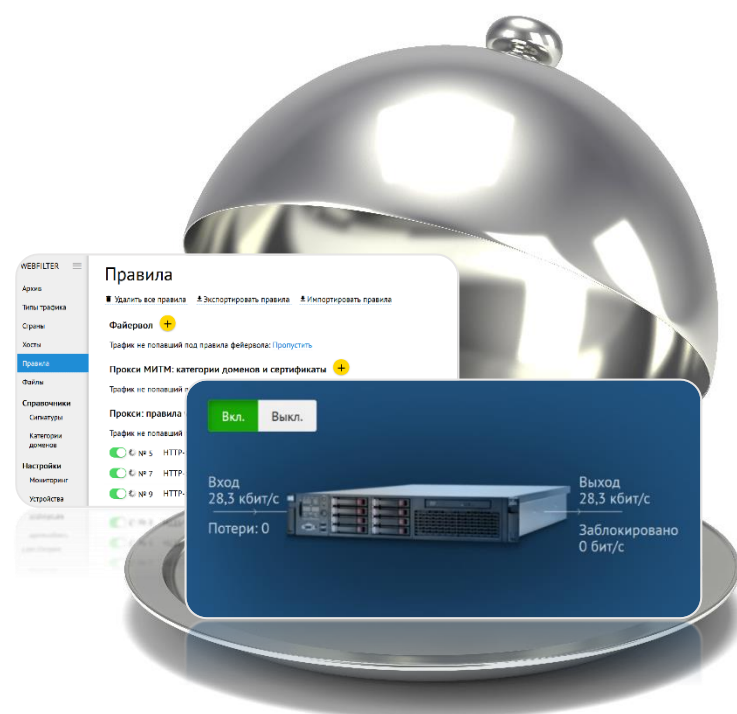


WebFilter^{NGFW}



Устройство класса Next Generation Firewall для защиты от киберугроз в государственном секторе, корпоративных сетях и сетях IoT

Особенности:

Противодействие киберугрозам: обнаружение аномальной сетевой активности, обновляемая база угроз;

Высокая скорость работы: может устанавливаться в высоконагруженных сетях передачи данных (в том числе и на стороне провайдера);

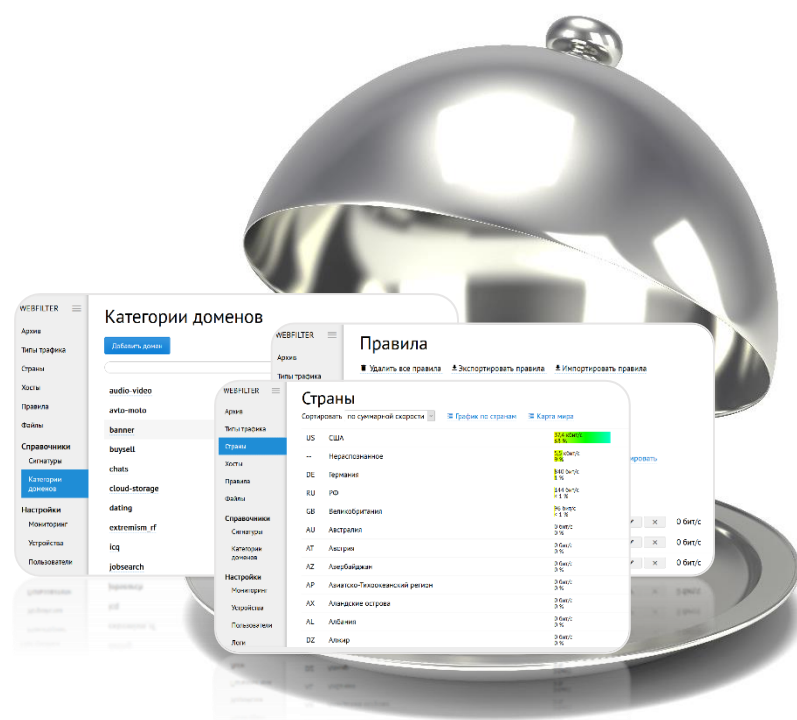
Полностью российская экспертиза и техподдержка, устойчивость к санкционным рискам.

Возможности:

- Сбор и анализ статистики в фоновом режиме, не оказывая влияния на сеть.
- Обработка сырых данных и выявление аномалий в сетевом трафике.
- Более ста современных сетевых протоколов: HTTP, HTTPS, FTP, SSH, SMTP, IMAP и т. п.
- Фильтрация трафика в реальном времени с применением динамических правил.
- Выборочное терминирование SSL-соединения на основе гибких правил и перенаправление уже расшифрованного трафика на модуль анализатора.
- Обновляемая база категорий доменов: социальные сети (vk.com, facebook.com), поисковые системы (google.com, yandex.ru), банки (sberbank.ru, vtb24.ru), видеосервисы (youtube.com, rutube.ru).

WebFilter^{NGFW}

Гибкое управление сетевым трафиком:



- Перехват/разрешение/блокирование/логирование соединений, фильтрация по содержимому: технология Deep Packet Inspection – DPI.
- Идентификация/классификация/терминация соединений: браузеры, мессенджеры, протоколы приложений, устройства.
- Фильтрация трафика по содержимому: технология Deep Packet Inspection (DPI).
- Выборочный перехват и анализ HTTPS-трафика: технология выборочного MITM (Man-In-The-Middle).
- Сопоставление трафика пользователю.
- Интеграция с Active Directory.

WebFilter^{NGFW}

Выборочный перехват и анализ
HTTPS-трафика: технология MITM →
Man-In-The-Middle

