Fidelis Cybersecurity

DATASHEET

Fidelis Network® with Amazon Web Services Virtual Private Cloud (VPC) Traffic Mirroring

Enable Cloud Network Traffic Analysis

Enable Cloud Network Traffic Analysis

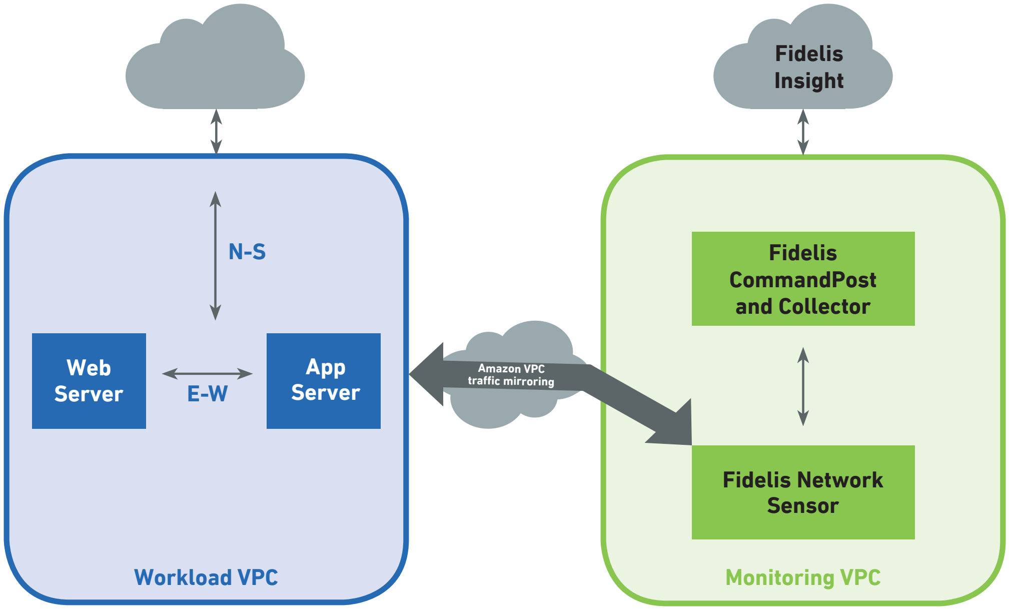
Enterprise security operations are complex, with siloed visibility across networks, endpoints, and cloud environments, combined with too many tools for understaffed and overwhelmed teams to manage. Security teams need bi-directional visibility into network traffic across all ports and protocols and need valuable metadata to analyze threats and data leakage. This comprehensive visibility combined with contextual threat intelligence leads to detections across the entire threat life cycle. This also allows organizations to respond quickly and effectively to malicious activity at every stage of the kill chain and mitigate data leakage and exfiltration.

Solution Overview

Customers of Fidelis Network enabling the Amazon Web Services (AWS) Virtual Private Cloud (VPC) Traffic Mirroring can quickly deploy cloud network traffic analysis for north-south and east-west communications within EC2 instances. The solution also provides a monitoring boundary between Fidelis Network sensors deployed in AWS VPCs and customer applications and workloads.

Solution Benefits

- **Visibility** – AWS VPC Traffic Mirror provides visibility to application traffic for north-south communications, often through web front ends, and east-west traffic often between back end process workloads and databases.
- **Simplicity** – AWS VPC Traffic Mirror does not require any third -party agents and directly communicates with cloud hosted Fidelis Network sensors across VPCs where the sensors are segmented from applications in a monitoring boundary.
- **Speed** – Fidelis Network cloud sensors can each analyze 1 Gbps of network traffic with no data sampling or packet drops, so every port and protocol is fully analyzed with Deep Session Inspection (DSI).



Quickly enable AWS cloud workload traffic analysis with Amazon VPC traffic mirroring to Fidelis Network.

AWS VPC Traffic Mirror –

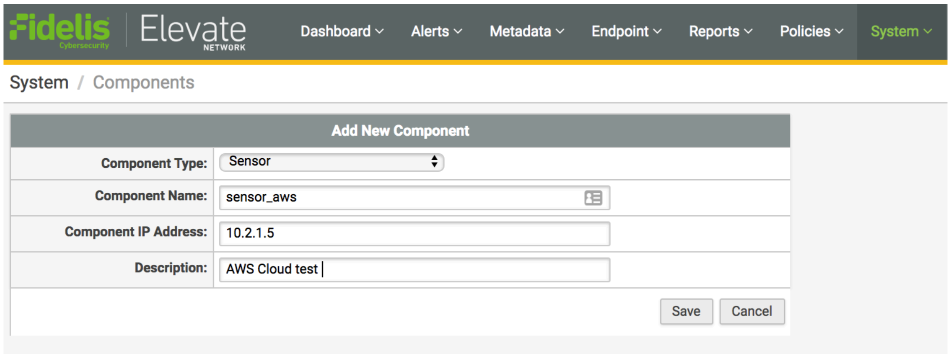
Coupled with Fidelis Network cloud sensors you can:

- Monitor north-south and east-west communications of AWS hosted applications
- Monitoring boundary between SecOps and application owners
- No third-party agents or software required

Fidelis Network

Get direct cloud-based traffic analysis of AWS hosted applications via the Amazon Web Services (AWS) Virtual Private Cloud (VPC) Traffic Mirror including north-south and east-west communications via VPC mirroring to Fidelis Network AWS hosted sensors. Analysis of traffic using Deep Session Inspection (DSI) includes hundreds of metadata attributes and custom tags for real-time and retrospective analysis for threat detection, threat hunting and data loss and theft detection. Fidelis also provides a Managed Detection and Response (MDR) service for 24/7 cloud monitoring of AWS hosted sensors with proactive incident response (IR) services.

- **Fidelis Network includes direct, internal, cloud, email and web sensors** for unmatched visibility for hybrid multi-cloud networks.
- **Deep Session Inspection (DSI)** of AWS cloud workload communications for all ports and protocols to analyze sessions, content, and obfuscated files and archives.
- **Cross session and multi-faceted analysis, plus machine learning anomaly detection** enable real-time and retrospective analysis for threat detection, threat hunting and data loss and theft detection. Security analysts can query, pivot and hunt on content and context.
- **Metadata for hundreds of attributes** and custom tags with the ability store up to 360 days within cloud or on-premises providing content and context not seen in firewall logs or SIEM dashboards.
- **1Gbps sensor analysis capacity** with no data sampling or packet drops, multi-sensor configurations scale with network performance requirements.
- **Fidelis Insight provides threat intelligence** based on threat research team (TRT) research and analysis, plus multiple threat intelligence feeds.
- **Expand to Fidelis Elevate™** with endpoint detection and response (EDR) and deception for a complete threat detection, threat hunting and data loss and theft detection platform or managed service.



System / Components

Add New Component

Component Type:	Sensor
Component Name:	sensor_aws
Component IP Address:	10.2.1.5
Description:	AWS Cloud test

Easily add Fidelis Network sensors in AWS to accept VxLAN data via VPC peer from the AWS VPC Traffic Mirror.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.