DATASHEET

Fidelis Network® with Netgate TNSR

Protect Your Applications and Data Hosted in AWS Cloud

Enable Cloud Network Traffic Analysis

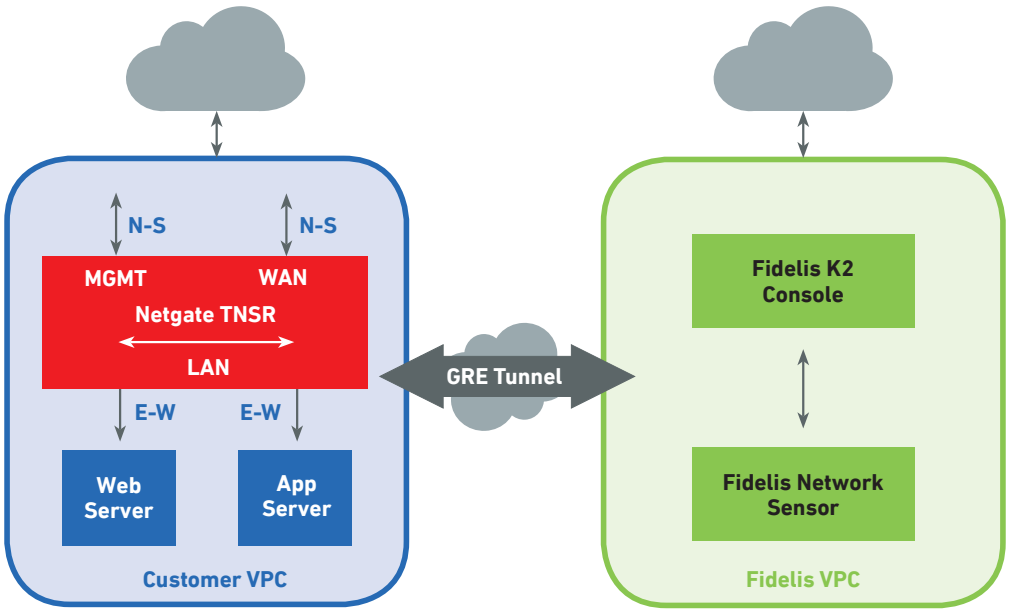
Cloud network traffic analysis is critical for threat and data loss detection as well as threat hunting. As applications and workloads continue to migrate to cloud, mainly into Infrastructure-as-a-Service (IaaS) using virtual machines (VMs), adoption rates are projected at 40-60% by 2021 and up to 85% the year after for some organizations. Office and campus networks will remain with some legacy applications while many data center components move to cloud and on-premises data centers are reduced or closed.

Solution Overview

Customers of Fidelis Network with Netgate TNSR can quickly deploy cloud network traffic analysis for north-south and east-west communications of AWS cloud VMs deploying TNSR for high performance traffic mirroring. Communications use GRE tunnels between AWS Virtual Private Clouds (VPCs) to send mirrored interface VM cloud traffic by TNSR to Fidelis Network within its own VPC for analysis to detect, investigate and respond to threats and data theft/loss.

Solution Benefits

- **Visibility** – Netgate TNSR provides visibility to AWS cloud application VM traffic for north-south communications, often through web front ends, and east-west traffic often between back end VM process workloads and databases.
- **Simplicity** – Netgate TNSR interface mirrors VM traffic using GRE tunnels between VPCs to send mirrored traffic to cloud-based Fidelis Network within its own VPC for analysis — no third-party agents are required or reconfiguring of applications.
- **Speed** - Fidelis Network sensors can each analyze up to 2Gbps of network traffic with no data sampling or packet drops, so every port and protocol is fully analyzed with Deep Session Inspection™ (DSI) for content and context.



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

Netgate TNSR

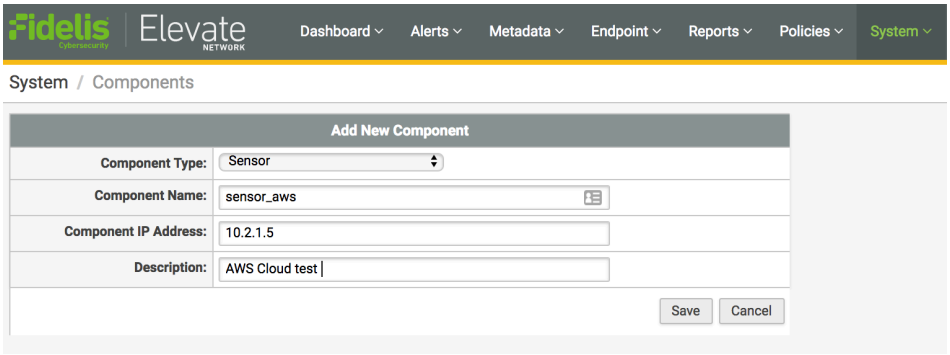
An advanced open source-based firewall, router and VPN platform with breakthrough enterprise-class performance, management and service expansion flexibility. Netgate TNSR mirrors traffic to Fidelis Network while simultaneously maintaining secure connections between VPCs and back to the enterprise. TNSR can route traffic intelligently between applications (east-west traffic) as well as traffic between VPCs, out to the Internet, or over secure VPN links back to the enterprise (north-south traffic).

- **Transparency** as Netgate TNSR is the data path, so all network traffic is mirrored to Fidelis Network in a separate VPC for analysis in real-time and retrospectively.
- **Automation** enables adding new network connections between VPCs or changing parameters of an existing connection using the TNSR API without manual intervention.
- **Performance** from 1Gbps to over 100Gbps with Netgate TNSR provides the freedom to scale.

Fidelis Network

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 VMs 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 VM-based 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.
- **2Gbps 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.



Easily add Netgate TSNRs to mirror traffic to Fidelis Network® while maintaining secure connections between VPCs and back to the enterprise.

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.

©Fidelis Cybersecurity