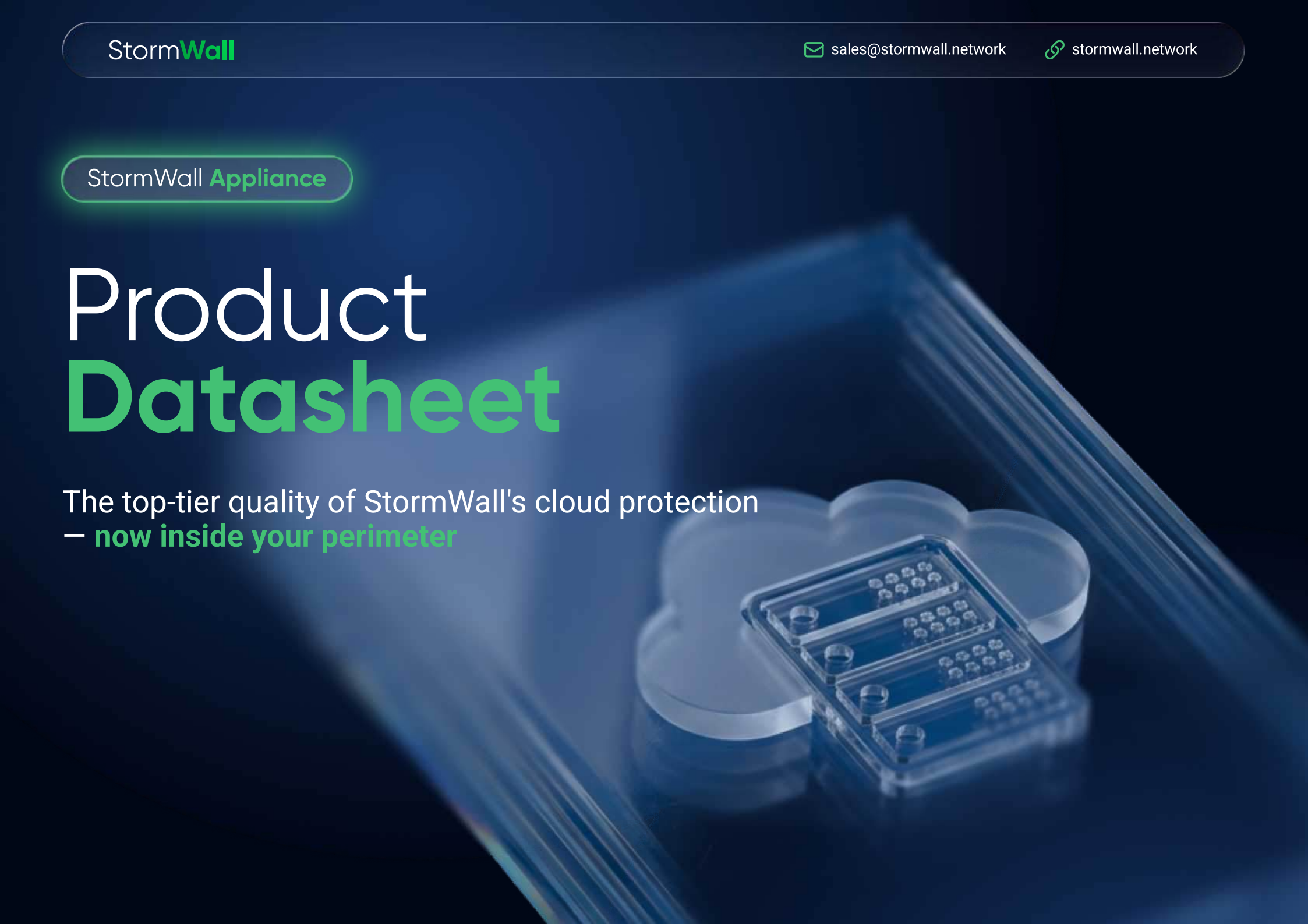
StormWall **Appliance**

Product Datasheet

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



StormWall Appliance

L3–L5 DDoS protection deployed within the customer infrastructure

1. Overview

Telecommunications operators, cloud providers and enterprises face a common problem: DDoS attacks remain the primary risk to service availability, and their scale, sophistication and frequency continue to grow. Attacker tactics have evolved — IoT botnets, off-the-shelf DDoS toolkits and stresser-for-hire services have made attacks cheap and widespread, while legacy defenses such as signature-based IPS and simple rate limiting can no longer keep up. What is needed is protection that separates attack traffic from legitimate traffic without disrupting business services — effective, cost-efficient and easy to manage.

StormWall Appliance is a software solution for protecting network infrastructure and services against DDoS attacks at OSI layers L3–L5. The product is deployed in the customer infrastructure and performs local traffic processing and filtering. The solution is shipped as software and does not require a proprietary hardware platform.

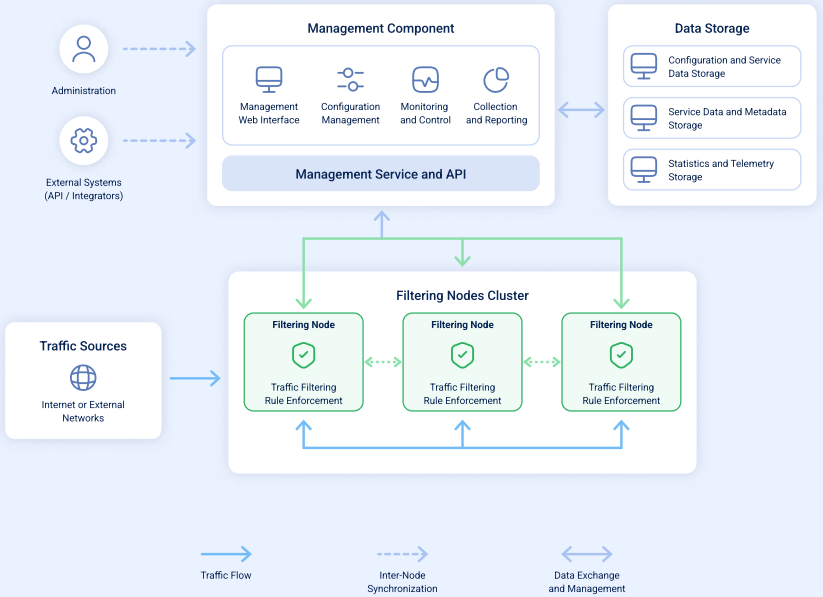
Solution Architecture

StormWall Appliance consists of two main components:

- **Firewall Appliance** — the management component that includes the web interface, backend services and management subsystem. It provides centralized control of the system, configuration of filtering policies, statistics collection and health monitoring of the Filtering Nodes.
- **Filtering Nodes** — servers that analyze and filter user traffic in real time. Nodes operate in parallel in an Active-Active configuration, providing horizontal performance scaling and system fault tolerance. Runtime state is synchronized directly between nodes, independently of the management component.

Key Benefits

- Broad DDoS attack coverage. A multi-layered filtering system delivers protection against attacks at OSI layers L3–L5, including TCP-, UDP- and protocol-oriented attacks, using per-packet inspection and TLS ClientHello analysis without decrypting user traffic.
- Deployment within the customer infrastructure. The solution processes and filters traffic locally, making it possible to meet data residency, information security and industry regulatory requirements.
- Hardware-agnostic software architecture. The product is delivered as software and supports deployment on physical servers and in virtual environments that meet the system requirements.
- Horizontal scaling. The Active-Active architecture makes it possible to grow system performance by adding Filtering Nodes without changing service logic. High-performance packet processing based on DPDK ensures efficient use of compute resources.
- High availability. All Filtering Nodes participate in traffic processing simultaneously. If a node fails, traffic is automatically redistributed across the remaining nodes; if the management component becomes unavailable, filtering continues using the previously loaded configuration.
- Centralized management. A single management interface provides configuration of protection policies, system health monitoring, access to statistics and centralized control of all Filtering Nodes.



Architecture and Components of StormWall Appliance

Firewall Appliance

Firewall Appliance is the management component of the system. It provides centralized control of Filtering Nodes, configuration of protection policies, monitoring of system state and collection of statistics.

Main functions:

- centralized configuration management;
- distribution of filtering policies and rules;
- health monitoring of the Filtering Nodes;
- collection, storage and visualization of statistics;
- administrative interface and API for system management.

The following data stores are used:

- **PostgreSQL and MySQL — configuration and service data;**
- **ClickHouse — statistics and telemetry.**

Filtering Nodes

Filtering Nodes analyze and filter user traffic in real time.

Main functions:

- analysis and filtering of network traffic;
- enforcement of protection policies;
- detection and blocking of malicious traffic;
- exchange of runtime information between cluster nodes.

Packet processing is implemented using DPDK, delivering high traffic throughput and minimal latency. Each Filtering Node instance is bound to a dedicated CPU socket, and the compute load is distributed across the cores of that CPU.

Fault Tolerance

Filtering Nodes operate in an Active-Active configuration, participating in user traffic processing at the same time.

Internal state is synchronized directly between the Filtering Nodes, independently of the management component. If Firewall Appliance becomes unavailable, traffic processing and filtering continue using the previously loaded configuration. In this state, centralized management functions, configuration changes and statistics viewing are not available.

Scalability

The solution supports several deployment options:

- deployment of the management component and a Filtering Node on the same physical server;
- deployment of the management component and a Filtering Node on the same physical server;
- deployment in a virtual environment;
- geographically distributed architecture.

Multiple Filtering Node instances may be launched on a single physical server. As the number of Filtering Nodes grows, the load rises primarily on the management server — in particular, its RAM and disk subsystem used to store statistics in **ClickHouse.**

3. Deployment Options

The architecture of StormWall Appliance supports several deployment options depending on performance, high-availability and available compute infrastructure requirements. The management component and the Filtering Nodes may be deployed on a single physical server, on separate servers or in a virtual environment, including geographically distributed installations.

3.1. Compute Resource **Allocation Principles**

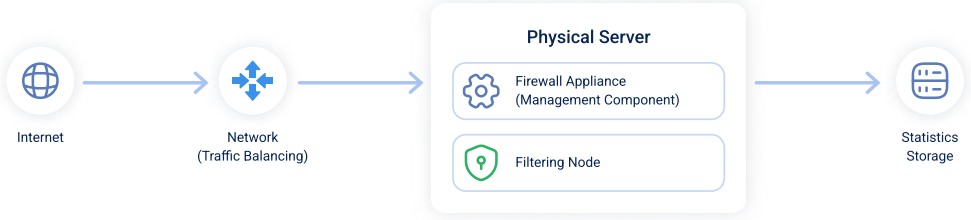
- **One Filtering Node instance — one physical CPU.** To achieve maximum performance, each Filtering Node instance is allocated a dedicated physical CPU. Traffic processing is distributed across the compute cores of that CPU.
- **Performance scaling.** On servers with multiple CPUs, several Filtering Node instances may be deployed — one per CPU. The number of instances is determined by the server hardware configuration and the licensing parameters.
- **Flexible placement of the management component.** Firewall Appliance does not require a dedicated CPU and may be deployed on the same server as the Filtering Nodes, on a separate physical server or in a virtual machine.
- **System scaling.** As the number of Filtering Nodes grows, the load rises primarily on the Firewall Appliance server — in particular, its RAM and disk subsystem used to store statistics. CPU compute requirements increase only marginally.

3.2. Standard Deployment **Configurations**

Configuration	Description
Co-located deployment	Firewall Appliance and one Filtering Node are deployed on the same physical server
Multi-CPU filtering server	A single physical server hosts several Filtering Node instances — one per physical CPU. Firewall Appliance may be deployed on the same server or separately
Distributed deployment	Firewall Appliance is deployed on a separate physical server or in a virtual machine (VMware, KVM, Hyper-V); Filtering Nodes are deployed on dedicated physical servers
Geographically distributed deployment	The management component is placed in a central location, while the Filtering Nodes are distributed across geographical locations

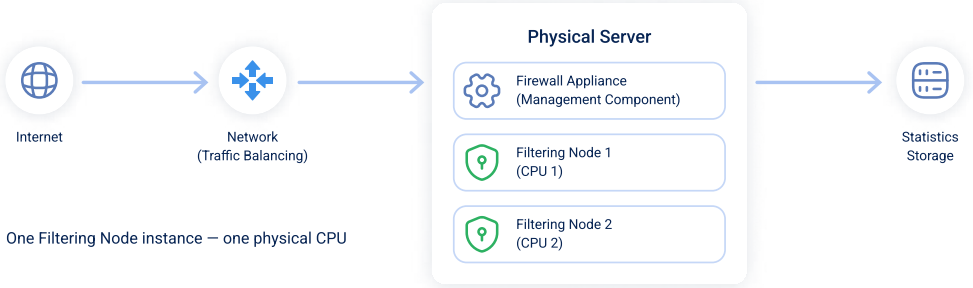
01 Co-Located Deployment

Firewall Appliance and one Filtering Node are deployed on the same physical server.



02 Multi-CPU Filtering Server

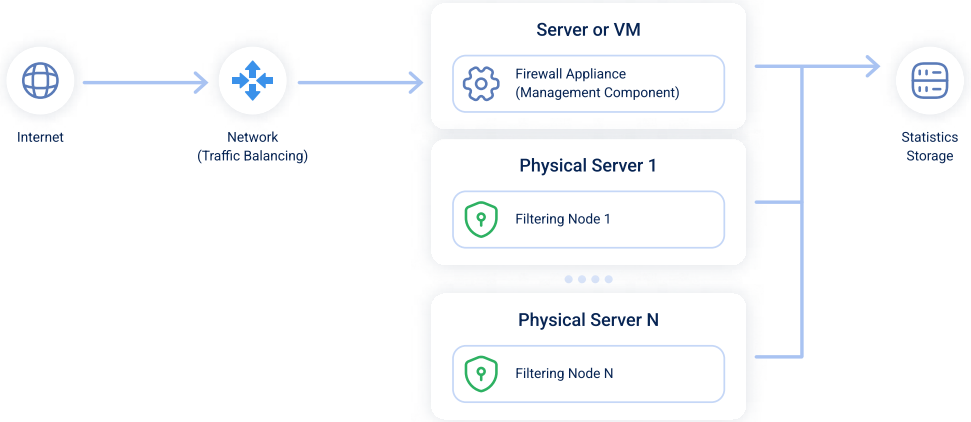
A single physical server hosts several Filtering Node instances — one per physical CPU. Firewall Appliance may be deployed on the same server or separately.



One Filtering Node instance — one physical CPU

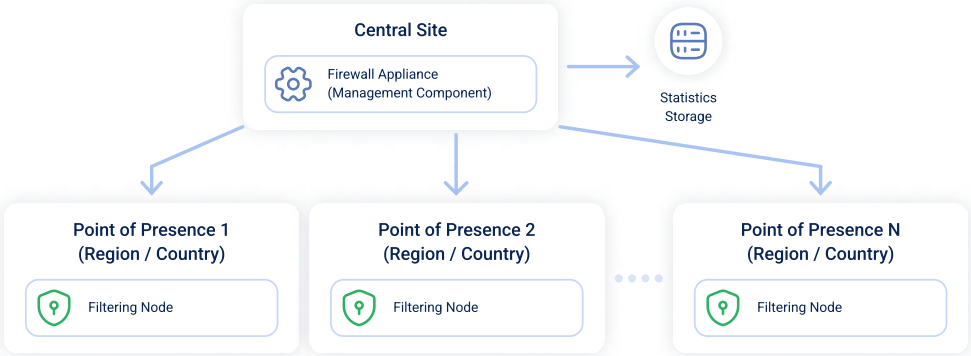
03 Distributed Deployment

Firewall Appliance is deployed on a separate physical server or in a virtual machine, and Filtering Nodes — on dedicated physical servers.



04 Geographically Distributed Deployment

The management component is placed in a central location, and Filtering Nodes are distributed across geographical locations.



Common Operational Principles

Regardless of the selected deployment configuration, the system operates on common principles:

- Filtering Nodes operate in an Active-Active configuration;
- runtime data is synchronized directly between the Filtering Nodes;
- user traffic is distributed across the nodes by the external network infrastructure;
- if a Filtering Node fails, its traffic is automatically redistributed across the remaining nodes;
- if Firewall Appliance becomes unavailable, the Filtering Nodes continue processing traffic using the previously loaded configuration.

4. Threat Landscape and Supported DDoS Attack Types

4.1. Modern DDoS Threats

Modern DDoS attacks are characterized by high intensity, use of multiple attack vectors and rapid changes in scenarios during the attack. Common attack sources include botnets, distributed networks of compromised devices (IoT), DDoS-for-hire platforms (Stresser/Booter) and specialized traffic generation tools.

In practice, adversaries combine several methods at once — volumetric attacks, attacks on network and transport protocols, and attacks aimed at exhausting the resources of protected services.

StormWall Appliance detects and filters DDoS attacks at OSI layers L3–L5 and provides protection against the most common modern attack vectors.

4.2. Mitigation of Different DDoS Attack Types

Filtering is performed in real time based on per-packet inspection. Each packet is sequentially examined by a set of specialized protection mechanisms and filtering rules, after which legitimate traffic is forwarded to the protected infrastructure. Security policies are composed of ready-to-use protection mechanisms and can be adapted to the specifics of the protected services.

Attack Class	Examples
TCP protocol attacks	SYN Flood, SYN/ACK Flood, ACK Flood, FIN/RST Flood, TCP Spoofing, malformed TCP flags, etc.
TCP connection table exhaustion	Established-connection floods, slow connections, etc.
L3/L4 packet-based attacks	UDP Flood, ICMP Flood, IP Protocol Flood, PPS Flood
Reflection / Amplification	DNS Reflection, NTP Reflection, SSDP, CLDAP, Memcached and other UDP reflection attacks
IP fragmentation attacks	Fragment Flood, ICMP Fragment Flood, UDP Fragment Flood
DNS attacks	DNS Flood, malformed DNS queries, resource-intensive record-type queries
TLS and QUIC attacks	TLS ClientHello Flood, QUIC Flood, bot traffic in encrypted connections
Attacks on gaming services	Steam Query Flood, Source Engine Query, FiveM, RakNet, SA-MP, TeamSpeak 3
Attacks from specific networks and regions	Botnets from specific ASNs, geo-based attacks, Carpet Bombing
Abnormal IP packet parameters	MTU violations, abnormal packet sizes

Note: The set of filtering mechanisms and supported protocols is continuously extended as new DDoS countermeasures become available.

5. Protection Mechanisms and Countermeasures

StormWall Appliance uses a multi-layered protection system that combines specialized mechanisms for traffic analysis, filtering and management. Security policies are composed of ready-to-use protection mechanisms and can be adapted to the specifics of the network infrastructure, application services and the profile of legitimate traffic.

Filtering is performed in real time based on per-packet inspection. Protection mechanisms can be used jointly, providing effective mitigation of both individual attack vectors and complex multi-vector DDoS attacks.

Mechanism	Capabilities
TCP protocol protection	Validation of TCP traffic against RFC requirements, including correctness of connection establishment, packet sequencing, TCP flags, fragmentation handling and connection lifecycle management. Protection mechanisms based on RFC 793 (Transmission Control Protocol), RFC 1122 (Requirements for Internet Hosts), RFC 1323 (TCP Extensions for High Performance), RFC 2018 (Selective Acknowledgment), RFC 5961 (Improving TCP's Robustness to Blind In-Window Attacks) and RFC 6528 (Defending against Sequence Number Attacks) are supported
Rate limiting	Bandwidth (BPS) limits, packet-rate (PPS) limits, limits on new and active TCP connections, multi-tier cascade rate limiting, resource-exhaustion protection
DNS protection	Native DNS filters supporting RFC 1034 (Domain Names — Concepts and Facilities) and RFC 1035 (Domain Names — Implementation and Specification). DNS packet validation, filtering by record type, domain name and query class, and DNS traffic rate limiting
TLS and QUIC protection	Analysis of TLS ClientHello parameters without decrypting user traffic, in accordance with RFC 5246 (TLS 1.2), RFC 8446 (TLS 1.3), RFC 6066 (Server Name Indication, SNI), RFC 7301 (Application-Layer Protocol Negotiation, ALPN), RFC 8999 (Version-Independent Properties of QUIC) and RFC 9000 (QUIC Transport Protocol). Supports JA3/JA4 fingerprint analysis, TLS version checks, SNI, ALPN, and QUIC client authorization
Challenge-based authorization	Verification of client legitimacy using challenge mechanisms for the protection of gaming and specialized protocols
Geo and ASN filtering	Traffic filtering by country, autonomous system (ASN) and other network attributes
Static and dynamic access lists	IP allowlists and blocklists, IP Sets support, dynamic access lists with automatic time-to-live (TTL). Rules can be composed of multiple parameters including source and destination IP addresses, subnets, port numbers, transport protocols and their combinations
Deep Packet Inspection (DPI)	Filtering by network- and transport-protocol header values, individual packet fields, value ranges, hex masks, byte offsets, payload signatures, packet sizes and custom traffic-processing conditions
Packet parameter enforcement	Enforcement of packet size limits, PMTUD support (RFC 1191), IP fragmentation handling (RFC 791, RFC 815), filtering by protocol, port, packet type and other network-traffic parameters
Integration with network infrastructure	Transparent L2 insertion, VRF integration, operation within the existing network infrastructure
Monitoring and analytics	Collection of traffic and security-event statistics, storage and visualization of data in a single web interface
Management and automation	Centralized management via the web interface; REST API for configuration automation, security-policy management, statistics retrieval and integration with external systems

Note: The set of filtering mechanisms and supported protocols is continuously extended as new DDoS countermeasures become available.

6. Supported Hardware Platforms

To achieve the stated performance, ensure stable operation and receive full technical support, we recommend using hardware platforms that have passed internal StormWall testing. Deployment on platforms outside the list of tested configurations is permitted; in such cases the compatibility of the hardware is assessed on a case-by-case basis.

6.1. General Requirements

Parameter	Requirement
Architecture	x86-64-v2 or AMD Zen2
Minimum configuration of a Filtering Node	4 physical compute cores; 16 GB RAM; at least 64 GB disk; a network adapter with at least 1 Gbps bandwidth
Traffic processing	HugePages support and a DPDK-compatible network adapter are required
Power management	Adaptive power management is supported at the traffic-processing level. CPU frequency control must be delegated to the operating system

6.2. Processors

Vendor	Requirements and Compatibility	Tested by StormWall
AMD	AMD EPYC processors based on Zen 2 architecture or higher	EPYC 7702 (64 cores), EPYC 7742 (64 cores), EPYC 7543 (32 cores), EPYC 7763 (64 cores), EPYC 7773X (64 cores)
Intel	Intel Xeon processors supporting the x86-64-v2 architecture or higher, including the Intel Xeon Scalable line	Xeon E5-2696 v4 @ 2.20 GHz, Xeon E5-2699 v4 @ 2.20 GHz, Xeon E5-2699A v4 @ 2.40 GHz

Later generations of the specified processor lines are considered compatible provided that the architecture and instruction-set requirements are met. Compatibility of a specific model outside the list of tested configurations is confirmed on request.

6.3. Supported Network Adapters

Network adapters with DPDK support that have passed internal StormWall testing are supported.

Physical Adapters

Vendor	Driver	Compatible Models	Tested by StormWall
Intel	i40e	Intel 7xx	Intel Ethernet Controller XL710 for 40GbE QSFP+
NVIDIA (Mellanox)	mlx5	ConnectX-5, ConnectX-6	MT27800 — ConnectX-5, MT28800 — ConnectX-5 Ex, MT2892 — ConnectX-6 Dx

Virtual Adapters (for deployments in virtual infrastructure)

Adapter	Virtualization Platform
VirtIO	QEMU
VMXNET3	VMware

Please use the latest available driver version and virtualization components for the corresponding platform.

6.4. Server Platforms and BIOS Settings

The StormWall Appliance solution is not tied to servers from any specific vendor. Server platform compatibility is determined by the ability to apply the required BIOS settings and the required hardware configuration. If needed, compatibility of a specific server platform is assessed individually.

A Filtering Node supports adaptive power management: CPU core frequency changes with the current traffic-processing load. For this mechanism to work, CPU frequency control must be delegated to the operating system and deep C-states must be disabled.

To ensure stable and predictable DPDK performance on filtering servers, a BIOS profile aimed at maximum performance must be used. NUMA must be enabled; network adapters must be installed in PCIe slots with sufficient bandwidth and must be local to the NUMA node on which the DPDK threads run.

CPU and PCIe power-saving settings should be disabled. DPDK threads should be pinned to physical CPU cores. Specific NUMA/NPS values and other platform-dependent parameters are determined based on the server, CPU and network adapter architecture.

Functional BIOS-Settings Requirements

BIOS Parameter	AMD	Intel	Requirement / Value	Priority
System Performance Profile	✓	✓	Performance / Maximum Performance	Required
NUMA	✓	✓	Enabled	Required
NUMA / NPS configuration	✓	✗	NPS1/NPS2/NPS4 chosen based on CPU, memory and NIC topology	Must be configured
NUMA memory optimization	✓	✓	Enabled; memory should be evenly distributed across NUMA nodes and memory channels	Required
NIC placement relative to NUMA	✓	✓	The NIC must be connected to a PCIe slot local to the NUMA node running the DPDK threads	Critical
CPU C-States	✓	✓	Disabled — to minimize latency and improve performance predictability	Recommended
Deep CPU power states (C3/C6 and equivalents)	✓	✓	Disabled	Recommended

Functional BIOS-Settings Requirements

BIOS parameter	AMD	Intel	Requirement / Value	Priority
CPU power management	✓	✓	Performance mode	Recommended
SMT / Hyper-Threading	✓	✓	Enabling is recommended	Recommended
Memory frequency	✓	✓	Maximum supported by the CPU and installed memory modules	Recommended
Memory module population	✓	✓	Symmetric channel population according to the server vendor's recommendations	Required
PCIe ASPM / PCIe power saving	✓	✓	Disabled for network adapters	Recommended
PCIe speed	✓	✓	Maximum supported by the network adapter, CPU and motherboard	Must be verified
Above 4G Decoding	✓	✓	Enabled	Required and recommended
Hardware Prefetcher	✓	✓	Enabled / vendor default	Recommended
AMD IOMMU / Intel VT-d	✓	✓	Enabled when using VFIO or SR-IOV; not required for standard DPDK access to a physical NIC	As needed
SR-IOV	✓	✓	Enabled only when using virtual functions (VF)	As needed
Hardware virtualization (AMD-V / Intel VT-x)	✓	✓	Enabled when using virtualization; not required for DPDK on a physical server	As needed
AMD Determinism Control	✓	⊗	For the performance profile, use the mode that delivers maximum and predictable performance	AMD
L3 Cache as separate NUMA nodes	✓	⊗	Disabled as the baseline configuration; changes are allowed only after verifying the performance of a specific platform	AMD
Intel SpeedStep / equivalent dynamic frequency control	⊗	✓	For older Intel generations — disabled when using a fixed performance profile; on modern Xeon controlled by the vendor performance profile	Intel
Energy Efficient Turbo	⊗	✓	Disabled if minimum latency and performance predictability are the priorities	Intel

6.5. Use of Untested Hardware Platforms

StormWall allows the solution to be deployed on hardware platforms not included in the list of tested configurations.

In such cases:

- StormWall specialists provide consulting support for installation and configuration;
- hardware compatibility is assessed on a case-by-case basis;
- the stated performance, scalability and fault-tolerance characteristics are not guaranteed;
- if hardware-specific issues are identified, support may recommend switching to one of the tested platforms.

7. System Requirements

The following requirements are the minimum required to install and run StormWall Appliance components. The recommended hardware configuration is determined by the deployment architecture, the volume of protected traffic, the number of Filtering Nodes and the retention period of statistical data.

7.1. Firewall Appliance Server

Parameter	Minimum Requirement
Operating system	AlmaLinux 9.0 or later
Architecture	x86_64
Deployment platform	Physical server or virtual machine (VMware, KVM, Microsoft Hyper-V)
CPU	At least 8 physical compute cores
RAM	At least 16 GB
Disk subsystem	SSD, at least 128 GB
Network connectivity	HTTPS access (ports 8444 and 9444) to licensing.stormwall.network and HTTPS (TCP/443) to repo.stormwall.network

Notes:

- When deployed in a virtual environment, guest tools compatible with the Linux kernel in use must be installed.
- At least 30 GB of disk space is recommended for system components and at least 50 GB for ClickHouse statistics storage.

7.2. Filtering Node Server

Parameter	Minimum Requirement
Operating system	Alma Linux 9.X only
Architecture	x86-64-v2 or AMD Zen2
Deployment platform	Physical server
CPU	At least 4 physical cores
RAM	At least 16 GB
Disk	At least 64 GB
Bandwidth	Per the licensing parameters
Network adapters	Per the licensing parameters. At least one adapter with 1 Gbps or higher bandwidth and DPDK support

Notes:

- A dedicated physical CPU must be used for each Filtering Node instance.
- When deployed in a virtual environment, guest tools compatible with the Linux kernel in use must be installed.
- To achieve the stated performance, we recommend using the supported server platforms, processors and network adapters listed in Section 6.

General Recommendations

- The minimum system requirements are sufficient to install and run system components.
- Actual performance depends on the volume of protected traffic, the number of Filtering Nodes, the number of concurrent connections and the chosen deployment architecture.
- As the number of Filtering Nodes grows, the load rises primarily on the Firewall Appliance server — first and foremost, its RAM and the disk subsystem used to store statistics.
- For high-load installations, dedicated physical servers on supported hardware platforms are recommended for the Filtering Nodes.

8. Licensing

StormWall Appliance uses a software licensing system. The primary licensing parameter is the active port capacity. Depending on the selected license, the maximum available hardware resources of the Filtering Nodes are also defined, including the number of CPU cores, RAM size and maximum bandwidth.

By default, an online licensing model is used, in which the Firewall Appliance management component requires access to the licensing server at licensing.stormwall.network over HTTPS (ports 8444 and 9444) for license activation and periodic status checks. Once network connectivity is restored, license activation may be performed without reinstalling the system.

For infrastructures without external network access or with elevated isolation requirements, an offline licensing model is available. In this case, the license is delivered as an individual Guardant hardware key, allowing the system to operate without connecting to the StormWall licensing server.

StormWall Appliance

For any questions related to deploying the solution,
please use the contacts below:

+44 20 3695 6722

sales@stormwall.network

https://stormwall.network