SKUDONET

TRY SKUDONET FOR 30 DAYS
info@skudonet.com / SKUDONET.com

Enterprise Edition

Open Source Load Balancer & Application Delivery Controller

SKUDONET Enterprise Edition is a highly scalable and secure load balancing and ADC solution designed to handle large volumes of traffic in any environment—physical, virtual, or cloud. Built on Linux Debian, it combines open-source innovation with advanced enterprise-grade features, without hidden costs or the complexity of other providers.

Why SKUDONET Enterprise Edition?

All-inclusive from the start

SKUDONET Enterprise Edition integrates all advanced features and continuos updates without the need for additional modules.

Advanced Security Features

Integrated Web Application Firewall (WAF), real-time blacklists, DoS/DDoS mitigation, and SSL/TLS encryption.

Scalability & High Availability

Multi-node clustering, real-time session replication, and failover mechanisms designed for high-traffic.

Optimized Traffic Control

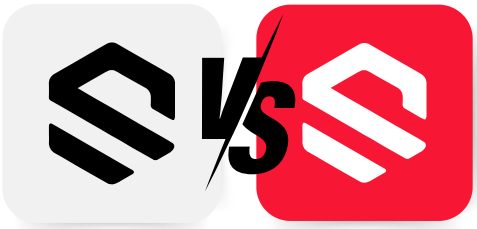
Multi-protocol balancing (HTTP/S, TCP, UDP, SIP, WebSockets), session persistence and intelligent traffic routing.

Flexibility Across Environments

Deployable on virtual machine, bare metal environments, on-premises infrastructures, and public & hybrid cloud.

Expert Support

Dedicated 8x5 or 24x7 support options ensure fast response times and access to expert engineers.



Feature Comparison Table

Features	Community Edition	Enterprise Edition
Advanced HTTP	✗	✓
Advanced TCP Load Balancing and Persistence	✓	✓
Advanced UDP Load Balancing	✓	✓
Advanced Health Checks	✗	✓
Automation (API REST+JSON)	Basic	✓
Advanced Security	✗	✓
Real-Time Monitoring and Logs	Limited	✓
Automatic Upgrades	Basic	✓
Technical Support	✗	✓
Stateful Cluster and High Availability	✗	✓
SSL/TLS Termination and Inspection	✗	✓
DDoS Protection	✗	✓
Botnets Protection	✗	✓
Configuration Backup and Replication	Limited	✓
Web Application Firewall (WAF)	Limited	✓
Global Service Load Balancing (GSLB)	✗	✓

SKUDONET Enterprise Features

Security

- **Reverse Proxy**
  Route all Internet traffic to your application servers through SKUDONET, ensuring that only intended services are exposed while logging all requests.

- **HTTP Validation**
  Inspect incoming requests to ensure they adhere to HTTP protocol specifications before passing requests to application servers.

- **Advanced DDoS Protection**
  Detects and blocks malicious traffic using adaptive filtering based on predefined metrics and thresholds.

- **Anomalous Behavior Protection**
  Identifies and mitigates unusual traffic patterns by evaluating multiple behavioral indicators.

- **Security Rule Management**
  Allows real-time updates to security rules and configuration in memory without requiring a service restart.

- **Traffic Management**
  Employ security rules to analyze HTTP(S) traffic conditions, enabling the routing or blocking of requests based on defined criteria.

- **Botnets Protection**
  Detect and mitigate threats from malicious bots, ensuring protection against unauthorized data scraping and automated attack attempts.

- **Real-time block list**
  Connects to our real-time blocking system using DNS, providing protection against zero-day attacks.

- **Header Validation Module**
  Ensure that HTTP header names and contents are properly filtered and conform to established HTTP standards for security and compliance.

- **Reporting system**
  The system includes an attack reporting module that allows searches by date and exports reports to PDF for further analysis.

- **Web Application Firewall (WAF)**
  Implement an advanced WAF that offers comprehensive protection against a wide range of threats, including SQL injection, cross-site scripting, and other vulnerabilities.

Load Balancing

- **Multi-Method Load Balancing**
  Employ a variety of load balancing techniques, including round robin, least connections, URI-based distribution, and IP address balancing, to optimize traffic management

- **Intelligent Traffic Routing**
  Route requests to designated application clusters based on host and URL, as well as other factors such as backend health status, number of active connections, and SSL client certificate, ensuring optimized traffic management.

- **Stickiness/Persistence**
  Ensure user sessions are maintained using TCP/IP information or various HTTP request attributes, to provide a consistent and seamless experience across multiple requests.

- **Robust Security Rules Engine**
  Implement a sophisticated system of security rules that utilize various TCP/IP information and HTTP attributes.

- **Global Server Load Balancing (GSLB)**
  Distribute client requests across geographically diverse data centers, ensuring high availability through intelligent routing.

- **Bandwidth Management**
  Manage and control the bandwidth of incoming and outgoing data through your load balancers to prevent congestion and reduce latency.

High Availability

Health Monitoring
Utilize a combination of active and passive health checks to monitor backend servers and ensure only healthy instances receive requests.

Uplink Load Balancing
Distributes communication lines and internet connections, aggregating bandwidth and ensuring redundancy for network connectivity.

Connection Limiting
Control the maximum number of concurrent connections to application servers by redirecting excess traffic to alternative server clusters or queuing requests when the set limit is reached.

Seamless Configuration Reloads
Ensure uninterrupted service by reloading the configuration without dropping existing connections.

Stateful Cluster
Maintain session persistence and application state across a cluster of servers, ensuring that user sessions are consistently routed to the same server throughout their lifecycle.

Virtual Router Redundancy Protocol
A robust implementation designed for active/passive clustering, ensuring fault tolerance by allowing multiple routers to function as a single virtual router.

Traffic Shadowing
Duplicate incoming requests from one environment to another for safe testing of new features and updates. This method allows for the identification of bugs, CVEs, and zero-day vulnerabilities, ensuring enhancements are thoroughly vetted before live deployment.

Administration

Dynamic Configuration Interface
Facilitate real-time adjustments to configuration and operational parameters, allowing for seamless modifications and monitoring of load balancing processes without interrupting service availability.

Dynamic DNS Service Management
Utilizes DNS queries to dynamically manage and scale application servers, enabling efficient service discovery and load balancing by integrating with a service registry.

Multi-Server Provisioning
Facilitate the rapid deployment of numerous application servers using a unified template, enabling efficient runtime configuration and management.

Configuration Management API
Enable programmatic control over your setup by utilizing an HTTP interface to efficiently add, alter, or delete configuration sections.

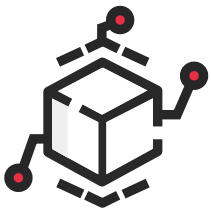
Let's Encrypt
Uses a connector to Let's Encrypt for creating and managing digital certificates, ensuring secure communications. Includes integration with cloud providers such as Azure, AWS, Linode, Namecheap, and more.

Monitoring
Real-time data on traffic volume and the status of load-balanced services, allowing for adjustments to the balanced traffic.

Request Logging
Capture detailed request information with robust logging capabilities, supporting both syslog and cloud-native logging solutions.

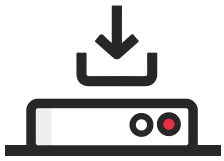
Security rules with LUA Scripting
Enhance your security protocols by integrating Lua scripts that interact with the request and response flow.

ENTERPRISE EDITION PRODUCTS



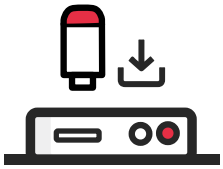
SVA10000 Virtual Appliance

Integrate SKUDONET into your virtual environment with pre-installed templates.



Hardware Load Balancer

A robust, specialized hardware ADC designed for optimal performance.



SBA10000 Bare Metal Appliance

Install SKUDONET on your existing hardware with a ISO image.

Cloud Load Balancer

Deploy SKUDONET in AWS or Azure, and scale effortlessly with your cloud infrastructure.

SERVICE PLANS

Basic Plan

450€
/ node per year *

Includes

- ☑ **Software Updates & Product Upgrades**
- ☒ No technical support
- ☒ No remote assistance
- ☒ No assistance in case of system failures
- ☒ No cybersecurity services

Standard Plan

950€
/ node per year *

Includes

- ☑ **Software Updates & Product Upgrades**
- ☑ **Technical support via ticket**
- ☑ **Max response time of 8 working hours**
- ☒ No remote assistance
- ☒ No phone call service
- ☒ No cybersecurity services
- ☒ No collaboration with technical teams

Advanced Plan

2,500€
/ node per year *

Includes

- ☑ **Software Updates & Product Upgrades**
- ☑ **Technical support via ticket**
- ☑ **Access to remote assistance**
- ☑ **Max response time of 8 hours and 4 for system outages**
- ☑ **24x7 call service for critical issues**
- ☑ **Cybersecurity services**
- ☑ **Collaboration with third-party technical teams**