StormWall

sales@stormwall.network

stormwall.network

StormWall **Appliance**

Product Brochure

The top-tier quality of StormWall's cloud protection
— **now inside your perimeter**

What Is StormWall Appliance

StormWall Appliance is an on-premises solution for protecting network infrastructure and services against modern DDoS attacks at OSI layers L3–L5.

The product is built on **StormWall's proprietary technology,** which leverages low-level packet-processing mechanisms (DPDK) and optimized high-speed filtering algorithms.

The system can handle substantial traffic volumes with minimal latency — even under intense DDoS attacks.

What You Get

13 Years of Our Expertise
The solution is built on our expertise in DDoS protection from our cloud platform.

Single All-Inclusive License
Protection at OSI L3–L5, application-layer filters, clustering, dashboards, and API — all included in one license.

Fully Outsourced Protection
Our SOC takes over your protection — writing rules, mitigating attacks, and handling incidents (Private plan).

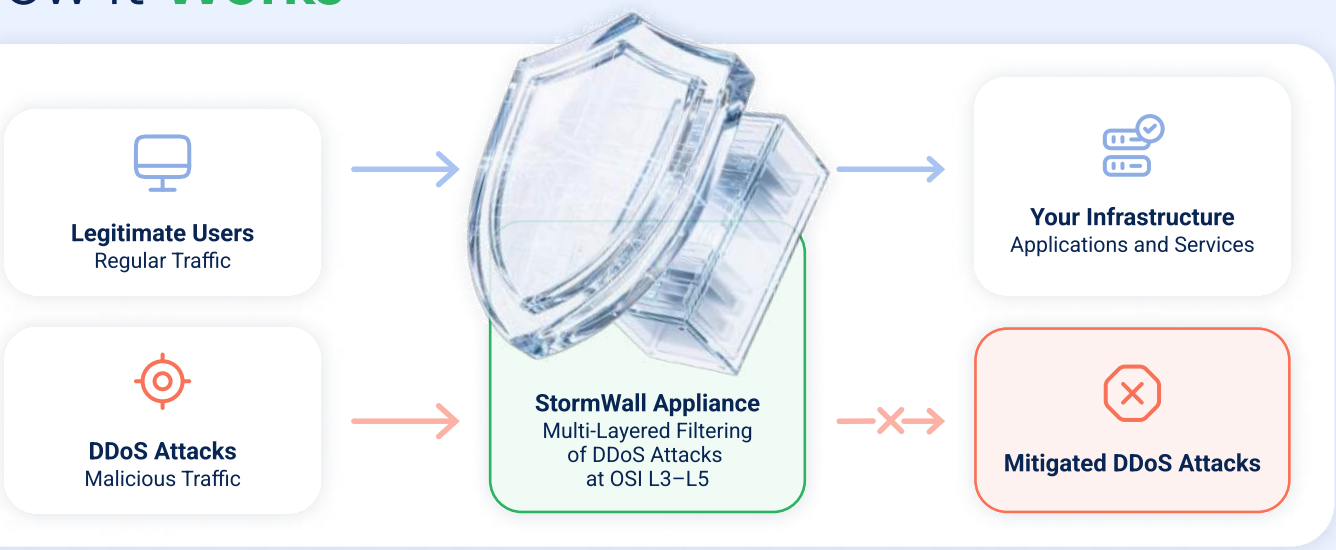
Simple, Fast Integration
The Appliance integrates easily into your infrastructure without requiring major changes to how it operates.

Flexible Licensing
Pay based on active port capacity. License types: Perpetual (one-time payment) or Subscription (from 12 months).

Clustering and Scalability
The solution protects infrastructure of any scale — from individual services to carrier networks.

Compliance-Ready by Design
StormWall Appliance is designed to meet GDPR and PCI DSS obligations, keeping your traffic entirely within your perimeter.

How It Works



Solution Components

Firewall Appliance

The system's management component.

Key functions:

- Centralized configuration management
- Distribution of filtering policies and rules
- Monitoring of filtering-node status
- Collection, storage, and visualization of statistics
- An administration interface and API for managing the system

Filtering Nodes

Process and filter traffic in real time.

Key functions:

- Network traffic analysis and filtering
- Enforcement of protection policies
- Detection and blocking of malicious traffic

DPDK-based packet processing delivers high performance and minimal latency. Each node instance uses a dedicated processor socket, with load distributed across cores.

Attacks It Protects Against

Volumetric DDoS Attacks

Protection against floods and bandwidth exhaustion

Reflection and Amplification Attacks

Filtering of UDP attacks with source spoofing and amplification

Fragmentation Attacks

Filtering of IP fragmentation and MTU anomalies

Attacks on the TCP Stack

Protection against SYN and TCP floods and connection-table exhaustion

Attacks in Encrypted Traffic

Filtering of attacks in TLS/QUIC traffic without decrypting it

Attacks on DNS Services

Protection against DNS floods and other DNS attack vectors

Attacks on Gaming Services

Specialized protection for gaming platforms and protocols

Attacks From Specific Networks

Traffic filtering by ASN, IP prefixes, and network policies

StormWall Appliance provides protection at the network, transport and session layers (OSI L3–L5). OSI L7 attacks are filtered by the **StormWall cloud platform**. The two solutions work together, enabling a **hybrid protection model**.

Included in One License

- DDoS protection at OSI L3–L5
- Protection for gaming protocols: RakNet, SA-MP, CS, Steam
- L7-filter support for DNS, QUIC, and TLS JA3 fingerprinting
- Traffic capture and analysis in PCAP format
- Updates with zero protection downtime
- Works within isolated networks
- Clustering of scrubbing nodes
- Basic support included in year 1
- REST API for external integrations
- Customizable dashboards and metrics

Licensing Models

Subscription (min. 12 months)

Annual prepayment, with optional renewal. Low entry cost and an OpEx model — a flexible fit for a growing company.

Perpetual

One-time purchase — the license is yours forever. Only support is paid for, starting from year 2. Cost-effective if you're planning for 3+ years.

For 2- and 4-processor servers, 2 or 4 software instances are installed respectively. Scrubbing bandwidth is distributed evenly among them. License cost is determined by the combined active port capacity.

The exact cost is calculated individually based on active port capacity, socket count, and support level.

Request a Quote →

Three Support Levels

Basic

17% of cost / year (1st year free)

- Ticket-based support, no guaranteed SLA
- Regular patches and updates
- Documentation and knowledge base
- Client handles attack response and rule configuration independently

For mid-sized teams and growing clients

Most Popular

Advanced

30% of cost / year (+13% in year 1)

- 24/7 ticket intake with guaranteed SLA
- P1/P2/P3 priorities (see below)
- Out-of-cycle patches for non-critical bugs
- Active implementation support

For teams with information-security expertise

Private

Custom, on request

- ✓ StormWall SOC takes over protection 24/7
- ✓ Dedicated technical account manager
- ✓ P1 SLA — immediate, 24/7
- ✓ Rule configuration and attack mitigation handled by our team
- ✓ Regular incident reports

Fully outsourced protection — for teams without in-house DDoS expertise

Incidents by Priority

P1 — CRITICAL

Complete unavailability

Advanced	**1 hour**
Private	**immediately, 24/7**

P2 — HIGH

Partial degradation of the service

Advanced	**8 business hours**
Private	**2 hours**

P3 — NORMAL

Non-critical errors and questions

Advanced	**next business day**
Private	**next business day**

Technical Requirements

Firewall Appliance Management Node

Parameter	Requirements
OS	AlmaLinux 9.0 or later
Architecture	x86_64
Deployment	Physical server or virtual machine (VMware, KVM, Microsoft Hyper-V)
CPU	At least 8 physical CPU cores
Memory	At least 16 GB
Disk	SSD with at least 128 GB
Network	licensing.stormwall.network (ports 8444/9444) + repo.stormwall.network (port 443)

Filtering Node

Parameter	Requirements
OS	Alma Linux 9.X only
Architecture	x86-64-v2 or AMD Zen2
Disk	SSD with at least 64 GB
Deployment	Physical server
CPU	At least 4 physical CPU cores
Memory	At least 16 GB
Bandwidth	As specified by the license
Network adapters	Mellanox Connect 5/6, Intel 7xx

Key Recommendations

- These requirements cover the baseline installation and startup of the system's components.
- Performance depends on the volume of protected traffic, the number of filtering nodes, the number of concurrent connections, and the deployment architecture.
- As the number of nodes increases, so do the requirements for the Firewall Appliance server — primarily memory and disk I/O for storing statistics.
- For high-load deployments, we recommend using supported hardware platforms and dedicated physical servers for filtering nodes.

StormWall

sales@stormwall.network

stormwall.network

How to Get **Started**

01
Qualification
Fill out the questionnaire or request a demo from our sales team. We'll discuss your objectives, traffic volumes, and requirements.

02
Hardware Check
Send us your server configuration — we'll verify compatibility and recommend the optimal setup.

03
License Issuance
The license is issued for your specific configuration: active port capacity, support level, and number of installations.

04
Installation
The solution is installed from our private repository. Deployment takes as little as one day.

05
30-Day Free Trial
Evaluate under live traffic free of charge, then move directly into commercial operation.

Why **StormWall Appliance**

- ✓ Consultation on architecture and deployment options
- ✓ Product demo based on real-world scenarios
- ✓ Pilot testing within your infrastructure
- ✓ Selection of the optimal configuration and licensing model
- ✓ Fast quote preparation
- ✓ On-site support (for government agencies and critical information infrastructure operators)

Ready to Protect Your **Infrastructure?**

Contact us — we'll walk you through the details, show you a live demo, and help you choose the right configuration.

Submit a Request