Zero Trust Security Approach To Server Application

Containerized IPS

Chaitanya Lala

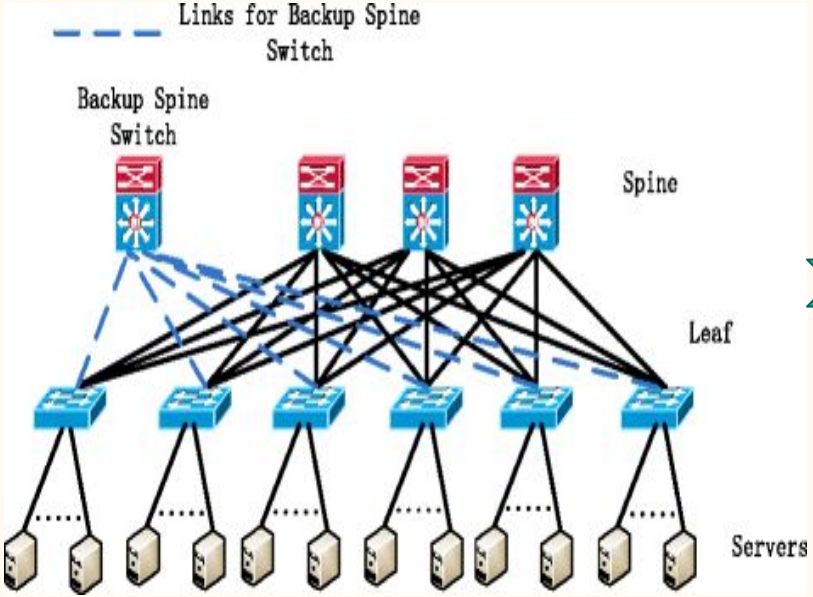
Partha S Ghosh

chaitanya.lala@gmail.com & psglinux@gmail.com | SJSU | CMPE-209-Network Security

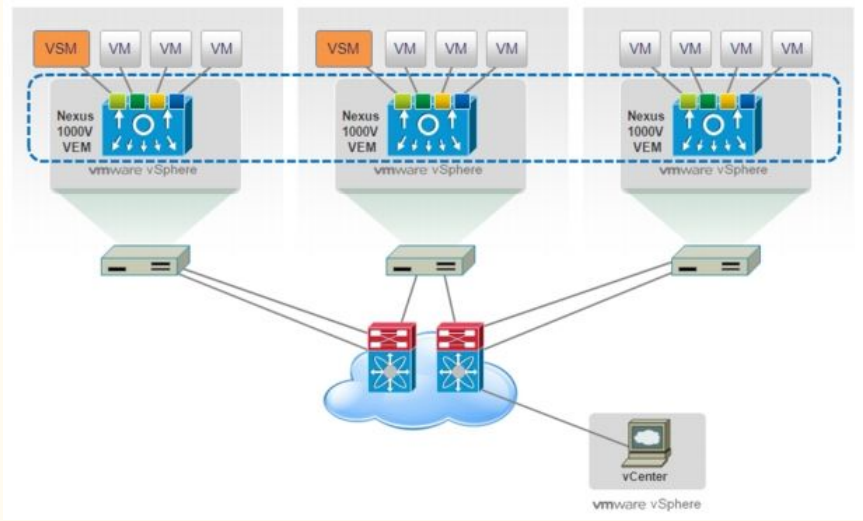
Agenda

- Why Containerized Security ?
- Research and Experiments
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

Why do you care about containerized Security



standalone servers



virtualized servers

New Horizon in Server and Application

New Features

- On Demand VM creation
- VM Mobility
- Multitenancy on the Same Physical Servers
- Rapid deployment velocity
- Deploy Applications at scale
- Network is Virtualized
- Containers

New Problems

- Network cannot take care of Security effectively
- How can traffic for VM be sanitized ?
- How do we secure Applications ?
- How do we Apply Security Policy ?

Solution

- Secure Applications in the VM
- Containers For Security
- Merge Container and Strong Open Source Solution to solve the security problems

Agenda

- Why Containerized Security ?
- Research and Planning
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

Research and Planning

1 Defining Scope : Ubuntu as Host VM, Containers, Suricata/Snort

2 Research : Linux Namespace (Prototype), Docker Networking, Snort/Suricata

3 Plan: Divide Development phases, Automation, Integration, Presentation etc

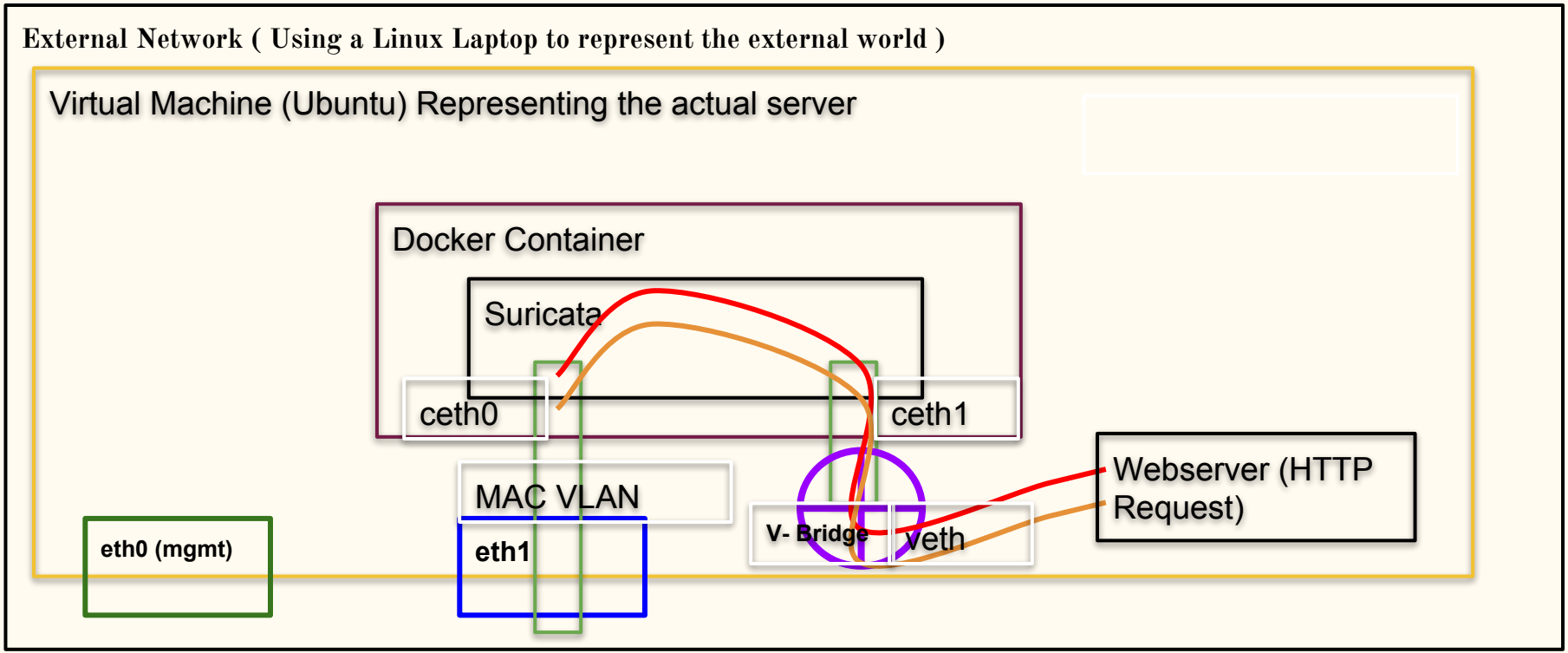
4 Development : Incremental Build and Test

5 Testing

Agenda

- Why Containerized Security ?
- Research and Experiments
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

System Arch and Packet Flow



Agenda

- Why Containerized Security ?
- Research and Experiments
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

%Done ?

- Docker Container on demand on a VM
- Create the docker, VM , Bridge Network topology
- Suricata Deployed in Container
- Able to achieve Filtering through Suricata
- We Observe a performance of 20Gbps through docker
- Ability to spin a Web server
- Filtering of HTTP traffic to Web server
- Test Infrastructure upon Deployment

```
https://github.com/chaitanyalala/cmpe-209-project
```

Agenda

- Why Containerized Security ?
- Research and Experiments
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

- Add IDS support (Not only IPS)
- Make rule generation dynamically controlled by a management controller
- Increase I/O throughput by integrating zero-copy technologies for packet rx/tx
- Automatically update rules
- Employ Low level DOS mitigation techniques provided by the OS

Agenda

- Why Containerized Security ?
- Research and Experiments
- Product Components and Packet Flow
- Where Are We ?
- Future Roadmap
- Conclusion

1.Collaboration
2. Evaluate Potential Customers for the for the product
3. Look for Features that customers would need.

Q & A

Thanks!