**Product Overview: Sycope Probe** is a powerful, purpose–built network monitoring appliance designed for real–time traffic analysis. By continuously analyzing data packets at line rate speeds, the Sycope Probe produces comprehensive NetFlow, IPFIX, and metadata, pro–viding complete visibility into network usage and behavior.

Sycope Probe, at its core boasts, a high–performance packet analysis engine capable of processing traffic at multi–Gbps speeds. By examining data traffic, Sycope Probe creates detailed records of communication between endpoints. These records include: source/destination IPs, packet/byte counts, timestamps, and much more, furnishing administrators with crucial insights for capacity planning, security, troubleshooting, and other tasks.

Sycope Probe supports both NetFlow (v5/v9) and IPFIX, offering flexibility in how flow records are ex–pored. **Application–layer visibility allows administrators not only to see volumetric traffic data but also to identify specific applications and protocols in use on the network.**
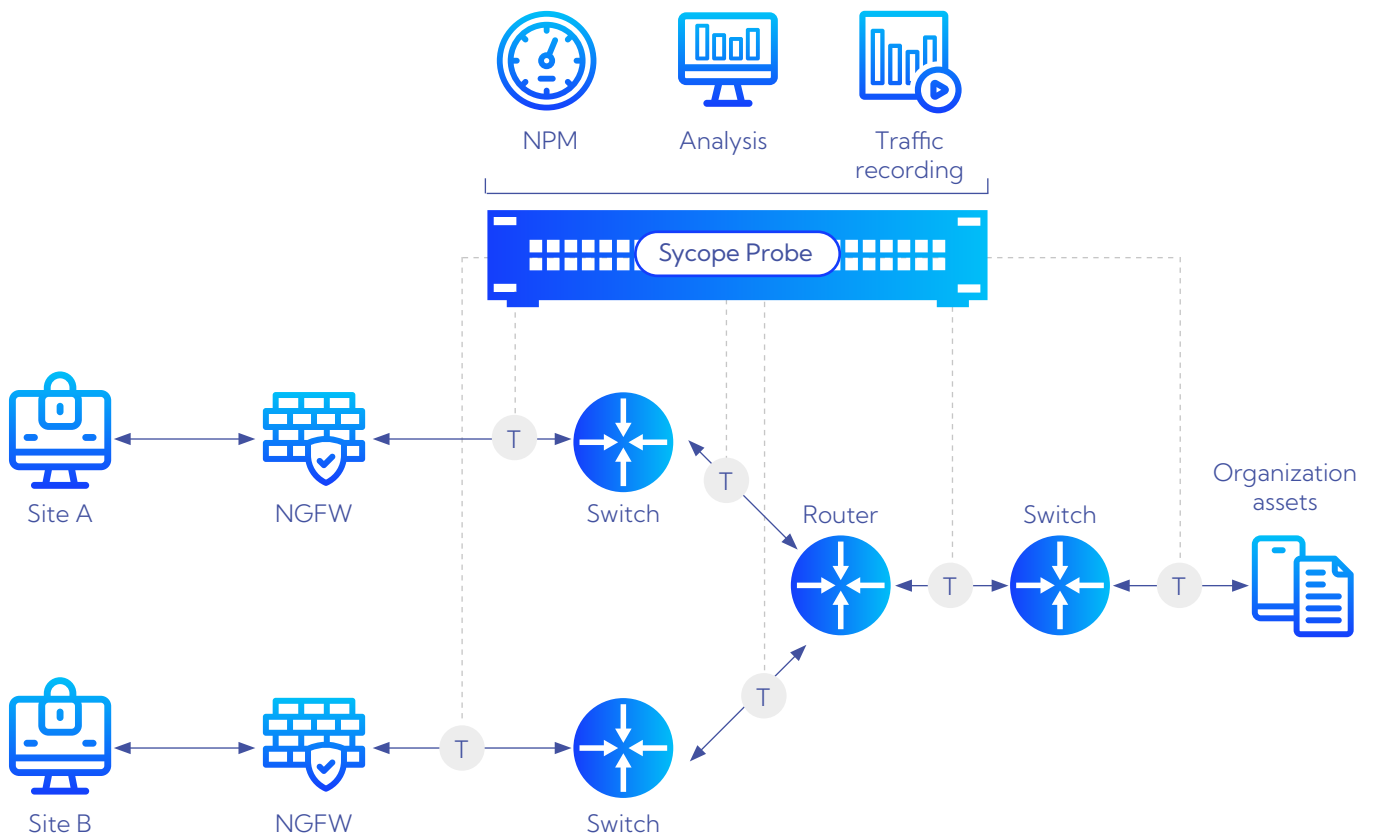


**Sycope Probe offers a comprehensive suite of features and capabilities, empowering organizations to:**

| enhance network visibility | expand cybersecurity | optimize network performance |
| --- | --- | --- |

# Benefits

### Complete Troubleshooting and Diagnostics

Real-time flow monitoring provides an end-to-end understanding of the performance of the entire IT environment. This offers comprehensive monitoring and analytical tools to handle high-speed, modern network infrastructures. Alongside real-time flow monitoring Sycope Probe can packet-capture on demand.

### Ensuring Accurate NetFlow Generation in Cases of Exporter Failures

If you can't or don't want to use your network devices as NetFlow exporters, you can still generate dependable flow data and metadata, as well as record the traffic by using a probe appliance. Sycope Probe is offered as both hardware and a virtual appliance, allowing you to monitor your entire network infrastructure effectively.

### Visibility into L7

Most of the NetFlow exporters provides only L3, L4 and volumetrics information. Sycope Probe as dedicated appliance which sees every packet of the communication, can analyze L7 data and enhance IPFIX with it.

### Easy Deployment and Management

Sycope Probe is designed for swift and simple deployment. A user-friendly web UI assists administrators with configuration and setup. The Sycope Probe integrates smoothly into various environments, boasting support for all major flow technologies, interface types, and L2-L4 protocols.

### Adaptable Scaling Options

Thanks to its modular design, administrators can add more Sycope Probes as required, covering increasingly extensive network sections. This scalability ensures consistent growth while safeguarding your monitoring investment. It can also monitor links ranging from 1Gbps to 100Gbps, offering significant scalability.

Sycope Probe is hardware-neutral software. It capitalizes on advanced commercial platforms based on diverse CPU architectures (X86/PowerPC/ARM) and is **available in both physical and virtual environments**. This ensures a quick migration of network visibility functions to cutting-edge hardware, coupled with a highly competitive cost structure. With its capability to offer full packet-level visibility through real-time flow analysis, **Sycope Probe equips users with the intelligence necessary to manage modern network infrastructures and workloads**.

# Key features

Sycope Probe's key features that enhance network visibility and security include:

| | |
|---|---|
| NetFlow/IPFIX Data Records | Sycope Probe can generate and export flow records in standard formats (NetFlow/IPFIX) to various collectors, enhancing compatibility with different legacy equipment and minimizing performance impacts. |
| Metadata Generation | Sycope Probe tracks Indicators of Compromise (IoC) such as URLs and patterns, creating metadata summaries for SIEM solutions. This reduces data volume substantially, enabling more in-depth analysis. |
| API Integration | Sycope Probe provides a RESTconf API for integration, facilitating show, add, and edit operations on filters. |
| Packet Capture | Sycope Probe can store traffic data to disk in pcap format or transfer it to internal/external storage for offline analysis. |