sycope

flowcontrol

Visibility, Because We Care

What applications are used? Are they all legal? What servers and hosts are the source of the network traffic? Are these actually servers? Is the operator's incoming traffic properly marked? Which interfaces of routers show the highest load? Where does the traffic come from and where does it go?

Sycope FlowControl gives you a prompt answer to these questions

Network Engineers around the world are getting similar tasks. Their tasks regarding the improving of network performance is increasingly important to the success of the digital business projects. Every day most of them start a day at work with one mission to complete – providing security and usability of the network. They have knowledge and experience, but Sycope provides additional great visibility in the context of network traffic.

Visibility, because we care.

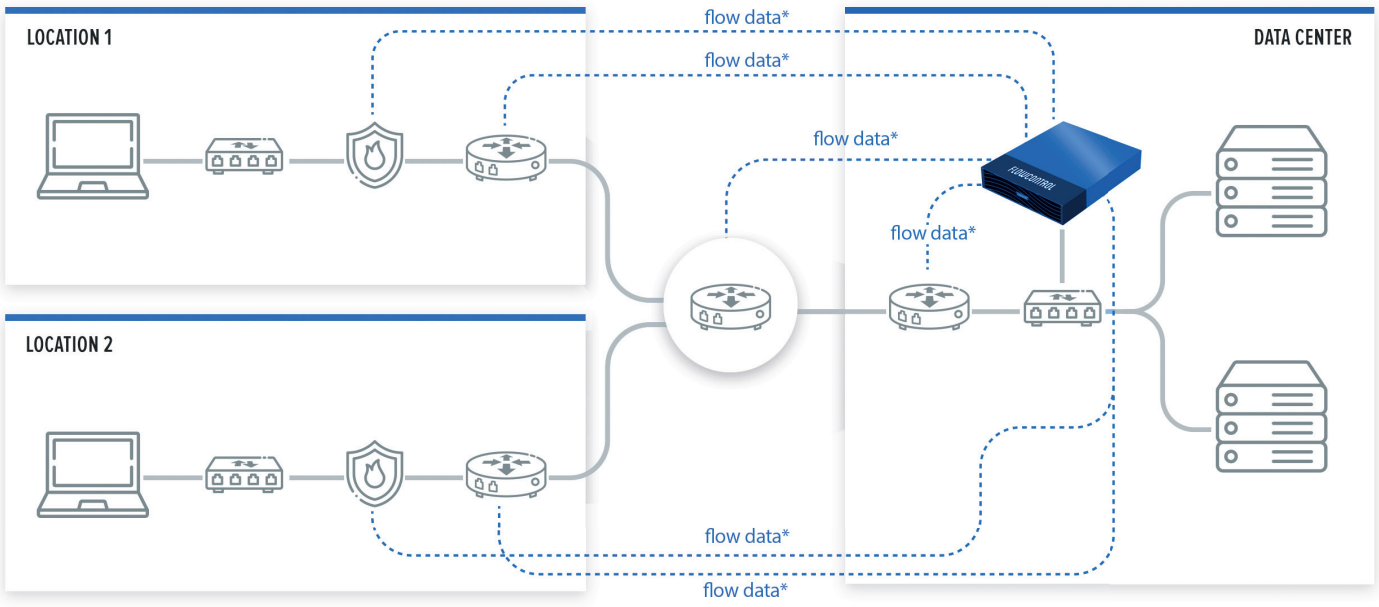
Sycope FlowControl was created by engineers for engineers to deliver just the necessary information on time. Connect and use – a single day of implementation is sufficient – key information, KPIs and security rules are available immediately after the first data are obtained. Furthermore, in Sycope, huge amounts of network data do not have to mean spending hours of tedious analysis on it. Thousands of hours spent analysing multiple organisation infrastructure resulted in ready-to-use scenarios and an advanced view such as tables, charts, graphs and metrics presented in a legible manner. All of them are practical, easy to use and allow for quick identification and analysis of the network issue.

FlowControl key features

- Visualisation of network connections, geolocation.
- Identification of applications and hosts responsible for network load.
- Detection of incidents, security policy violations, DDoS attacks, undesirable communication.
- High efficiency (250,000 flows per second) and speed.
- Functional validation of the QoS policy.
- Detection and mitigation of DDoS attacks.
- Network traffic analysis at the level of a single TCP/UDP port.
- Verification and analysis of L3 network segmentation.
- Network Address Translation (NAT) monitoring using translation information and NetFlow statistical data.
- Cyber Threat Intelligence (CTI) helps filter and prioritise the immense volumes of complex cybersecurity information organisations are forced to deal with today.
- Flexible tools for data analysis based on big data mechanisms, e.g. Google search.
- Easy installation and configuration – basic implementation where a base flow export configuration takes one day.

What is FlowControl?

FlowControl is a dedicated solution for network traffic analysis and threat detection, using the NetFlow, SFlow, IPFIX and NSEL protocols. The main tasks of the system are the collection and analysing of data. The system records, processes and analyses all the parameters contained in NetFlow and related protocols, enhanced by SNMP data, geolocation and editable blacklists and whitelists of IP addresses. With FlowControl you can diagnose Network issues in your organisation, including network connection settings, or the so-called bottlenecks in network communication. The system analyses, among others, TCP/IP parameters in layers 3 and 4 (source and target IP address, protocol, port), traffic attributes, as well as interface numbers by traffic direction (incoming/outgoing), including the IP addresses of NetFlow generating network devices. The security system was implemented and created based on the ATT&CK MITRE methodology. The usage of BGP FlowSpec enables the mitigation of DDoS attacks. FlowControl offers many of advanced indicators, reports and summaries based on the practical experience of the engineers who created this solution, gained during 20 years of work for the largest companies and institutions in the world.



**flow data – shall be understood asNetFlow v5 v9, NSEL, IPFIX, sFlow.*

Implementation of the FlowControl system in a network on the example of a two-branch company.

Flexible data analysis mechanisms

- Visualisation of data relating to the entire network, groups of parameters or individual parameters (port, interface, host, IP) in any time window.
- • Easy top-down access – with just a single click, the drill-down mechanisms enable viewing of data for a specific port, interface or IP number.
- Advanced discovery methods of security incident context.
- Maintaining the time context and filters between views.
- The possibility of saving complex search filters and time context (bookmarks).
- The XND module uses data from the NetFlow protocol to detect DDoS attacks on specific services performed by a monitored group of hosts. The system analyses DDoS parameters within the defined time frames and enables the blocking of a service via FlowSpec.
- Flow Filtering function gives the customer the possibility to filter input NetFlow data focusing only on the important information, which improves the Mean Time to Resolve (MTTR), improves retention metrics and facilitates drilldown & search operations.
- Flow Forward function gives the customer the unique option to simplify configuration on the network devices, allowing a single destination of the NetFlow export and eliminating NetFlow traffic duplication load. FlowControl, for instance ,will gather and analyse but also simultaneously forward all the NetFlow traffic to 3rd party solutions, allowing all systems to work on the same data.
- Support for IPv6.

Alerting and reporting system

In terms of alerting, it is using advanced mechanism allowing for creating multiple logical conditions in a single rule:

- Alerts are generated based on meeting predefined conditions, e.g. after exceeding the set limit for using a particular port or application traffic volume.
- An alarm message is sent by email, Syslog or an SNMP trap.
- Alerting mechanism allows to have multiple logical conditions in a single rule.
- Reporting system – allows you to summarise network and security parameters and send reports directly to your email.

High efficiency

- All Views are generated without the need for constant data reloading.
- Negligible load on the network and network devices.
- Flexible managing of data retention.

Accessible administration tool

- The system has been provided with interactive dashboards including diagrams, graphs, tables and maps displaying important information which simplifies and speeds up the process of handling network issues, enabling fast access to crucial information.
- Clear dashboards delivering reliable and comprehensive information.
- Only one day of implementation is sufficient to ensure that key information, metrics and KPI are available immediately after the data is collected.
- The self-explanatory nature of FlowControl means that it does not require dedicated training sessions; IT staff can start working immediately after the implementation process has been finished.
- Data retention function allowing for storing flows for a custom time period.

Innovative in each step

- The security model is built on the MITRE framework; Sycope was the first on the market to integrate MITRE in a Network Monitoring System based on NetFlow.
- Smart deduplication retains unique information from multiple records, only presenting actual traffic volume, regardless of the filters applied.
- Searching for data in the system using analysis tools like Google search and peripheral vision.

Comprehensive system administration tools

- Granularity of permissions to individual system components and views for different groups of users.
- Possibility of authentication through the LDAP protocol or Radius service.
- Update Portal containing all system updates for both XN and XNS modules available 24/7.

FlowControl consists of three fully integrated modules – XN, XNS and XND.

- The XN module is the primary module, acting as a collector and at the same time enabling monitoring and analysis of network traffic.
- The XNS module contains numerous rules and algorithms that analyse IT security incidents.
- The XND module is responsible for the detection and mitigation of DDoS attacks.

FlowControl XN
Network Performance & Visibility

FlowControl XNS
Detection of
Security Threats

FlowControl XND
DDoS/DoS mitigation

FlowControl XN — network monitoring

FlowControl XN gathers and analyses data recorded with NetFlow, SFlow, IPFIX and NSEL protocols for network performance and capacity.

Fast access to critical information

The system was provided with interactive diagrams, tables and maps containing critical data, statistics and indicators, enabling the analysis of network behavior patterns and supporting the incident handling discovered issues. It offers the following functions, among others:

- Detailed statistics of the most active hosts, applications and interfaces.
- Information on network traffic in the context of incoming and broken down into incoming and outgoing streams.
- Lists of connections per IP address, protocol, port, country, ASN or QoS.
- Data on bandwidth and interface load generated by hosts, applications, services and users.
- Information on incoming and outgoing traffic, including

A simple and clear graph shows the stations generating the most traffic as well as applications that support it and interfaces with the highest utilization.

geolocation and ASN mapping for public IP addresses.

- Paths of network traffic for monitored devices presented in flexible views.
- Statistics to monitor proper configuration and implementation of the QoS policy in place.
- Automatic refreshing of daily, weekly and monthly historical data. Large selection of the data search period (hour, day, week, month, quarter, year and custom date.
- Analysis of extra NetFlow fields: Type icmp, Code icmp, headlines for IPv6, routing headlines IPv6 based on types, routing headlines IPv6 based on included addresses, flow label IPv6.

Easy access to external services

- The system enables access to external services, such as VirusTotal, directly from the view under analysis (using right click button) and further analysis of data.
- Feeds server – dynamic identification of the global threats based on integration with the Sycope Cyber Threat Intelligence (CTI) platform.

NetFlow deduplication

If the flows are duplicated from multiple sources, FlowControl deduplicates data in order to retain a unique information record only. Apart from its other benefits, the deduplication mechanism allows the following:

- Presentation of actual traffic volume values, regardless of the filters applied.
- Displaying the traffic path based on NetFlow fields received for the same transmission from multiple routers.

Cisco ASA firewall monitoring

By supporting Cisco ASA/NSEL devices, the system enables full access to traffic network at firewalls, which are often the only Layer 3 devices at a specific location and, thanks to that:

- Enables data analysis for firewalls only.
- Eliminates inconsistencies in a situation where NSEL statistics are combined with typical NetFlow data sent by other devices.
- Supports NSEL fields that go beyond a NetFlow record.

NetFlow analysis including autonomous systems (AS)

FlowControl is designed to meet the needs of different sized organisations from medium-size to large operating multiple connections. Supporting autonomous system (AS) technology for BGP enables the following:

- Viewing and filtering data based on AS numbers.
- Visualising traffic paths based on source/transit AS.
- IP to ASN mapping automatic and manual (in case of the need for a custom ASN name).

Advanced analytics

The system offers advanced analytics including:

- Network Address Translation (NAT) – extended NetFlow analysis based on NAT fields exported mainly from edge routers and firewall devices gives an analyst a simple way to match the traffic crossing private and public subnets or networks. Furthermore, additional path monitoring visualisations facilitate investigations of network issues and post incident evidence gathering.
- MPLS – extended Netflow analysis based on MPLS fields exported mainly from core routers gives an analyst MPLS labels analysis options.

Grouping NetFlow statistics

- Presentation and analysis of network segmentation for user-defined groups mapped by location, function or business role.
- Groups may be analysed both for outgoing and incoming traffic.
- Increased analyses provided by expansion of the event generation system with priorities, additional metrics, and thresholds for triggering events.
- Packet size analysis - extended Netflow analysis based on Min packet Length and Max Length fields allows an operator to investigate traffic issues resulting from both nonstandard communications patterns and performance problems symptoms, both on the network devices and transmitting endpoints.

The distribution of traffic by key applications with the details of each of them facilitates the identification of network problems related to a specific application.

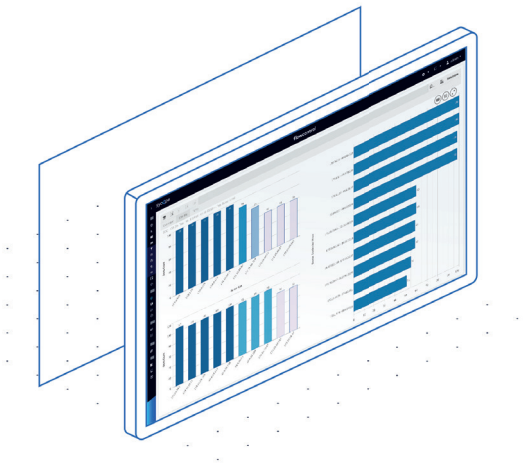
FlowControl XNS – IT security

The XNS module is an extension of the FlowControl XN system, used to detect and analyse security anomalies and threats in the context of the entire organisation. It uses tactics and techniques of threats referring to the ATT&CK MITRE methodology. FlowControl XNS uses two independent engines – Threat Detection and Threat Analysis. The Threat Intelligence engine generates alerts based on correlation with reputation lists of IP addresses and suspicious countries. The Threat Detection engine detects threats based on correlation and aggregation of connections between the values of various parameters and statistics of NetFlow and similar protocols.

Detection of attacks, tactics and techniques

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies both in the private sector, and in government. The use of the ATT&CK MITRE methodology enables detection of security threats and analysis of events sequences in the context of tactics used by cybercriminals. The XNS contains more than 50 rules regarding seven MITRE tactics: Command and Control, Credential Access, Discovery, Exfiltration, Impact, Initial Access and Lateral movement. Examples of threats detected by the XNS.

Technique	Threats examples
Application Layer Protocol	Cleartext Application OT Device Discovered IP Reputation Risks: Malware, Open DNS
Non-Standard Port	Suspicious Port
Proxy	IP Prox TOR
Man-in-the-Middle	Unauthorised LLMNR/NetBIOS Activity
Brute Force	Brute force attack
System Network Configuration Discovery	Abnormal flows ratios Unauthorised NFS Export Outside The Local Network
Network Service Scanning	Horizontal Scan Vertical Scan Multicast DNS (mDNS) from the Internet Unauthorised NFS Export Outside The Local Network Unprotected Docker Daemon Virus Outbreak
Permission Groups Discovery	Unauthorised Internet Access Unauthorised DHCP Activity Unauthorised DNS Activity
Data Transfer Size Limits	High Data Transfer Unusually High Data Transfer SPAM
Endpoint/Network Denial of Service	DDoS DNS Amplification Attack DoS - ICMP Flood DoS - TCP Flood DoS - UDP Flood
Drive-by Compromise	P2P Activity
Phishing	Phishing SPAM
Remote-Dienste	Unauthorised RDP Connection
Ressourcen-Hijacking	Crypto Mining



Top 10 IP addresses generating the most suspicious activity.

Sycope CTI (Cyber Threat Intelligence)

Security feed algorithm implemented in Sycope CTI actively monitors number of sources, analyses, and generates a unified list of current Indicator of Compromises (IoCs), based on which FlowControl is able to detect threats related to a reputation risk. Sycope CTI refresh IoC a few times per day, which gives high quality of the delivered security feeds and thus reduces the number of false alarms.

Security Operating Centre

The XNS module was equipped with diagrams, indicators and tables adapted to the specifics of SOC team operations, based on NetFlow protocol analysis:

- Rapid detection of threats to the organisation level, taking into account various alert categories.
- Analysis of dynamics of changes of numbers and type of suspicious events in a minute-by-minute frame.
- Conducting analysis by the type of attack, suspected source and target hosts, and applications.
- Detailed analysis of the source and cause of a given security alert through detailed NetFlow statistics, available with a single click.

Risk analysis

Key indicators referring to the risk level are presented in weekly summaries and enable the tracking of trends and assessment of effectiveness of undertaken preventive actions. Separate, dedicated dashboards present:

- Information about the number of attacks, divided by techniques and tactics used by cybercriminals.
- Risk assessment indicators generated take into account the severity of alerts and hosts to which the anomalies and threats apply.
- Key Performance Indicators prepared for managers, enabling the conducting of management analyses.
- Data which enable the assessment of the degree to which the regulatory requirements, standards and rules (such as UoKSC, CIS) are met.

Limiting the number of false positive alerts

The XNS module has been equipped with multiple mechanisms, which enable the configuration of alerts, adapting them to the specifics and needs of the organisation and adopted security policy. They include, among others:

- A configurator which enables a quick activation and de-activation of individual security rules.
- User friendly configurator with a graphical interface, which enables – in a simple way – rules attributes.
- Editable whitelists containing a set of trusted IP addresses, which may be used directly in the rules.
- Integrations with external services to perform verifications of suspicious IP in other reputation databases.

Access to the knowledge database directly from the application

- The interpretation of detected events is aided by both a built-in knowledge database and links to external reputation services available with a right mouse button click, e.g. Virustotal.
- An accessible description of a security alert supplemented with additional information and a link to a full description of the tactic or technique in question on the ATT&CK MITRE website facilitate the analysis of the given event in a wider context. Techniques classified by MITRE are known by security experts all over the world, so our rules are understandable to IT Security.

Build-in analytical scenarios

The scenarios implemented in the module facilitate analysing and drawing conclusions concerning the most important security-related aspects.

- Use Cases of the threat analysis enables the identification of the most suspicious IP addresses, and then the analysis of correlations with other IP addresses or other network artifacts.
- Scenarios used for the analysis of internal or external attacks enable multi-dimensional analysis of the suspected IP address (or group of addresses):
  - Presentation of tactics and techniques used during attacks and generated alerts.
  - Analysis of the direction of attacks and participating hosts, taking into account source and destination addresses.

Quick access to information about the most common threats, detected by the Threat Intelligence engine.

Integration with other systems modules

- The FlowControl XNS module is integrated with both the XN module and the XND module.
- Transferring filters defined in the XNS module to the XN module facilitates a detailed analysis of the incident or source of the alert.
- XNS module enables forwarding security alerts to external systems, such as SIEM including QRadar, ArcSight and Splunk.

Description of tactics and techniques used in the attack facilitates the assessment of attackers' intentions.

FlowControl XND

The Anti-DDoS XND module uses data from the NetFlow protocol to detect DDoS attacks on specific services performed by a monitored group of hosts, enabling use of BGP FlowSpec to block the attacks.

Attack mitigation

The module enables the identification and mitigation of both single and multi-vector DDoS attacks of varying intensity. Based on the FlowSpec protocol, it propagates traffic filters to edge devices. The module detects:

- Volumetric attacks, which reduce the availability of the service by saturating a network connection.
- Protocol attacks, which use a specific property or vulnerability of a given protocol.

Basic information about DDoS attacks grouped in one place.

Flexible attack detection rules

The XND module monitors changes of flows characteristics using static and dynamic parameters.

- Static parameters enable the definition of values used in the process of attack identification, e.g. the number of source IP addresses, bytes, flows.
- Dynamic parameters enable establishing the allowable deviations from the baseline, created by comparing the current and historical traffic characteristics.
- The possibility of adapting limit values of parameters to individual groups of devices and applications facilitates the scaling of the system, both for the entire organisation and taking into account specific services or subnets.
- The possibility of manual IP addresses blocking – allowing you to protect your system from unwanted traffic.

Advanced DDoS analysis

The module includes predefined dashboards for multi-dimensional attack analysis, presenting among others:

- Attack start time and end time in the context of the attacked service and group to which the attacked host belongs.
- Type of attacked service, e.g. HTTP(s), FTP and DNS.
- Characteristics of DDoS parameters during the attack, e.g. the number of source ASNs, IP addresses, network flows, packets, bytes, and also PPF (Packets per Flow), BPP (Bytes per Packet).
- Multidimensional visualisations showing the characteristics of network traffic during D/DDoS attacks.

Graphical analysis of DDoS parameters.

Sycope is focused on designing and developing highly specialised IT solutions for monitoring and improving network and application performance as well as IT security both in on-premise architecture and in hybrid, private and public cloud environments.

Our solutions were created and developed by engineers, who have been working on the issues of network performance, application efficiency and IT security for over 18 years. Using the solutions from global APM/ NPM and SIEM providers, they have completed more than 400 projects for such customers as Franklin Templeton Investment, The Ministry of Defense, NATO, National Bank of Poland, T-Mobile, Ikea, ING Group, Orange and Alior Bank. In addition to many successful implementations, the team's competence has been confirmed by many individual certificates, including: personal security clearance up to 'Confidential' and 'NATO Secret' clauses, CISA, CISSP, ISO 27001 Lead Auditor, IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Certificate AS Data Platform Technical, Certified Ethical Hacker, and Offensive Security Certified Professional.

This made them convinced that engineers who work in large organisations do not need a system that presents all available data about networks, devices and applications. What they need instead is selected, specific information presented as rapidly as possible. That is why the new system called Sycope has been created.

Poland:
Goraszewska 19
02-910 **Warsaw**

Ireland:
The Sweepstakes
Ballsbridge
Dublin D04 C7H2

Czech Republic:
Freyova 12/1,
190 00 **Praha**

contact@sycope.com
www.sycope.com