FlowControl is a dedicated solution for network traffic analysis and threat detection, using the NetFlow, SFlow, IPFIX and NSEL protocols. It functions as both a data collector and analyser. Among others, its functionalities include: diagnosing problems in network infrastructure, including network connection settings, or the so-called bottlenecks in network communication. It provides detailed information on the traffic generated by users, communication between servers and applications. It enables error monitoring and anomaly detection in the user’s environment. Implemented and created based on the ATT&CK MITRE methodology, the rules and mechanisms for the detection of security incidents enable the detection of attacks and undesirable activities in the network. The use of BGP FlowSpec enables the blocking of DDoS attacks. FlowControl offers a number 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.

Key features of the solution

• High efficiency (250,000 flows per second) and speed.
• Flexible tools for data analysis based on big data mechanisms, e.g. Google search.
• Detection of incidents, security policy violations, DDoS attacks, undesirable communication.
• Visualisation of network connections, geolocation.
• Identification of applications and hosts responsible for network load.
• Functional validation of the QoS policy.
• Detection and neutralisation of DDoS attacks.
• Communication analysis at a level of a single network port.
• Verification and analysis of L3 network segmentation.
• Easy installation and configuration – basic implementation where a base flow export configuration takes one day.
Comprehensive network traffic analysis

FlowControl is built 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 blocking of DDoS attacks. FlowControl 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. 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. To monitor every network of any complexity and architecture, a single virtual appliance is sufficient, which lowers investment costs and reduces implementation time.

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 behaviour patterns and supporting the detection of anomalies and causes thereof. It offers the following functions, among others:

- Detailed statistics of the most active hosts, applications and interfaces.
- Information on network traffic broken down into incoming and outgoing streams.
- Lists of connections, including protocols, ports, IP addresses and traffic profile for respective connections.
- Data on bandwidth and interface load generated by applications, services and users.
- Information on incoming and outgoing traffic, including geolocation of public IP addresses.

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

2. 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.
• NetFlow-generating and related devices located in maps and plans.
• Statistics enabling the assessment of proper configuration and implementation of the QoS policy in place.
• Automatic refreshing of daily, weekly or monthly historical data analysis results.

Easy access to public sources
• The system enables access to public sources, such as VirusTotal, directly from the view under analysis (using right mouse button) and further analysis of data.

NetFlow deduplication
If the flows duplicate 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 to 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.

Grouping NetFlow statistics
• Presentation and network segmentation analysis for user-defined groups broken down by location, function or business role.
• Groups may be analysed both for outgoing and incoming traffic.

NetFlow analysis including autonomous systems (AS)
FlowControl is designed to meet the needs of large organisations 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.
• Presentation of the sources, targets and traffic distribution across connections or operators.

FlowControl — a prompt answer to key question

• What applications are used? Are they all legal?
• Who uses the applications?
• What servers are the source of the traffic? Are these actually servers?
• Which servers are reached by the traffic? Should they be reached?
• What applications generate the highest traffic?
• Who occupies all the available bandwidth?
• Is the operator’s incoming traffic properly marked?
• Which interfaces/routers show the highest load?
• Is the own and transit traffic being properly routed?
• Is a sufficient bit rate ensured by the connections?
• Is the traffic being properly directed?
• What applications run on the servers?
• What ports are used by the servers?
• Where does the traffic come from and where does it go?
• What servers generate the traffic? Is it legal?
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 rules and algorithms built on the basis of ATT&CK MITRE methodology and two independent threat detection engines – Threat Intelligence and Threat Detection. 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

The use of the ATT&CK MITRE methodology enables both detection of incidents and analysis of event sequences and tactics used by cybercriminals. The XNS module contains 65 proprietary rules which detect, among others:

- Attacks that intend to circumvent security features.
- Credential-based attacks, e.g. "brute force" type attacks and LLMNR/NetBIOS communication-based attacks.
- Forbidden network activities, including port scanning, attempting to gain unauthorised access to specified services, and also anomalies in network traffic.
- Remote access-based attacks, e.g. through RDP.
- Activities which indicate C&C attacks, including, among others:
  - Activities on suspicious ports (based on blacklists and whitelists).
  - Non-encrypted connections to critical servers and services.
  - Connections with suspicious IP addresses, e.g. Botnet, Malware, C2, Ransomware.
  - Security policy breaches consisting of the use of TOR, Open DNS or Open Proxy, prohibited P2P activities.
  - Potential data leaks.

Security Operating Center

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 at 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.

Minimisation of the number of false positive alerts

The XNS module was 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 the rapid activation and deactivation of individual security rules and of alerts which they activate.
- A legible editor with a graphical interface, which enables the rapid and convenient change of parameters used in the rules.
- Editable whitelists containing a set of trusted IP addresses, which may be used directly in the rules.
- Ready-made interfaces which enable the connection of external feed databases and additional verification of risks related to a detected incident.

Access to the knowledge database directly from the application

The interpretation of detected events is aided by both a built-in knowledge database and by links to specialised websites available with a right mouse button click.

- 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.
- Suspected IP addresses may be verified in external sites (e.g. VirusTotal) directly from the XNS module.
Ready-made analytical scenarios

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

- A hazard analysis scenario 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.

Integration with other systems

The XNS module is integrated with the XN&XND modules and enables the exporting of data to SIEM class systems.

- Transferring filters defined in the XNS module to the XN module facilitates a detailed analysis of the incident or source of the alert.
- The possibility of exporting alerts with their call parameters to SIEM systems, including, among others, QRadar, ArcSight and Splunk.

FlowControl XND – anty DDoS

The 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.

Flexible attack detection rules

The XND module monitors changes of flow 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
itates the scaling of the system, both for the entire organisation and taking into account specific services or subnets.

Advanced DDoS analysis

The module has predefined dashboards for multi-dimensional attack analysis, presenting, among others:
- Attack start time and attack 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).

FlowControl

High efficiency

- Views are generated without the need for constant data reloading.
- Negligible load on the network and network devices.
- Scalable mass storage enables to flexibly manage data retention periods.

Alert system

- Alerts are generated on meeting pre-defined 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.

Flexible data analysis mechanisms

- Presentation 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.
- Searching for data in the system using analysis tools like Google search.
- 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 to block a service via FlowSpec.

Versatile system administration tools

- Separate accounts for the system administrator and users allows to determine their respective permissions with greater precision.
- Possibility of authentication through the LDAP protocol or Radius service.
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 the 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, 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.