Решения Palo Alto Networks для защиты контейнеров

Евгений Кутумин
Russia@paloaltonetworks.com

PCNSE,OSCP, GIAC

Palo Alto Networks Россия и СНГ
канал на Youtube
tiny.cc/paloaltorussia

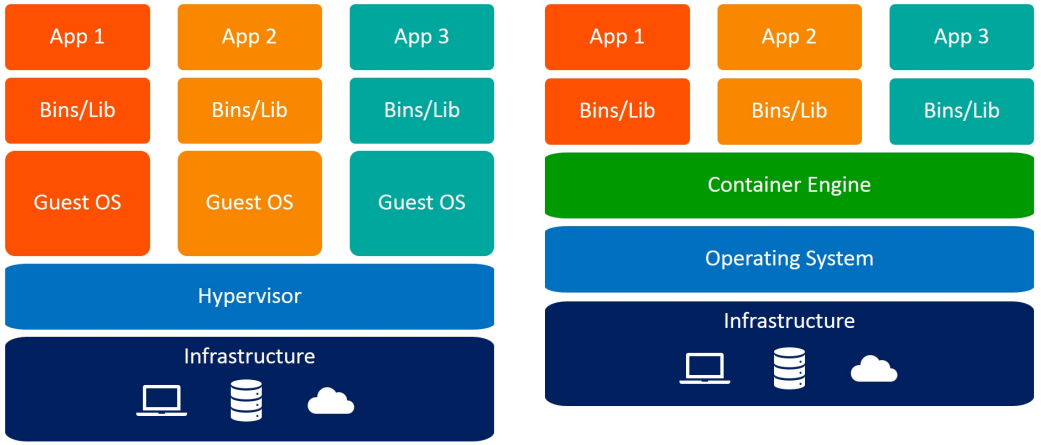
Контейнеры получают все большее распространение в IT

К 2023 году более 70% организаций будут использовать в продуктивной среде три и более приложений, работающий в контейнерах

Gartner, 2019

Преимущества использования контейнеров

- Мало весят и мало потребляют ресурсов
- Изолированы друг от друга
- Не привязаны к Guest OS
- Репозитории контейнеров Dockerhub
- Автоматизация



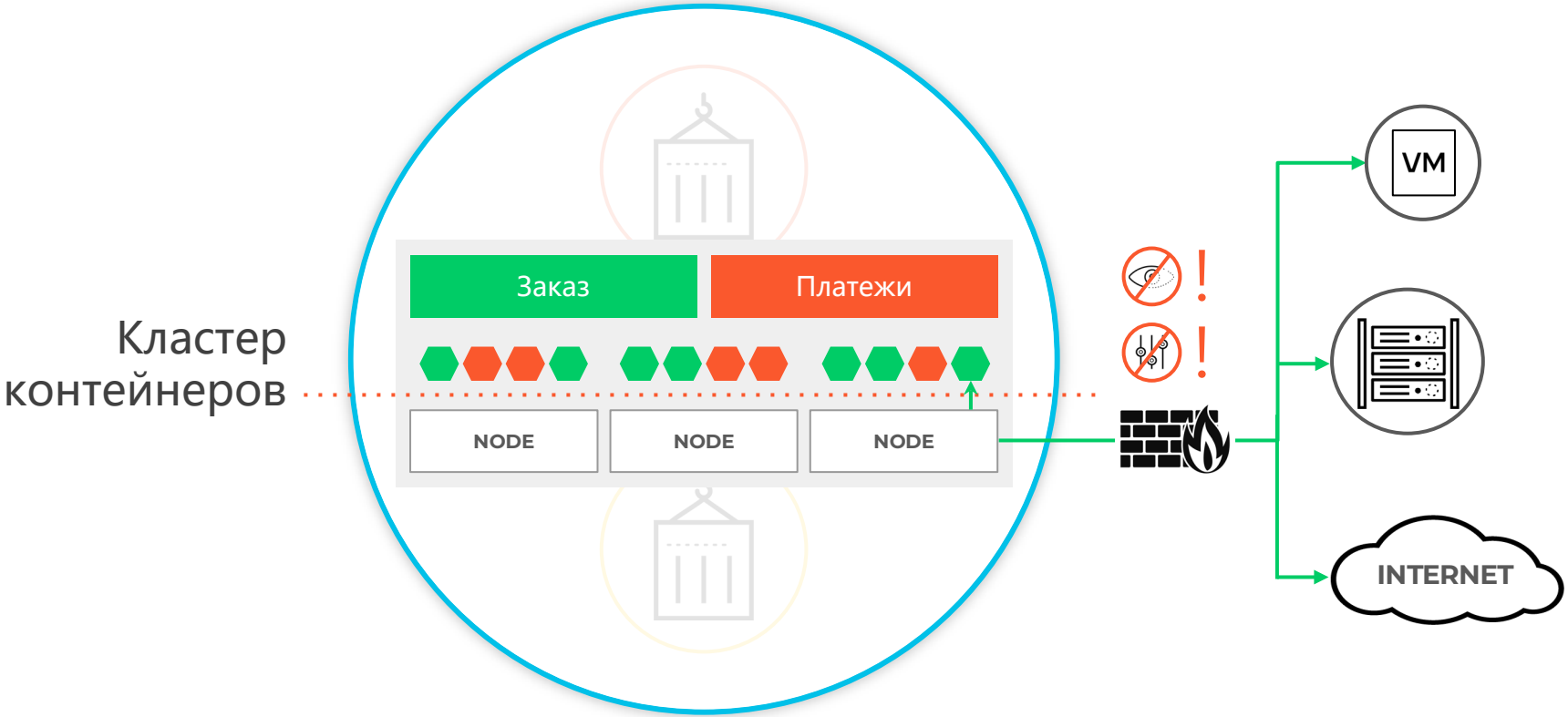
Проблемы при защите контейнеров

Нет полной картины происходящего и нет контроля

Рассогласованные инструменты и средства управления

Отсутствие автоматизации и возможностей по масштабированию

Классические форм-факторы МЭ не получают полной картины



Представляем контейнерный NGFW CN-серии

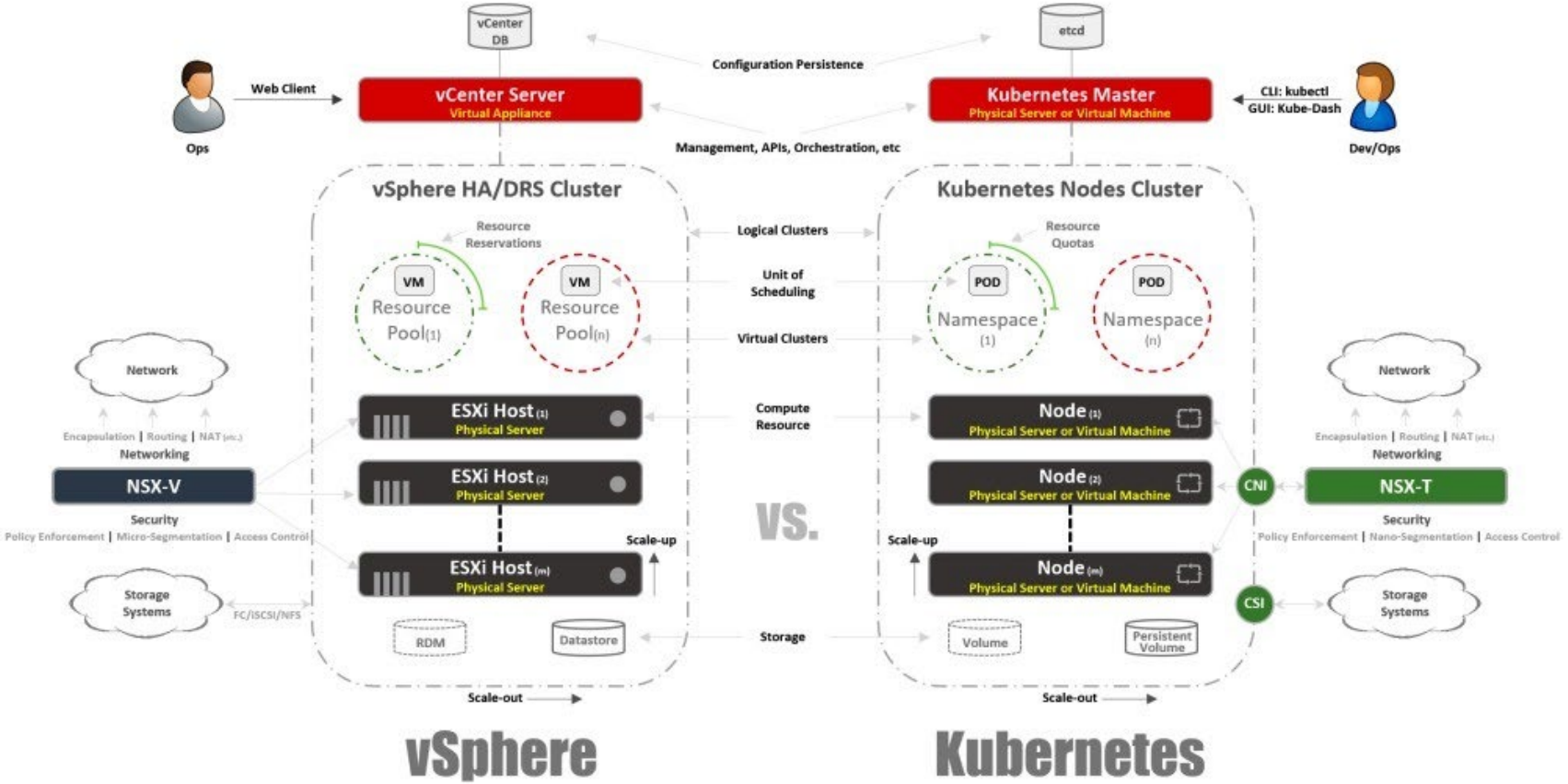
NGFW для среды Kubernetes

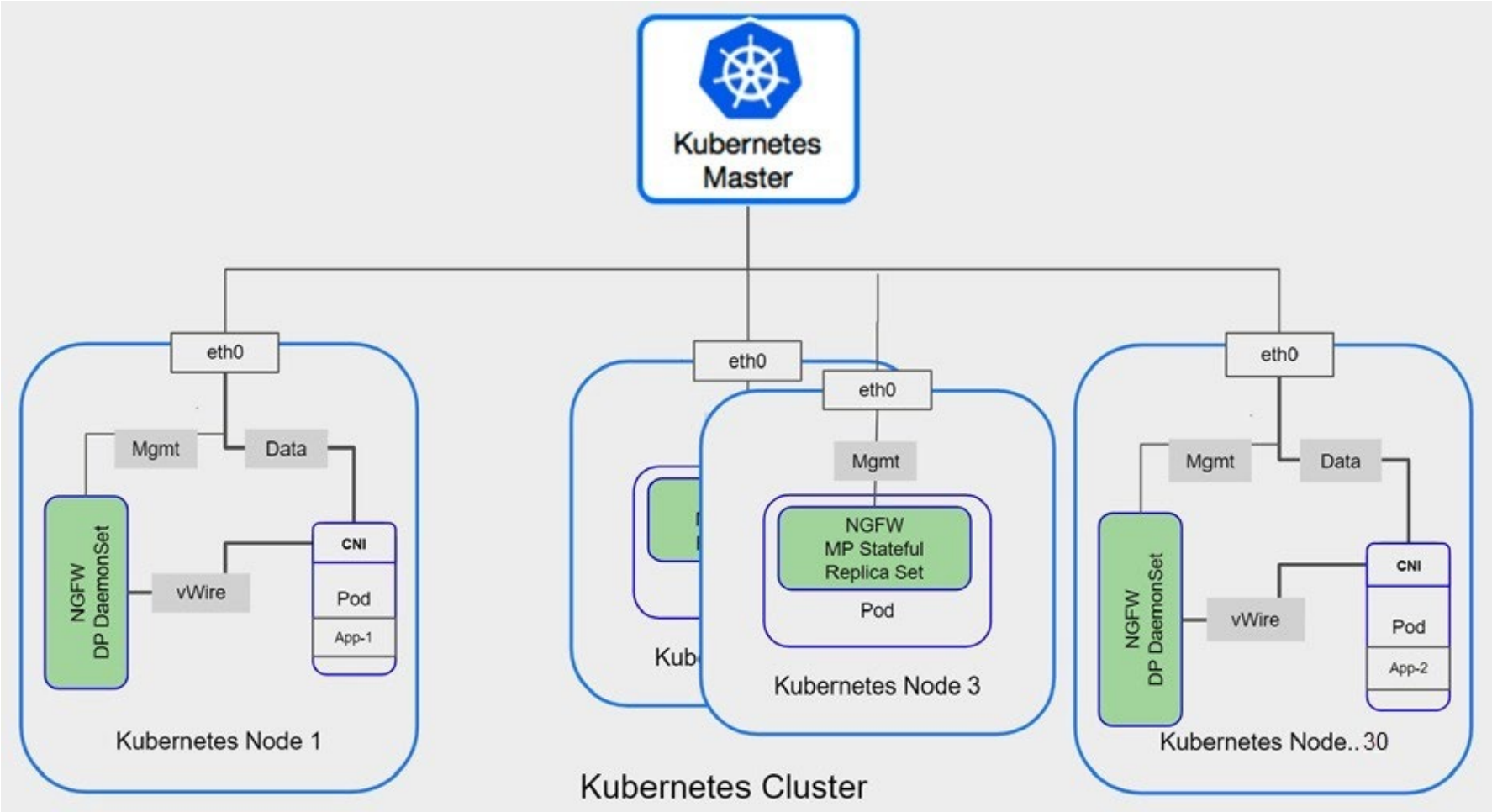
Возможности сервисов безопасности Palo Alto Networks в форма-факторе контейнера

Защита сети на уровне L7 и предотвращение угроз

Интеграция с Kubernetes

VMware vs K8 (терминология)

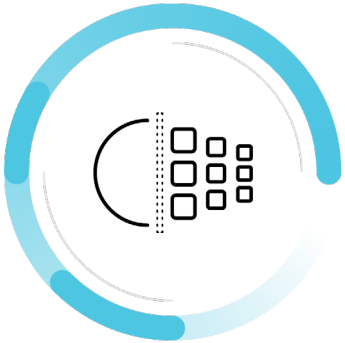




Типовые сценарии использования CN-серии Palo Alto Networks

Защита на L7 в направлении Восток-Запад

Реализация границ доверия между namespaces и другими типами рабочих нагрузок



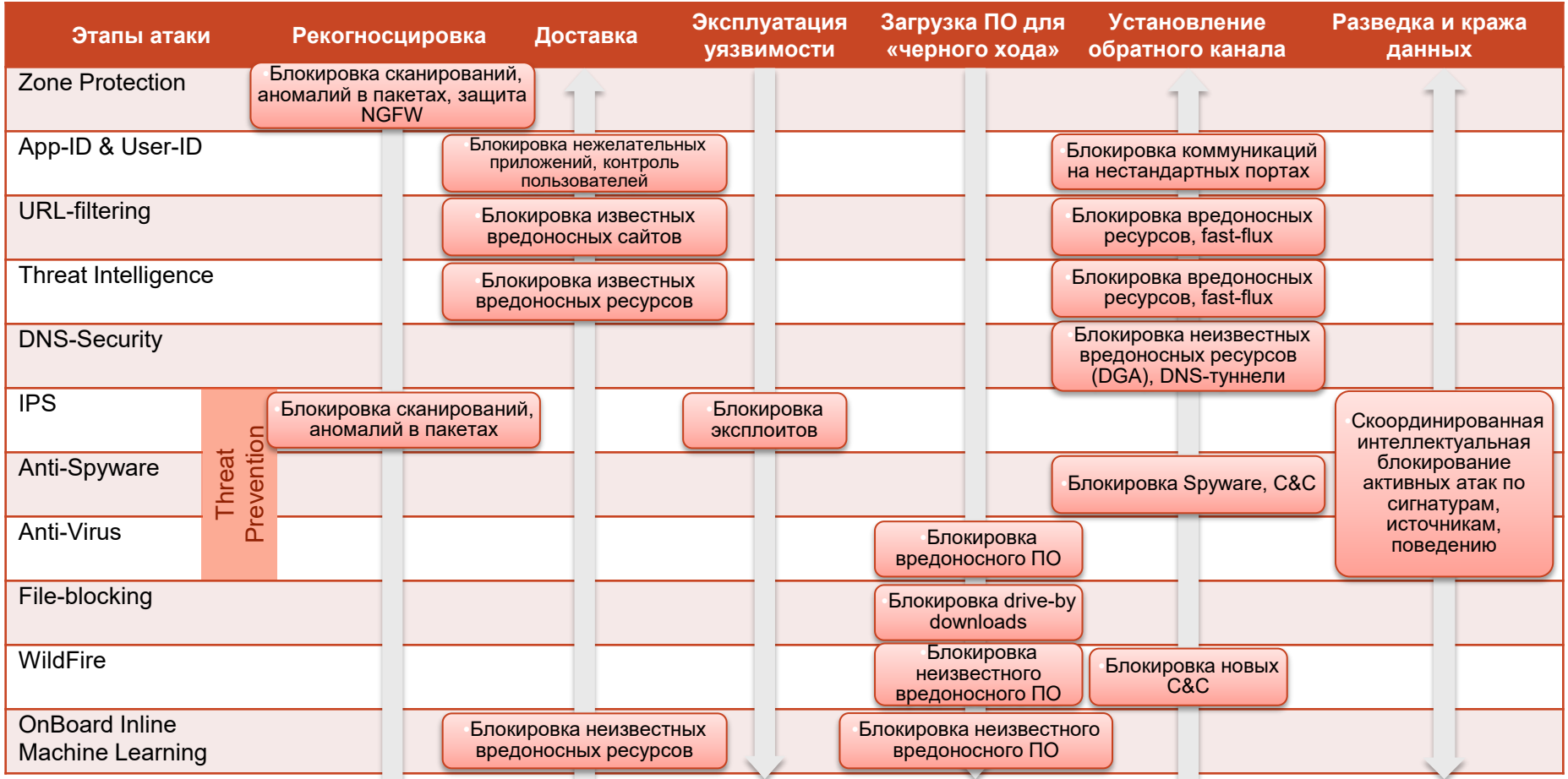
Инспекция исходящего трафика

URL-фильтрация проверка содержимого на L7

Инспекция входящего трафика

Блокировка известных и неизвестных угроз

Глубокоэшелонированная защита



Функции, которые не поддерживаются CN-series

The following capabilities supported on PAN-OS are not available for the CN-Series:

- Authentication
- Logs to Cortex Data Lake
- Enterprise DLP
- Interfaces other than virtual wires are not supported.
- IoT Security
- IPv6
- NAT
- Policy Based Forwarding
- QoS
- SD-WAN
- Tunnel Content Inspection, supported on CN-Series running 10.0.3 or later
- User-ID
- WildFire Inline ML
- No Support for GlobalProtect and Software updates from the Device Deployment tab on Panorama.

  Only Plugin and Dynamic Updates for content release versions are supported.

Product Details

Software	Versions
PAN-OS	10.0
K8s Panorama Plugin	1.0.0
Container Runtime	Docker, CR-IO
Provider Managed Kubernetes	Azure AKS, AWS EKS, GCP GKE, Openshift 4.2
Native K8s	1.13, 1.14, 1.15
Kubernetes Host VM OS	Ubuntu 16.04, 18.04, RHEL/Centos 7.3 +, CoreOS 21XX, 22XX
CNI Plugins	Calico, Weave, Flannel, Azure, AWS

Metric	Performance per core
App-ID	**500 mbps**
Threat	**250 mbps**

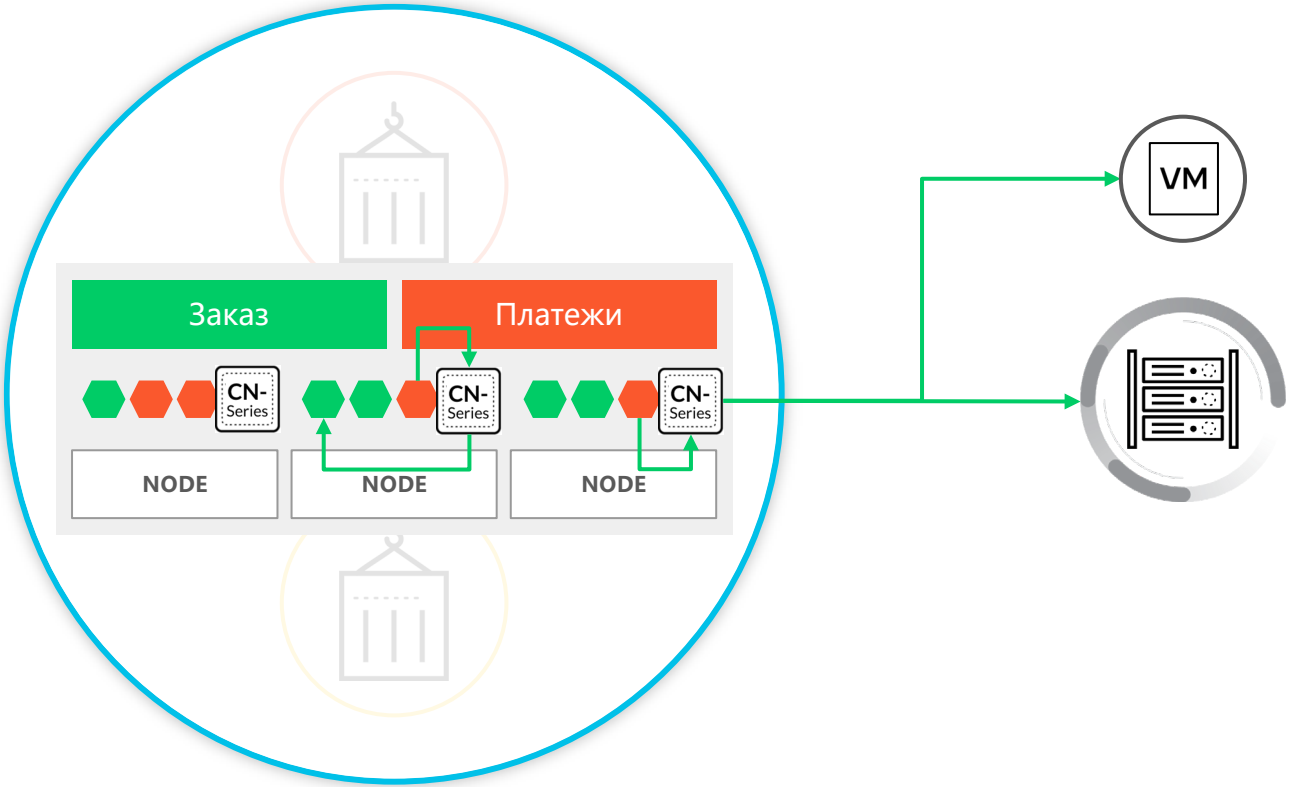
Лицензирование CN-Series

Компоненты лицензирования	Описание
Лицензирование	Количество CN-Series firewall = K8s нод
Бандлы CN-Series	• Basic Bundle: (CN-Series + Support) • Bundle One: (CN-Series + Support + TP) • Bundle Two: (CN-Series + Support + TP + Wildfire + URL + DNS)
Время	1 год, 3 года, 5 лет
ELA	7 токенов для 1ого CN-Series NGFW
Max количество DP на 1 MP	30

Рекомендуемые подписки: TP WF

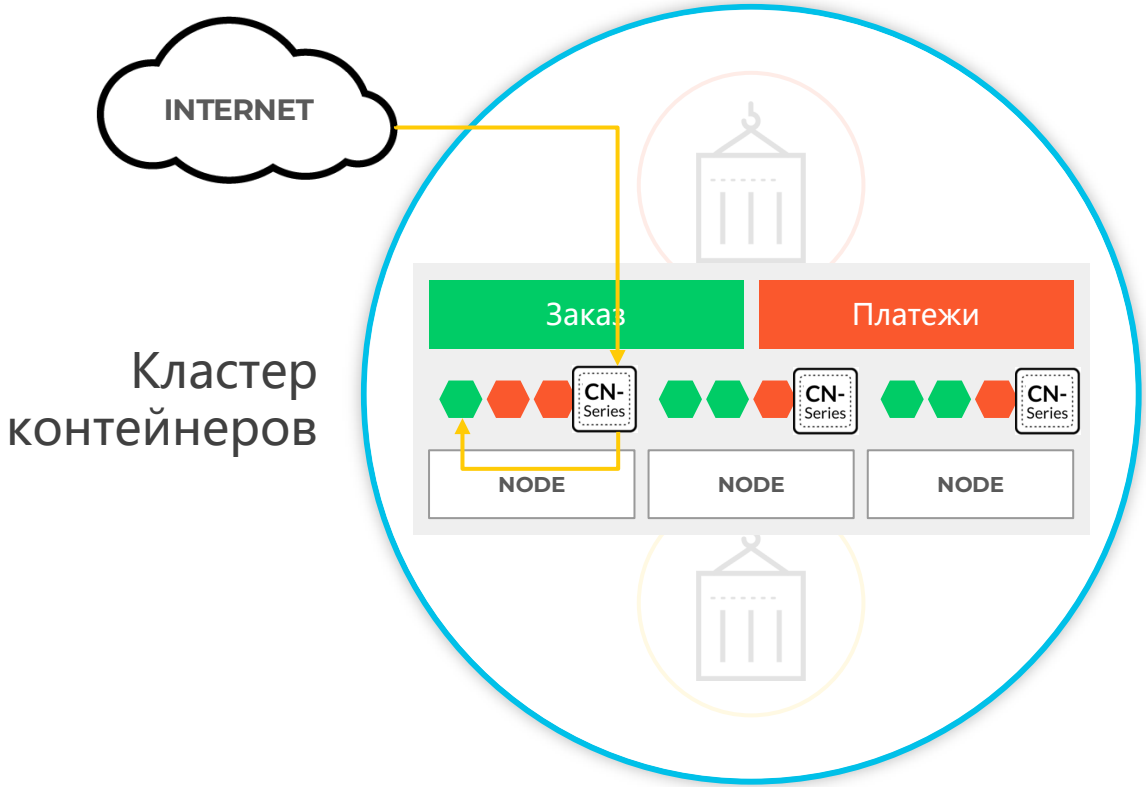
Сценарий 1: проверка на L7 east-west трафика

Кластер контейнеров



Сценарий 2: проверка входящего трафика (AV, URL)

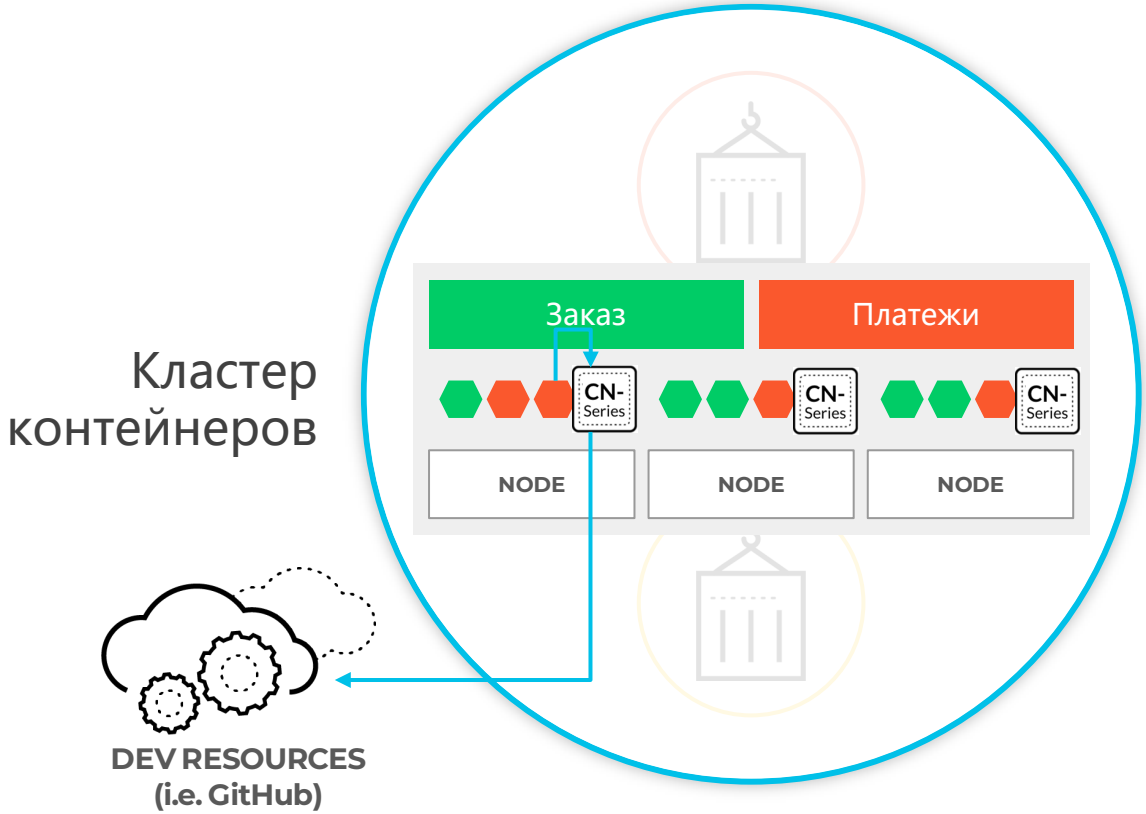
Рекомендуемые подписки: TP WF



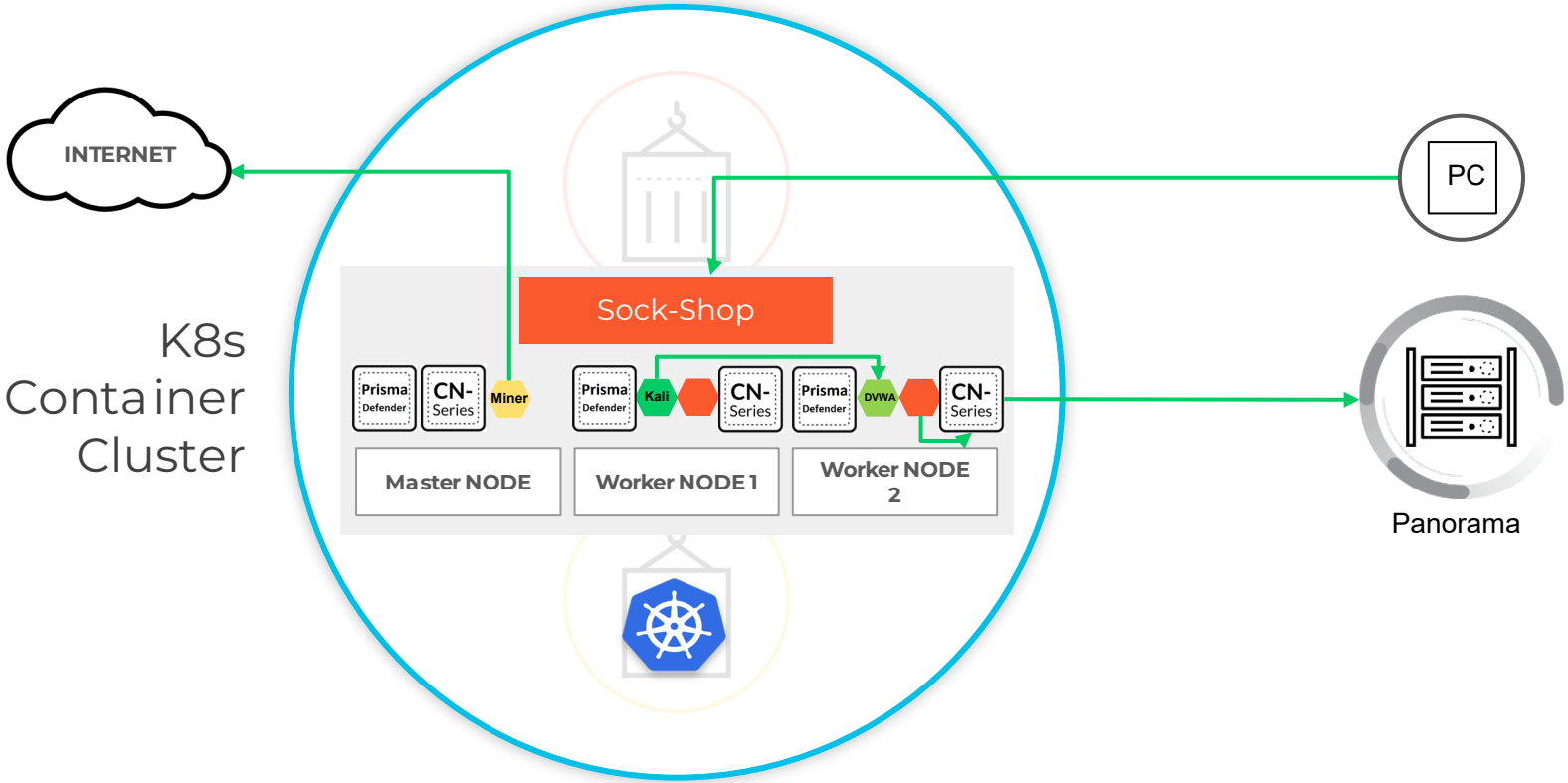
Кластер контейнеров

Рекомендуемые подписки: UF DNS

Сценарий 2: проверка исходящего трафика (Antibotnet + IPS)



Lab demo



DEMO

Спасибо!

paloaltonetworks.com

Palo Alto Networks Россия и СНГ
канал на Youtube
tiny.cc/paloaltorussia