CN-Series Container Firewall

Prevent known and unknown threats in Kubernetes environments with the industry's leading Next-Generation Firewall

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.

CN-Series container firewalls deliver:

- **Inline network security** to provide visibility and enforcement of Kubernetes environments by using native Kubernetes context to protect against known and unknown threats.
- **Dynamic scaling of network security** without compromising DevOps speed and agility.
- **Consistent tooling and Management** Align with the demands of modern DevOps teams to easily deploy and manage CN-Series.
- **Centralized security management** CN-Series firewalls are managed from the same management console (Panorama) as other Palo Alto Networks next-generation firewall platforms (including physical, virtual, containerized, and public cloud) to provide Network Security teams with a single-pane-of-glass console to protect against known and unknown threats.

Overview

Traditional network security solutions are not designed to provide full protection for modern microservices-based applications. As businesses continue to move faster, the network security team needs to keep up with agile modern application rollout to protect against malicious actors.

The Palo Alto Networks CN-Series containerized firewall is the best-in-class next-generation firewall purpose-built to secure the Kubernetes environment from network-based attacks. The CN-Series firewall enables network security teams to gain application visibility into Kubernetes environments, dynamically scaling network security without compromising DevOps speed and agility, while aligning with the demands of modern DevOps teams to easily manage CN-Series.

CN-Series NGFWs use Palo Alto Networks' patented App-ID technology to identify both the application and the content within a connection, providing full content inspection as opposed to Layer-3/Layer-4 access control of traditional firewalls. Further controls and analysis are delivered through advanced cloud-based security services, such as URL Filtering, Threat Prevent, WildFire, and DNS Security.

CN-Series ensures a frictionless CI/CD pipeline deployment while delivering unparalleled runtime network protection through unified management across all your firewalls.

CN-Series firewalls can be easily deployed using DevOps-friendly tools including Helm charts and Terraform templates. CN-Series Firewalls can be managed from Panorama—the same management console as all Palo Alto Networks firewalls—giving network security teams a single pane of glass to manage their organizations' overall network security posture.

Conventional NGFWs can only be deployed at the edge of a Kubernetes environment and therefore cannot determine the specific application where traffic originates. To overcome this challenge, CN-series container firewalls move security into the Kubernetes environment, giving them precise visibility into and control over container traffic.

How the CN-Series Works

CN-Series firewalls deploy as two sets of pods: one for the management plane (CN-MGMT), and another for the firewall data plane (CN-NGFW). The management pod always runs as a Kubernetes service. The data plane pods can be deployed in two modes: Daemonset or Kubernetes Services.

In Kubernetes Services deployment mode, the firewall data plane runs as a Kubernetes service in a dedicated security node. When deployed in Kubernetes Services mode, CN-Series takes advantage of the native autoscaling capabilities of Kubernetes to ensure threat protection in even the most dynamic environments. Kubernetes service deployments are best suited for large Kubernetes environments where a distributed deployment would be resource-intensive and cost-prohibitive.

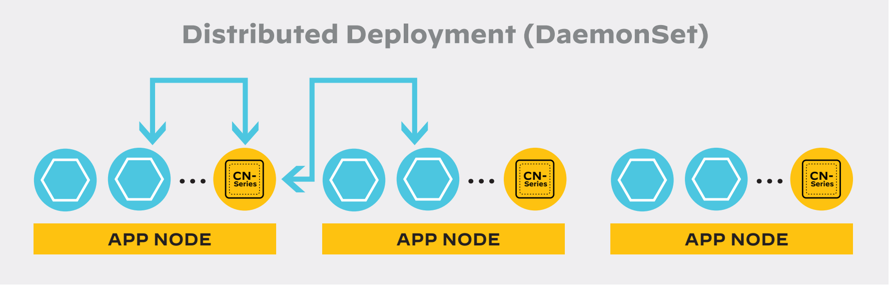

Figure 1: Distributed deployment mode. The firewall dataplane runs as a daemon set on each node.

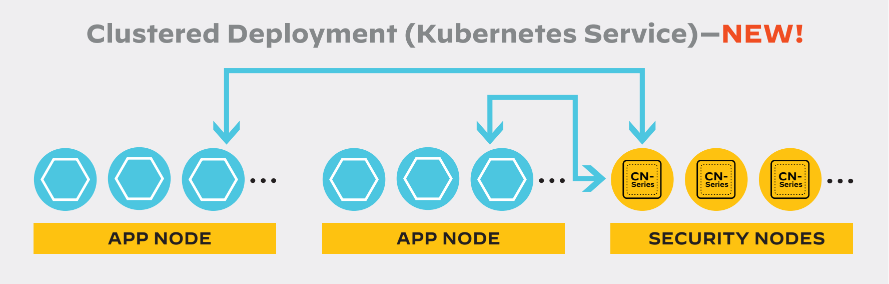

Figure 2: Cluster deployment mode. The firewall dataplane runs as a Kubernetes service in a dedicated security node.

Through the Panorama console, network security admins can use in-cluster Kubernetes labels, such as namespaces, to create granular security policies to identify workloads.

Customers can deploy CN-Series firewalls in Kubernetes environments hosted on-premises or in public clouds. CN-Series firewalls can also be deployed into cloud-managed Kubernetes offerings, including Google Kubernetes Engine (GKE®), Azure Kubernetes Service (AKS), and Amazon Elastic Kubernetes Service (EKS) as well as on-premises environments include RedHat OpenShift. To see the list of supported environments for CN-Series, please refer to CN-Series Supported Environments webpage.

One-click deployment via Kubernetes package managers, such as Helm, is also available and community-supported.

CN-Series deployed in CNF Deployment mode

For organizations that are not only modernizing their applications but also modernizing their infrastructures. The PAN-OS 10.2 release introduced a third deployment mode called the CNF mode. With the CNF deployment 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 can secure traffic more efficiently with a 5X performance increase.

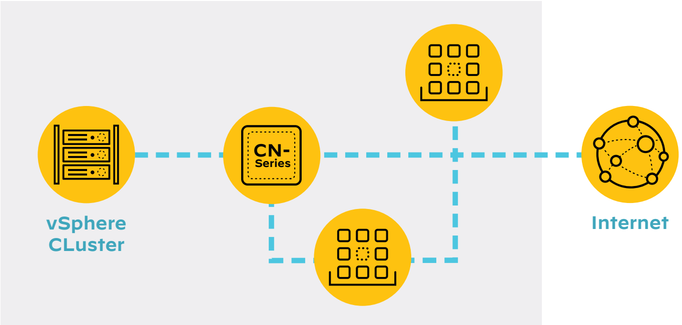

Figure 3: CNF deployment mode.

CN-Series Use Cases

Prevent Data Exfiltration from Kubernetes Environments

CN-Series firewalls offer many security capabilities to prevent the exfiltration of sensitive data from Kubernetes environments. Advanced URL filtering service provides guardrails for developers and other users to ensure that they aren't connecting to potentially malicious sites. Our firewall's ability to inspect traffic content, coupled with our DNS Security service guard against data exfiltration to make sure critical information stays in the environment where it belongs.

Prevent Lateral Spread of Threats Across Kubernetes Namespace Boundaries

In many Kubernetes environments, the Kubernetes namespace is the trust boundary. CN-Series firewalls can be inserted to provide application traffic protection and advanced threat protection into Kubernetes environments to secure the allowed connections between two containerized applications of different trust levels. CN-Series can also secure the allowed connections between containers and other workload types.

Prevent Both Known and Unknown Inbound Threats

Like many applications, attacks can use any port, which limits the effectiveness of port-based network security controls. With application-centric security policies, CN-Series firewalls augment basic port-based access controls and inspect network traffic to ensure only allowed applications are permitted across open ports.

Network security teams can prevent threats riding on inbound traffic to the container environment with our Threat Prevention and Wildfire malware analysis services. Turning on our Threat Prevention and WildFire® malware prevention services on the CN-Series firewall protects your Kubernetes environment against any file-based threats, including exploits, malware, spyware, and previously unknown threats, attempting to sneak through open ports.

CN-Series Key Capabilities

Whatever the security needs of your container environment, the CN-Series is built to deliver.

Application Visibility and Inline Threat Prevention

- **Application visibility and control:** Get immediate visibility into application traffic within your Kubernetes environment. Define application-based policies to control application traffic and enforce Zero Trust best practices.
- **Threat prevention and sandboxing:** Threat Prevention and WildFire services can be enabled on CN-Series firewalls to block exploits, prevent malware, and stop both known and unknown advanced threats.
- **Exfiltration prevention and URL filtering:** The CN-Series enables content inspection and SSL Decryption, preventing sensitive information from leaving your network. Advanced URL Filtering uses machine learning to categorize URLs and block access to malicious sites that deliver malware or steal credentials. Automation ensures protections are always up to date.

Automated Scalability and Configuration

- **Autoscale with Kubernetes:** CN-Series firewalls can leverage the autoscaling capabilities of Kubernetes to ensure protection in even the most dynamic environments.
- **Flexible tag-based policy model:** CN-Series firewall policies can be defined by application, user, content, native Kubernetes labels, and other metadata to deliver flexible security policies aligned with business needs.
- **DevOps-friendly configuration:** CN-Series firewalls can be specified in a YAML file and can be easily integrated into infrastructure deployment files for fast, repeatable deployments. Configuration templates can be found in our official CN-Series GitHub repository.
- **Community-supported Kubernetes Helm chart:** For development teams using Helm to manage their Kubernetes applications, a CN-Series Helm Chart has been created to simplify firewall deployment and management.

Flexible Deployment and Consistent CNI Integration

- **Flexible deployment options:** Customers can choose to deploy CN-Series firewalls in distributed or clustered modes, depending on use case, budget and environmental configuration.
- **Simple insertion:** The CN-Series supports multiple container network interface (CNI) plugins for use in different types of Kubernetes deployments.

On-Premises and Cloud Support for Kubernetes

- **Public cloud:** CN-Series firewalls can be deployed in hosted container environments such as GKE, AKS, Amazon EKS, and Red Hat OpenShift®.
- **On-premises:** CN-Series firewalls can also be deployed into Kubernetes environments hosted on-premises.

Centralized Security Management

- **Consistent management:** Manage the CN-Series from Panorama—the same management console you use for your hardware and virtual form factor Palo Alto Networks firewalls.
- **Plugin architecture:** Panorama plugins for GKE, AKS, Amazon EKS, and OpenShift allow you to manage network security for each environment from Panorama.
- **Centralized logging:** Panorama centralizes logging to simplify auditing and compliance.

Size and Scale Security Based on Immediate Needs—In Minutes

CN-Series licensing is similar to VM-Series licensing. Both VM-Series and CN-Series Firewalls are licensed based on Software NGFW Credits. CN-Series firewalls are licensed based on the number of Data Plane vCPUs. To manage credits for CN-Series:

1. Procure Software NGFW Credits. Use the Software Firewall Credit Calculator to decide the number of credits you need.
2. Allocate or reallocate credits across different deployments to activate your choice of security products and security services in just minutes.
3. Manage and monitor credits via the Palo Alto Networks customer support portal.

To check the supported environments for CN-Series, please visit the CN-Series Supported Environments web page.

To check the CPU and memory requirements for CN-Series, please visit the CN-Series System requirements web page.

The latest CN-Series Performance and Scaling numbers are available on CN-Series Performance and Scaling web page.

Find more information about CN-Series container firewalls here.

paloalto
NETWORKS

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