internet2.0

MILITARY-GRADE

CYBER PROTECTION

Cloaking Firewall for AWS
Product Document

Cloaking Firewall for AWS

Introducing the Cloaking Firewall for AWS: Invisible Defence for the Cyber Age

Harness the power of the Cloaking Firewall to fortify your AWS servers. In an era where cloud infrastructure is pivotal, ensuring the security of your AWS environment is paramount. The Cloaking Firewall acts as a vigilant guardian, meticulously inspecting and filtering traffic to and from your AWS instances. By leveraging its advanced capabilities, such as algorithmic IP blocking based on real-time scans and events, it provides a robust shield against potential cyber threats. Whether you're running web applications, databases, or complex workloads on AWS, the Cloaking Firewall ensures that your digital assets remain invisible to malicious actors, safeguarding the integrity, confidentiality, and availability of your data in the cloud.

Crafted specifically for AWS, the Cloaking Firewall seamlessly integrates both virtual and logical components. It's not merely a gateway; it's a harmonious ensemble of security protocols tailored for the cloud. While the Cloaking Firewall offers a robust layer of defence, it's essential to remember that comprehensive cybersecurity extends beyond a single tool. Strengthen your entire AWS infrastructure, and let the Cloaking Firewall serve as the foundational pillar of your cloud-based cyber defence strategy.

Elevate your AWS security with the Cloaking Firewall, a state-of-the-art solution infused with groundbreaking technology. Transcend conventional defence barriers and render your AWS resources virtually undetectable to potential cyber threats. Our pioneering system defends against pervasive internet scans, a tactic frequently employed by cyber adversaries to identify vulnerabilities. With the Cloaking Firewall safeguarding your AWS environment, you're not merely shielded; you're in stealth mode. Venture confidently into a secure cloud era, where our subscription-driven expertise ensures you remain at the forefront of cybersecurity.

Seamlessly fortifying your AWS infrastructure has never been easier with the integration of the Cloaking Firewall. Designed to cater to the diverse needs of AWS users, it offers both the time-tested reliability of IPSec and the modern efficiency of WireGuard:

- IPSec – Unwavering & Trustworthy: IPSec, a stalwart in the VPN world, guarantees the confidentiality, integrity, and authentication of data, making it a prime choice for those seeking a robust connection to their AWS resources.
- WireGuard – Contemporary & Swift: Recognized for its streamlined architecture, WireGuard stands out as a modern VPN protocol, delivering unparalleled performance and agility.

By integrating the Cloaking Firewall with your AWS environment, you're not only enhancing security but also optimizing connectivity. Whether you're running mission-critical applications or hosting sensitive data on AWS, the Cloaking Firewall ensures a secure, high-speed, and resilient connection, tailored to your specific operational needs.

Cloaking Engine

The exclusive Cloaking Technology of Internet 2.0's Cloaking Firewall for AWS hampers the efforts of threat actors by making your network undetectable during recon scans and other covert scanning techniques.

Intrusion Detection / Prevention System

Our Intrusion Detection and Prevention Systems (ID/PS) employ advanced deep packet inspection for web traffic analysis. Suspicious activity is identified and blocked, preventing comms with command and control nodes.

Advanced Firewall

Fully configurable Next-Gen Firewall with advanced capabilities, such as automated algorithmic blocking of IP addresses based on scans and events. This state-of-the-art system also integrates seamlessly with existing network infrastructures.

Encrypted Data Communication

Enable secure data transmission for remote users via VPNs. Site-to-site IPSec or the 21st Century Wireguard protected tunnels can be established between networks. Data encryption is set to AES 256 GCM.

Features Overview

Advanced Security: The Cloaking Firewall is built on a robust foundation of security features. It offers stateful firewalling, deep packet inspection, and intrusion detection and prevention systems. This ensures that your network is shielded from a wide range of cyber threats.

Automatic Threat Blocking: Real-time IP and packet signature analysis is a game-changer. The Cloaking Firewall continuously scans incoming traffic for known malicious patterns. Upon detection, it instantly blocks the threat, ensuring that harmful data never infiltrates your network.

Networking: The Cloaking Firewall makes use of AWS's Elastic Network Adapters (ENA) to take advantage of performance and for packet inspection allowing for blocking of malicious packets.

Traffic Shaping: With the Cloaking Firewall, you have granular control over your network's bandwidth. Prioritize mission-critical applications, allocate bandwidth for specific tasks, and ensure that your network runs smoothly even during peak usage times.

Flexible VPN Options: Remote work and inter-office connectivity are made simple with the Cloaking Firewall. It supports a range of VPN protocols, including OpenVPN, IPsec, and WireGuard. This ensures secure, encrypted connections, whether you're accessing resources from home or connecting multiple office locations.

Intrusion Detection & Prevention System (IDPS): The Cloaking Firewall incorporates Suricata as a premier open-source IDPS, designed to provide real-time intrusion detection, inline intrusion prevention, and network security monitoring. Here's a deep dive into its features and capabilities:

- High-Performance Engine: Suricata is engineered for high-speed networks, ensuring that even with heavy traffic, it remains efficient in detecting and blocking threats.
- Multi-Threading: Leveraging multi-threading capabilities, ensures optimal utilization of available hardware resources, delivering faster threat detection and response times.
- Inline Intrusion Prevention: Beyond just detecting threats, the IDPS can operate in an inline mode, actively blocking malicious traffic based on its signature, anomaly, and protocol-based rules.
- Protocol Parsing: Deep protocol analysis, ensuring that threats hidden deep within layers of network protocols don't go unnoticed.
- SSL/TLS: Inspection of the metadata of TLS traffic, which includes details like the certificate exchanged during the TLS handshake, the TLS version, and the cipher suite being used. This allows for identification of potentially malicious or suspicious domains, expired certificates, or the use of outdated and insecure TLS versions or cipher suites.
- Using JA3 Fingerprints: JA3 is a method to create fingerprints of the TLS client and server handshakes. These fingerprints can be used to detect malicious or suspicious traffic patterns without decrypting the actual content, allowing for faster performance.

Reporting with integration to SIEMs or Threat Defence®:

Knowledge is power, and with the Cloaking Firewall, you're not just limited to in-built analytics. The platform is partnered with Threat Defence®, an Australian-based cybersecurity company known for its advanced threat intelligence and reporting capabilities:

- Geolocation Insights: Understand where threats are originating from with detailed geolocation data, allowing for more targeted defence strategies.
- Customizable Dashboards: Tailor your reporting interface to show the metrics that matter most to you. With Threat Defence®, you can create custom dashboards that provide a snapshot of your security posture.