Identity Management, Authentication, and Access Control with VyOS

Paolo Cruschelli
Enterprise Cloud Architect

Creator: Daniil Baturin, Yuriy Andamasov, Santiago Blanquet Bru De Sala

VyOS is an open source network operating system based on Debian.

VyOS is built upon the latest community version of Vyatta Core edition (Brocade).

VyOS code is maintained by Sentrium S.L.

Features:

- Routing (BGP, OSPF, MPLS, Multicast, policy based routing)
- Security (Stateful L4 Firewall)
- VPN (IPSEC, GRE, OPEN-VPN)

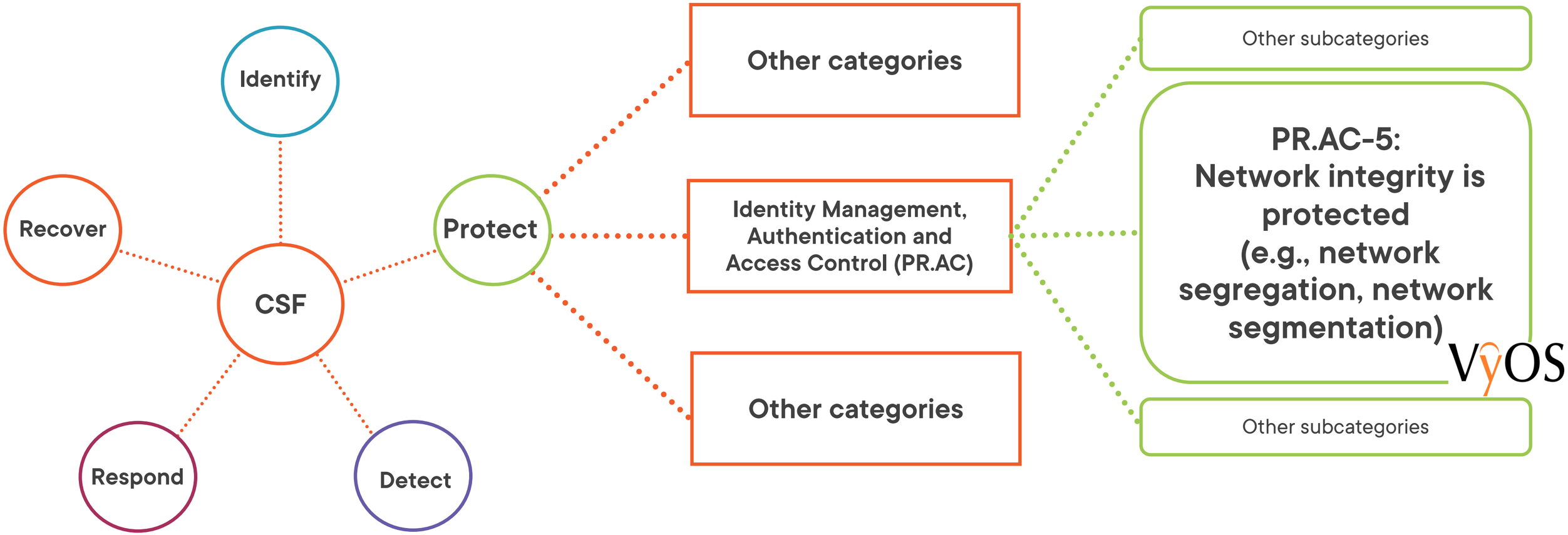
How to get it:

- Current LTS version Release 1.3 (Equuleus) is a licensed product
- Built from code
- Download full feature Rolling Release

Deployment models : bare metal, virtualized, cloud (AWS, Azure, Google cloud)

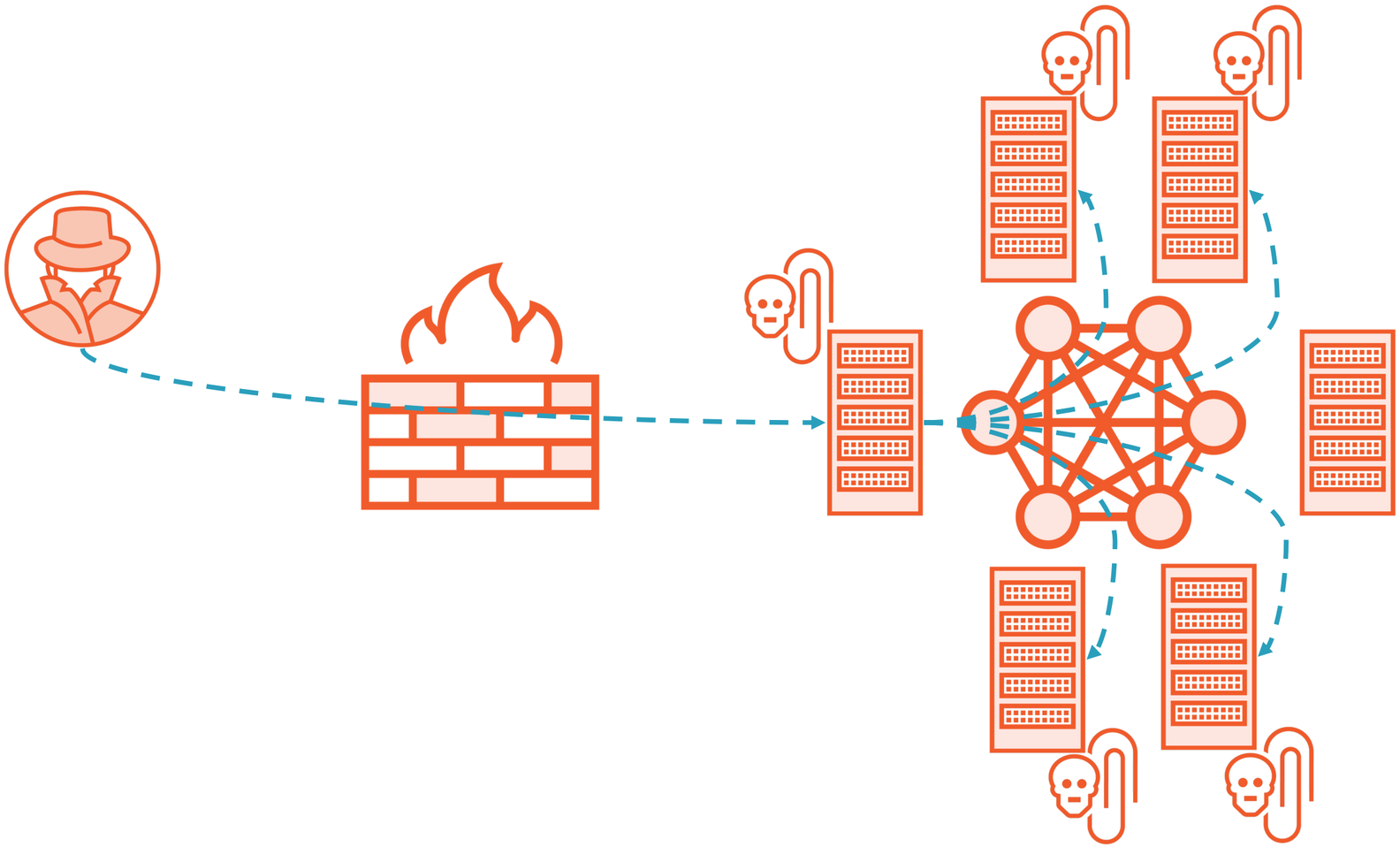
https://vyos.io/

NIST Cybersecurity Framework



VyOS

Lateral Movement Attack Explanation



Network Segmentation and Segregation

Segmentation

Partitioning a network into smaller networks

Reduce the exposed surface

VLAN, VRF, VPN

Segregation

Enforcing a ruleset for controlling the communications between hosts and services.

Implement security policy

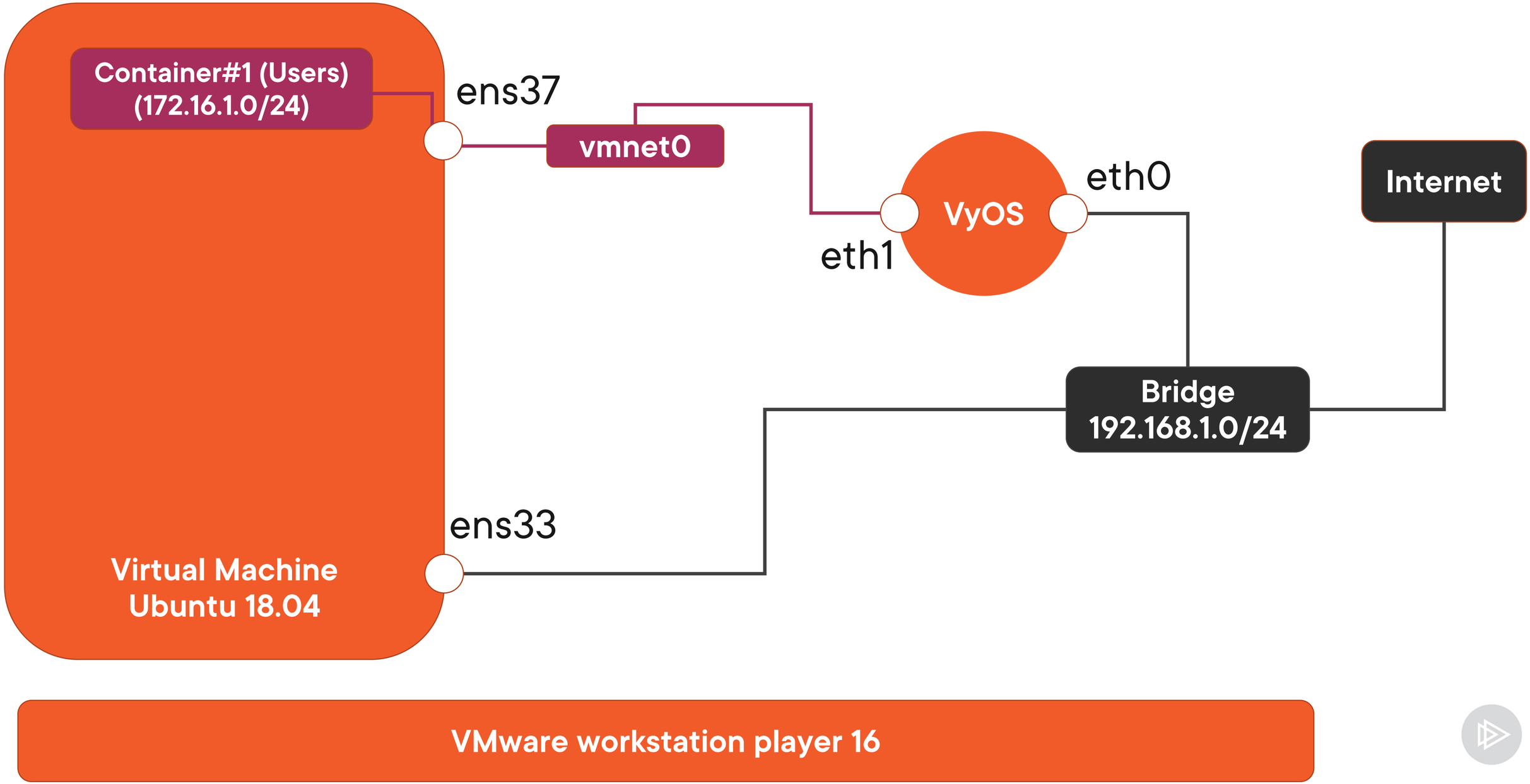
Firewall, ACL

Demo

In this demo you will learn the following:

- **Download and install VyOS router**
- **Basic configuration for remote management**
- **Basic routing and NAT commands**

VyOS Installation and Basic Configuration



Demo

In this demo you will learn:

- **How to configure VyOS API to enable programmatic access**
- **Basic VyOS API call with simple python scripts**

VyOS configuration

Legacy CLI-based approach

Manual configuration

Error prone

All Devices must be configured separately

Time consuming

API based approach

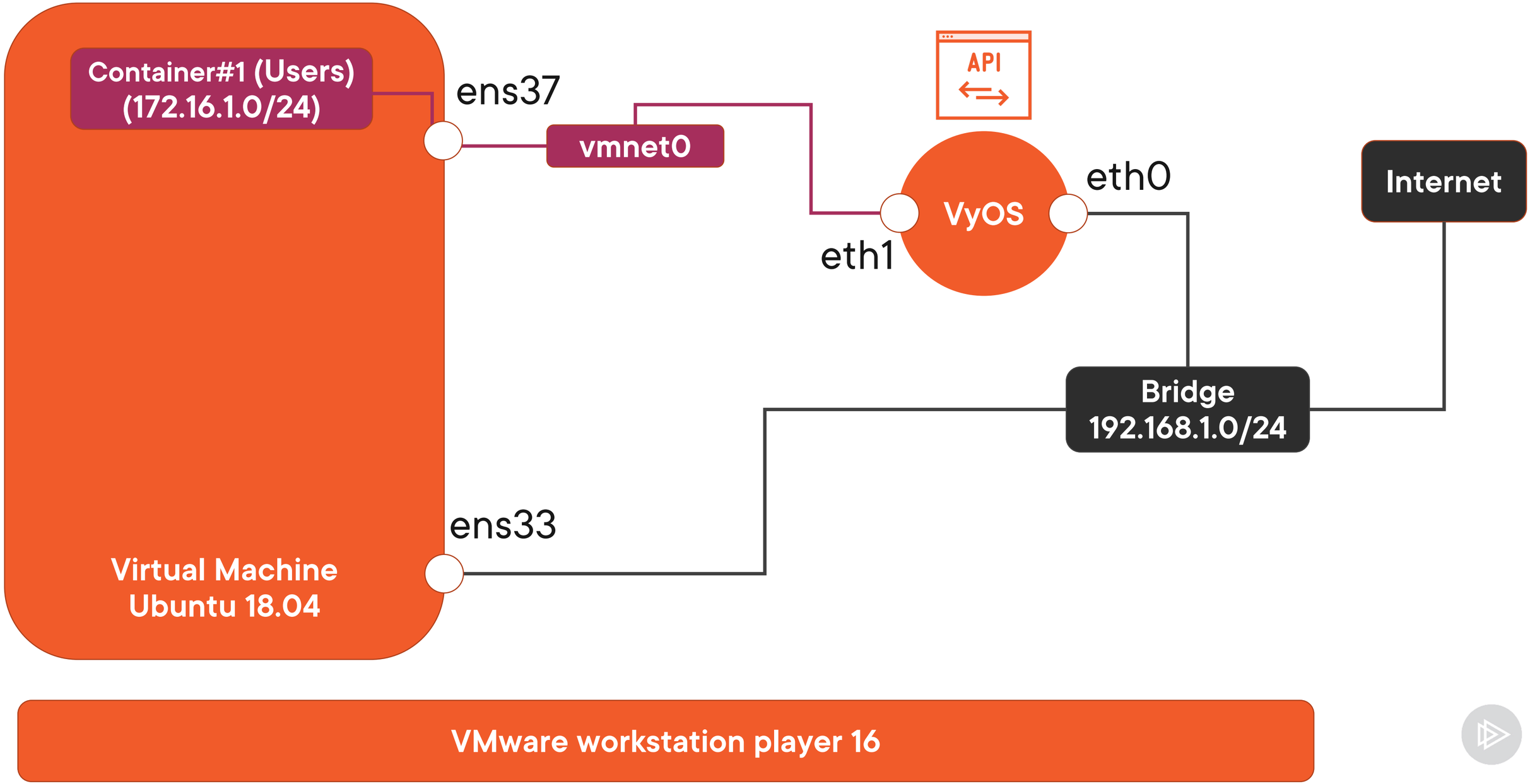
Programmatic configuration

Templating capabilities

Entire infrastructure can be configured at the same time

Real-time configuration

VyOS Installation and Basic Configuration

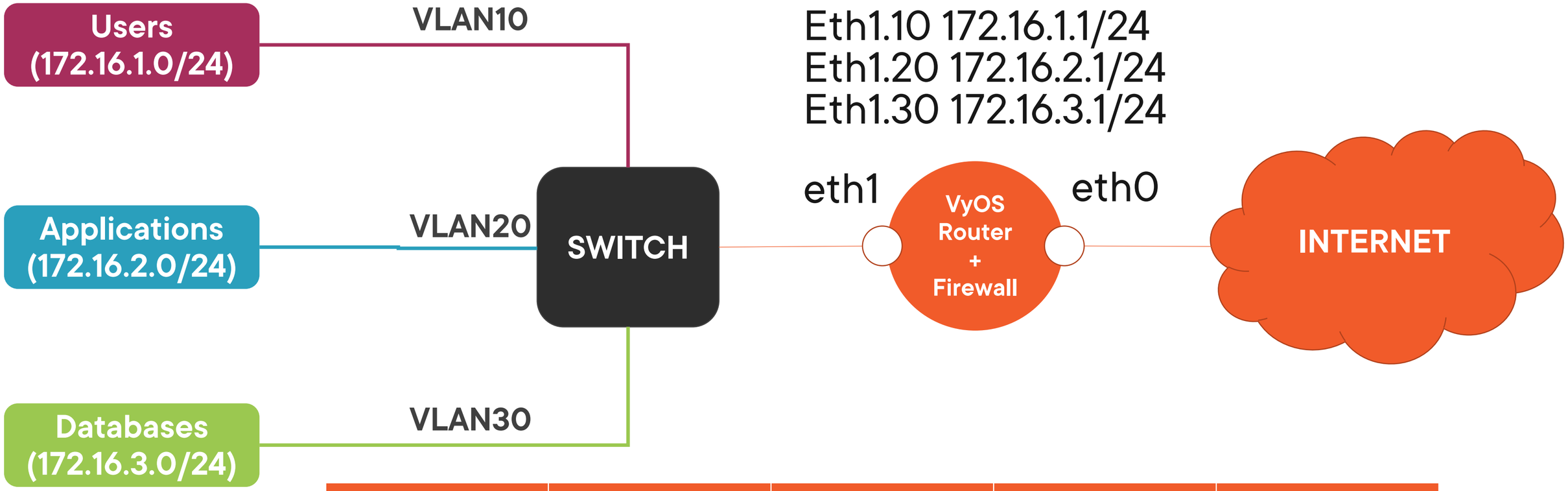


Demo

In this demo you will learn:

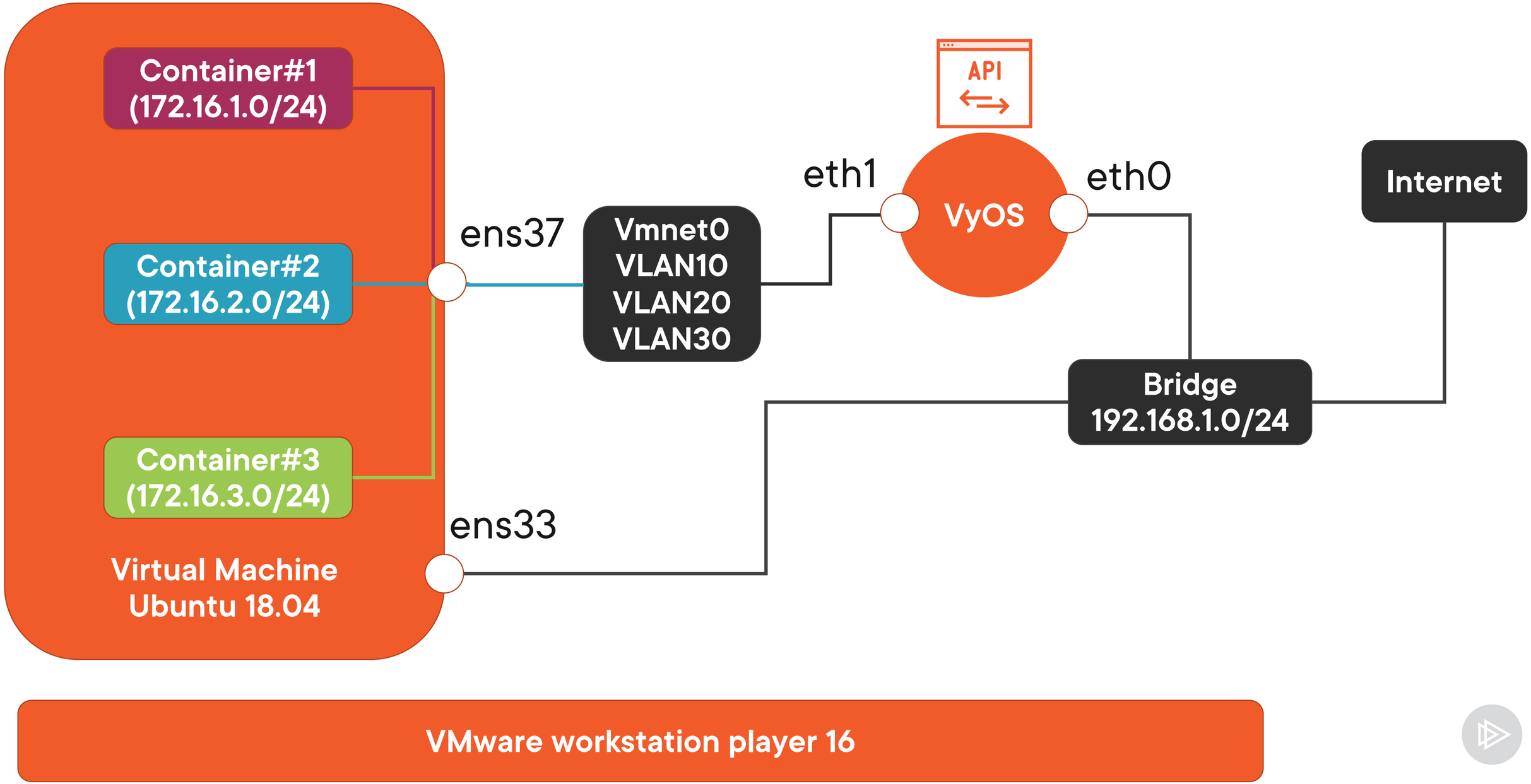
- **How to set up network segmentation and segregation with VyOS configured with VLAN and Firewall policy**

Network Segmentation and Segregation with VLAN



	Users	App	databases	internet
Users	Allowed	Allowed	Not allowed	Allowed
App	Allowed (*)	Allowed	Allowed	Allowed
databases	Not allowed	Allowed (*)	Allowed	Not allowed
internet	Not allowed	Not allowed	Not allowed	Allowed
(*) only if already established				

Network Segmentation and Segregation with VLAN

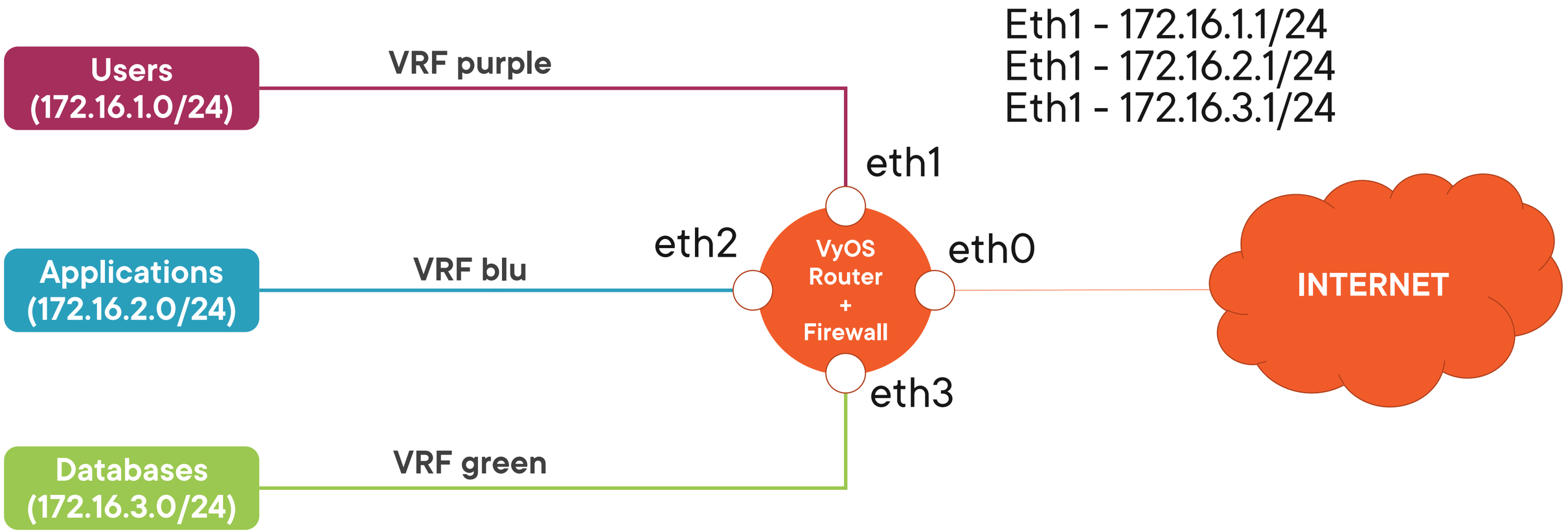


Demo

In this demo you will learn:

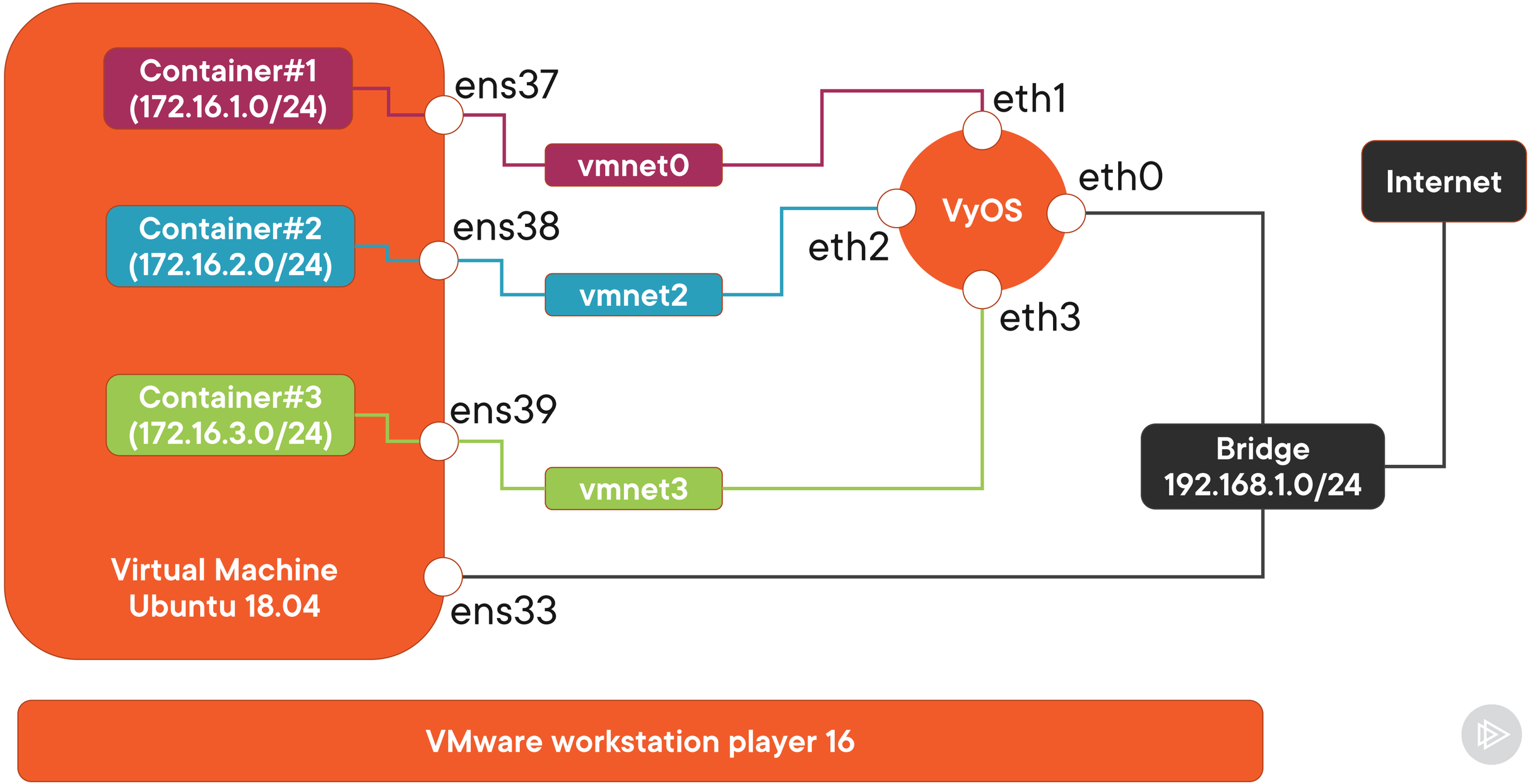
- **How to set up network segmentation and segregation with VyOS configured with VRFs**

Network Segmentation and Segregation with VLAN



	User1	App	Database	internet
User1 (172.16.1.2)	allowed	Allowed		allowed
App (172.16.2.2)	allowed		allowed	
Database (172.16.3.2)		allowed		
Internet	allowed			

Network Segmentation and Segregation with VRF



Resources

More Information

Capabilities not covered

Automated configuration with Ansible

https://docs.vyos.io/en/equuleus/automation/index.html

VyOS API fine tuning

https://docs.vyos.io/en/equuleus/configuration/service/https.html#http-api

Roadmap

Release 1.4 (Sagitta) under development

https://docs.vyos.io/en/latest/introducing/about.html

New features (Public Key Infrastructure)

https://docs.vyos.io/en/latest/configuration/pki/index.html

Thank you

Overview/ Summary

VyOS API configuration

VyOS API calls with simple python scripts

VyOS features (VLAN, VRF, Firewall) for network segmentation and segregation