Knowledge Check

Traditional enterprise network security was implemented using:

1/1 point (ungraded)

- [x] Designing a physical topology of network devices (firewalls, routers, switches)
- [x] Static IP address ranges
- [ ] Active Directory

✔

Submit

✔ Correct (1/1 point)

1/1 point (ungraded)

- [x] Assumes a flat pod network
- [x] Is defined using network policy
- [x] Is abstracted from the network by using label selectors
- [x] Relies on network plugins to enforce network policy
- [ ] Relies on capabilities of the underlying network

✔

Submit

✔ Correct (1/1 point)

How do traditional firewalls work with Kubernetes?

1/1 point (ungraded)

- [ ] Don't use them
- [x] Use them at the perimeter

✔

Submit

✔ Correct (1/1 point)

Calico network policies:

1/1 point (ungraded)

- [x] Provide features beyond Kubernetes network policies
- [x] Can be namespaced or non-namespaced
- [x] Can be used alongside Kubernetes network policies
- [x] Can be used to protect hosts as well as pods
- [ ] Are higher priority than Kubernetes network policies
- [x] Are managed using calicoctl
- [x] Can be used to enforce security within an Istio service mesh
- [x] Can reference Calico network sets in their rules using label

✔

Submit

✔ Correct (1/1 point)

Network policy best practices include:

1/1 point (ungraded)

- [x] Per namespace or cluster wide default deny or default app policies
- [x] Ingress and egress rules for every pod
- [ ] Using separate policies for ingress vs egress
- [x] Defining standard schemas for network policies and pod labels

✔

Submit

You can manage trust across teams using:

1/1 point (ungraded)

- [x] Calico network policies alongside Kubernetes network policies
- [x] Referencing namespace or service accounts in Calico policies
- [ ] Giving dev teams access to Calico network policies and security teams access to Kubernetes network policies

✔

Submit

✔ Correct (1/1 point)

Calico host endpoints can be used to:

1/1 point (ungraded)

- [x] Secure the host interfaces to the underlying network
- [ ] Secure physical hosts on-premise or private cloud but not public cloud virtual machines

- [x] Secure the host interface to pods
- [x] Secure the host loopback interface
- [x] Secure Kubernetes node ports

✔

Submit

✔ Correct (1/1 point)