Decoding Network Traffic Patterns for Faster, Stronger Cyber Defense

Key Takeaways

- Network traffic pattern analysis enables early threat detection by identifying deviations from normal behaviors.
- Building a string baseline is essential to quickly spot anomalies like data exfiltration, port scans, and lateral movement.
- Real-time monitoring helps security teams detect and respond to threats before they escalate.
- Combining flow data with packet-level analysis improves both visibility and investigation accuracy.
- AI and machine learning strengthen detection of unknown and evasive attack patterns.
- Monitoring east-west traffic uncovers hidden internal threats often missed by perimeter tools.
- Effective baselining, segmentation, and alerting enhance both security posture and network performance.

Analyzing network traffic patterns is the heart of a successful security strategy. Network traffic pattern analysis involves monitoring and analyzing data as it moves across a computer network, using various communication protocols to ensure proper data delivery. As organizations continue to grow their digital landscapes, cyber threats have also progressed in complexity and now utilize sophisticated evasion techniques to evade detection. Conventional security countermeasures are no longer able to cope with such dynamic and persistent security threats, hence now organizations are relying on network traffic analysis to detect and mitigate any security incidents.

Network traffic patterns analysis can give us a proactive way to detect anomalies or potential threats before they reach out to cause harm. By monitoring data flows and real-time network traffic, security teams can spot anomalous behavior, including unauthorized access, network data exfiltration, or malware communication. This continuous monitoring is essential for understanding network usage, bandwidth utilization, and performance, especially in data center environments.

Whether you are trying to detect a port scan, identify bandwidth hogs, catch lateral movement inside your corporate network, or justify upgrading your internet link, the approach starts the same way: understand what normal looks like, then watch for anything that breaks that pattern. This blog walks through exactly how to do that.

Fidelis Network® enables organizations to effectively detect, respond to, and mitigate threats through advanced network traffic analysis capabilities and contextual intelligence, securing enterprise networks against the cyber risks they face today.

What Are Network Traffic Patterns?

Network traffic patterns refer to the flow data and behavior of data as it travels across a network. Data packets follow specific communication protocols to ensure proper routing, delivery, and compatibility between devices. They include details such as the volume, direction, and frequency of data packets exchanged between devices.

There are two types:

1. normal network traffic patterns and
2. abnormal network traffic patterns.

Understanding the difference is the starting point for effective network traffic analysis and monitoring.

Aspect Normal Traffic Patterns Abnormal Traffic Patterns Volume Consistency in flow data during business hours, with stable data transfers and predictable bandwidth utilization as key metrics for measuring network traffic and network usage. Sudden spikes in data transfer (e.g., potential

data exfiltration

), unexpected increases in bandwidth utilization. Direction Typical internal communications between servers and endpoints. Unusual outbound connections to unknown IPs or locations. Frequency Regular access to frequently used applications or services. Excessive repeated requests to a single endpoint (e.g.,

DDoS attack

). Behavior Devices communicating within expected time frames and protocols. Communication with command-and-control servers or unknown devices. Example Employees accessing shared files on internal servers. Large volumes of data being sent to an unknown external IP at midnight.

Flow analysis and measuring network traffic are essential techniques for identifying and understanding network traffic patterns.

- **Guide: Close the Visibility Gaps Before They Slow Your Hybrid Threat Detection**

Why Does Network Traffic Pattern Analysis Play a Critical Role in Detection and Response?

Anomaly detection in Network Traffic Analysis (NTA) works on a simple premise: establish a baseline of normal activity, then flag anything that falls outside it. Bulk file transfers outside business hours, unexpected outbound connections, or sudden protocol changes are all red flags that security teams can act on quickly.

Real-time network traffic analysis also surfaces lurking vulnerabilities before attackers can exploit them. Malware often reveals itself through anomalous outbound connections or irregular communication patterns. Spotting these anomalies early allows security teams to intercept threats before they cause substantial damage. Network forensics and incident response both depend on this continuous, detailed visibility.

Examples of patterns indicative of threats include:

- **Unusual data transfer:** Unusual data transfers, such as the movement of a high volume of network traffic data outside of business operations hours, could indicate a

form of data exfiltration. Analyzing packet data and inspecting network packets can help identify suspicious activity and unauthorized data transfers.
- **Traffic spikes:** Sudden increases in inbound or outbound traffic may indicate a Distributed Denial-of-Service (DDoS) attack or unusual internal activity.

Detecting these patterns can help prevent a security incident and supports network forensics by enabling teams to investigate security incidents through detailed analysis of flow data, packet data, and network packets.

Key Challenges Faced by Security Teams in Network Traffic Analysis

- **Encrypted traffic:** Malicious activities concealed within encrypted traffic is extremely tough to identify and evaluate.
- **High data volume:** The volume of traffic in modern organizations, especially large data centers, can overwhelm analysis teams. High bandwidth utilization and increased network usage further complicate analysis, making it challenging to spot significant anomalies and hindering comprehensive network traffic analysis.
- **Dynamic network environments:** What counts as normal traffic changes constantly, making static baselines unreliable. Network telemetry and protocols like simple network management protocol are often used to collect data in these evolving environments.
- **False positives:** False positives mean identifying a harmless activity as an attack as it's tough to distinguish between legitimate traffic anomaly and malicious behavior.
- **Complexity in identifying hidden security threats:** Advanced attackers often disguise malicious traffic patterns, making it harder to identify and flag unusual activities, making malicious network traffic analysis challenging.

Performance monitoring and network management systems are essential for overcoming these challenges, particularly in data centers.

Data Packets and Network Traffic

Data packets are the building blocks of network traffic, serving as the primary means by which information is transmitted across a network. Each data packet contains essential components: source and destination addresses, a data payload, and control information that ensures accurate routing and delivery. As these packets travel between network devices, they collectively form the flow of network traffic that powers communication within and beyond an organization's network infrastructure.

Network traffic analysis (NTA) relies on examining these data packets to gain deep visibility into network activity. By analyzing network traffic patterns at the packet level, security teams can identify patterns that indicate normal network behavior as well as anomalies that may signal potential security threats. For example, a sudden surge in data packets sent to an unfamiliar destination could point to unauthorized access attempts or even a data breach in progress.

Effective network traffic analysis solutions enable organizations to monitor network traffic in real time, providing actionable insights that help detect and respond to security incidents before they escalate. By continuously analyzing network traffic, security teams can quickly identify and mitigate threats such as data exfiltration, malware communication, or abnormal traffic patterns that could impact network performance.

In addition to enhancing security, analyzing network traffic also helps optimize network performance. By identifying bottlenecks, unusual traffic volume, or inefficient data flows, network administrators can make informed decisions to improve network performance and

ensure reliable connectivity across the enterprise.

Ultimately, understanding and analyzing data packets is fundamental to effective network traffic analysis. With the right network traffic analysis solutions in place, organizations can safeguard their network infrastructure, detect and prevent data breaches, and maintain optimal network performance in an ever-evolving threat landscape.

How Can You Effectively Analyze Network Traffic Patterns?

Session Inspection:

Application session inspection focuses on analyzing the application-level data over a network session, including elements such as duration, involved endpoints, and communication patterns. Session inspection involves examining communication protocols, packet data, and network packets to identify anomalies and ensure proper routing and compatibility between devices. Flow analysis can also complement session inspection by providing deeper insights into traffic patterns and helping detect security threats.

Fidelis Network® delivers on this session inspection to gain deep clarity into every individual connection, and to identify anomalous or malicious behavior beyond what traditional techniques such as Deep Packet Inspection (DPI) can provide.

Changing the Game by Shifting From Packet Inspection to Deep Session Inspection

- Inspecting Content With Packet Inspection
- Analyzing Encoded Network Traffic
- Content AND Context

Download the Whitepaper Now!

Behavioral Analysis Using Machine Learning:

With its capability of analyzing network traffic data, machine learning can examine network traffic in real-time by detecting traffic that no longer behaves according to the normal behavior pattern. Machine learning models can help analyze normal network operations and detect suspicious anomalies like data exfiltration or unauthorized access attempts that rules-based methods may not catch.

Network telemetry and log data are used to train these models, enabling performance monitoring and providing insights into network usage. This approach enhances network visibility.

Signature-Based Analysis:

Signature-based analysis looks for known attack patterns, or malicious signatures, in the traffic. This technique uses predefined lists of threat signatures, enabling rapid detection of well-known exploits. Intrusion detection systems commonly rely on signature-based analysis for security analysis and detecting security incidents. Log data is often used alongside signature-based analysis to correlate events and enhance detection. Although it excels at detecting known threats, it has limitations regarding zero-day exploits or advanced persistent threats (APTs) that do not have any established signature.

Baselining and Network Traffic Anomaly Detection:

Normal network behavior is the baseline for good threat detection. As said, the traffic is compared against the historical network data to find the outliers, showing unusual patterns of activity within the organization which helps you to prevent the threats at the very beginning by taking smart actions like detecting and removing malware, insider threats, data exfiltration, data breaches, etc.

How to baseline effectively:

- Collect at least 30 days of passive traffic data before setting any alert thresholds.
- Segment your baseline by time of day, day of week, and network zone (workstations, servers, IoT, DMZ).
- Set alerts for deviations greater than two standard deviations from the mean, sustained for more than a few minutes, not just momentary spikes.
- Review and update baselines whenever major network changes occur, such as new applications, large user additions, or architecture changes.

How to Use Packet Capture and Flow Data Together to Detect Unusual Traffic Patterns and Possible Intrusions

Use flow data for wide-angle visibility and packet capture for deep investigation. They work at different layers and complement each other.

Flow data (NetFlow, sFlow, IPFIX) gives you metadata about every connection: who talked to whom, for how long, and how much data moved. It is lightweight, scales to high-bandwidth environments, and is ideal for detecting volume-based anomalies like DDoS traffic or large data transfers. It tells you nothing about payload content.

Packet capture gives you the full contents of every packet. With Wireshark or a similar tool, you can reconstruct sessions, decode malware callbacks, and perform network forensics. The tradeoff is storage and performance cost at scale.

A practical approach for corporate networks:

- Deploy flow collection from core routers and firewalls. Watch for deviations in volume, destination geography, and protocol ratios.
- Set up SPAN ports or network TAPs at key chokepoints (internet edge, data center perimeter, internal core switches) for targeted PCAP collection.
- When flow data triggers an alert, such as unusual outbound data volume at 2 AM, pivot to PCAP on that host or segment to inspect the actual session contents.
- Fidelis Network® correlates session metadata with content inspection in a single platform, removing the need to manually cross-reference two separate data streams.

What Metrics and Thresholds Should You Track in network traffic patterns to Catch DDoS Attacks and Port Scans?

Setting the right thresholds is where many organizations struggle. Too sensitive, and you drown in false positives. Too loose, and real attacks slip through. Here are key metrics with practical starting thresholds:

1. **Packets Per Second (PPS) / Bits Per Second (BPS):** Build a 30-day rolling average for peak and off-peak periods. A sustained increase of 3x to 5x above historical peak for more than 30 seconds is a strong DDoS indicator.
2. **SYN-to-ACK ratio:** Should be close to 1:1 under normal conditions. A ratio above 5:1 sustained for 60+ seconds strongly suggests a SYN flood.
3. **Unique destination ports per source IP:** A host scanning more than 20 unique ports in 30 seconds against multiple destinations is a reliable port scan alert threshold.
4. **ICMP traffic volume:** Should stay under 1% of total traffic. A spike to 5%+ often indicates a ping flood or reconnaissance sweep.
5. **New flows per second:** More than 1,000 new connection attempts per second from a single source IP signals a DDoS amplification attack or automated scanning.
6. **Geographic anomalies:** Connections from countries you have never done business with, especially toward sensitive internal systems, warrant automatic alerting regardless of volume.

Fidelis Network® automates threshold management through adaptive behavioral baselining, adjusting thresholds dynamically based on your specific network environment rather than static rules.

How to Monitor East-West Traffic to Detect Lateral Movement and Data Exfiltration

North-south monitoring alone misses a critical blind spot. Most ransomware attacks and APTs spend weeks or months moving laterally inside the network before exfiltrating data. Detecting this requires east-west visibility: monitoring traffic between internal servers and devices.

1. **Deploy sensors at internal core switches** using SPAN ports or network TAPs. Perimeter firewalls alone are not enough.
2. **Watch for anomalous use of administrative protocols** (SMB, RDP, WMI, PsExec) between workstations, not just from admin systems.
3. **Track large internal data transfers,** especially from endpoints to file servers. Legitimate users rarely pull large volumes in a single session.
4. **Use network segmentation as a detection mechanism:** any traffic crossing a segment boundary without authorization should trigger an alert.

Fidelis Network® covers both east-west and north-south traffic across on-premises, cloud, and hybrid environments. Combined with Fidelis Deception®, which places decoy assets inside the network, it immediately flags any attacker who touches them during lateral movement.

- **Read Ebook – Catch Threats Earlier with Deception-Enhanced NDR**

What Steps Should You Follow to Perform Network Traffic Analysis?

Network traffic analysis involves ongoing monitoring, capturing, and analyzing network traffic data to detect threats, optimize network performance, and ensure network security. a step-by-step breakdown:

- ## Step 1: Collecting Data

  Network traffic analysis starts by collecting data traffic from different parts of the network, including routers, switches, firewalls, and endpoints. Tools known as network sniffers, packet analyzers, or Network Detection and Response (NDR) solutions perform this task. Measuring network traffic and monitoring bandwidth utilization are essential at this stage, often leveraging network telemetry and protocols like Simple Network Management Protocol (SNMP) to gather comprehensive performance and traffic data.

- ## Step 2: Traffic Filtering

  The second step to network traffic behavior analysis is capturing data and filtering it to match relevant traffic within the session with the protocol, IP address, and port. It makes it easier to filter out the noise to spot packets that lead to enhanced security threats or network performance issues.

- ## Step 3: Packet and Session Inspection

  Packet headers and payloads are analyzed to provide information about the source, destination and content of communications. This may use techniques such as session inspection, protocol decoding and metadata extraction, depending on the tool. Analyzing packet data and network packets, as well as performing flow analysis, are crucial for understanding traffic patterns and identifying anomalies.

- ## Step 4: Behavior Analysis

  Advanced analytics assess traffic patterns by analyzing real-time traffic and mapping it against baseline established from the traffic history. Anomalous activity, such as increased file transfers or attempts to gain access that is outside of what is expected of a person, is identified by machine learning models or behavioral algorithms. The use of log data from network devices and applications further enhances anomaly detection by providing contextual insights.

- ## Step 5: Correlation and Threat Detection

  Cross-segment correlation of multiple networks is done to find any wider patterns or coordinated attempts at attack. In this stage signatures of known threats are detected, or previously undetected malicious behavior is identified based on deviations. Intrusion detection systems and network management systems play a key role in this process by integrating threat detection and comprehensive monitoring capabilities.

- ## Step 6: Alert Generation

  If any risk or anomaly is detected, alerts are raised for the IT teams. These alerts may indicate minor irregularities or high-priority threats such as DDoS attacks, or data

breaches.

- **Step 7: Response and Mitigation**

  The last step to network traffic analysis is security centers taking corrective actions according to the network analysis insights like blocking malicious traffic, updating a firewall or further investigation. Modern platforms such as Fidelis Network® typically include automated capabilities to facilitate faster mitigation.

Thus, network traffic analysis is fostered through a systematic process instead of just isolating them, thus ensuring network security and reliability. These steps support performance monitoring, network usage analysis, and enhanced network visibility.

- **Read Datasheet: Deep Visibility Across Hybrid Infrastructure with Fidleis Network**

Which Best Practices Can Help You Improve Network Traffic Pattern Analysis?

Network Traffic Analysis plays a crucial role in proactive network management and cybersecurity. By examining the flow data through your network, you can uncover hidden threats, optimize network performance, and make data-driven decisions to strengthen your infrastructure. Best practices include continuous monitoring, performance monitoring, and ensuring comprehensive network visibility to proactively detect issues and maintain optimal operations.

Effective network traffic pattern analysis involves monitoring network usage and bandwidth utilization, leveraging network telemetry, and conducting flow analysis to understand traffic patterns. Utilizing log data, network management systems, and network monitoring tools is essential for gaining actionable insights. These practices are especially important in data centers and data center environments, where east-west traffic and cloud integration require robust monitoring and analysis.

Implementing these best practices supports secure network traffic, enables thorough security analysis, facilitates network forensics, and enhances the ability to investigate security incidents. Intrusion detection systems, measuring network traffic, analyzing packet data and network packets, adhering to communication protocols, and using simple network management protocol (SNMP) are all critical components for comprehensive network traffic analysis and management.

Establish a Traffic Baseline

Analyze historic traffic data to define normal network behavior. Update baselines regularly to reflect new applications, user behavior changes, and bandwidth usage shifts.

Set Up Automated Alerts for Bandwidth and Performance

For teams looking to identify bandwidth hogs and justify infrastructure upgrades, configure your monitoring platform to alert when:

- Any single application or host exceeds 20% of total available bandwidth for more than 5 minutes.
- Link utilization exceeds 70% during business hours for three or more consecutive days.
- New protocols or applications appear in your traffic mix that were not present in the baseline.

Regular traffic reports segmented by application, user group, and time of day give you the documented evidence needed to make a business case for upgrades.

Segment Your Network

Segment the network into smaller, isolated sub-networks to better monitor network traffic. Segmentation is especially important in data centers and data center environments, where east-west traffic between servers must be closely managed and analyzed. Traffic segmentation helps in containing sensitive data and reduces the blast-radius of the breach. Tune detection mechanisms according to the environment — for example, separate user traffic from critical server traffic to detect unusual access attempts. Network management systems and network monitoring tools support segmentation and enhance network visibility and performance monitoring, making it easier to identify threats and optimize network performance.

Leverage Advanced Analytics Tools

Implement modern network traffic analysis solutions such as Network Detection and Response (NDR) systems, or Endpoint Detection and Response (EDR) solutions to effectively analyze the data in real time. These advanced analytics tools leverage flow analysis, network telemetry, and log data to monitor, inspect, and interpret network activity. Intrusion detection systems, security analysis, and network forensics are also key features, enabling detailed investigation and threat detection. Additionally, these tools enhance performance monitoring and network visibility, supporting proactive network management. Other platforms, such as Fidelis Network®, employ machine learning and behavioral-based network traffic analysis to rapidly detect known and unknown threats while minimizing false positives.

Monitor Encrypted Traffic

A significant portion of modern network traffic is encrypted, which can obscure potential threats. Invest in solutions capable of decrypting and analyzing encrypted traffic to detect malicious activities hidden within legitimate communications. Analyzing packet data and network packets, as well as understanding communication protocols, is essential for secure network traffic analysis.

Review and Update Threat Intelligence Regularly

Utilize current threat intelligence feeds to catch any new threat or tactic. Frequent updates keep your network traffic analysis effective at detecting both advanced persistent threats (APTs) or zero-day exploits using sophisticated techniques to avoid detection. In addition to threat intelligence feeds, sources such as log data, flow analysis, network telemetry, and simple network management protocol (SNMP) are crucial for gathering actionable threat intelligence. These sources help detect and investigate security incidents by providing comprehensive visibility and context for identifying and responding to threats.

By implementing these practices, organizations can enhance their ability of network traffic analysis which will eventually lead to enhanced threat detection, minimizing risks, and maintain robust network security.

Fidelis Network®: Enhancing Threat Detection Through Network Traffic Analysis

Fidelis Network® is the industry's best in class network traffic analysis tool, giving organizations the ability to enhance their network performance and overall cybersecurity posture by providing deep visibility into network traffic patterns and behaviors. It allows security centers to detect, investigate, and respond to threats in real-time due to its advanced detection and network traffic analysis capabilities.

Fidelis Network® ensures early threat detection, even for sophisticated and evasive cyberattacks. The platform integrates seamlessly with other security solutions to provide a holistic view of network activity, making it an essential tool for securing modern, complex networks.

Which Features and Capabilities Make Fidelis Network® Stand Out?

- **Deep Session Inspection:** Analyzes full network sessions, including network packets and packet data, ensuring a comprehensive understanding of all communications and supporting network forensics and security analysis.
- **Integration with Deception Technology:** Enhances threat hunting by using decoys to reveal attacker techniques and paths, and assists in investigating security incidents.
- **Inspection of Encrypted Traffic:** Fidelis Network® is capable of network traffic analysis of encrypted website traffic without sacrificing data protection, supporting secure network traffic and intrusion detection systems.
- **Actionable Threat Intel:** Frequently updates threat signatures and provides context to alerts for better-faster decision-making, improved network performance, and enhanced performance monitoring.
- **Extensive Coverage:** Spans East-West and North-South network traffic in on-premises, cloud, and hybrid environments, including data centers and the data center, for comprehensive network visibility and bandwidth utilization.
- **Advanced Network Management:** Integrates with network management systems and network monitoring tools, leveraging network telemetry, flow analysis, and simple network management protocol (SNMP) for measuring network traffic, monitoring network usage, and optimizing communication protocols.
- **Automated Response:** SOC teams can configure Fidelis Network® to automatically block malicious traffic, quarantine infected hosts, or trigger response playbooks on detection, significantly reducing MTTR.

Discover how Fidelis Network can help your organization!

Threat Protection offered by Fidelis Network® Detection and Response:

- Data Theft
- Lateral Movement in Network
- Malware Threat

Watch Pre-Recorded Demo

Get a Demo

Frequently Ask Questions

How can I effectively analyze network traffic for security threats?

Deploy sensors across your network, establish a 30-day baseline, then monitor for deviations in volume, protocol mix, and connection behavior. Combine flow data for broad visibility with packet capture for deep investigation. Use behavioral analysis for unknown threats and signature-based detection for known ones.

What are the best practices for network traffic analysis and monitoring?

Monitor both north-south and east-west traffic. Baseline by time of day and network zone. Inspect encrypted traffic. Keep threat intelligence feeds updated. Segment your network so unexpected cross-segment traffic is immediately suspicious.

What kind of solution do I need to detect lateral movement inside my network?

You need an NDR solution with internal east-west sensors, not just perimeter monitoring. It should ingest SPAN port traffic from core switches, detect anomalous administrative protocol usage (RDP, SMB, WMI), and correlate events across segments. Fidelis Network® combined with Fidelis Deception® is built specifically for this, providing both passive traffic monitoring and active detection via decoy assets.