

# Fortinet FortiWeb

?????????? ?? ???????????

Fortinet FortiWeb — это специализированный Web Application Firewall, предназначенный для защиты веб-приложений и API от угроз уровня HTTP/HTTPS. Решение выявляет и блокирует атаки из OWASP Top 10, поведенческие аномалии, попытки brute force/credential stuffing, вредоносных ботов, нарушения схем API и ошибки протоколов. FortiWeb может работать в режимах reverse-proxy, transparent и load balancer, контролируя весь трафик между клиентом и backend-серверами.

Помимо классического WAF-функционала, FortiWeb использует машинное обучение для анализа нормального поведения запросов, включает антибот-механизмы, инспекцию загрузок файлов, защиту API, контроль целостности cookie и Web-DLP для предотвращения утечки чувствительных данных (PCI/PII, файлы, ключевые слова). Система формирует отдельные журналы системных событий, трафика, атак, DLP-срабатываний, аномалий ML и ошибок backend-служб, обеспечивая подробную видимость веб-активности и инцидентов безопасности.

## Типы собираемых событий:

- **System Events** — изменение конфигурации, логины/логауты админов, ошибки служб, обновления сигнатур, состояние HA.
- **Traffic Events** — HTTP/HTTPS запросы, методы, URL, статус-коды, размеры запросов/ответов, время обработки.
- **Attack Events (WAF Security)** — SQLi, XSS, Command Injection, Path Traversal, File Inclusion, Protocol Anomalies, Brute Force, Credential Stuffing.
- **Machine Learning Anomalies** — отклонения от нормального поведения, аномальная структура запросов, параметры, частота запросов.
- **Bot Mitigation** — обнаружение вредоносных ботов, скраперов, автоматизированных клиентов, нарушения браузерных проверок.
- **DLP Events** — потенциальная утечка данных: PCI/PII, конфиденциальные шаблоны, ключевые слова, файлы в upload.
- **File Upload Protection** — результаты антивирусной проверки, недопустимые типы файлов, ошибки анализа архивов.
- **API Protection Events** — нарушения схемы OpenAPI, неправильные методы, неожиданные параметры, ошибки JSON/XML.
- **Threat Intelligence Hits** — совпадения с FortiGuard: злонамеренные IP, ботнет-источники, подозрительный трафик.
- **Backend / Server Errors** — недоступность backend-сервисов, ошибки health check, сбой reverse-proxy.

Если в инфраструктуре используется **FortiAnalyzer** в качестве централизованного сборщика логов, **настройка прямой передачи Syslog с устройства в SIEM не требуется.**

**В этом случае необходимо убедиться, что:**

- устройство зарегистрировано в FortiAnalyzer;
- события от устройства отображаются в FortiAnalyzer.

Передача событий в SIEM выполняется **централизованно с FortiAnalyzer**

## ???????? Syslog Policy

1. Зайдите в веб-интерфейс FortiWeb под учетной записью с правами администратора
2. В левом меню перейдите: **“Log&Report”** → **“Log Policy”** → **“Syslog Policy”**

The screenshot shows the FortiWeb management interface. The top navigation bar includes the FortiWeb logo, a menu icon, and a search icon. The left sidebar contains a list of navigation items: Dashboard, Network, System, Security Fabric, User, Policy, Server Objects, Application Delivery, Web Protection, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Log&Report, Log Access, Report, Log Policy, Syslog Policy (highlighted in blue), FortiAnalyzer Policy, SIEM Policy, FTP/TFTP Policy, Trigger Policy, and Log Config. The main content area displays a table with a single row containing the number '1'. Above the table are buttons for '+ Create New', 'Edit', 'Delete', and 'Ref. Detail'.

3. Нажмите **“Create New”**

4. В поле **“Name”** укажите имя policy, например `siem` и нажмите **OK**

5. В этом же окне **“Edit Syslog Policy”** нажмите **“Create New”**

FortiWeb

Edit Syslog Policy

Name

ID	IP Address(IPv4)	Port	Protocol
1	172.20.3.102	1514	UDP

Log & Report

- Log Access
- Report
- Log Policy
  - Email Policy
  - Syslog Policy
  - FortiAnalyzer Policy
  - SIEM Policy
  - FTP/TFTP Policy
  - Trigger Policy
- Log Config

6. В открывшемся окне **“New Syslog Server”** заполните:

- **IP Address(IPv4)** – IP адрес коллектора/syslog-сервера SIEM.
- **Port** – порт, на котором слушает коллектор (часто  для UDP/TCP или  для TLS).
- **Protocol** – ,  или  в соответствии с требованиями SIEM.
- **Format** – , либо другой формат в соответствии с требованиями SIEM.

В разделе **“Available Custom Fields”** вы можете добавить созданные у вас **“Custom Fields”**, для этого выделите необходимые поля и нажмите на стрелочку вправо **“→”**. После чего выбранные **“Custom Fields”** должны оказаться в блоке **“Selected Custom Fields”**

New Syslog Server

ID auto

IP Address(IPv4) 1.1.1.1

Port 3514

Protocol  UDP  TCP  TLS

Format  Default  CSV  CEF  JSON

Custom Fields

Available Custom Fields	Selected Custom Fields
XFF	

OK Cancel

7. Нажмите “OK”, далее еще раз в окне “Edit Syslog Policy” нажмите “OK”

?????????? ?????????? ?????? ???????

# Syslog

1. Перейдите в меню: “Log&Report” → “Log Config” → “Global Log Settings”
2. В блоке “Syslog” включите тумблер (Enable)
3. В поле “Syslog Policy” выберите созданную syslog policy, в нашем случае `siem`
4. В поле “Log Level” установите минимальный уровень, который хотите отправлять (по умолчанию Information)
5. В поле “Facility” выберите одно из local-use значений (например, `local7`) или то, которое принято в вашей SIEM-стандартизации
6. В блоке “Log Type” отметьте все типы журналов для отправки:
  - **Event Log** – системные события, логины админов, изменения конфигурации.
  - **Attack Log** – срабатывания WAF, DLP, ML, ботов и т.д.
  - **Traffic Log** – журналы HTTP/HTTPS-трафика

## 7. В итоге у вас должна получиться следующая конфигурация

The screenshot shows the FortiWeb configuration interface for Global Log Settings. The left sidebar contains a navigation menu with categories like Network, System, Security Fabric, User, Policy, Server Objects, Application Delivery, Web Protection, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Log&Report, Log Access, Report, Log Policy, Log Config, Global Log Settings (selected), Other Log Settings, and Sensitive Data Logging. The main content area is titled 'Global Log Settings' and includes several sections:

- Disk:** Log Level: Information; When log disk is full: Overwrite oldest logs; Log Type: Event Log, Attack Log, Traffic Log.
- Syslog:** Syslog Policy: siem; Log Level: Information; Facility: reserved for local use 7; Log Type: Event Log, Attack Log, Traffic Log.
- Custom Fields:** A table with columns Name, Value, and Delete. It contains one entry: Name: XFF, Value: X-Forwarded-For.
- Alert Mail:** Email Policy: (empty); Log Type: Event Log, Attack Log.
- FortiAnalyzer:** Log Level: Information; FortiAnalyzer Policy: (empty); Log Type: Event Log, Attack Log, Traffic Log.
- SIEM:** Log Level: Information.

An 'Apply' button is located at the bottom right of the configuration area.

## 8. Нажмите “Apply” для сохранения настроек

Revision #1

Created 2026-05-25 10:43:22 UTC by lerat

Updated 2026-05-25 10:47:34 UTC by lerat