internet2.0

MILITARY-GRADE
CYBER PROTECTION

Cloaking Internet Gateway (CIG)
Product Document

Cloaking Internet Gateway (CIG)

Introducing the Cloaking Internet Gateway: Invisible Defence for the Cyber Age

Dive into the future of Internet security with the CIG, your organization's dedicated sentinel for web traffic. Acting as the bridge between your internal network and the vast digital ocean of the Internet, CIG meticulously inspects, filters, and ensures every byte aligns with your security blueprint. Think of CIG as your organization's digital gatekeeper, championing data confidentiality, integrity, and availability.

Crafted with a blend of physical and logical components, CIG is more than just a gateway; it's a symphony of security protocols working in harmony. And while it stands as a formidable line of defence, remember: a holistic cybersecurity strategy spans beyond just one solution. Ensure your entire ICT environment is fortified, and let CIG be the cornerstone of your cyber defence strategy!

Experience next-generation protection with the Cloaking Internet Gateway (CIG), a premium security solution fortified with innovative technology. Go beyond traditional defence mechanisms; make your network virtually invisible to cyber attackers. Our advanced system shields your systems from internet-wide scanning, a primary method used by adversaries to pinpoint new targets. With the CIG, you're not just protected; you're off the radar. Dive into a safer digital future, where subscription-based excellence ensures you're always a step ahead of threats.

Integrating your site with the CIG is a straightforward process, designed with flexibility and security in mind. Whether you're a fan of the robustness of IPSec or the agility of WireGuard, you are covered:

- IPSec – Stability Meets Security: IPSec offers a tried-and-tested method, ensuring data confidentiality, integrity, and authentication.
- WireGuard – Sleek & Speedy: WireGuard, the modern VPN protocol, is known for its lightweight design and superior performance.

Cloaking Engine

The exclusive Cloaking Technology of Internet 2.0's Cloaking Internet Gateway (CIG) 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-as-a-Service

Fully configurable Next-Gen Firewalls 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.

Advanced Web Protection

Utilising ZenArmor, Web Application Firewall (WAF) filters unwanted HTTP Layer 7 traffic, ensuring efficient bandwidth utilization. It also manages application and service access, effectively neutralizing Real-time Zero Day Attack Campaigns.

Performance & Redundancy

The CIG boasts bandwidth throughput, ensuring swift and uninterrupted data flow even during peak traffic periods. We work with data centers that are certified and competitive bandwidth rates. Its built-in redundancy features, consistent performance and uptime.

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.

AUS: Level 1, 18 National Circuit, Barton, ACT, 2600, Australia   USA: 211 N Union St, Suite 100, Alexandria, VA, 22314
ABN: 17 632 726 946   EIN: 86-1567068

internet2-0.com | 1

Features Overview

Advanced Security: The Cloaking Internet Gateway 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 Internet Gateway continuously scans incoming traffic for known malicious patterns. Upon detection, it instantly blocks the threat, ensuring that harmful data never infiltrates your network.

Manageability: Whether you're safeguarding a small office or a multinational corporation, the Cloaking Internet Gateway helps to provide manage your security. As your business grows, The CIG is always up to the task.

Traffic Shaping: With the Cloaking Internet Gateway, 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 CIG. 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 CIG 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.

ZenArmor® Web Application Firewall (WAF): The Cloaking Internet Gateway integrates seamlessly with ZenArmor®, a powerful WAF designed to protect web applications from a myriad of threats.

- Holistic Web Protection: ZenArmor® defends against SQL injections, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common web application vulnerabilities.
- Real-time Monitoring & Blocking: ZenArmor® continuously monitors web traffic, identifying and blocking malicious requests in real-time, ensuring your applications remain uncompromised.
- Customizable Rule Sets: Tailor your protection based on your specific needs. With ZenArmor®, you can customize rule sets, ensuring that your web applications are shielded without affecting legitimate traffic.
- Advanced Bot Detection: Automated bots can wreak havoc on web applications. ZenArmor's® advanced bot detection mechanisms differentiate between legitimate users and malicious bots.
- Detailed Analytics & Reporting: ZenArmor® provides in-depth analytics and reporting, giving you insights into attempted attacks, blocked requests, and overall traffic patterns.

Reporting with integration to SIEMs or Threat Defence®:

Knowledge is power, and with The CIG, 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.