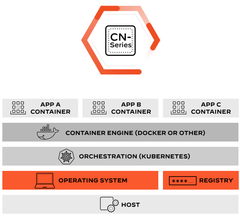
Secure Innovation with the Industry's First NGFW for Kubernetes

Container traffic is growing by leaps and bounds – and it's probably part of your network infrastructure. Or will be soon. That's why you need CN-Series containerized firewalls to prevent network-based threats in Kubernetes® environments.

Take a look at what the CN-Series can do for your organization. It's the industry's first NGFW for Kubernetes – and provides all the security features of Palo Alto Networks physical and virtual firewalls. Now you can rapidly secure containerized applications and workloads in Kubernetes environments – without slowing the speed of innovation.



70%

By 2023, more than 70% of global organizations will be running three or more containerized applications in production.[1]

Discover Security Built for Security Teams and Developers

Gain network visibility and control in Kubernetes environments

Integrate network security directly into the container environment. Get full visibility – including into the ever-elusive source IP of outbound traffic – and detect threats traversing namespace boundaries.

Streamline network security insertion in DevOps environments

Boost DevOps speed and agility. Use native Kubernetes orchestration to integrate firewall deployment directly into your DevOps process for frictionless deployments.

Align cloud native security across the environment

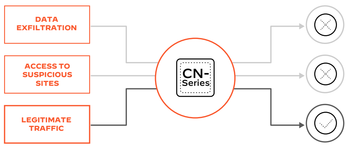
Enforce consistent levels of network security in cloud native environments. Share contextual information with other Palo Alto Networks firewall form factors.

Unify security management in hybrid infrastructures

Enforce consistent levels of network time and effort. Manage CN-Series firewalls with Palo Alto Networks Panorama, which provides a single console for managing all network security components.

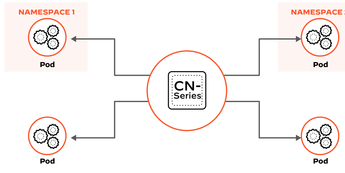
Get Protection to Keep DevOps Productive

Protect outbound traffic



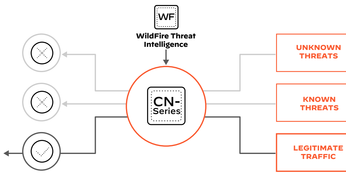
Prevent exfiltration. CN-Series firewalls can inspect all outbound traffic originating from a containerized application – and halt inadvertent access of suspect websites and command-and-control servers.

Protect east-west traffic



Enforce Zero Trust with threat prevention. Protect east-west traffic between pods in different trust zones – and between pods and other workload types.

Protect inbound traffic



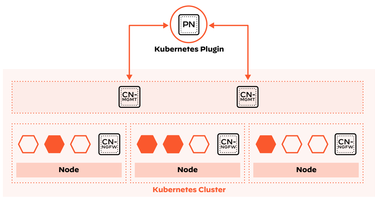
Defend against malware delivery aimed at container exploits and vulnerabilities – and keep the latest threats from breaching your network.

Leverage Deployment Designed for Kubernetes Orchestration

Deploy natively

Benefit from the way the CN-Series management and control planes deploy natively as a daemon set and pod, respectively.

Deployment model for CN-Series

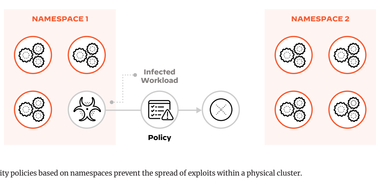


The CN-Series deploys natively as tandem control and data plane pods within the Kubernetes environment.

Use policies aligned to namespaces

Make the most of the environment. CN-Series security policies based on namespaces prevent the spread of exploits within a cluster.

Kubernetes cluster



Security policies based on namespaces prevent the spread of exploits within a physical cluster.

See the CN-Series in Action

Add Kubernetes protection to your network security posture for comprehensive threat protection. Find out how to safeguard innovation with a personalized demo.

REQUST DEMO

Source

1 Gartner research quoted by Janakiram MSV, "5 Modern Infrastructure Trends To Watch Out for in 2019," Forbes, December 20, 2018.