

Limitations

- Limitations for Deployment of Firewall Threat Defense Container, on page 1

Limitations for Deployment of Firewall Threat Defense Container

The Firewall Threat Defense container solution is validated on open-source Docker, Kubernetes, and Amazon EKS environments.

- If a reboot or shutdown is triggered from Management Center, the lina process inside the container may be terminated. This can result in traffic disruption. The container will not be gracefully restarted or recovered by this operation.

Caution Management Center currently allows reboot/shutdown operations for FTDc devices. These operations must not be used for container-based deployments.

- Docker does not guarantee consistent network interface order (for example, eth0, eth1) when a container with multiple networks is restarted. After a restart, verify and, if required, reconnect the Docker network interfaces for FTDc.
- SNMP polling behavior in Kubernetes:
  - Kubernetes applies Source NAT (SNAT) for external traffic by default.

    SNMP polling must be configured using the Kubernetes node IP instead of original source IP of the SNMP client.
  - As a result, the original SNMP client IP is not visible to the FTDc container.
- The following features are not supported:
  - Clustering
  - High Availability
  - Transparent mode
  - Subinterfaces are not supported only when using macvlan CNI.
  - IPv6 is not supported when using macvlan CNI.

  - Inline mode interface
  - SR-IOV CNI in Amazon EKS

- In afpacket mode, the Maximum Transmission Unit (MTU) must not exceed 8140 bytes, even though Management Center may allow higher values; such configurations are not supported for FTDc deployments.