iSCSI traffic in flight

All iSCSI traffic from that SVM must be protected with IPsec “in-flight” encryption between the SVM’s IP addresses and the iSCSI initiators.docs.netapp+2

Key requirement

ONTAP does not provide protocol-level encryption for iSCSI itself; the only supported way to encrypt iSCSI data in transit is to use IPsec. NetApp explicitly states that IPsec is the only option for in-flight encryption of iSCSI traffic.netapp+1

What must be done

To ensure all iSCSI traffic is encrypted for that SVM, the administrator must:

- Enable IPsec on the ONTAP cluster.docs.netapp+1
- Create IPsec security policies (SPD entries) that match the SVM’s iSCSI LIF IP subnets and the initiators’ IP subnets, specifying the encryption suite and authentication (pre-shared key or certificates).docs.netapp+2
- Configure the iSCSI initiators with matching IPsec settings so that all traffic between the initiator and the SVM LIFs is carried inside IPsec.netapp+1

In exam-style wording, the correct action is: “Configure IPsec encryption for the SVM’s iSCSI LIFs and initiator IP addresses so that all iSCSI traffic uses IPsec in-flight encryption.”