

# Extreme Virtual Packet Broker 2.0.0 Release Notes

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing)

# Contents

---

Document history.....	4
Overview.....	4
Summary of features and enhancements.....	5
System requirements.....	6
Document library.....	6
Known Issues.....	7
Resolved issues.....	8

# Document history

Version of Document	Summary of Changes	Publication Date
1.0	New document for the 2.0.0 release	February 13, 2019

## Overview

Extreme Virtual Packet Broker (vPB) 2.0.0 is a full-featured network visibility solution built for virtualized service provider and enterprise networks. It offers an end-to-end set of capabilities including traffic interception, filtering, load-balancing, and optimization for network monitoring and analytics tools.

vPB can perform various operations such as filtering (SMARTMatch), forwarding, VLAN tag insertion/deletion, header stripping, packet slicing, sampling and IPFIX export. vPB addresses the visibility challenge in virtual workloads.

### NOTE

vPB 2.0.0 is not backward compatible with vPB 1.0.0.

# Summary of features and enhancements

This release of Extreme Virtual Packet Broker (vPB) 2.0.0 supports the following features and enhancements:

- **Qcow2 image format**

vPB is packaged as a qcow2 image format, enabling it to be deployed on a KVM hypervisor host out-of-the-box.

- **Preconfigured vNICs**

The vPB qcow2 image includes five preconfigured vNICs:

- **Management:** For management
- **Ingress:** For receiving ingress packets
- **Egress:** For sending packets post-processing
- **IPFIX:** For exporting IPFIX metadata
- **Test:** For sending a test pcap to the Rx interface

- **SMARTMatch**

The SMARTMatch feature enables vPB to identify tunnels/flows/packets based on n-tuples and configure an action for the matched n-tuples.

SMARTMatch also supports flex-match capability to detect one or more regex or hex patterns anywhere within the L2 packet boundary and configure an action to either drop or forward the traffic to an egress path.

SMARTMatch supports these protocols: Ether, IP, TCP, UDP, SCTP, HTTP, HTTPS and SSH.

The following packet modification actions can be configured for a SMARTMatch rule:

- **Packet masking**

This feature enables masking of sensitive information in a packet either:

- > With a specific pattern at configured offset.

or

- > From the flex-match pattern start offset.

vPB supports up to four mask patterns for a given SMARTMatch alias.

- **Packet slicing**

Packet slicing feature enables truncation/removal of bytes from the packet trailer with a specified packet offset.

- **Header stripping**

Header stripping enables removal of a particular header from a packet.

vPB supports header stripping for:

- > 802.1BR Tag
- > VN-Tag
- > VxLAN
- > NVGRE
- > MPLS label
- > ERSPAN Type II
- > GTP-U

- **Sampling**

vPB supports sampling, which provides a representative view of IP traffic. Sampling is achieved by configuring a sampling policy, which specifies the drop percentage and an optional action. A sampling policy can be used as an action in a SMARTMatch rule.

- **IPFIX export**

vPB can be used to export session information in IPFIX (IP Flow Information Export) format. UDP is the supported transport protocol.

vPB includes a dedicated virtual interface for IPFIX export.

- **Tunnel termination**

vPB can terminate ERSPAN Type II, GREv0, GREv1, IPIP and VxLAN tunnels, and process the flows/packets inside these tunnels. vPB supports termination of multiple tunnels.

- **Tunnel initiation**

vPB can be configured to initiate GREv0 and VxLAN tunnels to transport egress traffic. A maximum of 10 egress Tunnels can be configured.

- **Logs**

vPB supports different log levels: Critical, Error, Warning, Info, and Debug. Critical and Error log levels are always on. CLI/REST API can be used to turn on/off the Warning, Info, and Debug log levels (per module, if applicable).

- **CLI and REST API**

vPB supports both CLI and REST API for configuration as well as statistics.

- **SNMP**

vPB supports SNMP v2 and SNMP v3 to send SNMP traps to a user-specified SNMP trap receiver.

For more information about each feature, see *Extreme Virtual Packet Broker Administration Guide*.

## System requirements

The table below shows the system specifications for vPB qcow2 image. Ensure that the KVM hypervisor meets these requirements:

**TABLE 1** System requirements

Entity	Specification	
vCPU	2	
RAM	4 GB	
HDD	16 GB	
vNIC	5	
Driver	e1000	
Hypervisor	qemu-kvm 1.5.3	
OS	<b>Release version</b>	<b>Kernel version</b>
	CentOS release 7.2 x86_64 x86_64 x86_64 GNU/Linux	3.10.0-327.el7.x86_64

## Document library

The following Virtual Packet Broker publications are available to customers:

- Extreme Virtual Packet Broker Administration Guide
- Extreme Virtual Packet Broker Software Installation Guide

- Extreme Virtual Packet Broker Command Reference Guide
- Extreme Virtual Packet Broker REST API Guide
- Extreme Virtual Packet Broker Release Notes (this document)

## Known Issues

This section lists known issues in this release. Note that if a workaround for an issue is available, it is provided.

Defect ID: VTAP-53
<b>Summary:</b> No IPFIX record is generated for template=272, when only DNS QUERY is received and its corresponding DNS RESPONSE is not received by vPB.
<b>Workaround:</b> No workaround
<b>Found in Release:</b> vPB2.0.0
Defect ID: VTAP-485
<b>Summary:</b> Pressing <b>TAB</b> after typing a CLI command that takes a single parameter causes invalid parameters to be displayed. For example, pressing <b>TAB</b> after typing <code>show tech brief</code> displays <code>show tech brief detail</code> , and pressing <b>Enter</b> displays the message, <b>Invalid Command</b> .
<b>Workaround:</b> Execute the CLI commands with only valid parameters. For example, execute either <code>show tech brief</code> or <code>show tech detail</code> , and not <code>show tech brief detail</code> as that is invalid.
<b>Found in Release:</b> vPB2.0.0
Defect ID: VTAP-534
<b>Summary:</b> If vPB goes down during load configuration, the CLI cannot communicate with vPB.
<b>Workaround:</b> Restart both vPB and CLI service.
<b>Found in Release:</b> vPB2.0.0
Defect ID: VTAP-540
<b>Summary:</b> If only one rule is configured, the <code>show smartmatch-stats rule rule-id=all</code> command does not display the rule.
<b>Workaround:</b> Run the <code>show smartmatch-stats rule rule-id=&lt;rule_id&gt;</code> command to display the rule.
<b>Found in Release:</b> vPB2.0.0
Defect ID: VTAP-544
<b>Summary:</b> After creating a maximum of 600k flows/tunnels, if VLAN header stripping is applied (in a SMARTMatch rule or on the interface), MPLS header is also stripped.
<b>Workaround:</b> No workaround.
<b>Found in Release:</b> vPB2.0.0
Defect ID: VTAP-547
<b>Summary:</b> If sampling is applied for more than 400 SMARTMatch rules, <code>show sampling-stats</code> command displays stats for only the first 400 SMARTMatch rules.
<b>Workaround:</b> Run the <code>show smartmatch-stats rule rule-id=&lt;rule_id&gt;</code> and <code>show interface-stats</code> commands to display the required stats.
<b>Found in Release:</b> vPB2.0.0

# Resolved issues

There are no resolved issues in this release.