internet2.0

MILITARY-GRADE

CYBER PROTECTION

IP-1000 Series
Cloaking Firewall
Technical Product Specifications

internet2.0

IP-1000 Series

Introducing the Cloaking Firewall: Invisible Defence for the Cyber Age

Experience next-generation protection with the Cloaking Firewall, 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 Cloaking Firewall, 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.

In the ever-evolving landscape of cybersecurity, the choice between a single or dual firewall system can significantly impact your network's protection and performance. Both configurations offer distinct advantages, allowing you to tailor your defence strategy based on your unique needs. The IP-1000 Series Firewall Appliance allows for the delivery of either for a single firewall or for a virtualized modular dual firewall architecture.

IP-1000 Base

A high calibre single firewall system providing a streamlined approach to network security. With a singular point of management, configuration and maintenance become notably more straightforward, ensuring rapid response times and reduced administrative overhead. This setup is ideal for organizations seeking a balance between robust protection and operational simplicity, ideal at the edge of the network.

IP-1000 DFM (Dual Firewall Modular)

Introduces a customisable added layer of security, embodying the principle of military defence in depth. By deploying two layers of firewalls, your network gains a secondary line of defence, ensuring that even if a threat bypasses the primary firewall, the secondary firewall stands guard. This configuration is particularly beneficial for businesses operating in high-risk environments or those that prioritize maximum security over simplicity.

Cloaking Engine

The exclusive Cloaking Technology of Internet 2.0's IP-1000 series 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.

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 firewall boasts exceptional bandwidth throughput, ensuring swift and uninterrupted data flow even during peak traffic periods. Its built-in redundancy features, including dual power supplies, guarantee consistent performance and uptime.

Encrypted Data Communication

Enable secure data transmission for remote users via VPNs. Site-to-site IPSec protected tunnels can be established between networks. Data encryption is set to AES 256 (GCM preferred).

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.

Scalability: Whether you're safeguarding a small office or a multinational corporation, the Cloaking Firewall scales seamlessly. Its modular architecture allows for easy expansion, ensuring that as your business grows, your firewall is always up to the task.

High Availability: Downtime can be costly. The Cloaking Firewall's high availability features ensure that in the event of hardware failure or other disruptions, traffic is automatically redirected, ensuring continuous network uptime. The IP-1000-DFM can have its firewalls configured for redundancy should a failover occur.

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): Suricata stands 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 Firewall 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 gain insights into network activity with comprehensive logs and analytics or by forwarding logs to a SIEM. Also with the Cloaking Firewall, you're not just limited to in-built analytics. The platform can be integrated with Threat Defence®, an Australian-based cybersecurity company known for its advanced threat intelligence and reporting capabilities.

Full Specifications

System Performance		
Recommended maximum clients	250-1000	
Firewall Throughput (Base | DFM)	U/L: 9.425 Gbps D/L: 9.295 Gbps	U/L: 9.135 Gbps D/L: 8.942 Gbps
OpenVPN Throughput (Base | DFM)	U/L: 9.425 Gbps D/L: 9.265 Gbps	U/L: 9.135 Gbps D/L: 8.942 Gbps
IPDS Throughput (Base | DFM)	U/L: 8.910 Gbps D/L: 9.160 Gbps	U/L: 8.360 Gbps D/L: 8.740 Gbps
IPsec Throughput (Base | DFM) (AES256GCM)	U/L: ~2.50 Gbps D/L: ~2.50 Gbps	U/L: ~2.50 Gbps D/L: ~2.50 Gbps
Maximum Concurrent Sessions	63,000,000	
Networking and Encryption		
IP versions	IPv4, IPv6	
DNS support	DynDNS, DNSSEC	
Routing protocols	RIP, IGRP, EGP, OSPF	
NAT	Dynamic, Static port forwarding	
VPN	AES 128, 192 & 256 (hardware accelerated), IKEv1, IKEv2, PSK, X.509	
Tunnelling	GRE, IPsec, ChaCha20, Curve25519	
VLAN	802.1Q, Max Tags 4094	
Hardware Specifications		
CPU:	Intel(R) Xeon(R) Silver 4314 CPU @ 2.40GHz: (12 or 16 cores, 24 or 32 threads)	
RAM:	128GB (8 DIMMs; Supports 3DS DDR4-3200: RDIMM / LRDIMM / Intel® DCPMM)	
Interfaces	2x Intel® Ethernet Controllers X550 10GbE RJ45	
Interface Options (Any Type)	4x RJ45 1GbE 4x RJ45 10GbE 4x SoC 10GbE SFP+	
Storage	1 TB (10x hot-swap 2.5'' SATA3 drive bays with 4 hybrid NVMe/SATA drive bays)	
MGMT interface	1x OOB RJ45 GbE	
High availability	Active/Passive, Clustering	
Security	Silicon Root of Trust (RoT) – NIST 800-193 Compliant Cryptographically Signed Firmware Secure Firmware Updates Automatic Firmware Recovery System Lockdown	
Power	Dual redundant onboard 240V PSU	
AC Input	700W: 100-140Vac / 50-60Hz 750W: 200-240Vac / 50-60Hz	
+12V	Max: 58A / Min: 0.5A (100Vac-140Vac) Max: 62A / Min: 0.5A (200Vac-240Vac)	
Dimensions	1u Rackmount: 437mm x 597mm x 43mm	
Weight	Net Weight: 11.34 kg Gross Weight: 17.24 kg	
Environmental	Operating Temperature: 10°C ~ 35°C (50°F ~ 95°F) Non-operating Temperature: -40°C to 70°C (-40°F to 158°F) Operating Relative Humidity: 8% to 90% (non-condensing) Non-operating Relative Humidity: 5% to 95% (non-condensing)	