Fortinet FortiWeb

Информация об источнике

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, сбои reverse-proxy.

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

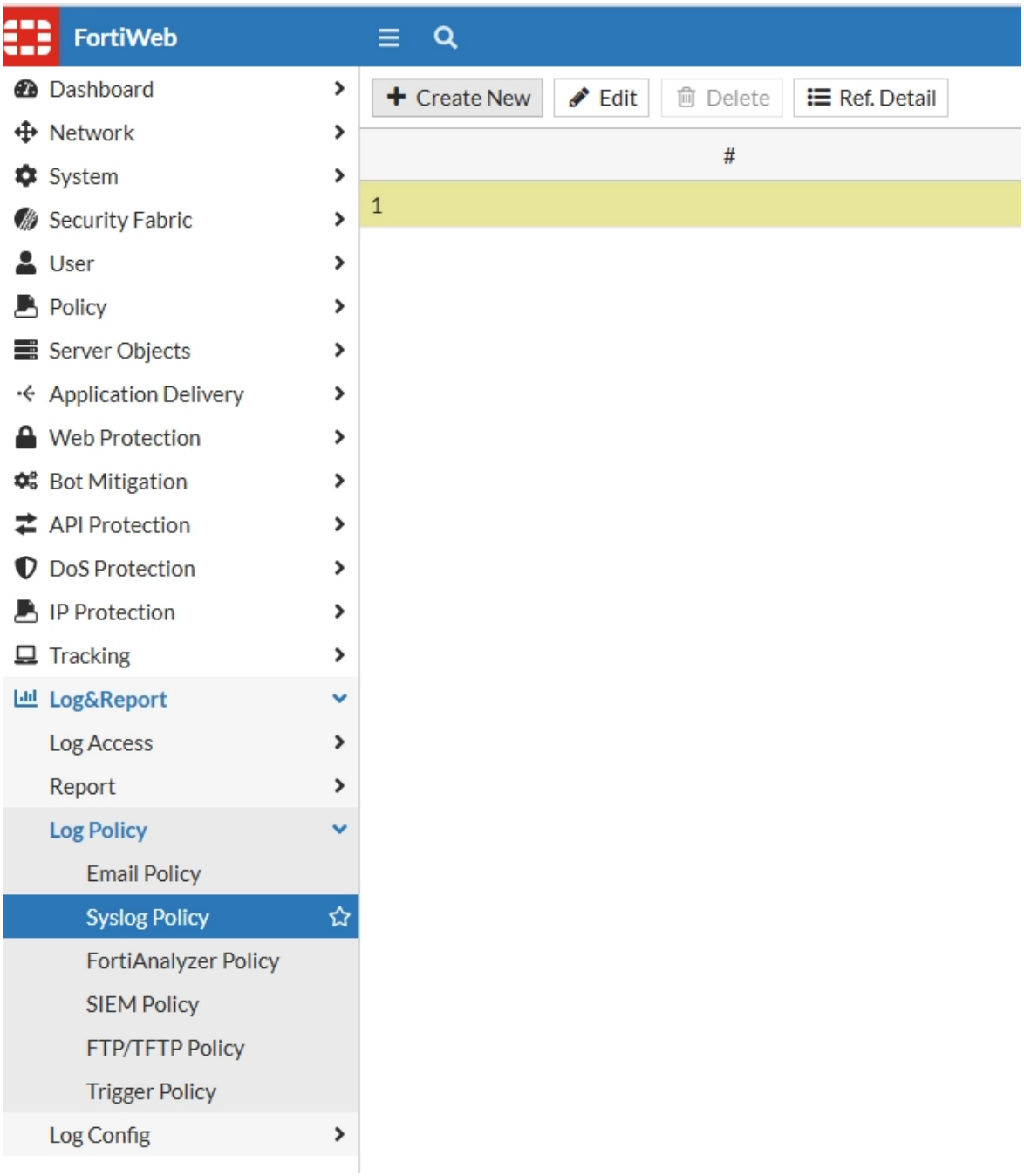
В этом случае необходимо убедиться, что:

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

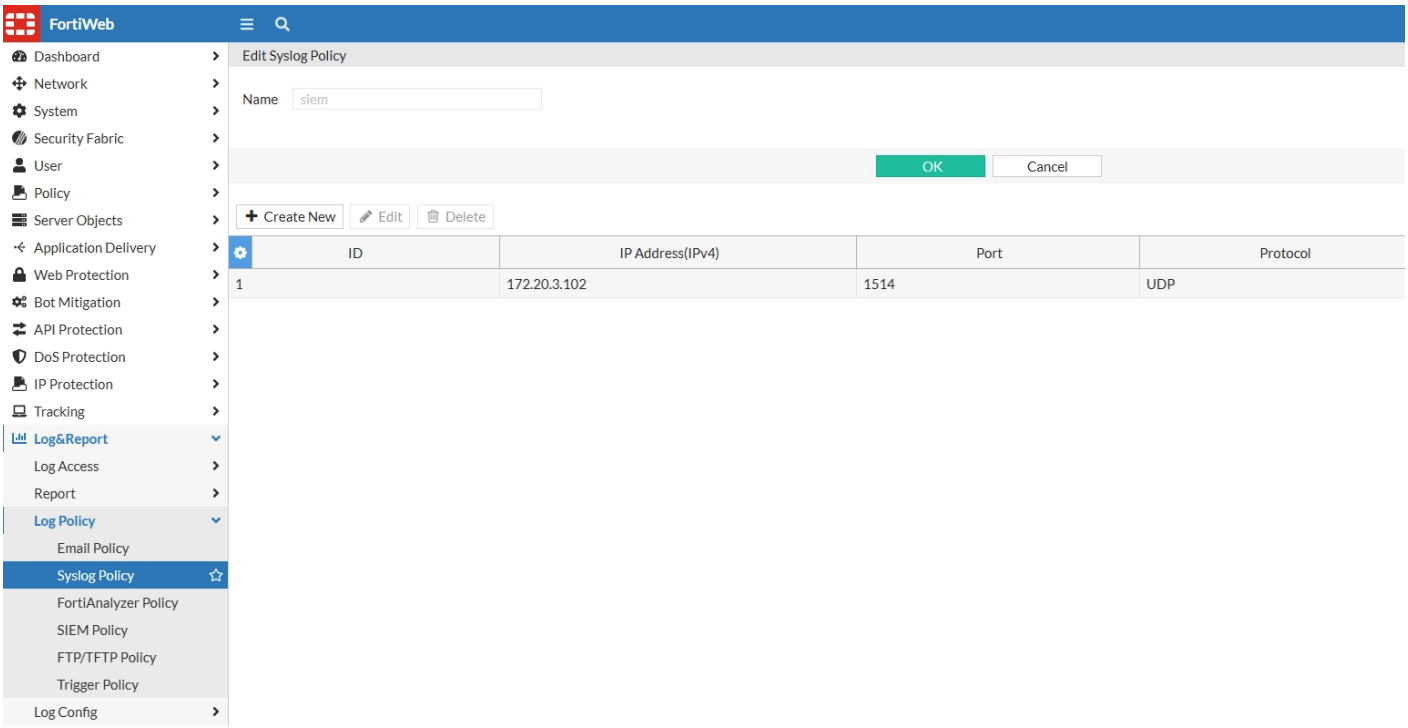
> Передача событий в SIEM выполняется **централизованно с FortiAnalyzer**

Создание 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”**

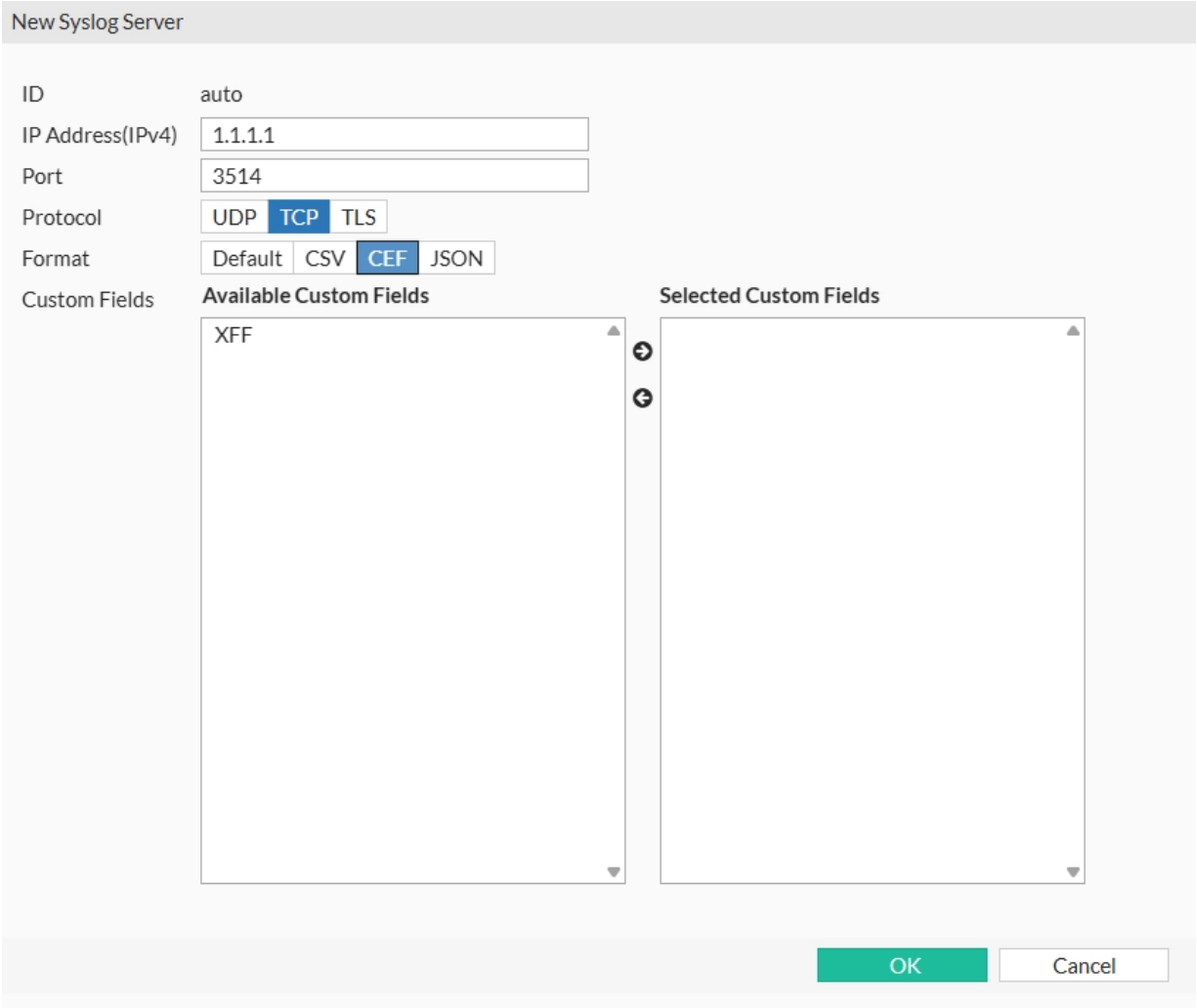


3. Нажмите “**Create New**”
4. В поле “**Name**” укажите имя policy, например `siem` и нажмите **OK**
5. В этом же окне “**Edit Syslog Policy**” нажмите “**Create New**”



6. В открывшимся окне “**New Syslog Server”** заполните:
   - **IP Address(IPv4)** – IP адрес коллектора/syslog-сервера SIEM.
   - **Port** – порт, на котором слушает коллектор (часто `514` для UDP/TCP или `6514` для TLS).
   - **Protocol** – `UDP`, `TCP` или `TLS` в соответствии с требованиями SIEM.
   - **Format** – ****`CEF` , 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”

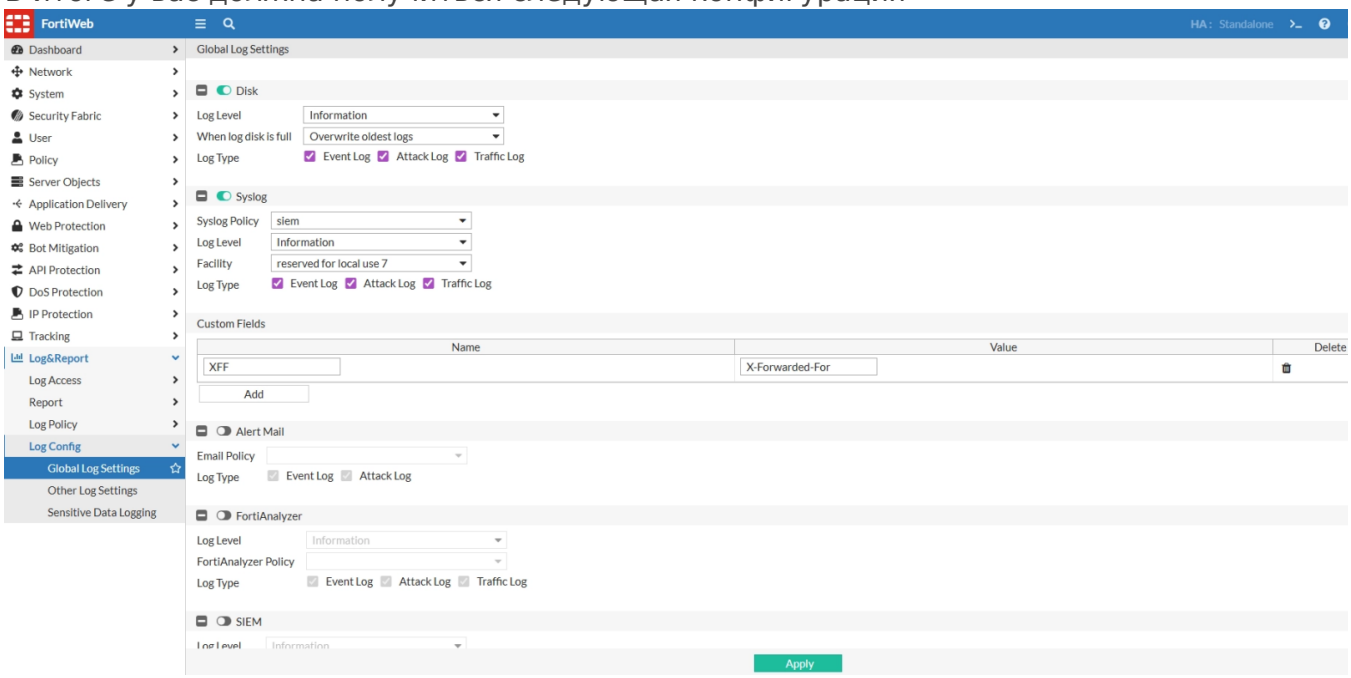


7. Нажмите “**OK**”, далее еще раз в окне “**Edit Syslog Policy**” нажмите “**OK**”

Включение отправки логов через 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



8. Нажмите “Apply” для сохранения настроек

Revision #1
Created 2026-05-25 10:43:22 UTC by lerat
Updated 2026-07-21 16:14:24 UTC by lerat