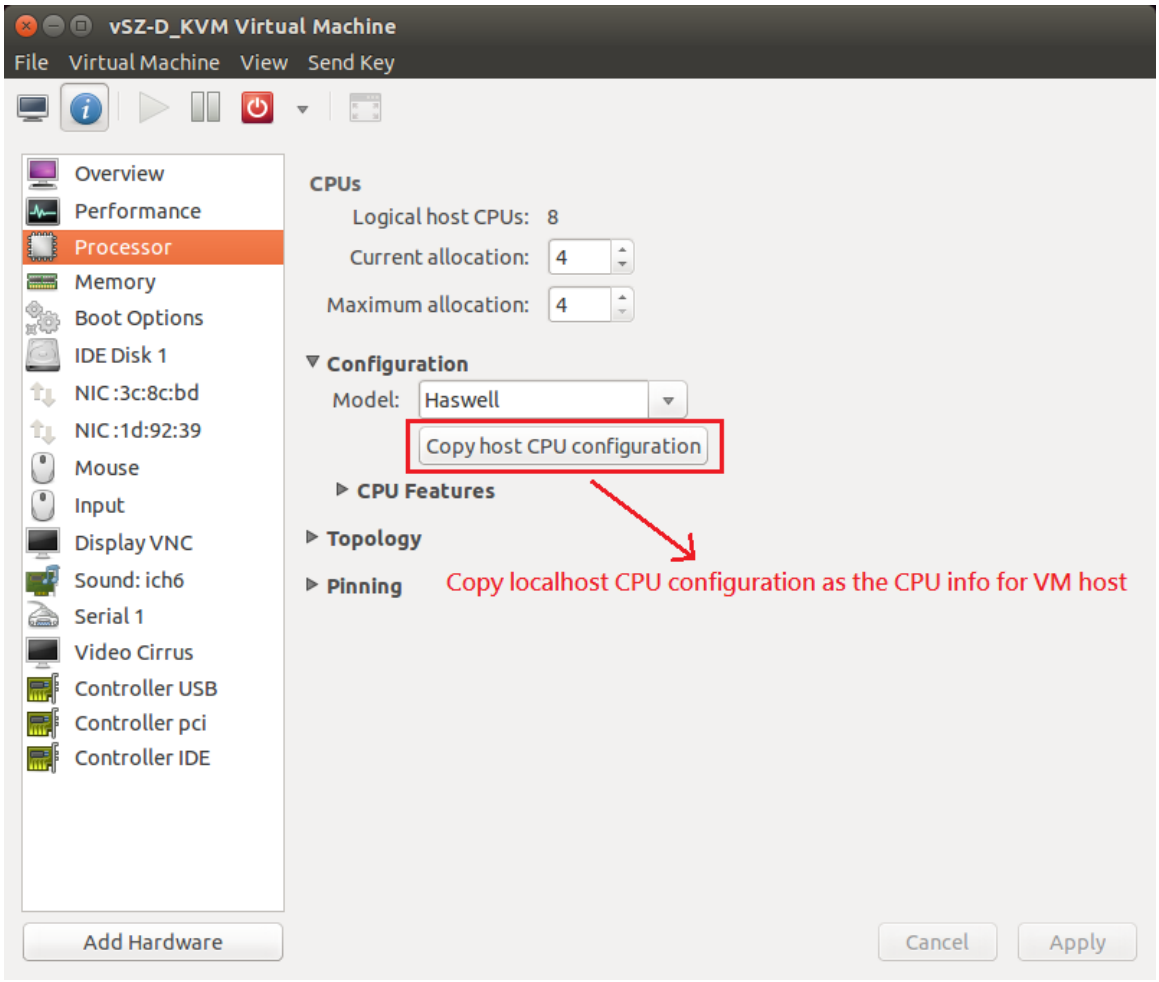
- For advanced CPU and memory resource configuration recommendations, refer to the *vSphere Resource Management Guide*, which is available on the VMware website.

KVM Specific Configuration

If you are installing a KVM on VMware, read these KVM specific configuration recommendations from Ruckus Wireless

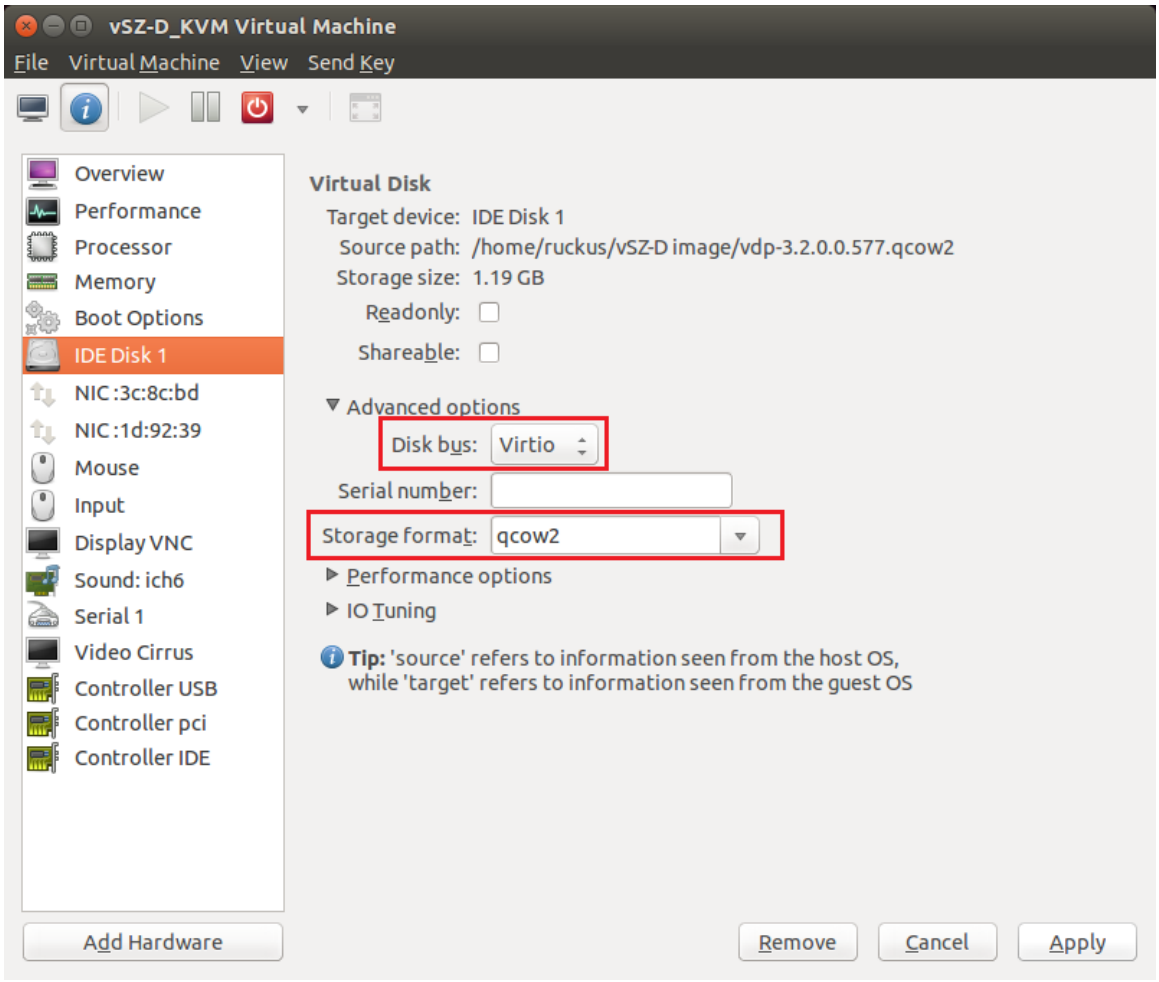
CPU Type

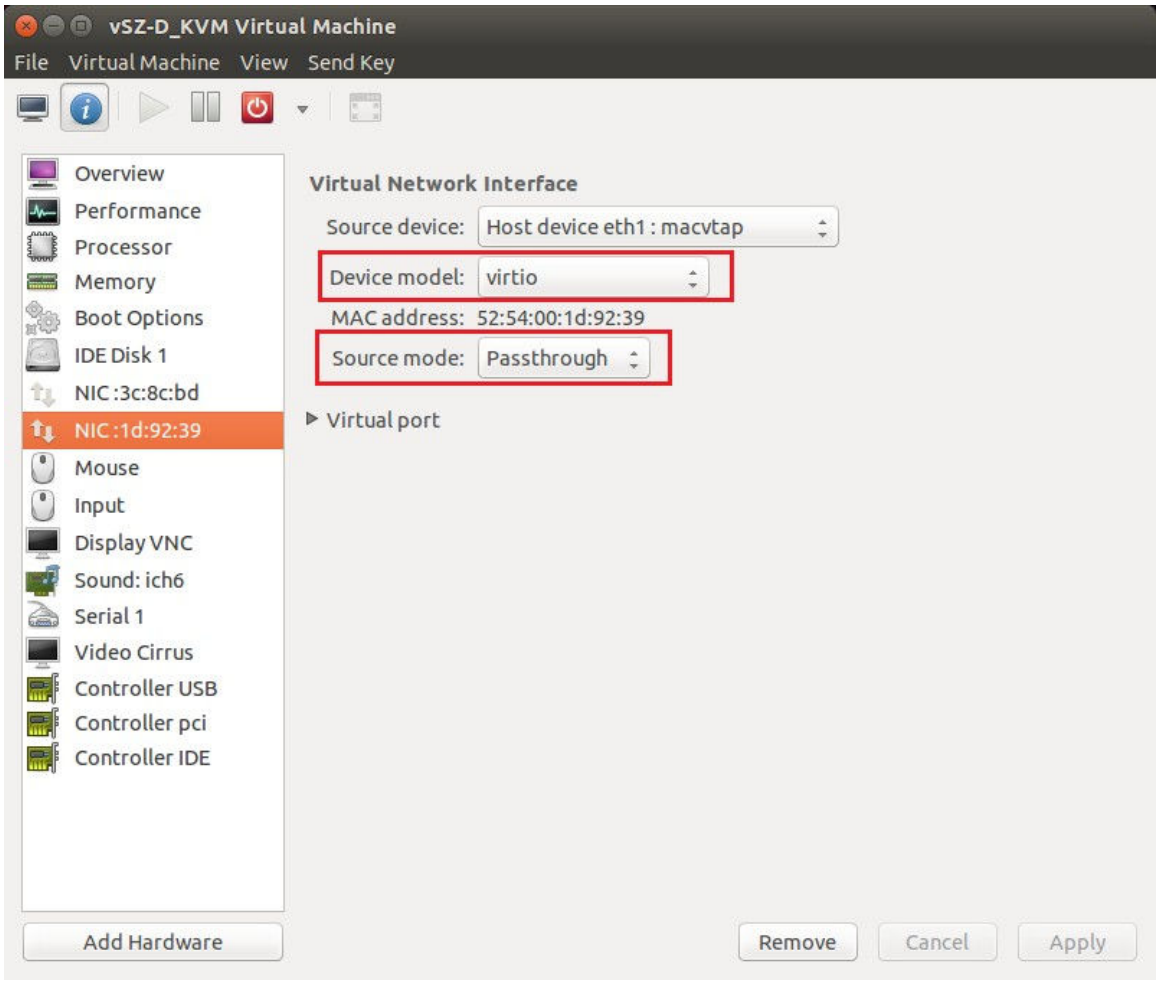
When selecting the CPU model, make sure you select one that is higher than Intel Core 2 Duo. On Linux, you can this information in `/proc/cpuinfo`.



Disk Configuration

Ruckus Wireless recommends using Virtio as the disk bus and qcow2 as the storage format.


vSZ-D_KVM Virtual Machine
File Virtual Machine View Send Key
Overview
Performance
Processor
Memory
Boot Options
IDE Disk 1
NIC :3c:8c:bd
NIC :1d:92:39
Mouse
Input
Display VNC
Sound: ich6
Serial 1
Video Cirrus
Controller USB
Controller pci
Controller IDE
Virtual Disk
Target device: IDE Disk 1
Source path: /home/ruckus/vSZ-D image/vdp-3.2.0.0.577.qcow2
Storage size: 1.19 GB
Readonly:
Shareable:
Advanced options
Disk bus: Virtio
Serial number:
Storage format: qcow2
Performance options
IO Tuning
Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS
Add Hardware
Remove
Cancel
Apply



NIC Configuration in Direct IO Mode

NOTE

Only the data interface needs to be configured to direct PCI passthrough. The management interface should always be configured to e1000 as the NIC driver.

Before adding a PCI device to the KVM, you need to complete the following steps:

1. Enable VT-d (for Intel processors) in the motherboard BIOS. Intel's VT-d ("Intel Virtualization Technology for Directed I/O") is available on most i7 family processors.
2. Add kernel boot parameters via GRUB to enable IOMMU (see figure below). To enable IOMMU in the kernel of Intel processors, pass **intel_iommu=on** boot parameter on Linux. For more information, read this tutorial.
3. After configuring the boot parameter, reset the computer.

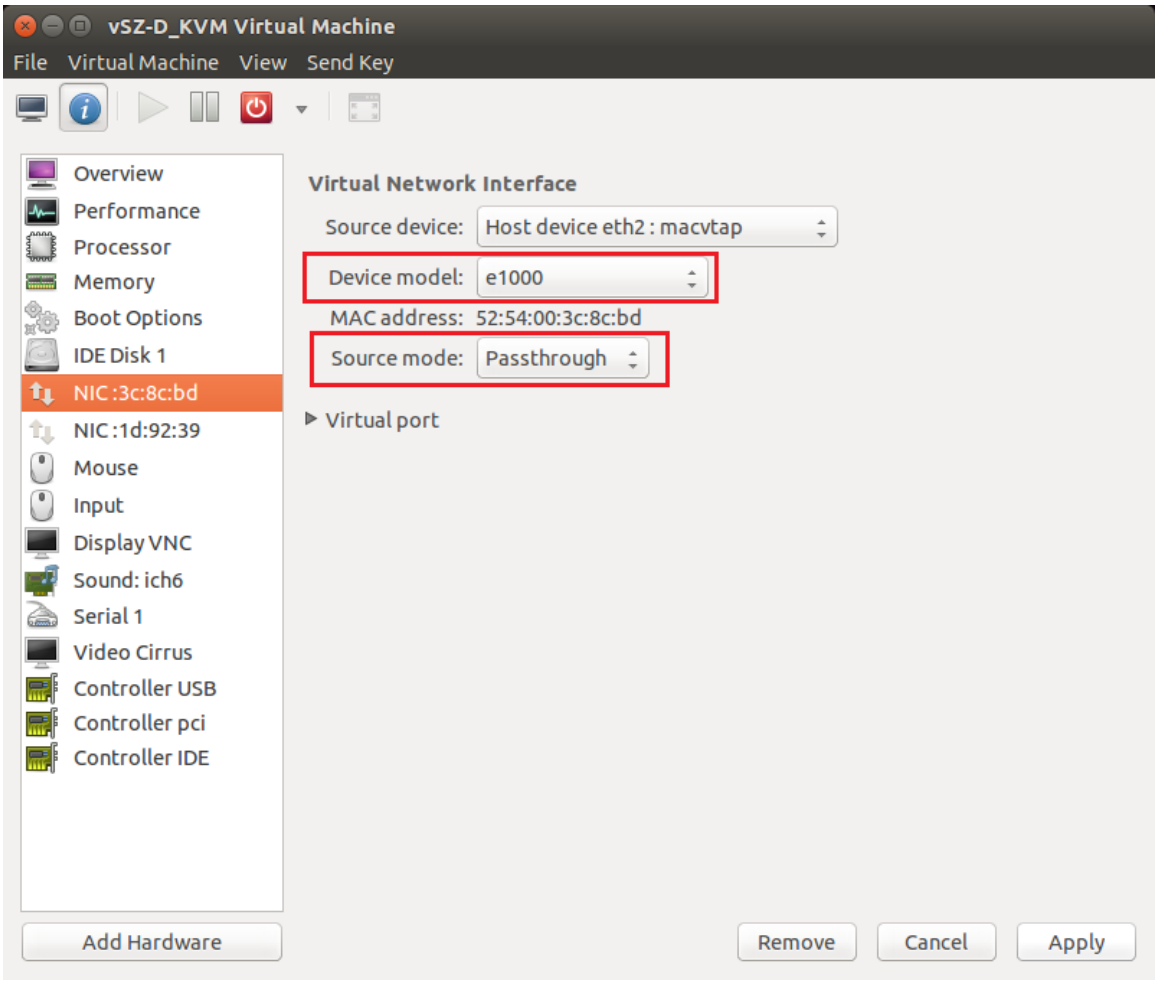
NIC Configuration in vSwitch Mode

NOTE

Configure only two ports for vSZ-D.

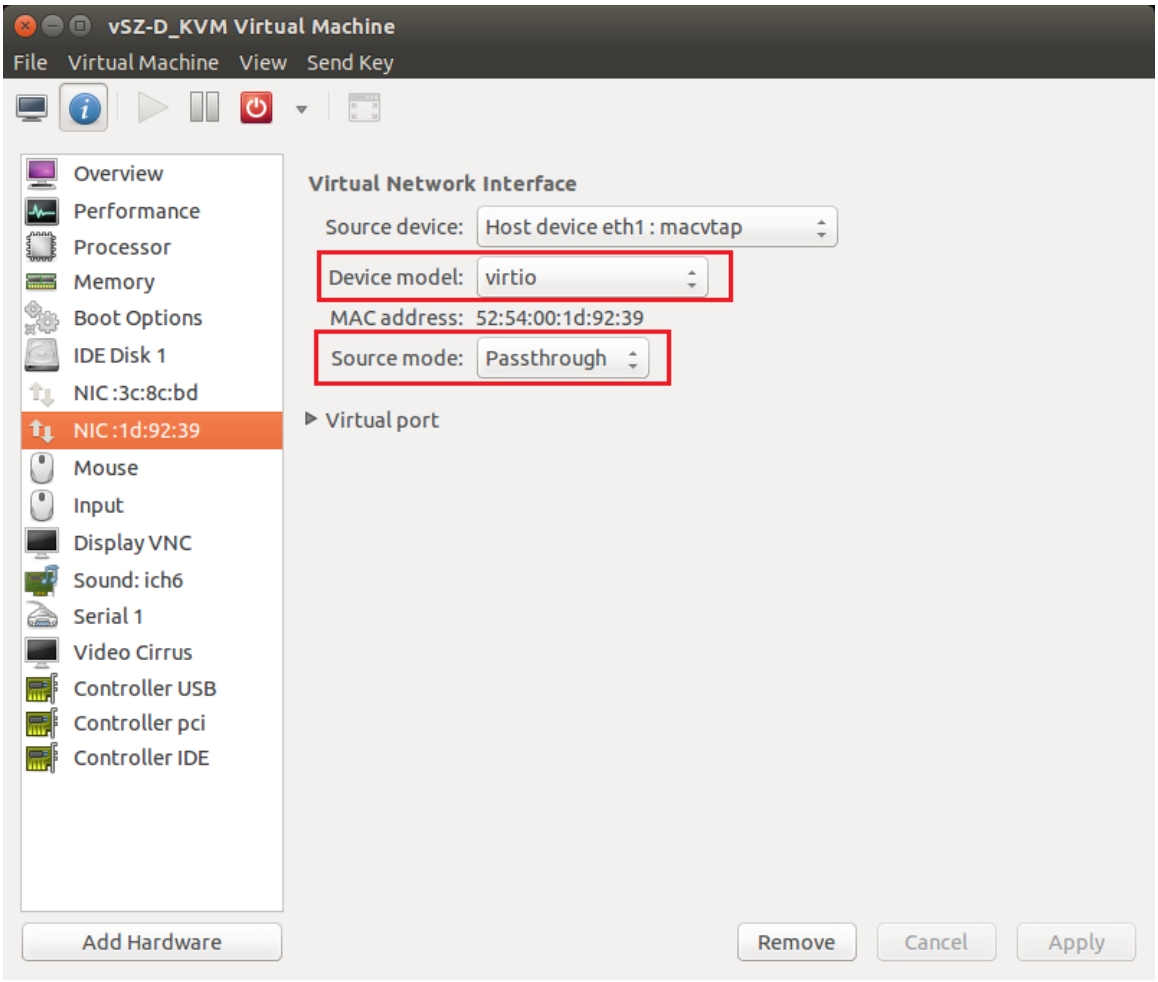
For the management interface, use the following settings:

- **Device model**: e1000
- **Source mode**: Either **Bridge** or **Passthrough** if you are using **macvtap** for the device type.



For the data interface, use the following settings:

- **Device model**: e1000
- **Source mode**: **Passthrough** if you are using macvtap for the device type. Only the passthrough mode can allow UE traffic to pass through the VM NIC.


vSZ-D_KVM Virtual Machine
File Virtual Machine View Send Key
Overview
Performance
Processor
Memory
Boot Options
IDE Disk 1
NIC :3c:8c:bd
NIC :1d:92:39
Mouse
Input
Display VNC
Sound: ich6
Serial 1
Video Cirrus
Controller USB
Controller pci
Controller IDE
Virtual Network Interface
Source device: Host device eth1 : macvtap
Device model: virtio
MAC address: 52:54:00:1d:92:39
Source mode: Passthrough
Virtual port
Add Hardware
Remove
Cancel
Apply

Upgrade Procedure

- Upgrade Procedure.....55

Upgrade Procedure

Procedure for upgrading to a new vSZ-D version.

Controller and vSZ-D Firmware Compatibility Matrix

The below table indicates the compatibiliy matrix. In general, Ruckus Wireless supports N-2 vSZ-D releases with vSZ.

TABLE 9 Controller and vSZ-D Firmware Compatibility Matrix

vSZ Release	vSZ-D Release		
	3.5	3.4	3.2
3.5	Yes	Yes	Yes
3.4	No	Yes	Yes
3.2	No	No	Yes

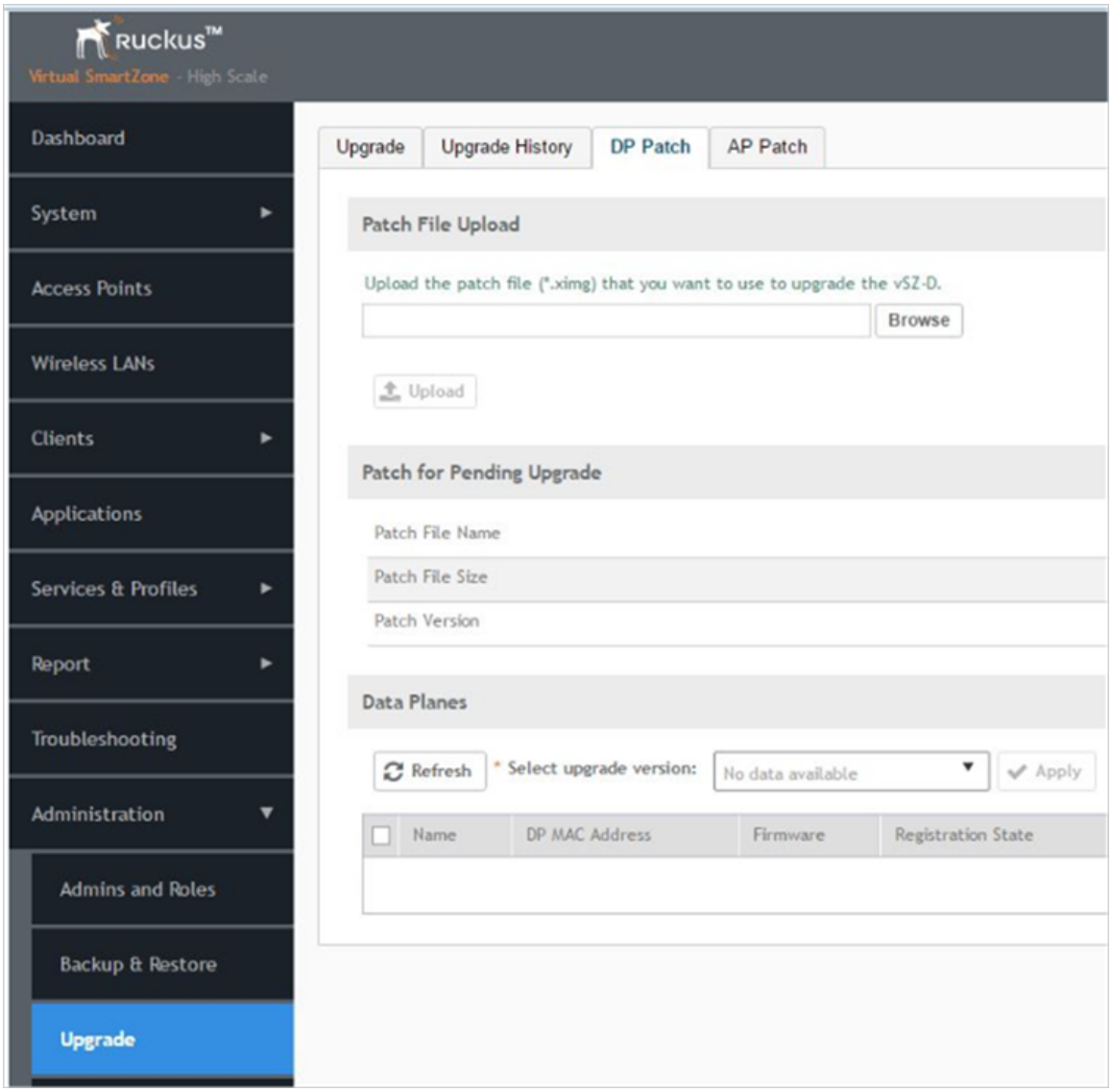
Follow these steps to upgrade the vSZ-D version.

NOTE
Before starting this procedure, you should have already obtained a valid software upgrade file from Ruckus Wireless® Support or an authorized reseller.

NOTE
If you are upgrading both vSZ and vSZ-D, Ruckus Wireless® recommends upgrading vSZ first before vSZ-D.

1. Copy the software upgrade file that you received from Ruckus Wireless® to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Go to **Controller web interface** > **Administration** > **Upgrade**

FIGURE 19 Upgrade Section



3. In the **Patch File Upload** section, click the **Browse** button, and then browse to the location of the software upgrade file.

   The file name of the software upgrade file is `vSZ-D-installer_{version}.ximg`.

4. Click **Upload** to upload the software upgrade file.
5. The **Patch Information** displays the new vSZ-D file details.
6. Select the vSZ-D instance that you want to upgrade from the **Data Plane** table and click **Apply**.

   The controller fetches the new vSZ-D version on a reboot.

7. To verify if the upgrade is successful after a reboot:
   - Go to **Controller web interface** > **Administration** > **Upgrade** to view a confirmation message that the data plane firmware upgrade is complete.
   - Go to **Controller web interface** > **Configuration** > **System** > **Cluster Planes** to view a confirmation message that the data plane is managed with an upgrade firmware version.

vSZ-D Performance Recommendations

vSZ-D has been designed to induce minimal latency in user data aggregation and forwarding. The unique design of the vSZ-D software enables consistent packet performance with minimal throughput degradation as the number of tunnels or the number of clients' increase.

The fast path processing of the vSZ-D is engineered to scale to the underlying NIC capacity profiles whether be it 1G or 10G speeds. vSZ-D is designed to scale and handle data tunnels and data forwarding capabilities at high scale.

The following are some important observations and recommendations related to the vSZ-D performance:

- To obtain the best throughput, Ruckus Wireless recommends operating vSZ-D in directIO mode. This recommended mode of operation applies whether the hypervisor used is VMware or KVM.
- vSZ-D supports vSwitch mode of operation for added flexibility in deployments where vSZ-D may be co-located with other VMs for service chaining on the same underlying hardware. Note that the current observations are that in the vSwitch mode of operation, there is an induced performance impact in comparison with the directIO mode of operation. This may be due to the latency or performance bottleneck in virtIO and vSwitch sharing. This is still being researched at the Ruckus Wireless R&D Labs.
- There is an expected performance impact when enabling encryption (AES 128 bit) on the Ruckus GRE Tunnels. This is due to the overhead induced by the crypto processing on Ruckus Wireless AP and vSZ-D due to the associated overheads of encryption and decryption on a per packet basis. The vSZ-D software is designed to introduce minimal latency and overheads associated in packet processing. vSZ-D takes advantage of the underlying Intel chip's crypto module for packet encryption and decryption and the associated impact is primarily bounded at the hardware level.

For specific recommendations and calibrations that may be needed for your deployment, contact Ruckus Wireless.