WHITEPAPER

128 TECHNOLOGY

SECURE VECTOR ROUTING FOR CONTAINERS

CONTENTS

Revision History **1**

Introduction **2**

SVR for Containers **3**

Performance 3

Security 4

Fairness 4

Visibility 4

Load Balancing 4

128T Container Networking **4**

Summary **6**

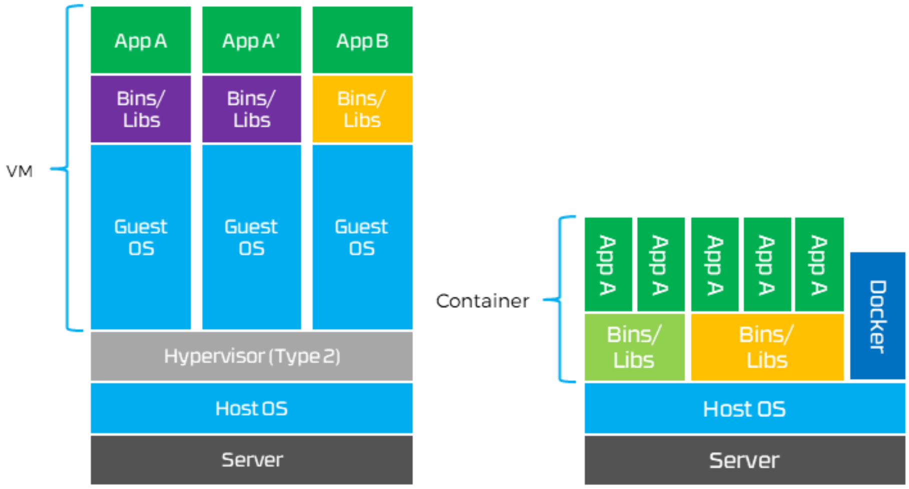
REVISION HISTORY

Version	Author	Description	Date
Draft 01	Ritesh Mukherjee	Initial Draft	September 18, 2017
Draft 02	Francisco Mendez	Container Networking	September 27, 2017
Draft 03	Patrick MeLampy	Security Section	September 29, 2017

INTRODUCTION

Container technology is analogous to shipping containers in freight transport. Intermodal containers can be used across different modes of transport – from ship to rail to truck – without unloading and reloading their cargo. These containers are a means to bundle cargo and goods into larger, unitized loads, that can be easily handled, moved, and stacked. Application containers take the same approach with software.

A container consists of an entire runtime environment: an application, plus all its dependencies, libraries, and configuration files needed to run it, bundled into one package. By containerizing the application platform and its dependencies, differences in Operating System (OS) distributions and underlying infrastructure are abstracted away.



With virtualization technology, the package that can be passed around is a virtual machine (VM), and it includes an entire operating system as well as the application. A physical server running three VMs would have a hypervisor and three separate operating systems running on top of it. By contrast a server running three containerized applications runs a single operating system, and each container shares the operating system kernel with the other containers. Shared parts of the operating system are read only, while each container has its own mount (i.e., a way to access the container) for writing. Some benefits of using containers include:

- Containers are lightweight and use far fewer resources than VMs. A single server can host far more containers than VMs.
- VMs take several minutes to boot up their OS while containerized applications can be started almost instantly. This makes them easy to instantiate when required and free up resources when not required.
- Containers allow for microservices. Applications can be split into modules on different containers instead of having an entire complex application inside a single container.

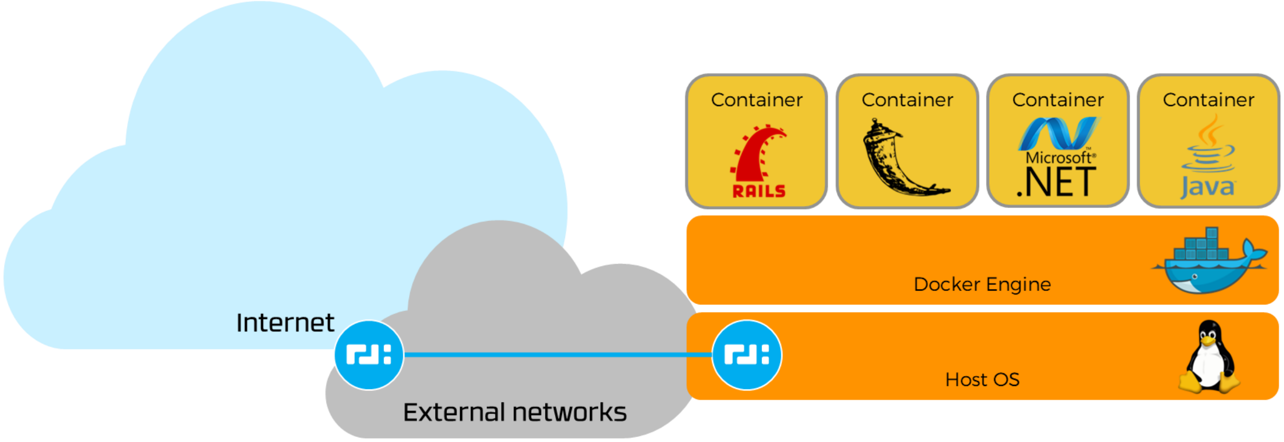
Containers reside on a host or a virtual host. They have complex networking demands to provide communication to other containers and to the outside world. Containers require a fast response infrastructure to provide a networking endpoint. They require fairness so one rogue container cannot overwhelm the pipe. They require load-balanced inbound connections. They require policies to enforce security. While containers themselves have an inherent level of isolation, the large quantity of containers and network connections to other resources can increase the area of attack.

Traditional virtual infrastructure solutions offer a Layer 2 (L2) solution configuring multiple workloads. This requires several layers of virtual LANs, bridging, and tunneling to make L2 networking work across multiple physical hosts. This solution does not scale to thousands of workloads, encapsulation causes obscurity, high availability and load balancing are difficult, requires a lot of configuration, and is difficult to troubleshoot.

SVR FOR CONTAINERS

128 Technology provides a Layer 3 (L3) solution for interconnecting VMs or Containers along with the benefits of Secure Vector Routing (SVR). This solution benefits from leveraging existing network infrastructure to manage containers. The L3 solution uses routing protocols to provide connectivity to containers. It is easier to interoperate with existing data center infrastructure including connecting containers, VMs and bare metal servers. L3 networking offers unprecedented scale. It provides complete isolation and security. The 128T router connects each workload directly to the network infrastructure.

SVR brings advanced networking to containers that go beyond traditional solutions available today.



PERFORMANCE

There are no overlays, tunnels, or VxLANs. The solution scales to millions of workloads without any overhead. Traditional solutions require multiple encapsulations and de-capsulations. This impacts scale and performance. Increase in packet sizes can also lead to packet fragmentation and associated issues. The 128T solution uses standardized routing protocols in combination with service and tenant definitions as the control plane and can handle millions of distinct routes. The solution can integrate with existing networking infrastructure in the data center and provide cloud connectivity.

SECURITY

SVR enables 128T routers to connect workloads securely without VLAN or VxLAN provisioning. The L2 broadcast domain can be eliminated. It supports the configuration of fine-grained connectivity policies for each workload that includes directionality (client-to-server), bandwidth limits, and encryption. 128T calls this Zero-Trust Security. This provides fine-grained separation of east and west traffic from all other traffic securing user information. Access policies are rendered into rules that are automatically applied between each and every workload and the physical network fabric in both ingress and egress directions. This provides for maximum possible network security and isolation without the inefficiency inherent in moving packets between overlay L2 segments via separate and distinct firewall functions in the cloud.

FAIRNESS

Network administrators can prevent one workload from overwhelming other workloads by policy defined policing of traffic on a session-by-session basis. These policies can be applied based to tenants and services enabling the ability to deliver fairness between containers sharing the same host resources.

VISIBILITY

SVR enables full traffic visibility between containers across both virtual and physical networks. Visibility to the containers helps application troubleshooting on the network. Insights into container health based on network traffic enables troubleshooting and planning. Rapid application and micro service deployment is now possible based on network traffic loads.

LOAD BALANCING

Elastic load balancing to different containers is an inherent capability of the 128T router. The 128T router can make real-time decisions based on the load on the different workloads.

128T CONTAINER NETWORKING

The 128T router as a software-based application would be deployed at the OS Linux level of each node of the Container cluster, along with the Container platform engine such as the Docker Engine.

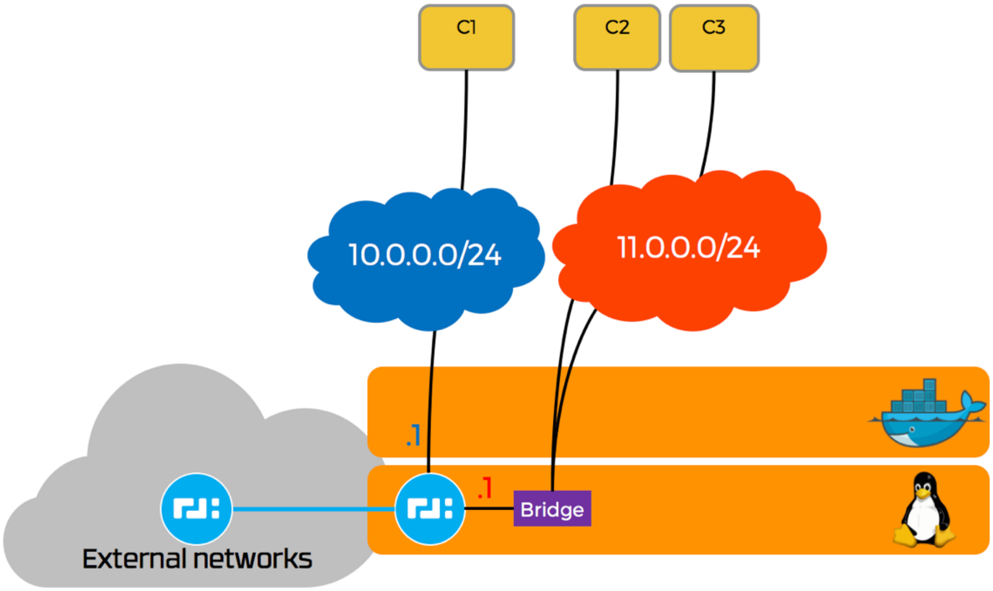
One of the many strengths of 128T routers is its capability of hyper segmenting a network. The ability of segmenting the network to smaller segments brings security and granular control into containerized applications.

128T routers offer two approaches to create virtual networks to which a Container can attach to.

Some containers that are part of an application require the highest level of security and isolation even among themselves. For those containers, the most well-suited networking model is a host interface based virtual network. 128T routers can create a virtual host interface that will effectively isolate a container from communicating with other containers running on the cluster where the 128T router is hosted. The container and the 128T router would only share the same L2 broadcast domain, where the 128T router would assume the role of L3 gateway for such broadcast. In this networking model, no other container would be part of that broadcast domain achieving the highest degree of isolation, segmentation, and performance.

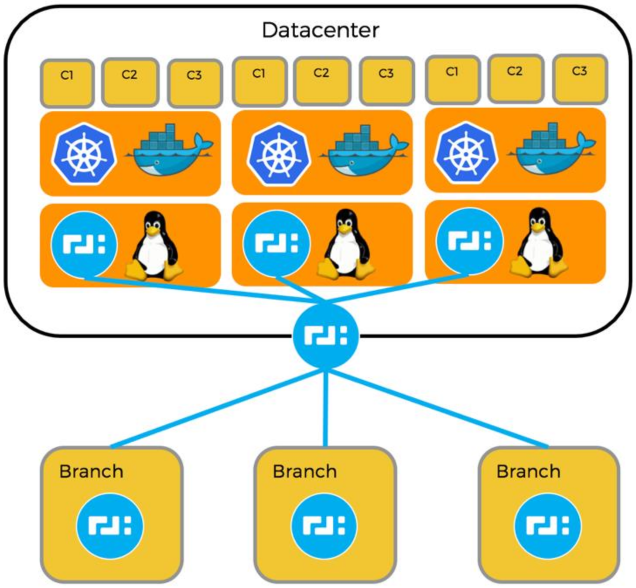
Other applications where containers do not require the highest level of isolation, a bridged networking model is an ideal fit. The virtual network created by the 128T router will allow multiple containers to be attached to the same L2 broadcast domain. This model will allow Containers to communicate freely among themselves, although an equivalent level of segmentation as in host based networking model can be achieved as well by setting filtering policies. The 128T router would assume the role of L3 gateway for this network, where granular control can be enforced when containers are communicating to other clusters or external networks.

The following figure depicts a 128T router with containers attached as a host based virtual network in the blue colored network and a bridge virtual network in the red colored network.



Containers are more often than not deployed, scaled and managed using an orchestration tool such as Kubernetes, Mesosphere, among few others. Kubernetes outlines several networking models based on requirements and makes few assumptions with regards to networking. Kubernetes aims to solve challenges seen in Cloud scenarios such as the portability difficulties of workloads in hybrid cloud scenarios, VMs to containers transition, deployments at big scale, etc. In order to achieve these functions, Kubernetes embeds network functions such as load balancing, creating logical abstractions to ease container availability, etc. However, Kubernetes relies on the implementation of networking functions by utilizing traditional and rudimentary Linux based networking technologies and/or third-party applications.

Once a container is attached to a 128T virtual network all the network functions offered by 128T routers become available such as hyper-segmentation, QoS, access control enforcement, firewalling, load balancing, encryption and authentication, analytics for greater visibility, etc. 128 Technology offers a much broader variety of network functions, simplifying the network at its core, making networks application aware and multi-tenant. When distinct network boundaries have to be traversed, as depicted in the figure below, from the branch to the datacenter, the source and tenant of the traffic is always known by each 128T router across the entire 128T network, and as such, context of the traffic is maintained at all times, and network policies can be enforced globally.



For additional benefits of 128T routers please refer to the 128 Technology Page.

SUMMARY

SVR provides a highly scalable networking and segmentation solution for containers. The solution does not require any encapsulation or overlays resulting in a high-performance solution. 128T routers also enable granular policy and segmentation rules that provide superior isolation and security. The model allows for access and service policies to be easily updated making it an agile solution. The 128T solution based on L3 routing provides a simple, resilient, and secure method for container networking.

128 TECHNOLOGY

www.128technology.com | info@128technology.com