Highlights

- Provides comprehensive network visibility, helping to secure, monitor, optimize, and monetize virtualized networks
- Scales dynamically to meet compute capacity requirements during surges in network traffic
- Improves operational efficiency by automating resource provisioning and simplifying feature additions
- Enhances monitoring productivity by allowing the dynamic modification of flow definitions and traffic optimization functions within the Extreme Networks virtual network visibility infrastructure

Extreme Virtual Packet Broker and Virtual TAP

Scalable Network Visibility for Virtualized Service Provider and Enterprise Networks

The virtualization of networking functions across service providers, data centers, and enterprise networks has grown significantly as network operators embrace next-generation architectures to improve service agility and operational efficiency. At the same time, it is becoming more difficult to protect these complex virtualized networks from malicious attacks. Monitoring for performance, service quality, and user experience as well as dynamic resource orchestration and issue remediation are critical to maintaining network health and performance.

Common network visibility solutions are designed for hardware-centric networks. For the new virtual environment, network operators need an effective, highly scalable network visibility and monitoring solution that is specifically designed for virtual networks. Our Virtual Packet Broker (vPB) and Virtual TAP (vTAP) delivers a full-featured network visibility solution for virtualized service provider and enterprise networks. It offers an end-to-end set of capabilities — including traffic interception, filtering, and optimization — to maximize the productivity of network monitoring and analytics tools. With the vPB and vTAP, you can analyze traffic flowing between application VMs and if required forward to special purpose tools for further analysis.

Improved Operational Efficiency and Scale

Our vPB and vTAP eliminate typical long deployment cycles associated with hardware through automated scale orchestration and simplified provisioning. They allow dynamic modification of flow-definitions and traffic optimization functions in the network visibility infrastructure when changes occur in the production network (such as the addition or removal of VMs, variations in traffic volume, and new flow patterns). This capability improves monitoring productivity and offers greater network agility. Our vPB is designed to also mask patterns in specific packets to protect sensitive information from unauthorized usage.

Customers typically deploy one or more vTAPs on a host, switch, or subnet to monitor traffic to and from application VMs. (see Figure 1) vTAPs can directly interact with special-purpose probes as well as export IPFIX metadata (to gain insights into network traffic) to analytical tools. Customers can deploy a vPB to aggregate traffic from a large number of vTAPs and implement filtering actions on aggregated traffic and extract metadata information.

When traffic flows between VMs (see Figure 1) the vTAP instances process tapped traffic for monitoring purposes and forward configured flows or packets using tunnels or VLANs to the vPB. The vTAP also exports IPFIX metadata to the IPFIX collector for the desired traffic flow. The vPB terminates the tunnels from the vTAPs, aggregates the forwarded traffic and routes selected flows or packets to the probes. The vPB also exports IPFIX metadata to the IPFIX collector.

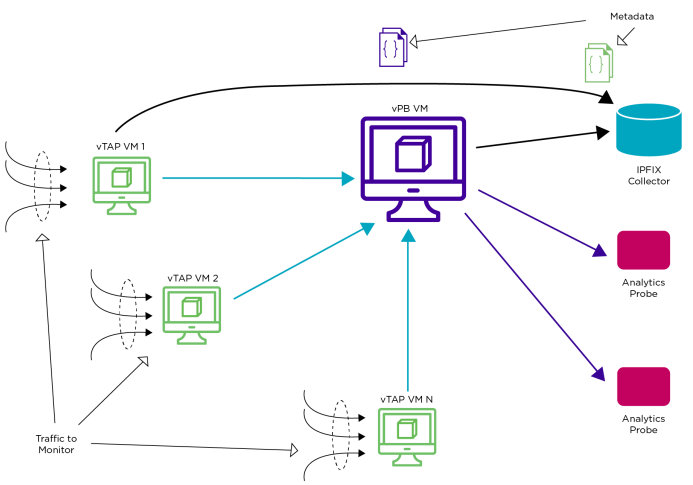

Figure 1: Sample traffic flow between VMs

Session and Packet Mode

The vTAP and vPB can be configured to run in two different modes that can be specified as part of the Interface Configuration.

Session mode:

The session mode identifies each unique traffic flow in the network and maintains this information in its memory during the lifecycle of each flow session. This mode enables the vPB and vTAP to apply policies, such as filtering, header stripping, and packet slicing on a per-flow session basis based on advanced criteria, such as signature or pattern matching in any packet payload.

It enables the following:

- Offloads flow session management from special-purpose probes to vTAP/vPB
- Samples out known application flow sessions using vTAP/vPB
- Forwards application flows based on custom-pattern and signature identification for further analysis
- Extracts and generates metadata for desired flows – all flows, specific flows, sampled-out flows, etc.

Packet Mode:

The packet mode configures the vTAP and vPB to apply policies on a per-packet basis. This is useful in deployments where flow session awareness is not required. This mode enables the vPB and vTAP to apply policies, such as filtering, header stripping, and packet slicing at per-packet granularity based on advanced criteria, such as signature or pattern matching in any packet payload. It enables the following:

- Offloads packet-level policy management from special-purpose probes to the vTAP/vPB
- Forwards and drops packets based on custom-pattern and signature identification for further analysis

Tunnel Management

The vTAP and the vPB can initiate and terminate tunnels.

They support these tunnel initiation types:

- NVGRE
- VxLAN

They supported these tunnel termination types:

- GRE
- ERSPAN Type II
- VxLAN
- IPIP

SMARTMatch

A SMARTMatch policy addresses the requirement for grouping multiple generic packet match rules.

A SMARTMatch rule allows:

- The filtering of tunnels, flows, or packets based on configured n-tuple parameters
- The configuration of a set of actions - forward to an egress destination or drop, Sample Flows, and Export IPFIX metadata on tunnels/flows/packets identified by the n-tuple match

A SMARTMatch rule supports flex-match, which allows detection of specific regex or hex patterns in flows and packets. Optionally, such flows or packets can be dropped or forwarded to a configured egress. A flex match can be pre-defined as a SMARTmatch alias and used within a rule. A rule can include up to four aliases. In the vPB, masking as an action is supported.

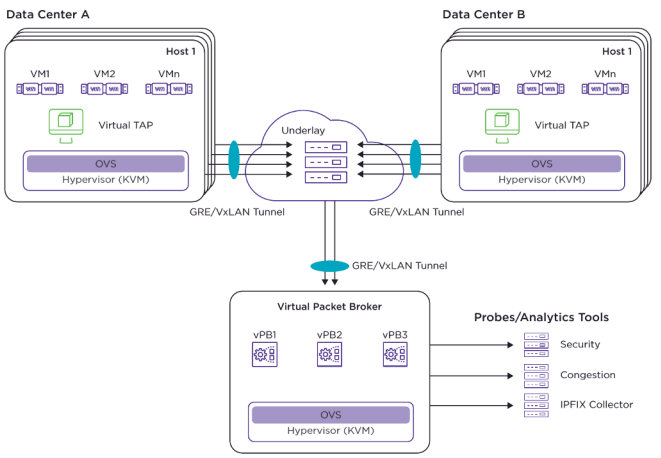

Figure 2: Virtual Packet Broker Deployment Architecture

Virtual Packet Broker and Virtual TAP Specifications

The table below shows the specifications for the qcow2 image. The KVM hypervisor on which the qcow2 image is deployed must meet these requirements.

Extreme vPacket Broker Specifications

Hypervisor	KVM
KVM Hypervisor Requirements	CPU: 2 vCPU RAM: 4GB HDD: 16 GB vNICs: 5 Driver: e1000
Operating System	CentOS release 7.2 Linux kernel version 3.10.0 - 123.el7.x86 64 or higher
Supported	CLI REST SNMP

Sampling

Sampling is a feature that reduces the traffic that flows towards egress. It is only relevant to Session Mode (see above) and can be applied on the Interface or as an action in a SMARTMatch rule. This feature can be used to set the percentage of flows that will be sampled out.

Header Stripping and Packet Slicing

This feature can be configured on the Interface or as an action in a SMARTMatch rule. The Header Stripping feature is used to strip off a specified packet header.

The vTAP and vPB supports Header Stripping for:

- The Packet Slicing feature discards the packet payload from a configured offset before forwarding the packet
- 802.1BR Tag or VN-Tag
- VXLAN
- NVGRE
- MPLS Label
- ERSPAN Type II
- GTP-U
- VLAN

IPFIX Metadata Generation

Both the vTAP and the vPB can export IPFIX metadata for session modes. The underlying transport is UDP or TCP (SCTP is not supported). Metadata is exported for terminated tunnels and flow sessions. A dedicated vNIC (flowexporter) is provided for this purpose. Alternately, the flow exporter or management vNIC (mgmt.) can be used for this feature.

Ordering Information

Part Number	License	Product Description
BR-NVA-VPB-AP1	VIRTUAL BROKER ADV PERPETUAL LICENSE	NVA Virtual Packet Broker (vPB),Advanced feature bundle (also includes Basic features),perpetual License aggregating up to 25 TAP end points
BR-NVA-VPB-BP1	VIRTUAL BROKER BASIC PERPETUAL LICENSE	NVA Virtual Packet Broker (vPB),Basic feature bundle,perpetual License aggregating up to 25 TAP end points
BR-NVA-VTAP-AP125	VIRTUAL TAP ADV 25 PERPETUAL LICENSE	NVA Virtual TAP (vTAP),Advanced feature bundle(Includes Basic Features),perpetual 25 instance License
BR-NVA-VTAP-BP125	VIRTUAL TAP BASIC 25 PERPETUAL LICENSE	NVA Virtual TAP (vTAP),Basic feature bundle,perpetual 25 instance License

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact