kentik

SENDING FLOW DATA TO KENTIK DETECT

Using Kentik Detect — whether in Public SaaS or Private SaaS configuration — involves enabling the cloud-based Kentik Data Engine (KDE) to ingest network flow records from your managed environment/devices. Flow data (NetFlow v5/v9, sFlow, and/or IPFIX) may be sent to KDE using any of the three techniques described below, all of which are in regular production use across the Kentik Detect user community.

DIRECT TRANSMISSION TO KENTIK PUBLIC IPs

The first and simplest approach is to configure your flow-generating devices to transmit flow data directly to Kentik's public VIPs, which you'll find on the Admin » Devices page of the Kentik Detect portal.

SECURE TRANSMISSION VIA KENTIK ENCRYPTING AGENT

Another common approach is to use Kentik's NetFlow proxy agent. The agent gathers flow records in your local environment, encrypts them, and transports the encrypted data to KDE. The Kentik agent software is available for download from Kentik and can run in a VM or on a local host.

SECURE TRANSMISSION VIA DIRECT NETWORK CROSS-CONNECT

Organizations that have a direct network presence in Equinix have another option, which is to establish a Private Network Interconnect (PNI) to the KDE cluster. This fully private link is the most secure approach.