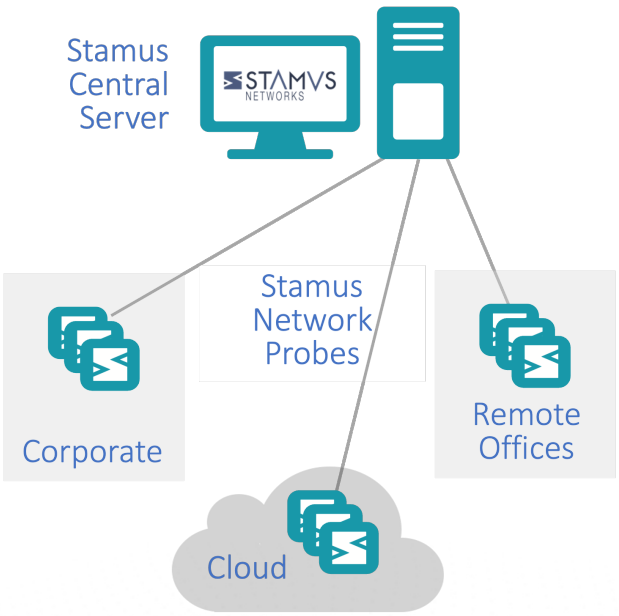
Product Brief

Stamus Network Probe™ AMI for Amazon Web Services®

Extending network visibility and threat detection into your public cloud workflows

Stamus Security Platform™ (SSP) is an open network detection and response solution that delivers actionable network visibility and threat detection. SSP consists of two components: Stamus Network Probe™ and Stamus Central Server™. Each plays a critical role in scaling the system. Stamus Central Server and Stamus Network Probes can be deployed in private cloud, public cloud, on-premise, or hybrid environments. Together they provide complete network-based threat detection and response across the enterprise hybrid attack surface.



SSP supports all combinations of physical, virtual, and cloud installations.

Stamus Network Probe

Stamus Network Probes inspect and analyze all network traffic using deep packet inspection to perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions. The probe delivers all this data to the Stamus Central Server for additional analytics, processing and another layer of threat detection.

The Stamus Network Probe software may be deployed in public cloud (IaaS), private cloud, data center, on premise, or in hybrid environments, providing complete visibility into an enterprise IT and OT activity.

Stamus Network Probe in Amazon Web Services (AWS)

When deployed in Amazon Web Services (AWS) environments, the Stamus Network Probe provides first party visibility into traffic moving in and out of and among IaaS workflows. This real-time analysis empowers you to:

- **Detect Threats Early:** Identify malicious activity hidden within legitimate traffic patterns.
- **Gain Deep Visibility:** Uncover suspicious lateral movements and anomalous behavior within your cloud environment.
- **Accelerate Incident Response:** Reduce dwell time and streamline threat mitigation with rich context and actionable insights.

Leveraging the efficiency and scalability of Amazon Web Services (AWS), the Stamus Network Probe is deployed as a pre-built Amazon Machine Image (AMI). This AMI encapsulates the Stamus Network Probe software along with its necessary configurations. Deployment is very straightforward: simply launch the AMI within your AWS environment, configure security groups to allow traffic from your workloads, and integrate the probe with your VPC. This streamlined process gets you up and running quickly, providing deep visibility into your cloud traffic for enhanced security.

Directing Traffic to the Probe

The Stamus Network Probe analyzes east-west traffic flowing among your cloud workloads. To achieve this, you'll need to configure traffic mirroring within your AWS environment. Here are the common methods for setting up traffic mirroring with the Stamus Network Probe:

- **Network Tap:** This hardware device replicates all traffic on a specific network segment. You can connect the tap to your VPC and configure it to mirror traffic to the Stamus Network Probe's designated network interface.
- **AWS Network Load Balancer (NLB):** If you're already utilizing an NLB to distribute traffic across your workloads, you can leverage its capabilities for traffic mirroring. By configuring forwarding rules within the NLB, you can direct east-west traffic to the Stamus Network Probe for inspection.
- **Security Groups:** Security groups act as firewalls within your VPC, controlling inbound and outbound traffic flow. By strategically defining rules within the security groups associated with your workloads, you can specifically route east-west traffic to the Stamus Network Probe for analysis.

Stamus recommends consulting the AWS documentation for detailed instructions on configuring traffic mirroring using each of these methods. This ensures proper integration with your existing AWS infrastructure.

Technical Requirements for the AWS Instance of the Probe

The Stamus Network Probe has minimal resource requirements and scales to meet your workload needs. The probes must be created with 2 network interfaces. One for packet monitoring and the second for administration, control, and sending telemetry to the Stamus Central Server.

For detailed specifications, please refer to the the table below

Monitored Bandwidth	Instance type	vCPU	Memory	Disk size (root)	Disk size (logs)
Up to 10Gbps	c5.12xlarge c5.18xlarge	48 72	96 GB 144 GB	gp3, 100 GB	gp3, 2000 GB
Up to 1Gbps	t3.2xlarge c5.4xlarge	8 16	32 GB 32 GB	gp3, 70 GB	gp3, 500 GB
Up to 100Mbps	t3.medium	2	4 GB	gp3, 50 GB	st1, 200 GB

Learn More

- Download the Stamus Security Platform datasheet for a detailed overview
- Visit the Stamus Networks website to explore the Stamus Security Platform
- Contact Stamus Networks directly for a demonstration or security consultation

STAMUS NETWORKS

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

5 Avenue Ingres
75016 Paris
France

contact@stamus-networks.com
www.stamus-networks.com

