Secure Innovation with the Industry’s First NGFW for Kubernetes

Container traffic is growing by leaps and bounds but traditional network security solutions are not designed to provide full protection for modern microservices-based applications. Additionally, the network security team needs to keep up with agile modern apps rollout, preventing these modern applications from vulnerabilities to cyber-attacks.

The Palo Alto Networks CN-Series containerized firewall is the best-in-class next-generation firewall purpose-built to secure the Kubernetes environments against modern application attacks and data exfiltration. The CN-Series firewall enables network security teams to gain full application (Layer 7) visibility into Kubernetes environments, dynamically scale network security without compromising DevOps agility, and align with the demands of modern DevOps teams to easily manage CN-Series.

Discover Security Built for Security Teams and DevOps Teams

Gain application (Layer 7) visibility and security enforcement using native K8S context to protect against known and unknown threats.

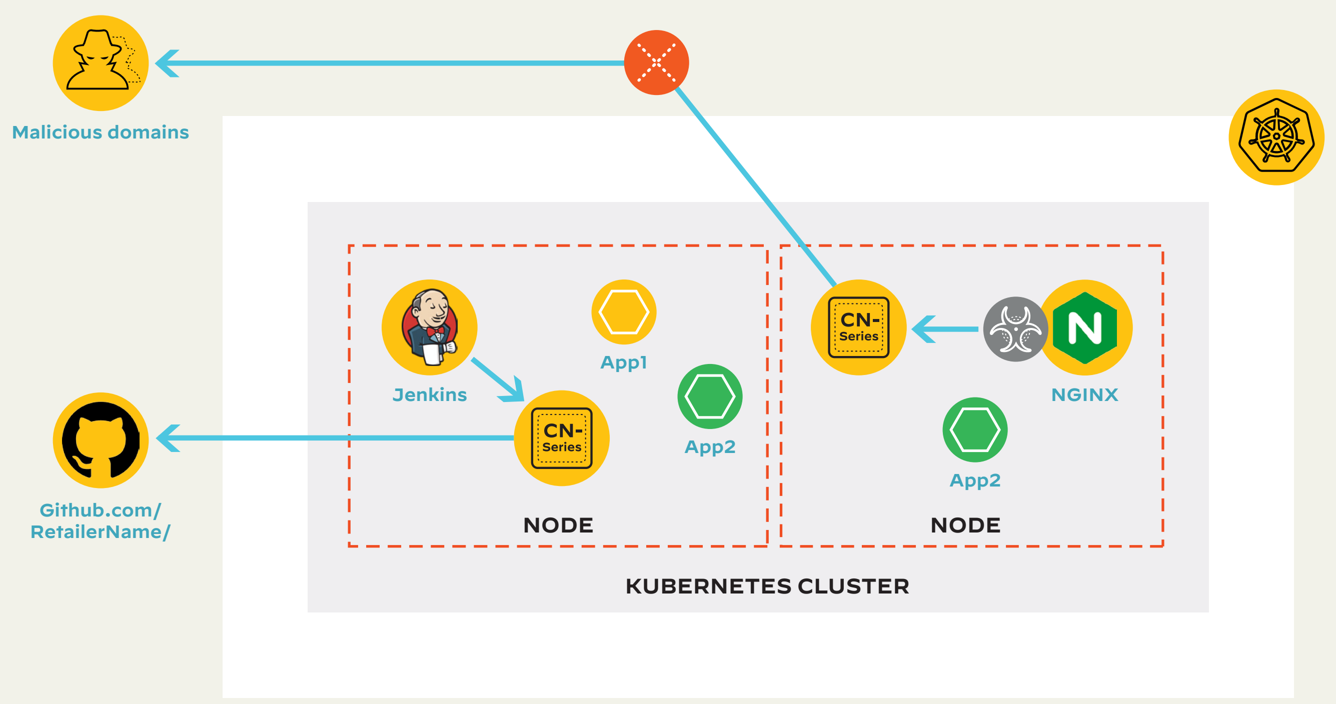
Dynamically scale network security without compromising DevOps speed and agility.

Consistent tooling and management aligns with the demands of modern DevOps teams.

Centralized security management Manage network security for physical, virtual, and containerized workloads from the same interface (Panorama).

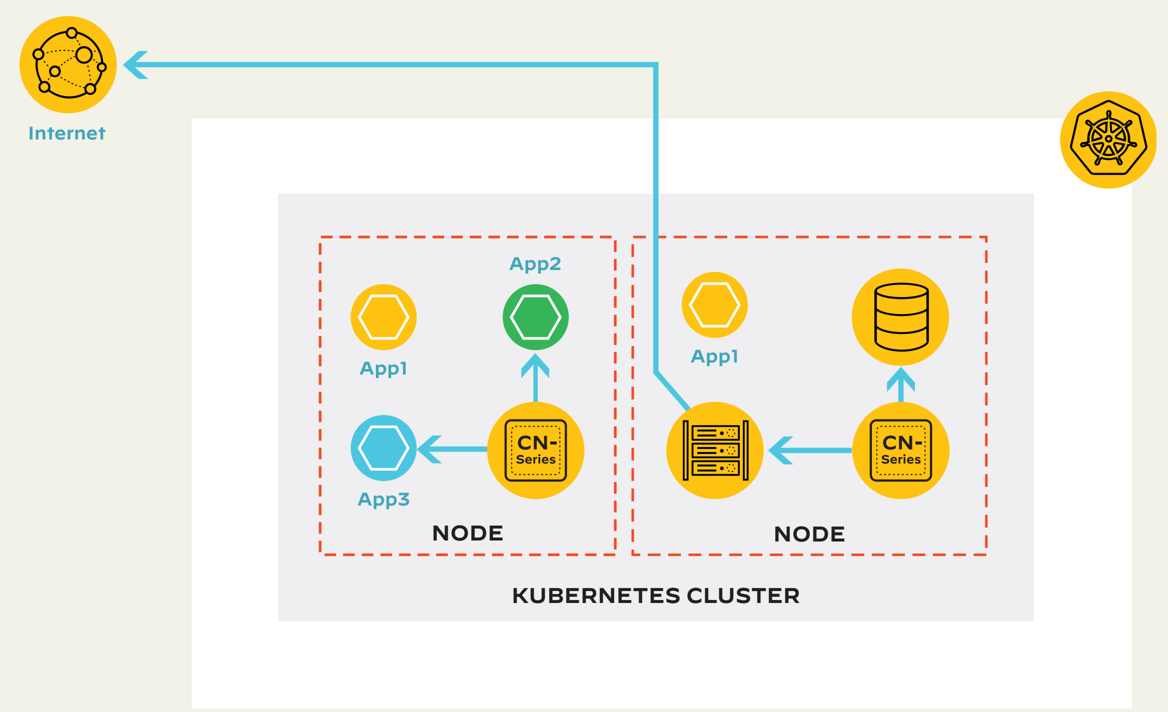
Prevent Data Exfiltration from Kubernetes Environments

Prevent the exfiltration of sensitive data from Kubernetes environments and ensure customers’ critical information stays in the environment where it belongs. The CN-Series inspects and controls allowed traffic at Layer 7, as well as enables our Threat Prevention subscription service to detect and stop threats that may be attempting to move laterally across the environment.



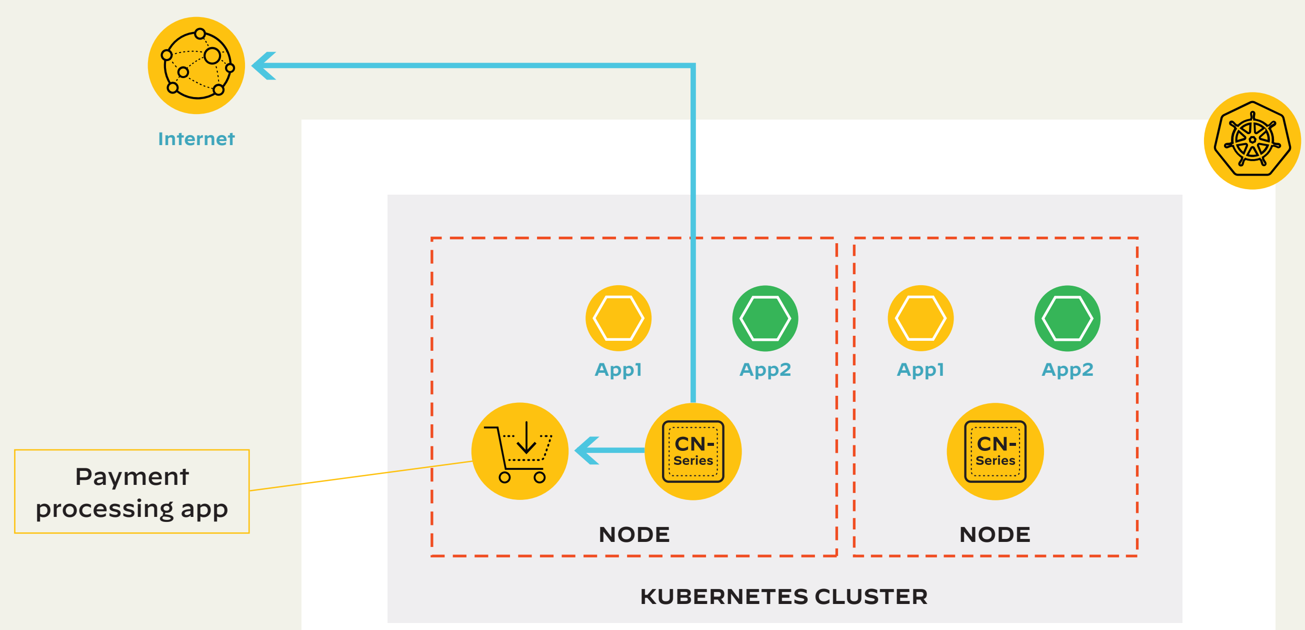
Prevent Lateral Spread of Threats Across Kubernetes Namespace Boundaries

Get Layer 7 traffic protection and threat protection into their Kubernetes environments to secure the allowed connections between two containerized applications running on the same cluster.



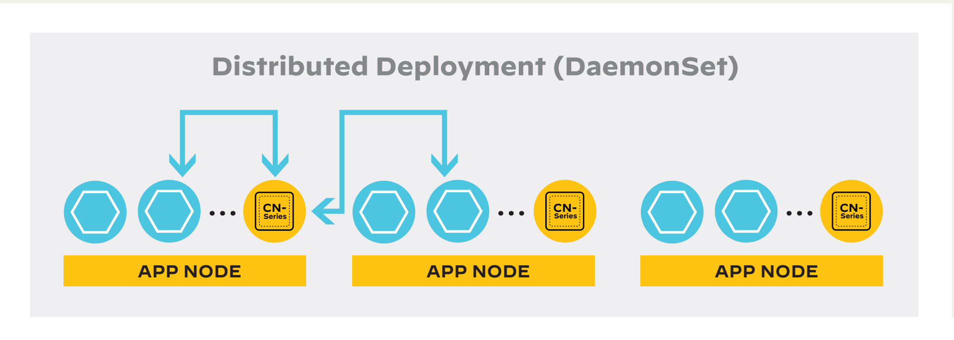
Prevent Both Known and Unknown Inbound Threats

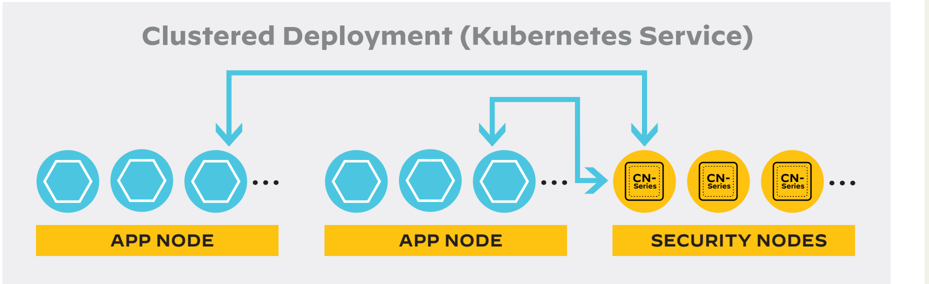
Prevent threats riding on inbound traffic to the container environment, ensure only allowed applications are permitted across open ports and protect against known and unknown threats attempting to sneak into the network.



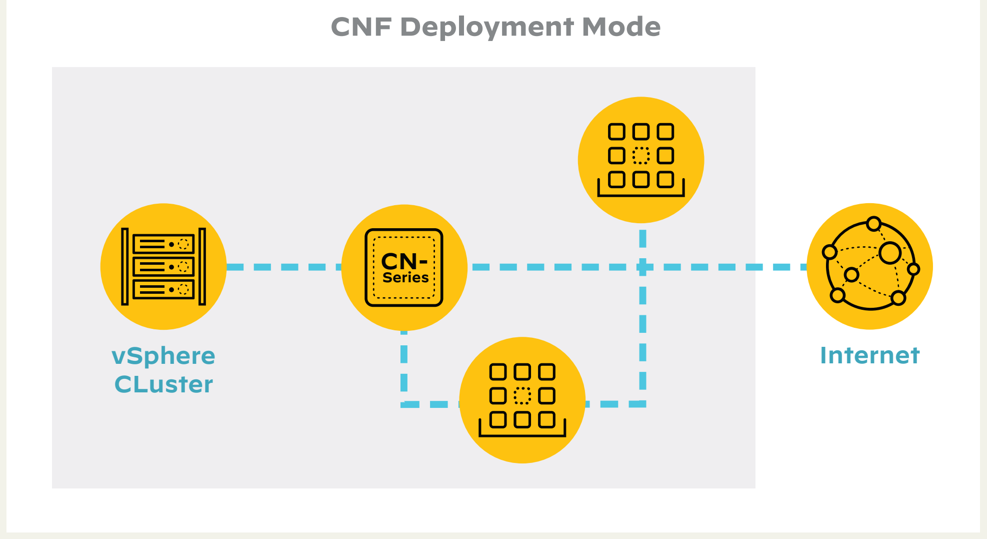
CN-Series Deployment Modes

To protect containerized applications, CN-Series can be deployed in two modes: DaemonSet or Kubernetes Services. In DaemonSet deployment mode, the firewall data plane runs as a daemon set on each node. DaemonSet deployment mode is best suited for latency-sensitive applications. In Kubernetes Services deployment mode, the firewall data plane runs as a Kubernetes service in a dedicated security node/nodes. In this deployment mode, CN-Series takes advantage of the native autoscaling capabilities of Kubernetes to ensure threat protection in even the most dynamic Kubernetes environments.





The PAN-OS 10.2 release introduced a third deployment mode called CNF mode. With CNF mode, CN-Series can protect both container and non-container workloads. This deployment mode makes CN-Series the only containerized 5G firewall that can scale up to 47 vCPUs and secure traffic more efficiently with a 5X performance increase.



IT’S TIME TO MAKE IT HAPPEN

See why CN-Series Container Firewalls are essential components of our Network Security Platform—and for Zero Trust in any cloud. Sign up for your personalized demo today.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

vm-series_six_zero trust_essentials_for_public cloud_zero_trust_infographic_8_20_2022