Secure Systems Group, Aalto University

Songlin Jiang

Virtual Network Systems among Containers

- We tried to implement a Virtual Network System using **Docker containers** instead of **VMs**
- **Containers** are much more **lightweight** than **VMs**, thus consuming **fewer resources**

Introduction

- We commonly use VMs to build and test **Virtual Network System** configurations
- **VMs** have many **drawbacks** that can get **overcome** by **Docker containers**
- However, no one has tried to implement a **Virtual Network System** using **Docker**

Table 1: Comparison between VMs and Docker containers

Items	Vagrant + VirtualBox	Docker Compose
Resource	Heavy	Lightweight
Kernel	Own	Shared
Scalability	Hard	Easy
M1/M2 Support	Limited	Fully
Image Hub	Unavailable	Docker Hub
Seamless	No	Yes

Docker Networking System

- **Docker** uses **pluggable** network subsystem

Table 2: Comparison between applicable Docker network plugins

Items	bridge	IPVLAN	MACVLAN
Resource	High	Low	Lowest
MAC	Different	Same	Different
Migration	No	No	Yes

- **NET_ADMIN** capability in Linux allows it to **manage** its own network inside a **container**
- **IPv6** is also **supported** in **Docker**

Case Study: VPN

- Experiment using **strongSwan** (**IPsec**)

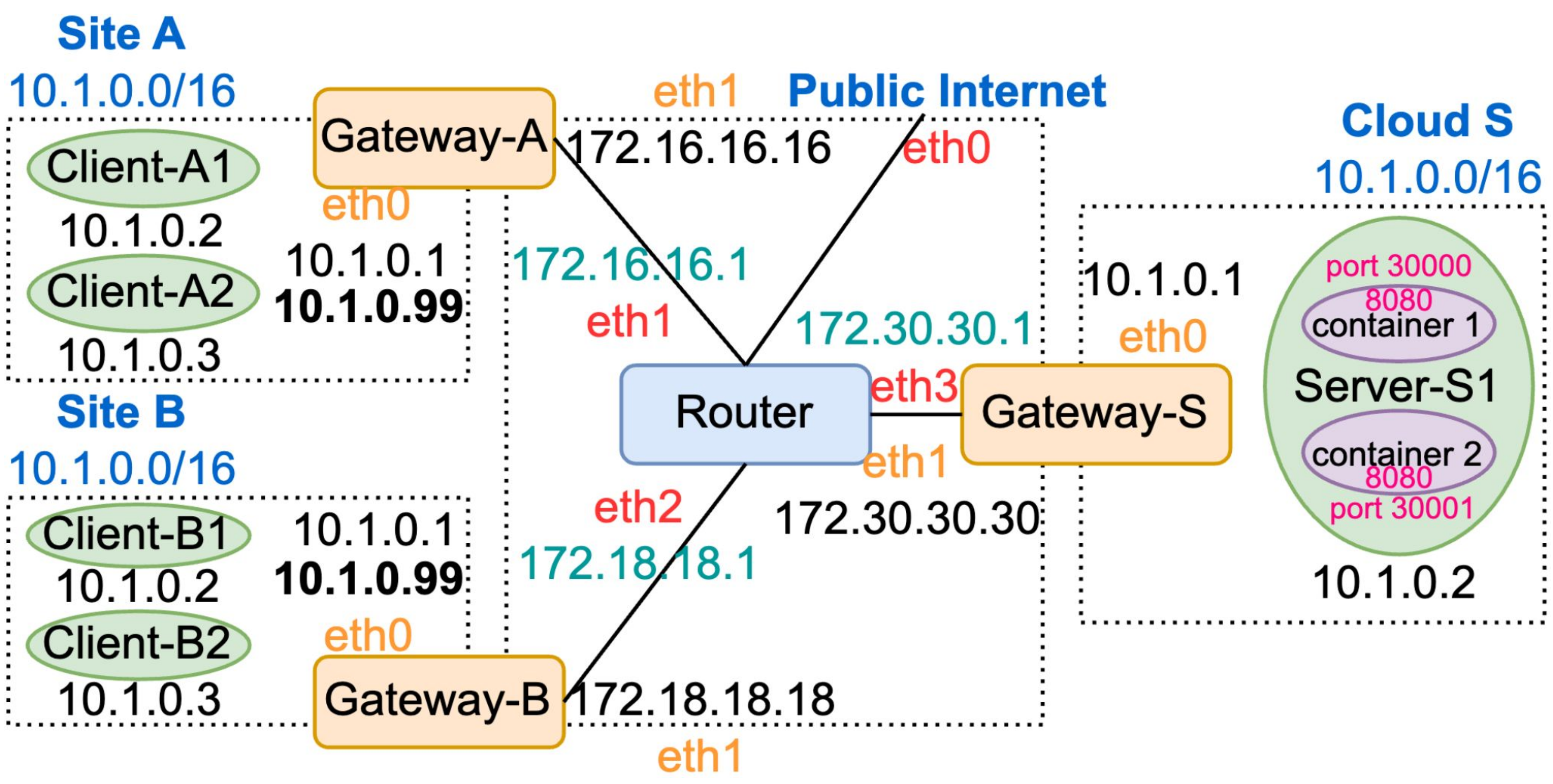

Figure 1: Example: Host-to-Host VPN Topology

Evaluation Result

Table 3: Performance Test Result in Average

Items	Boot Time	Memory
Docker Compose	75 s	278 MB
Vagrant + VirtualBox	689 s	4.5 GB

- The **container-based** solution **reduces**:
  1. **Fresh boot time** by nearly **90%**
  2. **Memory usage** by nearly **94%**
- Container networks are **isolated** from the host
- The Docker networking model **disallows** us to
  1. **Assign** the **overlapped IP address** ranges, even for network interfaces that won't get directly connected
  2. **Assign IP addresses ending in ".1**, as these addresses are reserved by Docker for gateways or routers
- Configure the IP addresses **manually inside containers** to **bypass** these **limitations**.

Aalto University

Scan to get Source Code