Fidelis Network® for Amazon VPC Traffic Mirroring

Over the last decade, cloud computing has become the backbone of modern business, transforming how organizations operate and scale.

Companies rely heavily on cloud services, with most of their applications and workloads migrating to efficient platforms like AWS due to the increased remote working requirements and demand for scalable, flexible, and cost-effective solutions that support business continuity and growth.

In this cloud setup, Amazon Virtual Private Cloud (VPC) enables businesses to create private network environments, giving them control over network setup, traffic management, and connections to on-site systems.

However, monitoring and securing the traffic within these environments can be challenging.

Why is that?

Monitoring, analyzing, and securing such complex environments is difficult because so much data flows to and from the cloud, as well as internally, including sensitive information. This makes the cloud, i.e., the VPCs, one of the prime targets for attacks.

This is where we need to consider cloud network traffic analysis, including traffic mirroring, and advanced security monitoring strategies.

What is Cloud Network Traffic Analysis?

Cloud network traffic analysis is significant and a must-have practice for organizations to identify and address security threats, prevent data loss, and ensure the smooth flow of cloud network traffic.

As more organizations adopt Infrastructure-as-a-Service (IaaS) solutions like virtual machines (VMs), effective monitoring of cloud network traffic becomes even more crucial to protect data, optimize operations, and ensure smooth workflow.

Why Cloud Network Traffic Analysis Is Critical:

- Helps identify unusual patterns and anomalies, detect threats, and prevent data breaches.
- Helps organizations comply with regulatory requirements and protect sensitive data.
- Helps detect network bottlenecks and performance issues to improve user experience.

How Does Cloud Network Traffic Analysis Work?

Network traffic analysis can be implemented using several techniques for capturing network traffic and analyzing data flow. Two common methods are:

Packet Capture and Inspection:

- Intercepts and inspects network packets in real-time.
- Provides detailed network visibility into the data flow, helping identify security issues.

- **Pros:** Granular insight into network traffic.
- **Cons:** It can be resource-heavy and slow down the network if not managed properly.

Flow Analysis:

Focuses on metadata (e.g., IP addresses, ports) to track traffic patterns.

- **Pros:** Less resource-intensive, ideal for large environments.
- **Cons:** Provides less detailed visibility than packet inspection.

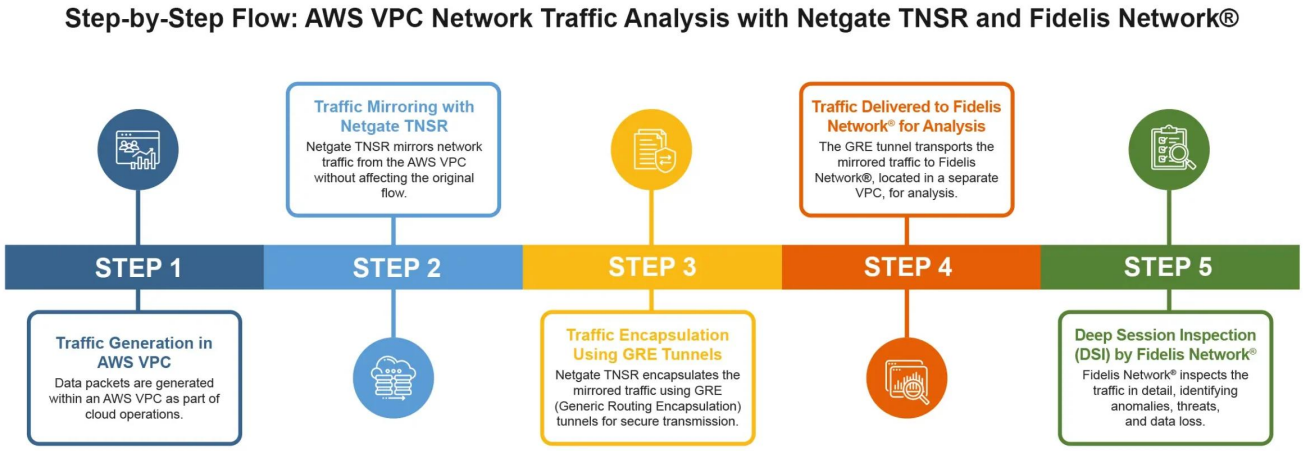
Challenges of cloud network traffic analysis are:

- Cloud environments handle a large amount of data, making it hard to capture and analyze every piece of traffic effectively.
- Cloud networks are constantly changing (services spin up and down based on demand), making it difficult for traditional monitoring tools to keep up with these rapid changes.

To overcome these challenges, organizations should consider robust tools and methods like Netgate TNSR, Fidelis Network Sensors and VPC traffic mirroring to capture both inbound and outbound traffic via Elastic Network Interfaces (ENIs) and analyze it using advanced methodologies such as Deep Session Inspection and other techniques.

AWS VPC Traffic Analysis with Netgate TNSR & Fidelis Network®

Here is the complete flow of how AWS VPC network traffic analysis works with Netgate TNSR and Fidelis Network®:



How Can Deep Traffic Analysis Strengthen AWS Security?

Uncover how leading organizations are leveraging advanced network traffic analysis to:

- Extend visibility to AWS cloud applications, workloads, and databases

- Simplify network traffic mirroring with no third-party agents required
- Analyze all ports and protocols without data loss or sampling

Download the Datasheet

Now, let’s go through the process in detail.

VPC Traffic Mirroring in AWS with Netgate TNSR

What is AWS VPC Traffic Mirroring?

VPC traffic mirroring works in AWS by allowing companies to capture and analyze network traffic from their Virtual Private Cloud (VPC). This gives them a detailed view of traffic for monitoring and troubleshooting. Essentially, it helps copy network traffic and sends it to a monitoring tool for analysis.

Netgate TNSR: Overview

Netgate TNSR is an advanced, open-source platform designed to manage and route network traffic in a highly secure, scalable, and flexible way. It provides real-time traffic mirroring, network load balancer functionality, and analysis capabilities, enabling organizations to monitor network data without interrupting the flow of traffic. Amazon EC2 can be used to host the Netgate TNSR solution, which is capable of handling high-speed network traffic.

How Netgate TNSR Works with AWS VPC Traffic Mirroring

Netgate TNSR works within AWS to monitor traffic for suspicious activities in near real-time, acting as a network mirror that sends high-speed traffic directly to any cloud-based traffic analysis engine, such as Fidelis Network®.
Other key aspects of Netgate TNSR include:

- **Intelligent Routing:** Netgate TNSR is capable of intelligently routing traffic between different applications, VPCs, and secure VPN links. Whether handling traffic within the same VPC (east-west) or between multiple VPCs (north-south), it ensures that network traffic is mirrored without performance degradation.
- **Automation and Flexibility:** The integration offers automated network management through TNSR API. This allows IT teams to effortlessly add or modify network connections between VPCs or adjust traffic parameters without the need for manual reconfiguration, enhancing operational efficiency.
- **Scalability and Performance:** From speeds of 1Gbps to over 100Gbps, Netgate TNSR provides the flexibility to scale as traffic demands increase, allowing organizations to monitor high-volume cloud environments without compromising performance.

Mirroring Process with Netgate TNSR

A traffic mirror session by Netgate TNSR handles the copying of packets from the traffic mirror source (where the traffic originates) to the traffic mirror target (usually a tool like Fidelis Network®), allowing deep analysis without disrupting the original traffic.

A Gateway Load Balancer can also be employed to distribute traffic more effectively across

multiple virtual appliances during the mirroring process, ensuring scalability and improved performance in traffic analysis.

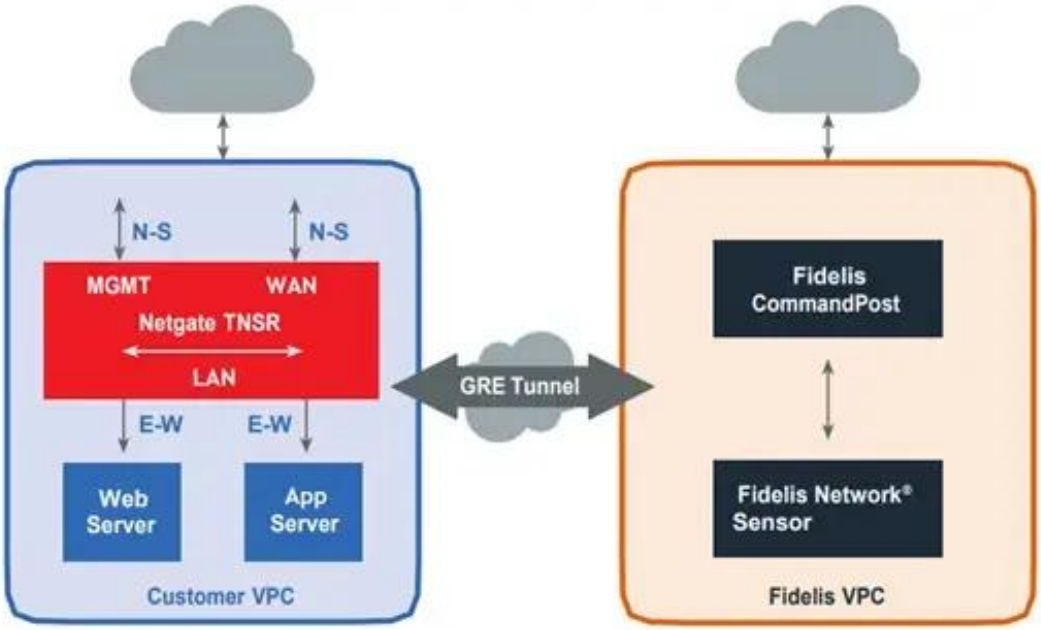
Additionally, traffic mirror resources, such as a traffic mirror filter, help determine which specific traffic should be copied and sent to your monitoring tool for analysis. This enables you to monitor performance without dealing with unnecessary data. The Instance Metadata Service (IMDS) can also provide specific information about the instance, offering deeper insights for your analysis.

Sending Mirrored Traffic from Netgate TNSR to Fidelis Network®

Using GRE Tunnels:

Netgate TNSR sends the mirrored traffic to Fidelis Network® which is within its own VPC using GRE (Generic Routing Encapsulation) tunnels.

GRE tunnels encapsulate data packets, allowing them to be transmitted over networks that don’t support the original protocol. This process ensures secure, uninterrupted delivery to Fidelis Network® for further analysis. This process involves wrapping the data in a new packet header, which is removed at the receiving end, revealing the original data.



Quickly enable AWS cloud VM traffic analysis with Netgate TNSR to Fidelis Network®.

Once the mirrored traffic reaches Fidelis Network®, what happens next?

Cloud Network Traffic Analysis with Fidelis Network®

What is Fidelis Network®?

Fidelis Network® is a powerful security tool that protects against network threats both in the cloud and on-premises. Unlike traditional tools like firewalls and antivirus, it constantly monitors

and analyzes network traffic in real-time to spot unusual activity and potential threats. Using advanced analytics and machine learning, it can detect threats within the network that other tools might miss, offering deep visibility across all ports and protocols.

It also features automated response technologies such as:

- Network Data Loss Prevention
- Sandboxing
- Deep Session Inspection
- Advanced Cyber Terrain Mapping

These capabilities make it a crucial addition to an organization's security infrastructure for proactive, real-time threat detection and response.

Enhanced Cloud Traffic Monitoring with Fidelis Network®

Once the mirrored traffic reaches Fidelis Network®, it utilizes its powerful Deep Session Inspection (DSI) technology, along with other features, to provide a comprehensive analysis of cloud traffic. It goes beyond typical network monitoring to detect suspicious activity, potential breaches, and data loss, both in real-time and retrospectively.

Key cloud traffic monitoring features include:

- **Deep Session Inspection (DSI):** Provides granular visibility into cloud network traffic, analyzing not just packet headers but also session details, file content, and obfuscated files.
- **Cross-Session and Multi-Faceted Analysis:** This approach gives deeper insights into network behavior and potential threats by analyzing multiple sessions at once. It uses advanced machine learning to detect anomalies and spot unusual patterns that may indicate malicious activity.
- **Metadata and Custom Tags:** Tags and stores hundreds of metadata attributes related to network traffic, offering deep context that traditional firewalls or SIEMs (Security Information and Event Management systems) might miss. This data can be retained for up to 360 days, providing long-term visibility and historical analysis capabilities.
- **Scalable Capacity:** Capable of analyzing up to 2Gbps of traffic without packet loss, ensuring no important data is overlooked. It also supports multi-sensor configurations to handle large-scale networks.
- **Comprehensive Threat Detection:** Offers proactive threat intelligence derived from research teams and various external threat intelligence feeds. This enables security teams to stay ahead of evolving threats and respond rapidly.

Conclusion

Protecting AWS VPCs is a critical security priority to ensure the health of your organization's overall cloud and network infrastructure. Traditional cloud network analysis has many limitations that are ineffective in today's advanced cloud and network environments. To protect your AWS VPC and ensure real-time threat detection in the cloud network, integrating tools like Netgate TNSR and Fidelis Network® NDR is essential.