The Top 14 Netography Fusion® Queries

Netography Query Language (NQL) Enables Security Teams to Search Enriched Flow Records and Create Custom Searches

Introduction to Netography Fusion:

Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud and edge environments. With the Netography Fusion platform, these teams gain visibility to network traffic and context across data, applications, devices, and users, and see what they are, what they are doing, and what's happening to them.

Netography Fusion enables organizations to greatly reduce cyber threat risks and costly downtime with remediation automation capabilities through alerts, custom detections, and integrations.

Unified visibility of network flows

Within minutes and without hardware, complicated network taps, and packet inspection agents, your team can monitor firewalls, routers, switches, load balancers, multiple cloud networks, and even devices that you've never had visibility of due to a lack of agent support, or encrypted network traffic, or complex global network topographies.

Ingest and leverage NetFlow, sFlow, and cloud flow for security

Netography Fusion is device type and flow type agnostic and ingests, enriches, and normalizes all flow data in real-time and continuously. Network Security pros are able to see all network traffic and get insights into North-South, East-West, On-Premises to Cloud, and Cloud to Cloud traffic all in one modern SaaS portal.

Add context to all traffic flows

With Netography Fusion's tagging and context labeling, your teams can visualize networks by application, location, compliance groups or any other scheme. The UX/UI is designed by network and security pros for

pros and has several unique, time-saving data points that enable analysts to “pivot” quickly, saving time and fatigue. Your analysts will quickly be able to answer questions like: “Who is talking to whom? Over what port? Is it being blocked or not? Where is that data going?”

Comprehensive and Easy to Use Search Capability

Netography Fusion’s Netography Query Language (NQL) is comprehensive yet familiar and enables security pros to search enriched flow records, create, save and use custom searches to rapidly analyze, investigate, and respond to suspicious traffic or incidents. For example, you’ll be able to isolate and analyze specific traffic, geo activity, bad-actors configurations, and more. It’s the industry’s most granular, flexible flow record search capability, and when combined with custom saved search flows, alerts, and saved searches can be applied to new or pre-built dashboards.

The Netography Query Language (NQL) is the basis for accomplishing many tasks within the product. Some examples are: searching for flows, alerts, or interfaces or filtering statistics and aggregations or defining custom algorithms to alert on.

Useful NQL queries help your teams pull insightful data from all your flow logs

Security Analysts:

Security analysts research and maintain an understanding and awareness of the overall cyber threat landscape (advanced persistent threat groups, malware campaigns, botnets, hacktivism, DDoS attacks, geopolitical activities, etc.) or identifying critical business needs or intelligence collection priorities, NQL queries are a powerful research platform. Whether they are following up on new open source intelligence (OSINT) or leveraging proprietary threat feeds to gather intelligence about threat methods and actors, Netography’s NQL capability will enable a seamless collaborative approach from search to alert to detection to remediation, all designed to support the organization’s defensive posture.

Incident Responders:

Working with established playbooks or documented response plans for cybersecurity incidents to minimize business impact, incident responders will be able to lead the collection and management of network security operations metrics and measures and produce high-quality outcomes and timely service delivery. With Netography’s real-time ingestion and the ingestion of global flow logs, incident responders can react quickly and limit the blast radius of new attacks.

Threat Hunters:

Threat hunters can harness vast amounts of flow data and use creative investigative techniques to identify & analyze adversary tactics, techniques, and procedures (TTPs). They will quickly develop and implement new security controls and detections based on various attack vectors.

Forensics:

Analyzing network data is a key component of any forensics investigation as your Forensics Analysts focus on emails or mobile network connections or the attack path that was used by the threat actor to breach the networks and cause an incident. With Netography Fusion's NQL capabilities, they can capture accurate detail and write a report based on their findings or provide evidence to other teams inside or outside the organization.

Easily Turn NQLs into Alerts and Detection Models

Your security and network teams can easily turn NQL into Netography Detection Models, which can generate alerts and automated remediation. For example, any NQL you create to discover specific traffic East-West, Geo-Activity, Bad Actors, or Systems Conf or Compliance Enforcement can become a custom Detection Model. The custom detection model configuration page in the Netography Fusion portal will automatically pull in the saved NQL and make it available as an algorithm for the detection model. With a few additional configuration options, including descriptions, thresholds, and alert policy, your team will greatly improve your security posture.

A list of the top Netography Query Language (NQL) Use Cases and some example queries.

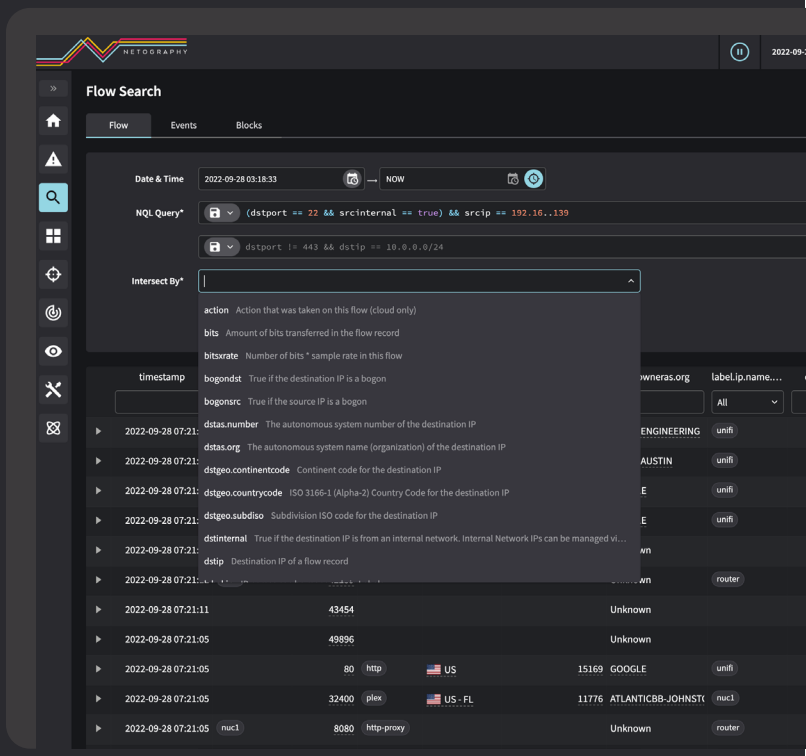
These sample and easy-to-use NQLs can be used for numerous security and network use cases. We have categorized these and provided a base query that you can customize to your own infrastructure and network topography.

Query examples include:

Search for flows, alerts, or interfaces
Filter statistics and aggregations
Define custom algorithms to alert on

Becoming familiar with NQL is easy for most users who have used similar tools before. These generic rules apply regardless of where in the service you leverage the query language:

Logic must be unambiguous. e.g., `A && B || C` will fail. Use parens to prevent ambiguity. IP fields can be searched with CIDR notation if desired. `10.0.0.0/24` will match `10.0.0.1`
Only integer fields can use numerical comparisons. `< <= > >=` Strings with spaces must be quoted with single quotes. Allowed Boolean operators are: `&& AND` and, || `OR` or, and `!` Allowed numerical operators are: `== != < <= > >=`



Search for and alert on specific traffic - for example, East/West or North-South or compliance requirements or in a forensics investigation

Name	Outbound traffic
Goal	Discover misconfigured deployments
Benefit	Prevent application issues or data leakage
Sample Query	`srcinternal == true && dstinternal == false`

Name	Internal traffic
Goal	Discover misconfigured deployments
Benefit	Prevent application issues or data leakage
Sample Query	`srcinternal == true && dstinternal == true`

Search for and alert on geo-activity - for example, traffic from countries of concern, or for responding to threats or proactively threat hunting.

Name	Outbound traffic to T1 CoC
Goal	Discover compromised devices
Benefit	Block devices and reduce risk of further intrusion
Sample Query	`dstgeo.countrycode == MM OR dstgeo.countrycode == CN OR dst-geo.countrycode == ER OR dstgeo.countrycode == IN OR dstgeo.countrycode == IR OR dstgeo.countrycode == NG OR dstgeo.countrycode == KP OR dstgeo.countrycode == PK OR dstgeo.countrycode == RU OR dstgeo.countrycode == SA OR dstgeo.countrycode == SY OR dstgeo.countrycode == TJ OR dstgeo.countrycode == TM OR dstgeo.countrycode == VM`

Sample NQLs by category

Name	Outbound traffic to non-approved geo
Goal	Discover compromised devices
Benefit	Block devices and reduce risk of further intrusion
Sample Query	`srcipname == PointOfSaleSystem AND (dstgeo.countrycode != US OR dstgeo.countrycode != CA)`

Bad-Actors - for example, finding traffic that is IP reputation-based, or botnets or phishing/spammers

Name	Connections to bad reputation
Goal	Discover compromised devices
Benefit	Find, alert and block connections to know bad reputation IPs
Sample Query	`dstiprep.count >= 1 or srciprep.count >= 1`

Configuration validation or misconfiguration - for example, finding traffic that should not exist between applications and systems or drift between deployments.

Name	Web application database
Goal	Detect mis-config or compromise
Benefit	Remediate or re-architect applications or infrastructure
Sample Query	`(srcipname == websvr && dstipname != appSvr) or (srcipname != websvr && dstipname != appSvr)`

Compliance - For example, enforce compliance for specific applications or regions or make your reporting or compliance audits easier with audit-ready proof of enforcement

Name	Legacy auth
Goal	Detect mis-config or compromise
Benefit	Enforce compliance controls for authentication
Sample Query	`srcinternal == true && protocol == udp && (dstport == 137 OR dstport == 138 OR dstport == 139)`

Name	Search for traffic between production environments and dev or test
Goal	Discover misconfigured deployments
Benefit	Prevent application issues or data leakage
Sample Query	`tags == Production && (tags == dev or tags == test)`

Name	FTP and Telnet usage
Goal	Discover devices using non-secure transfer protocols
Benefit	Enforce compliance controls for restricted services
Sample Query	`protocol == tcp && tcpflags.ack == true && (dstport == 21 || dstport == 23)`

Name	Outbound SSH
Goal	Discover devices using SSH outbound
Benefit	Enforce compliance controls for restricted services
Sample Query	`protocol == tcp && dstport == 22 && tcpflags.ack == true && dstinternal != true`

Name	Large outbound data
Goal	Discover devices sending > 100MB of data outbound
Benefit	Enforce usage or compliance controls or discover internal threats
Sample Query	`srcinternal == true AND dstinternal == false and bitsxrate > 838,860,800`

Name	x11 Discovery
Goal	Block x11
Benefit	Discover and reconfigure devices to ensure x11 is blocked.
Sample Query	`protocol == tcp and (dstport >= 6000 and dstport <= 6002)`

Name	BitTorrent traffic
Goal	Block BitTorrent on unauthorized networks
Benefit	Discover and reconfigure devices that allow BitTorrent traffic
Sample Query	`protocol == tcp and (dstport >= 6881 and dstport <= 6889)`

The NQLs shared here are just the start. We've seen customers create some truly custom NQLs that are helping their teams gain visibility to network traffic and context across data, applications, devices, and users, and see what they are, what they are doing, and what's happening to them. With these queries and the Netography Detection models built on top of them - teams are lowering their MTTD and MTTD for network security and network configuration issues and incidents.

Your Next Steps:

Netography Customers can access more documentation on NQL:
https://support.netography.com/hc/en-us/articles/360058244731-NQL-Overview-and-Basics

Netography Customers can also access a video demonstration of NQL:
https://support.netography.com/hc/en-us/articles/7760903074452-Netography-Query-Language-NQL-in-10-minutes-or-less

Netography Customers can access a video demonstration of creating Netography Detection Models:
https://support.netography.com/hc/en-us/articles/7760925975188-How-to-build-Custom-Detection-Models

As always if you have any questions, please contact your Netography customer success manager.

Not a Netography customer? Contact us, and we'd be happy to learn about your goals for Network security and visibility. https://netography.com/contact/

Netography® has created the first network-centric platform that reconstitutes capabilities disrupted by the combined impact of encryption and Atomized Networks across the security world. Enterprises have become functionally blind to the composition and activities of their networks, resulting in increased dwell time and more attackers leveraging the gaps between the capabilities of an organization's other tools and the siloed operations teams who operate them.

Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments. With the Netography Fusion platform, these teams gain visibility and control of network traffic and context across users, applications, data, and devices, to see what they are, what they are doing, and what's happening to them.

Netography is the only company that delivers Security for the Atomized Network®. Based in Annapolis, MD, Netography is backed by some of the world's leading venture firms, including Bessemer Venture Partners, SYN Ventures, A16Z, and more. For more information, visit netography.com.

NETOGRAPHY