TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Aparna Systems, Inc

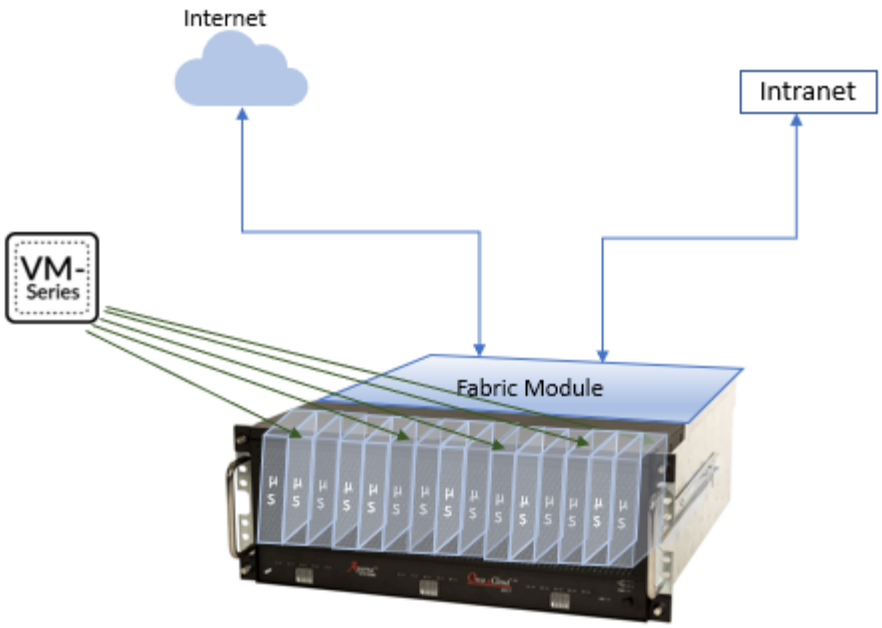
Contents

Partner Information

Partner information	
Date	03/22/2019
Partner Name	Aparna Systems
Web Site	www.aparnasystems.com
Product Name	Aparna Systems µCloud 4015
Partner Contact	Sam Mathan, CEO, 47800 Westinghouse Drive, Fremont, CA 94539
Support Contact	support@aparnasystems.com
Partner Product for Integration	Aparna Systems µCloud 4015
Product Description	Ultra-Converged Edge Cloud

Use case: Integration with Palo Alto Networks VM-Series Firewalls

The Aparna µCloud ™4015 system integrates two Top of Rack (ToR) switches and up to 15, sixteen core Xeon µServers in a self-contained 4U chassis. The ToR switches provide network connection for the µServers, layer-4 load balancing functionality and up to 640Gbps of external connectivity.



The Aparna µCloud ™ 4015 systems can run one instance of the Palo Alto Networks VM-700 VM-Series NGFW in each µServer in a scale-out configuration with layer-4 load balancing across all the virtual firewalls. A fully populated µCloud ™ 4015 will support an aggregate throughput of 75 Gbps at a throughput of 5Gbps per µServer/VM-700

Palo Alto Networks Products for Integration

Panorama can be used to manage the VM-Series firewalls in a scale-out cluster via a dedicated virtual management network. The VM-Series can also communicate with Palo Alto Networks' cloud-based services such as logging, GlobalProtect cloud services for mobile users and Wildfire for malware analysis.

The VM-Series instances have not been modified in any way and will continue operate as they do on any VM series installation. Connectivity to Palo Alto Networks cloud services was verified using the licensing and update functions of the VM-700.

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	Aparna Systems Versions Tested
Aperture			
AutoFocus			
GlobalProtect			
GlobalProtect Cloud Service			
Cortex Data Lake			
MineMeld			
NGFW			
Panorama			
RedLock			
Traps			
VM-Series	VM-700 Tested	PAN-OS 9.0 and 8.1.5	µCloud ™ 4015
WildFire			
Other			

Integration Benefits

The µServers and hypervisors are preconfigured for the VM-700 for ease of deployment.

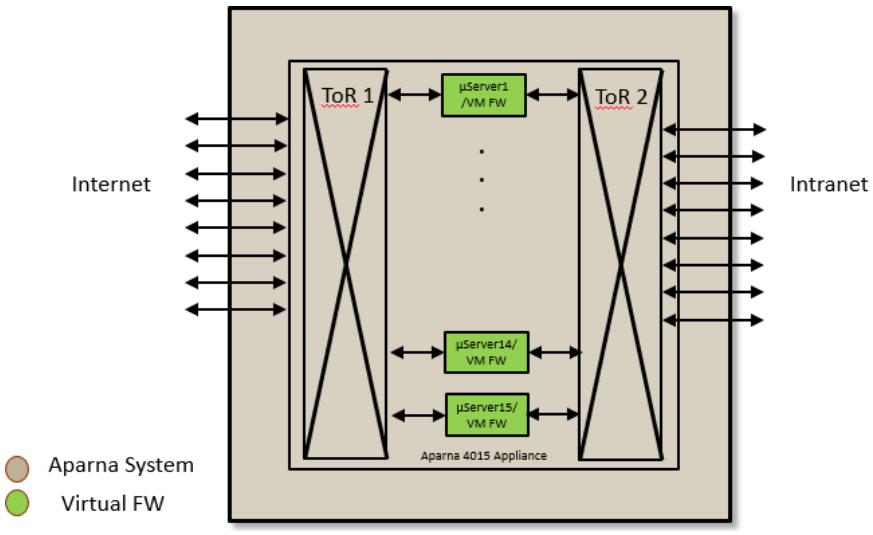
The ToRs embedded load balancing functionality is included and is shipped preconfigured for a scale-out deployment of VM-700.

The customer can incrementally add or remove the firewall capacity by adding or removing µServers with VM-700 to/from a 4015 in a seamless manner with minimal disruption to the running system.

Integration Diagram

The Aparna µCloud ™ 4015 system is a hardware-based platform expressly designed for running layer 4 through 7 applications in a Scale-Out Cluster architecture.

The µCloud ™ 4015 does not exchange information with the VM-Series instances.



Before you begin

- Dependencies needed before beginning
  - VM-Series Authorization Codes – one VM-Series instance per µServer
    - *Example: 15 µServers = 15 VM-Series Auth Codes (model VM-700)*
  - Physical network connectivity to connect to the customers network.
    - Network connections can be either 10GbE or 40GbE
- Requirements for successful integration
  - PAN-OS for VM-Series KVM base image (PAN-OS 9.0 or 8.1.2) from the Palo Alto Networks Support Portal – https://support.paloaltonetworks.com

- Dependencies OS, Version, Panorama, etc.
  Consult the Palo Alto Networks documentation for up-to-date Requirements and Prerequisites
  - Ensure each µServer is running:
    - Ubuntu Server 16.04 LTS
    - QEMU-KVM 2.5.0
    - libvirt 1.3.1
- API key requirements
  - Not applicable

VM-Series on KVM – Requirements and Prerequisites – PAN-OS 9.0
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/vm-series-on-kvm-requirements-and-prerequisites.html

Partner Product Configuration

- On each of the µServers:
  - Install Ubuntu Server 16.04 LTS as documented in the Operations Manual of Aparna 4015
  - Update "ixgbe" driver to version 5.5.1 from Intel website
    - https://downloadcenter.intel.com/download/28387
  - Enable SR-IOV and optimize KVM network configuration for performance as provided in the VM-Series Deployment Guide – see Performance Tuning of the VM-Series for KVM
    - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/performance-tuning-of-the-vm-series-for-kvm.html#*
  - Reboot the µServer

- On both Fabric Modules:

  - Login to each of the Fabric Modules as given in the Operations Manual of Aparna 4015 and enter the CLI mode of the Fabric Module with "imish" command. Refer to the Operations Manual for details.
  - From Fabric CLI, configure three sets of ports for each µServer as router ports from the default switch ports – a management port, an untrusted port (on either of the Fabric Modules) on one of the SR-IOV ports and a trusted port (on the other Fabric Module) on another SR-IOV port and assign IP addresses to these ports.
  - After setting up the 3 ports, save the configuration by writing to the NVRAM
  - Configure the load balancing with "load-balance" command from the OcNOS CLI interface
  - Configure port rate-limiting to 5Gbps on all firewall ports

- Aparna µCloud 4015 is ready for installation and provisioning of VM-Series

Palo Alto Networks Configuration

- *RECOMMENDED* – follow the configuration steps below and ensure the management interface is reachable and traffic flows through the VM-Series instance on one µServer – then repeat the process for the remaining µServers

- Download PAN-OS for VM-Series KVM base image (PAN-OS 9.0 or 8.1.2) from the Palo Alto Networks Support Portal – https://support.paloaltonetworks.com

- Transfer the disk-image file (QCOW2) to the µServer
- Refer to the VM-Series Deployment Guide for detailed step-by-step instructions
- Install the VM-Series Firewall on KVM
    - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-on-kvm.html*
- Provision the VM-Series instance
- Define Memory and CPU settings
- VM-Series System Requirements – VM-700 Model (per instance)
    - vCPUs – 16
    - Memory – 56 GB
    - Storage – 60 GB
    - *16x vCPUs are internally allocated as follows (no intervention required)*
        - *4x vCPUs – Management Plane*
        - *12x vCPUs – Dataplane*
- Configure the Virtual Disk settings – browse to the location of the QCOW2 disk-image
- Define three virtual network interfaces:
    - Management
    - Internal – (trust)
    - External – (untrust)
- Configure each of these ports for SR-IOV as “Network Source” and “Passthrough” as the “Source Mode”. Select “virtio” as the “Device model”
- Apply and Finish to finalize the settings
- Update the “qemu” configuration file (vm-name-700.xml) of each of the VMs created for CPU pinning as recommended by the installation guide of PA-700 VM
    - Enable SR-IOV on KVM
        - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/performance-tuning-of-the-vm-series-for-kvm/enable-sr-iov-on-kvm.html#*
    - Enable Multi-Queue Support for NICs on KVM
        - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/performance-tuning-of-the-vm-series-for-kvm/enable-multi-queue-support-for-nics-on-kvm.html#*
    - Isolate CPU Resources in NUMA Node on KVM
        - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/performance-tuning-of-the-vm-series-for-kvm/isolate-cpu-resources-in-a-numa-node-on-kvm.html*
- Reboot the µServer
- Set the firewall management IP address – Perform Initial Configuration of the VM-Series Firewall on KVM
- *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-using-virt-manager/perform-initial-configuration-on-the-vm-series-on-kvm.html#*
- Follow the instructions under License the VM-Series Firewall to activate the Authorization Code and import the license key
    - *https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/license-the-vm-series-firewall.html*
- Consider Bootstrapping the VM-Series image as it allows you to create a repeatable streamlined process for deploying additional VM-Series instances. You can either bootstrap the firewall with basic initial configuration, or you can bootstrap the complete configuration so that the firewall is fully

configured on boot up.

- Repeat the process for each µServers

Reference

- Bootstrap the VM-Series Firewall on KVM (optional)
- https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-on-kvm.html

- VM-Series Deployment Guide – PAN-OS 9.0
- https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment.html

Troubleshooting

- Common troubleshooting steps:
  - Management port is not accessible – check the configuration on the Fabric Module to make sure the IP address is properly set as given in the instructions.
  - Traffic does not flow through the firewall – using a web browser, connect to the VM-Series management interface, then switch to the Monitor tab view the Traffic Log – check the logs to see which policy is blocking traffic.
- Contact information for support
  - Email - support@aparnasystems.com
- Aparna Systems is a TSA Net member
- Helpful resources:
  - Document - Aparna 4015 Hardware Installation Manual
  - Document - Aparna 4015 Chassis Operating Manual

Technical Details

- *Logs being used*
  - As applicable to Palo Alto Networks VM-Series NGFW
- *Additional technical details*
  - On each µServer of 4015
    - Install of Ubuntu 16.04 LTS (Server) OS on each µServer, install KVM and add support for SR-IOV
    - Install Palo Alto Networks VM-Series KVM Base Image and configure to use SR-IOV interfaces
  - On each Fabric Module of 4015
    - Configure the network interfaces for routing and add static routes.
    - Apply µServer load balancing configuration.
  - Configure external switch interface settings to match with the Fabric Module configuration