cPacket Networks
CVU Family

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: February 10th, 2015

Partner Information

Product Information	
Partner Name	cPacket Networks
Web Site	www.cpacket.com
Product Name	CVU Family
Version & Platform	cVu -400NG
Product Description	cPacket's Traffic Monitoring Switches enable productive data center operations and efficient cloud applications by delivering distributed network visibility and response. Standard capabilities like any-to-any aggregation, replication, and coherent flow balancing are combined with unique capabilities like detailed real-time reports, historical trend analysis, on-the-fly microburst detection, automatic alerts based on customizable triggers, and granular filtering based on complete packet inspection and pattern search at wire speed.

Solution Summary

The cVu-400NG combines the functionality of matrix forwarding with advanced port intelligence. All the device's ports are smart. Beyond flexible forwarding, aggregation, replication, balancing, and filtering, the smart ports extract accurate performance metrics, perform on-the-fly complete packet inspection of every bit in every packet and every flow, filter, time-stamp, and trigger proactive alerts about undesirable traffic conditions. Configurable alerts can identify spikes, bottlenecks, and applications' misbehavior in real-time. Each smart port incorporates cPacket's proprietary Algorithmic Fabric chip, which enables on-the-fly inspection under any traffic conditions including min size, jumbo, and random packet mixes at line-rate.

By combining the cPacket cVu-400NG with RSA Security Analytics, you empower network forensic and packet capture devices by providing customized data streams aggregated from multiple points on the production network. Advantages of such a solution include preventing data loss, collecting more relevant data per packet capture device, de-duplication for tool optimization and masking to address compliance concerns.

RSA Security Analytics Tested Features	
cPacket cVu-400NG	
Flow / Traffic Mapping	Yes
De-duplication	Yes

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the cPacket cVu 400NG with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All cPacket cVu 400NG components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

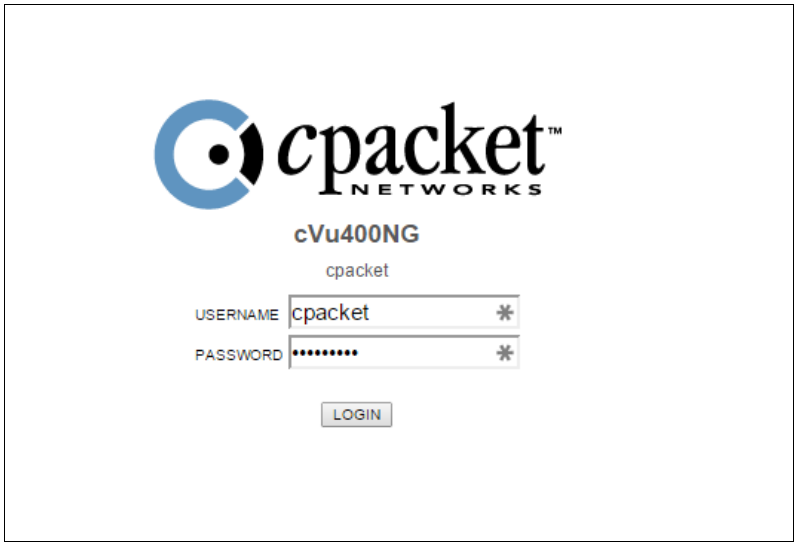
Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the cVu 400NG is properly configured and secured before deploying to a production environment. For more information, please refer to the cVu 400NG documentation or website.

cPacket cVu 400NG Configuration

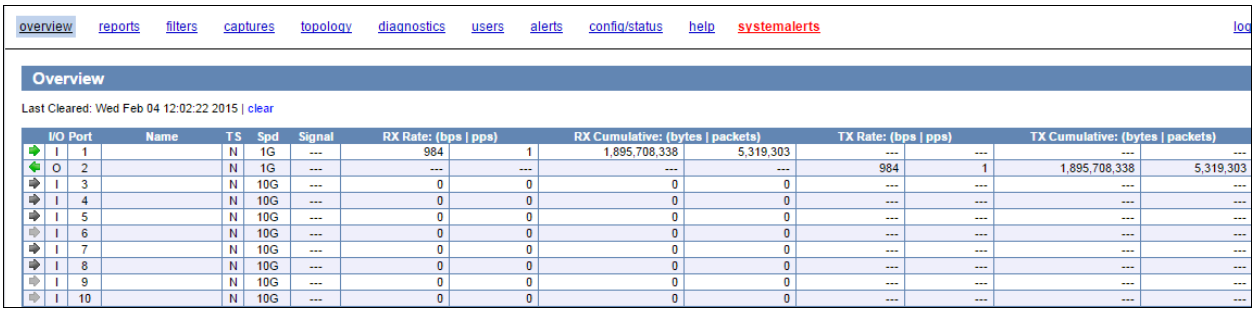
Launching the cVu Management Interface

Following installation, initial configuration and connection of traffic sources and destinations, a few short steps will confirm that the cVu is operating properly (sending and receiving traffic). Operation of the cVu is described in the following sections.

1. Enter **https://address** from a computer that has access to the cVu, where address is the address assigned to the device.



2. Use the default login and password proviced by cPacket, and verify that the reports are now active by selecting the **overview** link.

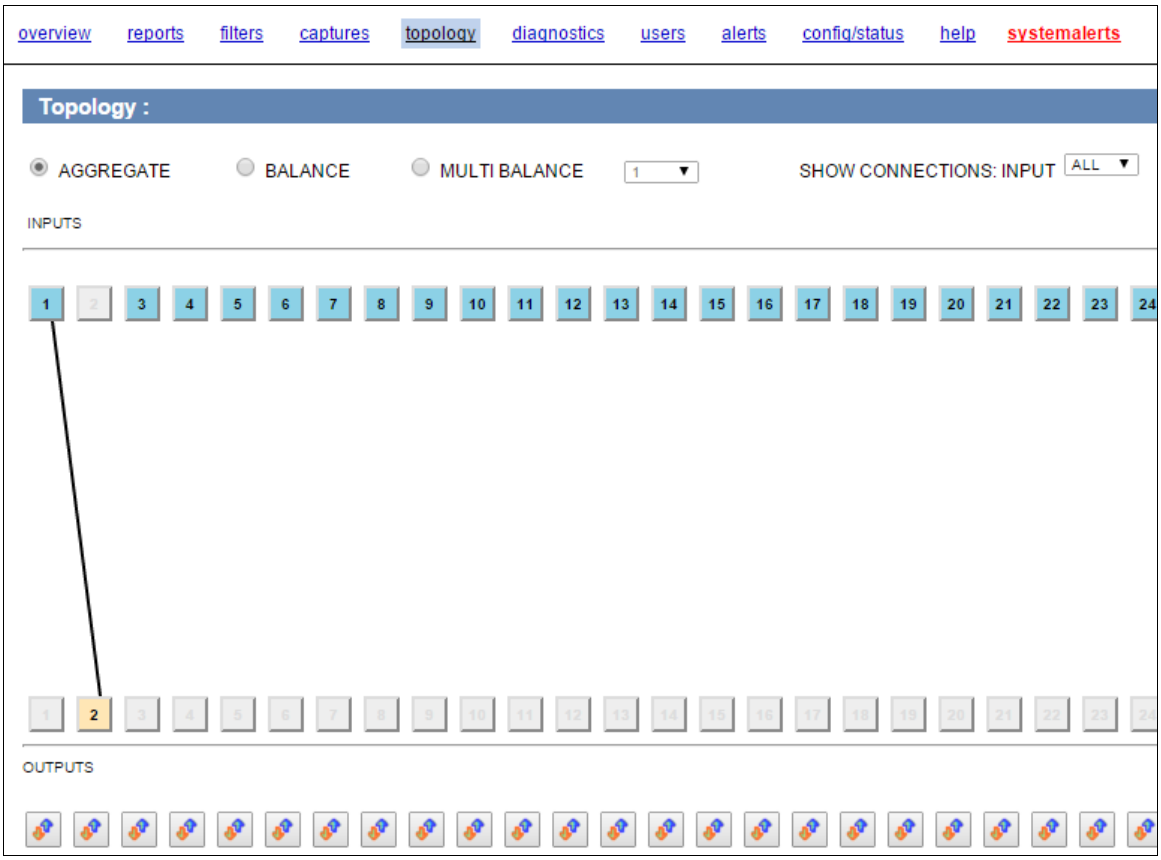


I/O	Port	Name	TS	Spd	Signal	RX Rate: (bps | pps)		RX Cumulative: (bytes | packets)		TX Rate: (bps | pps)		TX Cumulative: (bytes | packets)	
I	1		N	1G	---	984	1	1,895,708,338	5,319,303	---	---	---	---
O	2		N	1G	---	---	---	---	---	984	1	1,895,708,338	5,319,303
I	3		N	10G	---	0	0	0	0	---	---	---	---
I	4		N	10G	---	0	0	0	0	---	---	---	---
I	5		N	10G	---	0	0	0	0	---	---	---	---
I	6		N	10G	---	0	0	0	0	---	---	---	---
I	7		N	10G	---	0	0	0	0	---	---	---	---
I	8		N	10G	---	0	0	0	0	---	---	---	---
I	9		N	10G	---	0	0	0	0	---	---	---	---
I	10		N	10G	---	0	0	0	0	---	---	---	---

Configuring Port Connections

The topology page is where admin users define connectivity and functionality of the cVu 400NG's ports. Connectivity between the ports as well as functionality (aggregation/duplication and balancing destinations are defined here. In addition, port parameters such as speed (10G or 1G), direction (input or output) and timestamp insertion are configured. Ports can also be assigned descriptive names which allow easy identification of traffic sources and destinations through the filter and reports pages.

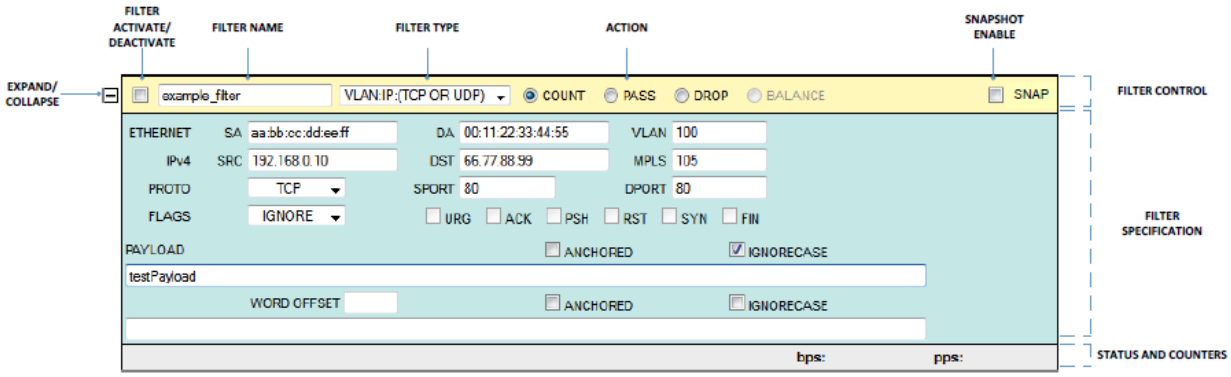
The figure below shows a simple In/Out connection where the output could be directed to an RSA Security Analytics Log Decoder or Packet Decoder:



Configuring Traffic Filtering

The cVu features extensive packet filtering capabilities derived from the use of cPacket's Complete Packet Inspection chip. The filters allow inspection of every bit in every packet, including header fields and payload, down to the last byte. Header field constraints may include equality, inequality, and arbitrary range checks. Payload pattern search may include anchored and non-anchored strings with wildcards anywhere in the packet.

Filters can be applied at either the input, allowing, for example, specification of traffic to be load balanced, or at output, enabling full flexibility for aggregating or balancing traffic. Each smart port supports definition of up to 24 complex filters.



For detailed instructions on creating filters and further filter configuration, consult the ***cVu 400NG Traffic Monitoring Switch User Guide***.

Certification Checklist for RSA Security Analytics

Date Tested: February 2nd, 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4.0	Virtual Appliance
cVu 400NG	14.4.2.sp1	Hardware Appliance

Security Analytics Test Cases	Result
Packet Loss	
Syslog TCP data consumed by the SA Log Decoder	✓
Syslog UDP data consumed by the SA Log Decoder	✓
Various packet data consumed by the SA Packet Decoder	✓
De-duplication	
Replaying data files to the SA Packet Decoder	✓
Traffic Mapping	
Mapping network service ports to dedicated ports	✓
Performance	
SA Log Decoder minimal EPS performance	✓
SA Packet Decoder minimal EPS performance	✓

JEC

✓ = Pass ✗ = Fail N/A = Non-Available Function