UserGate

7.1

БОЛЬШОЕ ОБНОВЛЕНИЕ

Игорь Шефер
Ведущий инженер UserGate

UserGate 7.1

IPSv3

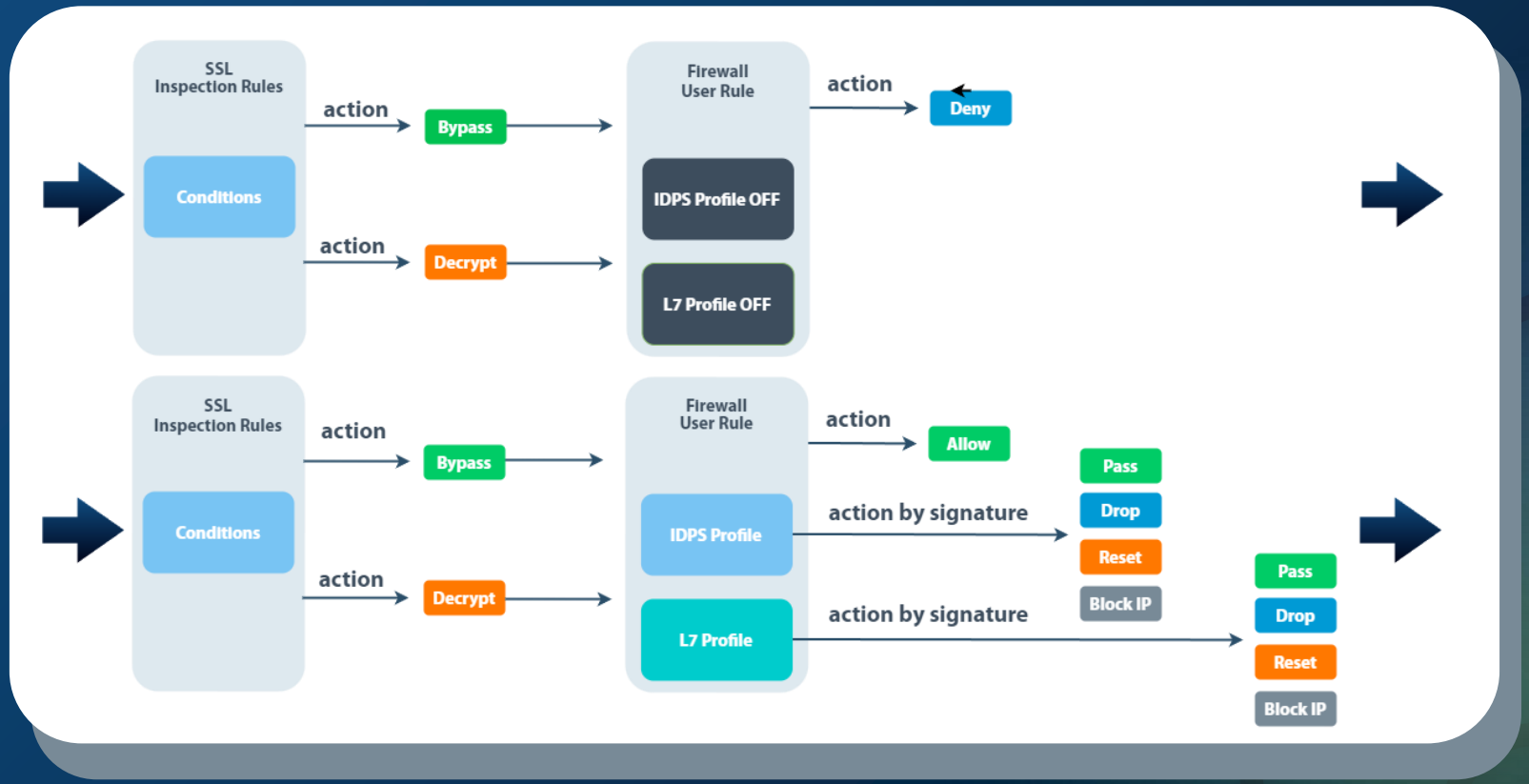
Движок

UserGate 7.1

- 3 версия движка
- Поддержка обработки расшифрованного SSL
- Возможность описывать сигнатуры СОВ и L7-приложений (UASL)
- Верификация
- Интеграция в политики МЭ
- Расширение списка действий (action) при срабатывании
- Применение действия (action) по каждой сигнатуре
- Возможность захвата пакетов при сработке СОВ и L7-приложений
- Полноценное управление в CLI

UserGate 7.1

Action Flow



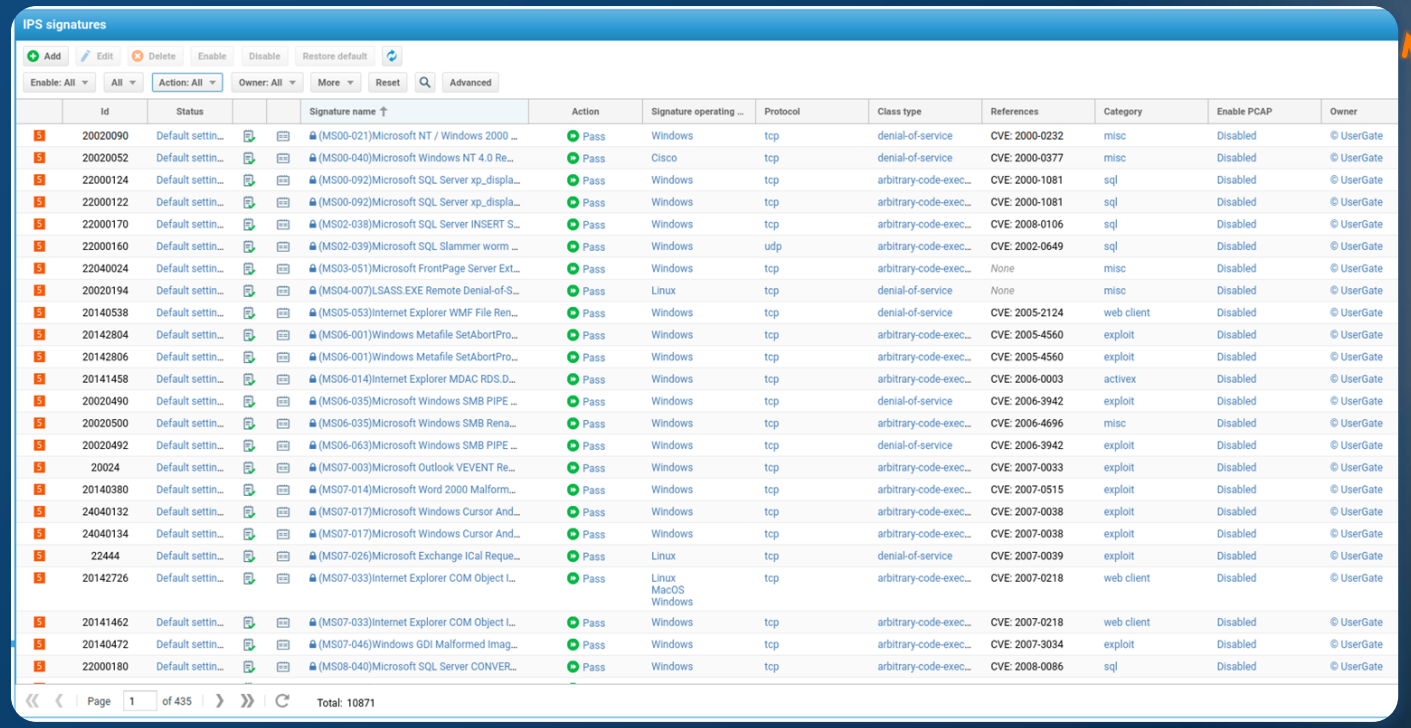
Новые кейсы

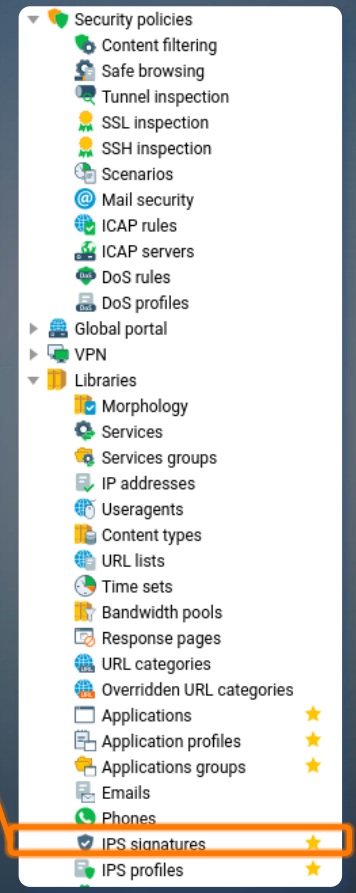
UserGate 7.1

- Детектирование и блокировка BruteForce сервисов
- Определение атак в зашифрованном трафике
- Сканирование пакетов на уровне протокольных диссекторов
- Белые списки приложений
- Обнаружение и блокировка туннелей
- Работа с метками в стриме

UserGate 7.1

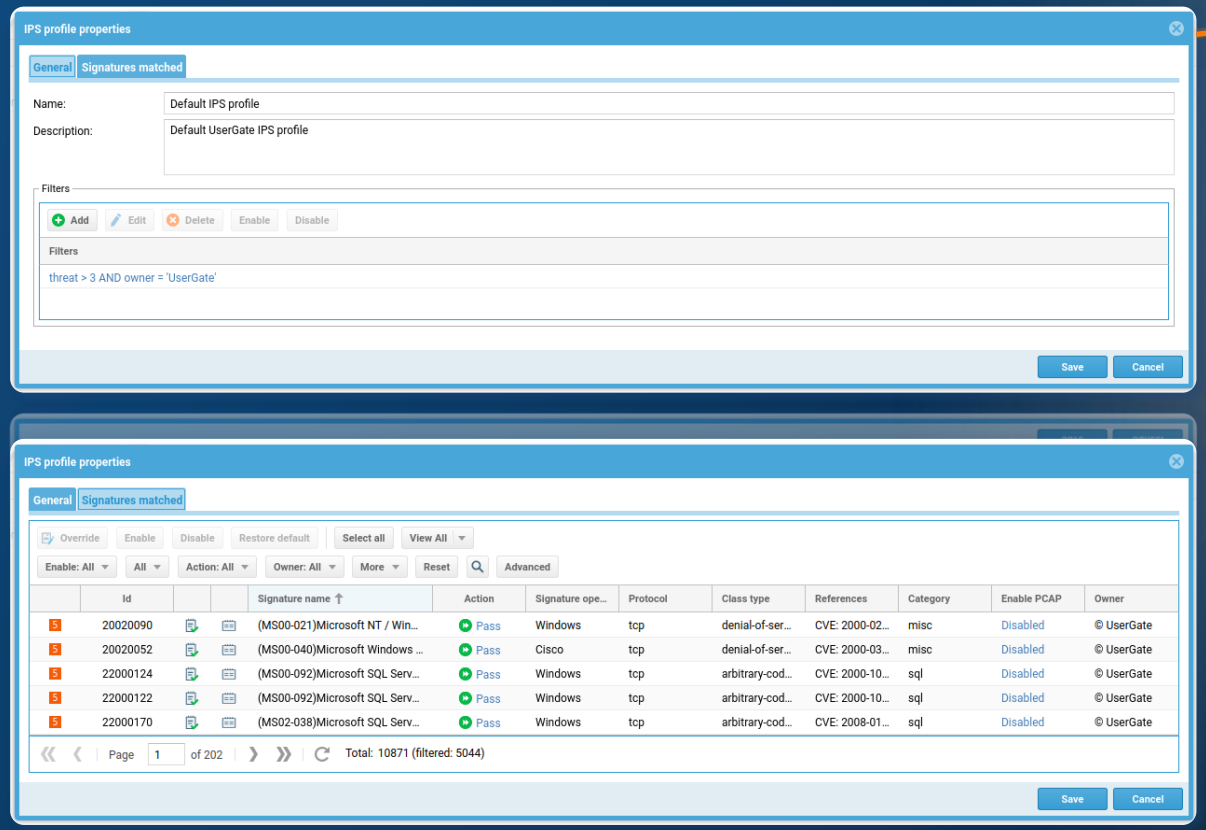
GUI. IPS-сигнатуры

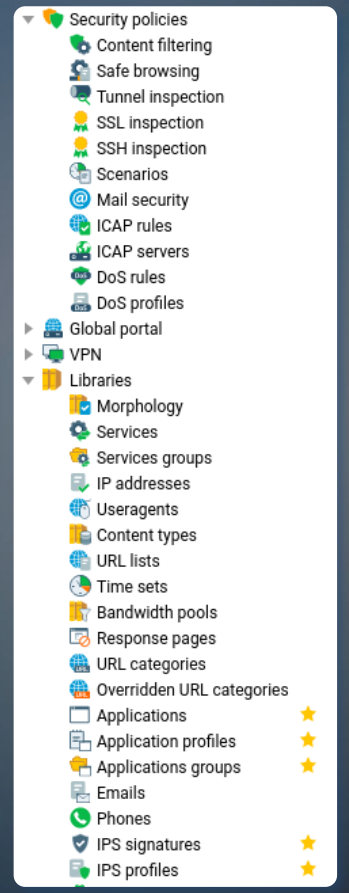




UserGate 7.1

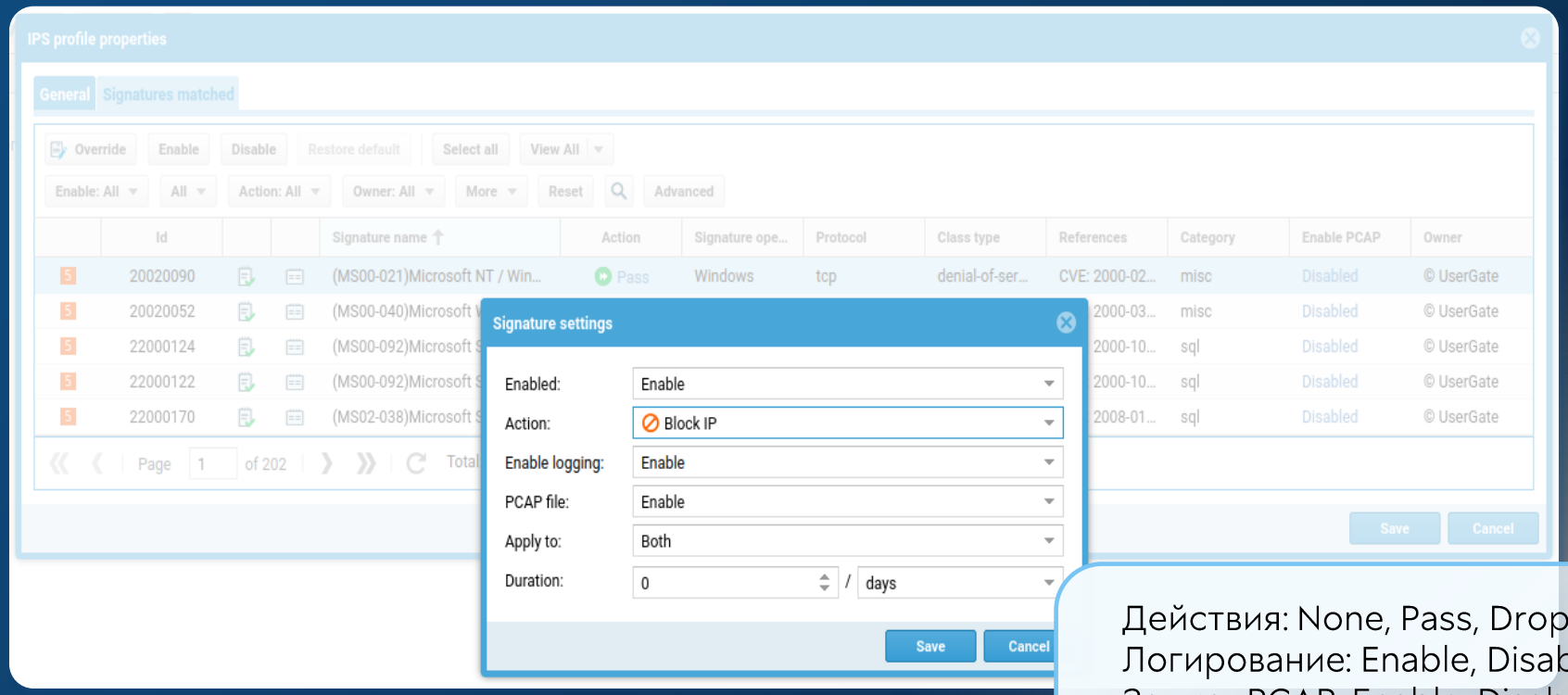
GUI. IPS профиль





UserGate 7.1

GUI. IPS профиль. Переопределение

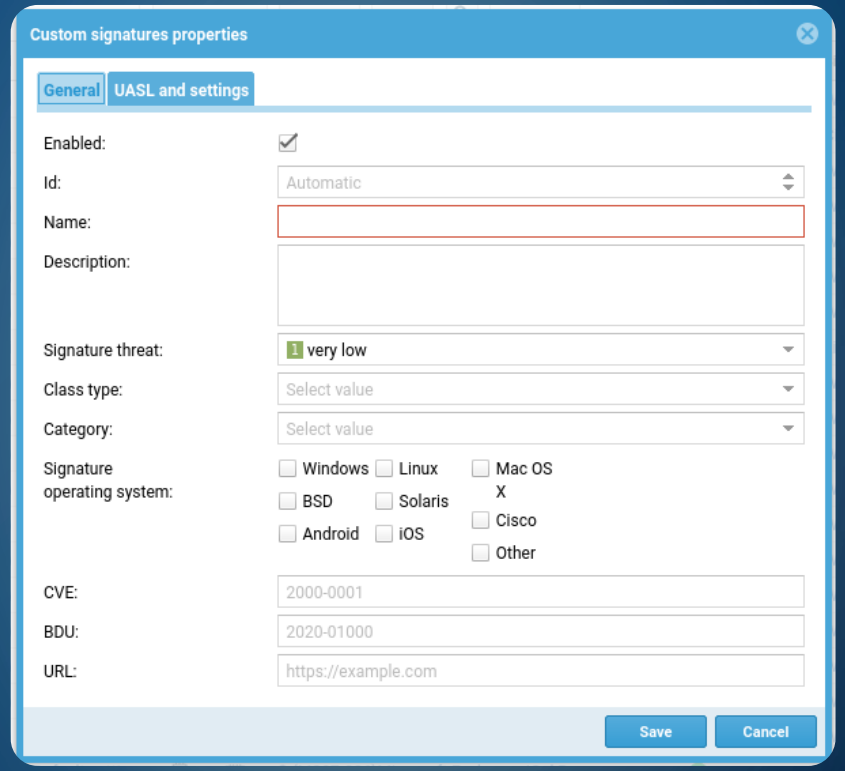


Действия: None, Pass, Drop, Reset, Block IP
Логирование: Enable, Disable
Запись PCAP: Enable, Disable
Применить к: Src, Dst, Both (активно при Reset и Block IP)
Продолжительность: days, hours, minutes

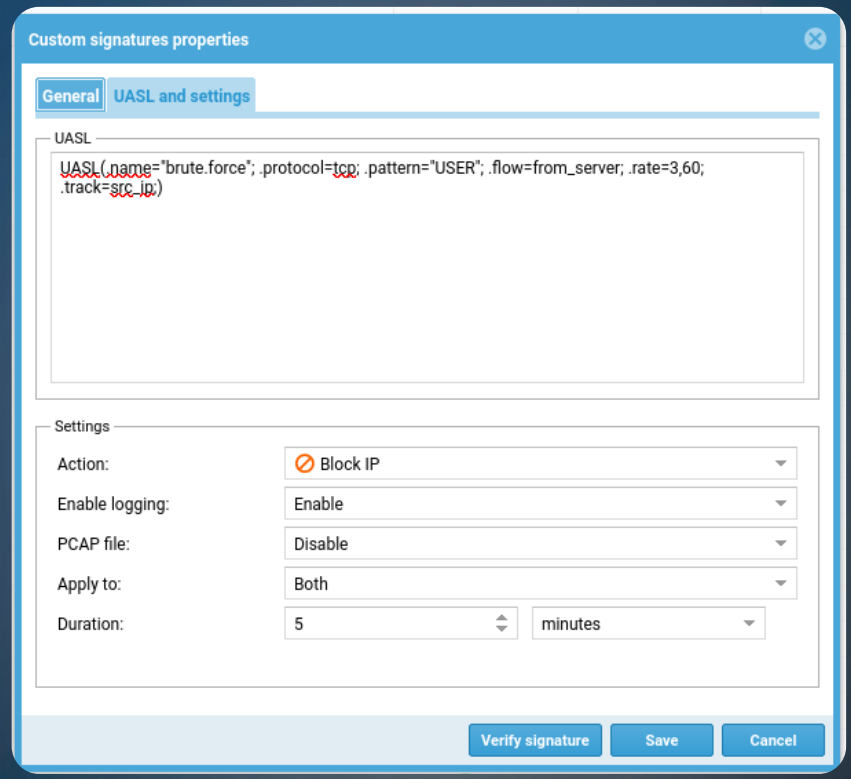
UserGate 7.1

GUI. IPS сигнатура. Создание

Шаг 1



Шаг 2



UserGate 7.1

GUI. UASL

Фильтр по IP-адресам:
- src/dst (IPaddr/IPsubnet)

Фильтр по TCP/UDP-портам:
- src/dst (equal, less than, greater than, in range)

Поиск паттернов (packet payload):
- pattern (string)

Модификаторы области поиска:
- icmp, tcp, udp etc

Частота срабатывания:
- rate (count, period); track (src/dst IP)

Направление анализа:
- from_client, from_server, bi_directional

Протокольные диссекторы:
- tcp dissector, udp dissector, icmp dissector etc

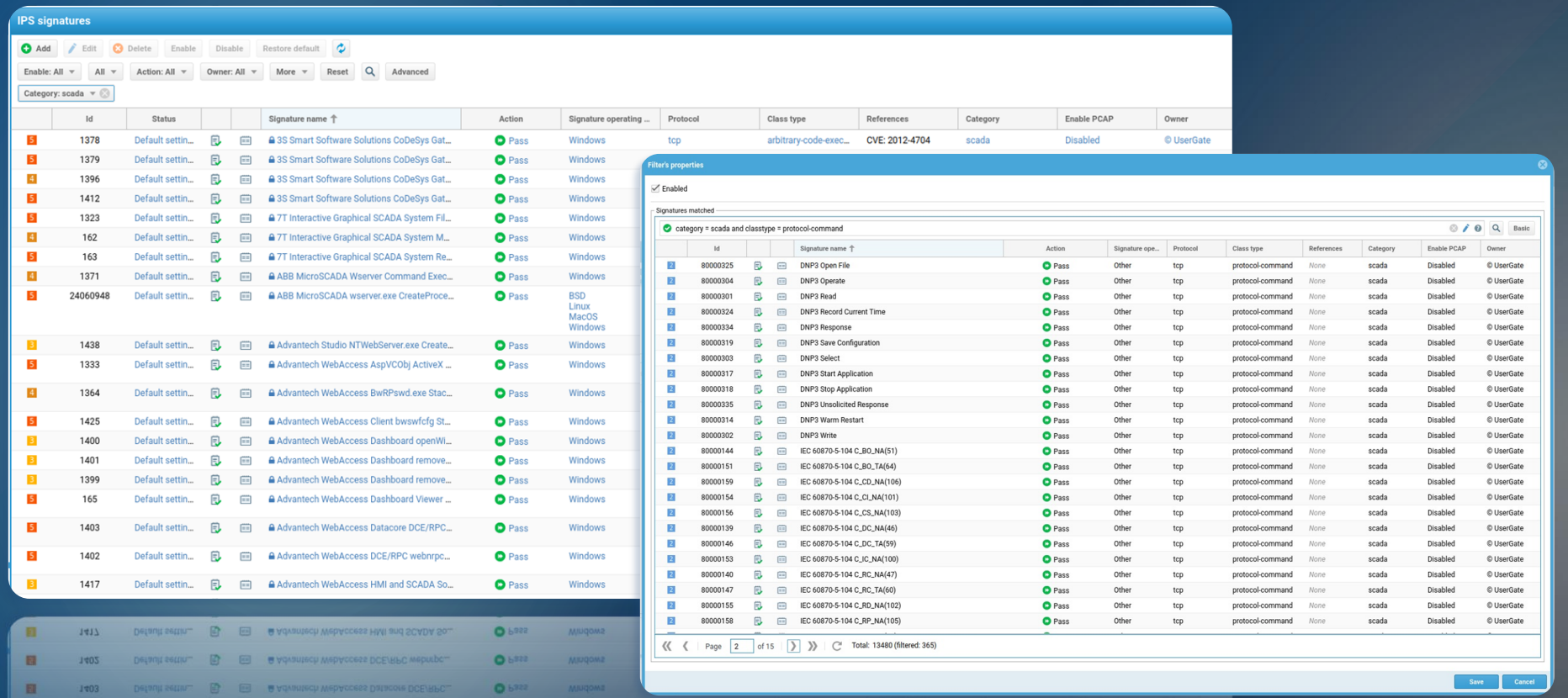
Матчинг бинарных данных
- byte_test, byte_jump

Пример:

```
UASL(.name='Scan';
.flow=from_client;
.tcp.flags = S;
.dst_port=1:1024;
.rate=100,10; .track=src_ip;)
```

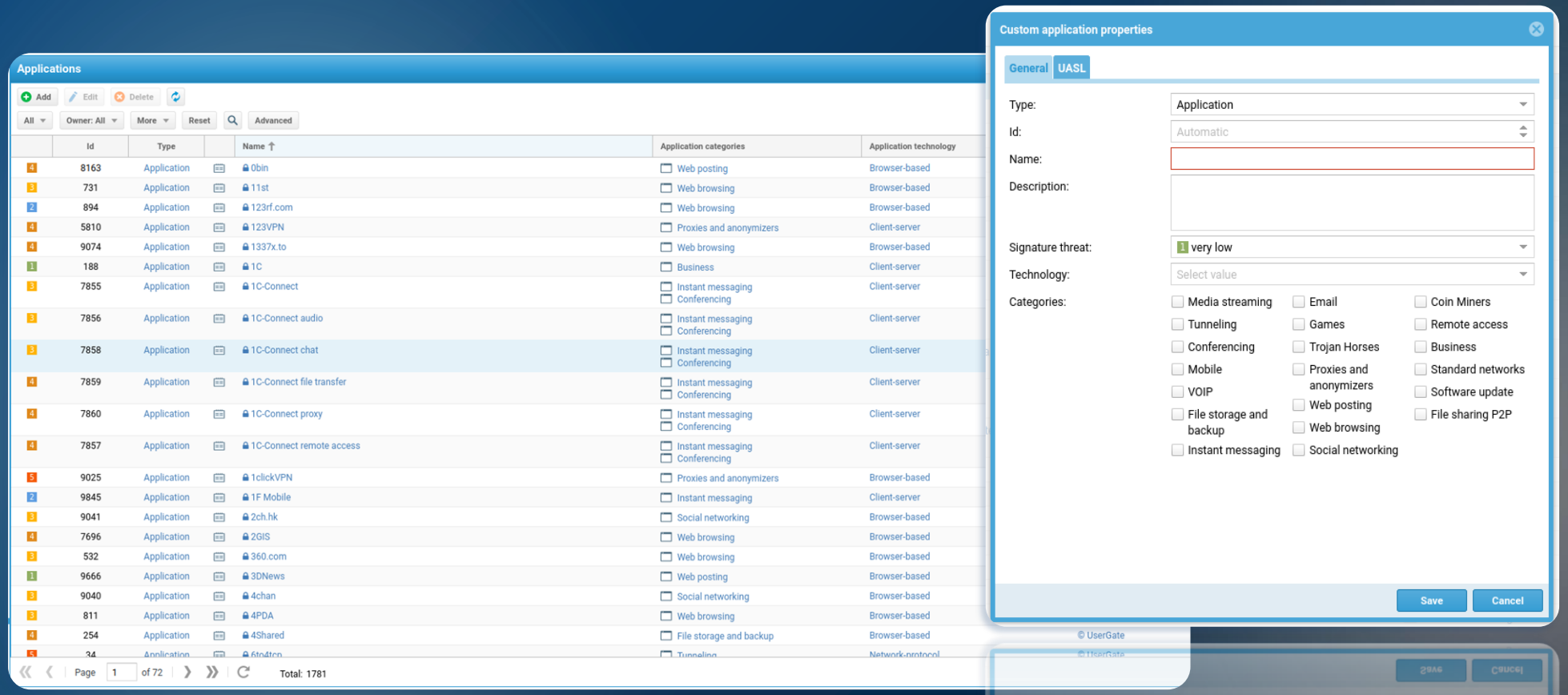
UserGate 7.1

GUI. SCADA



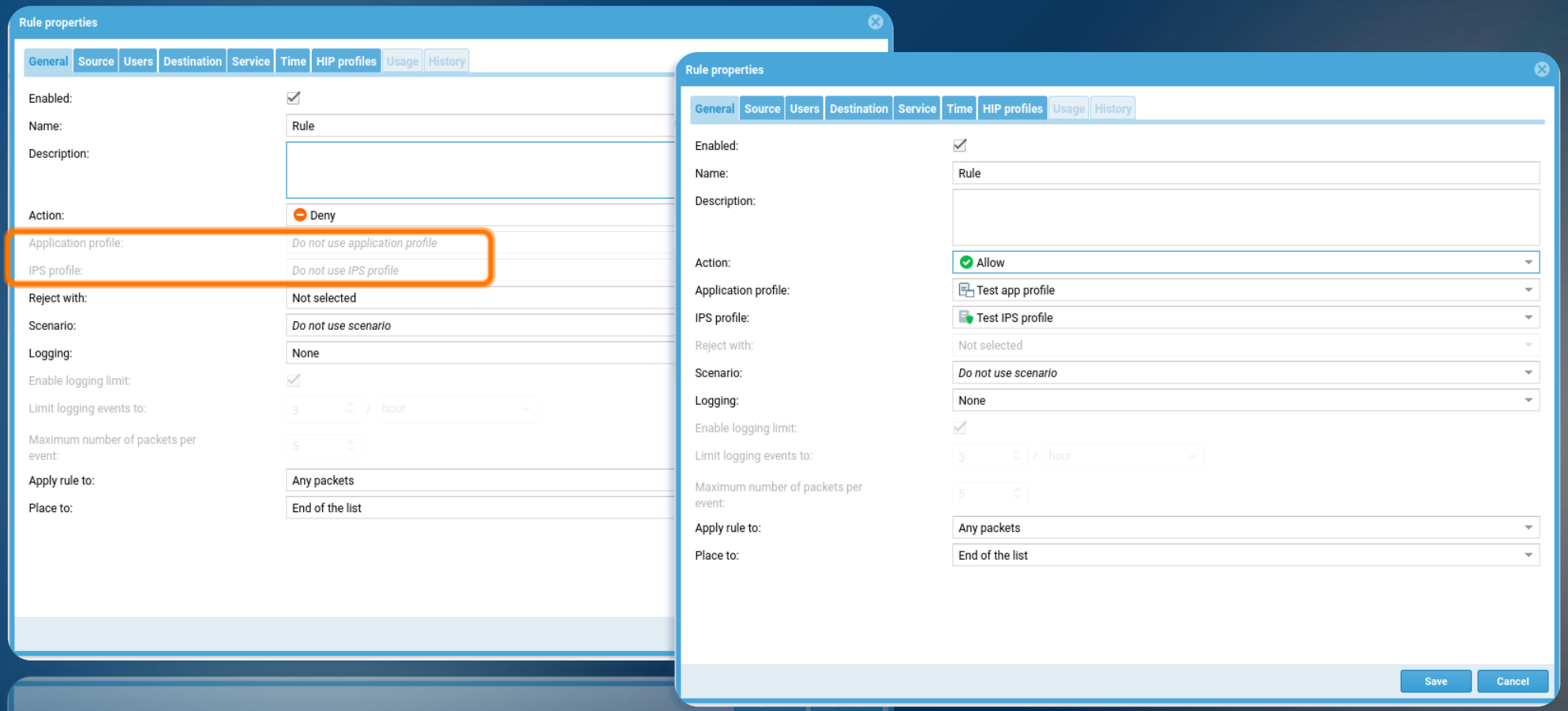
UserGate 7.1

GUI. Сигнатуры L7



UserGate 7.1

GUI. Правила МЭ



UserGate
7.1

UserID

UserGate 7.1

UserID. Задачи

Прозрачная идентификация пользователей

Синхронизация групп пользователей

Сегментация на базе принадлежности к группе LDAP или имени пользователя (Identity Based Network Firewall)

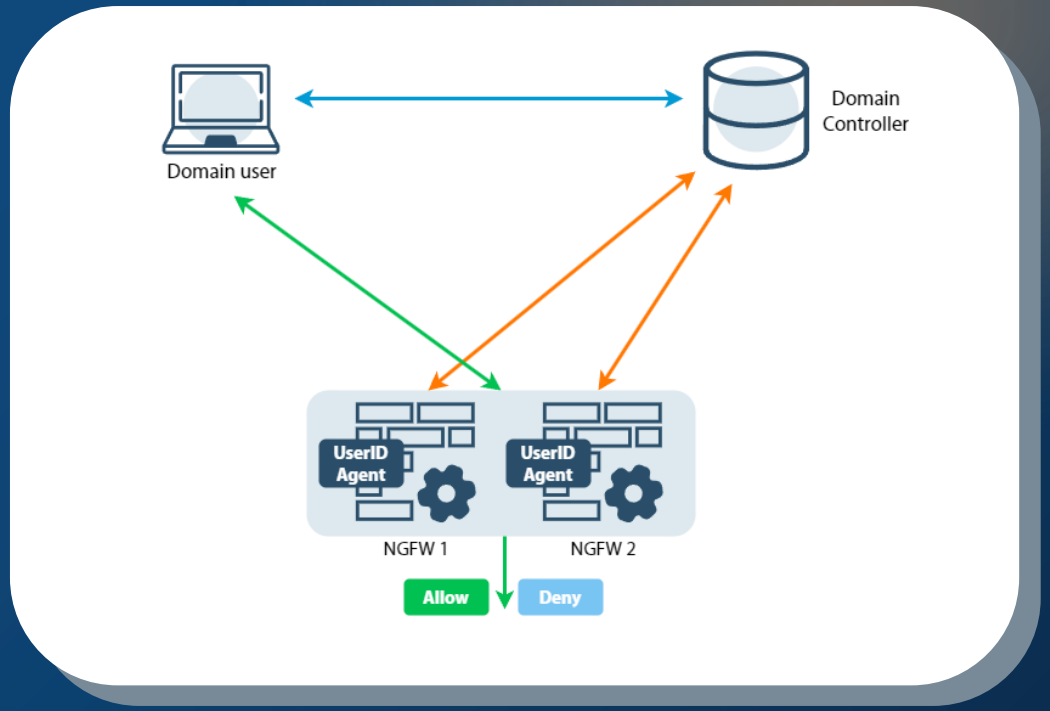
UserGate 7.1

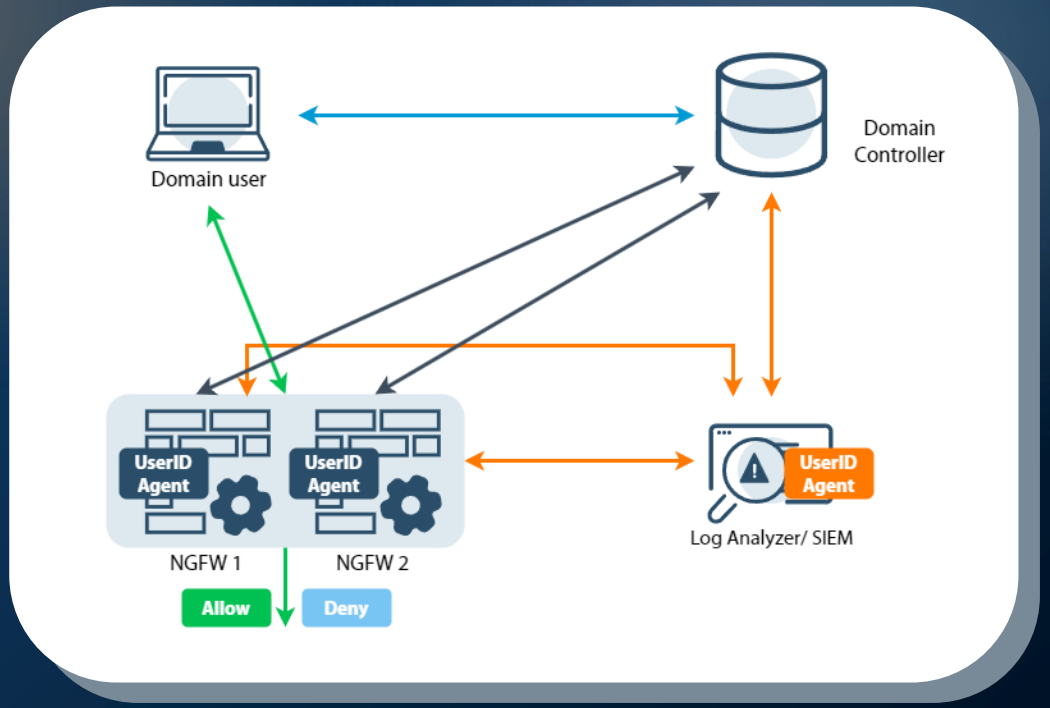
UserID. Возможности

- Идентификация посредством использования журналов DC по WMI (коды событий 4624, 4634, 4768, 4769, 4770) и/или по Syslog (RFC 3164, RFC 5424, RFC 6587)
- Использование фильтров и таймеров в настройках агента
- Режимы работы:
  a. Агент на борту NGFW
  b. Агент на борту LogAn
  c. Агенты на NGFW и LogAn
- Дистрибуция данных пользователей на NGFW

UserGate 7.1

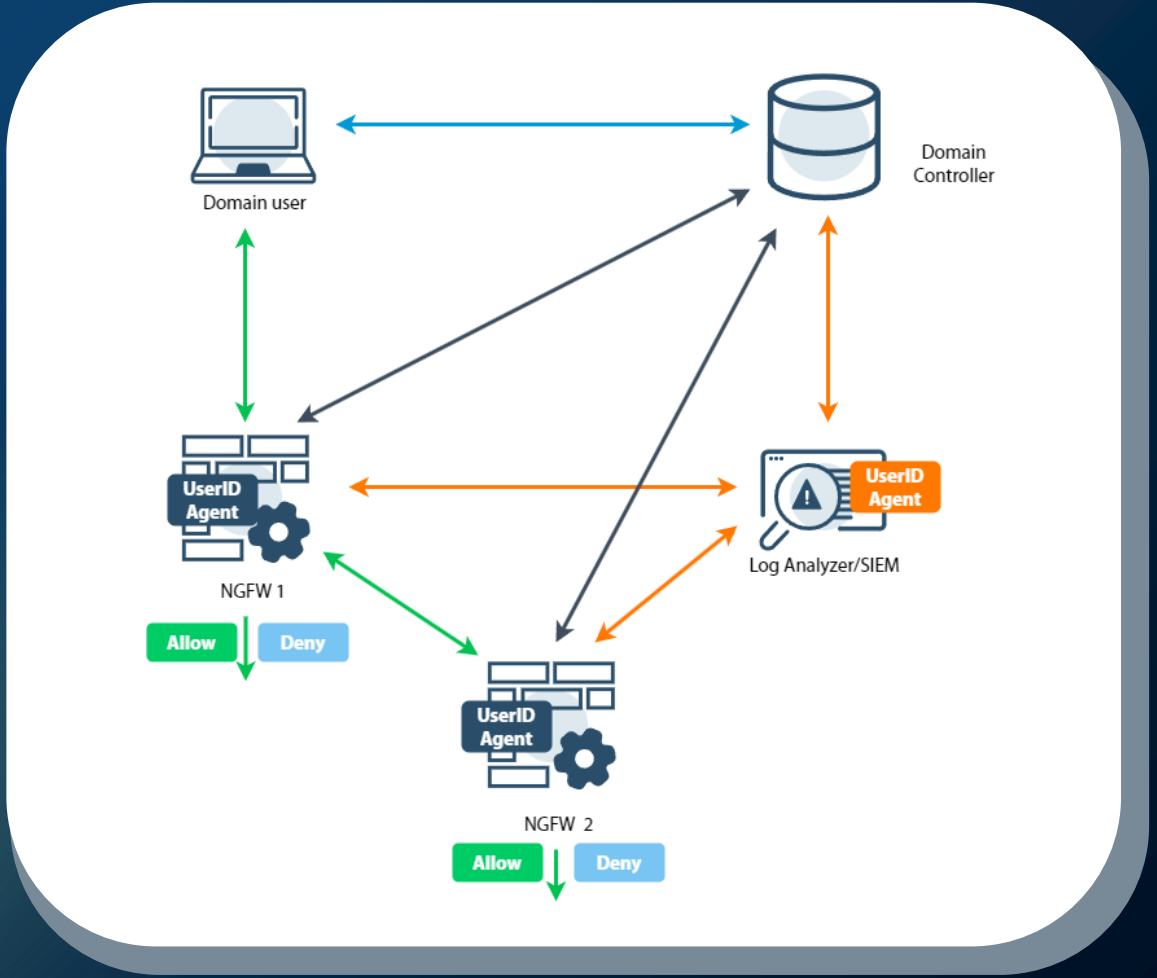
Вариант исполнения: Cluster NGFW



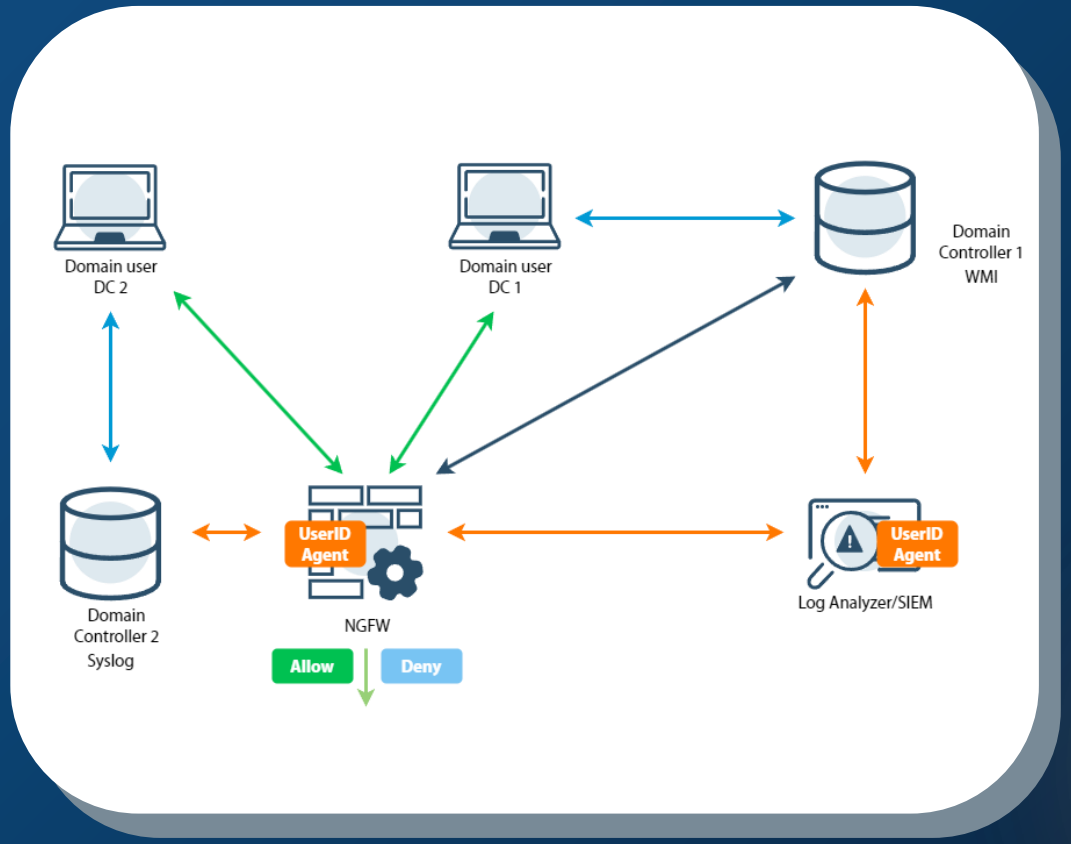


UserGate
7.1

Вариант исполнения: NGFW + LogAn/ SIEM Дистрибуция



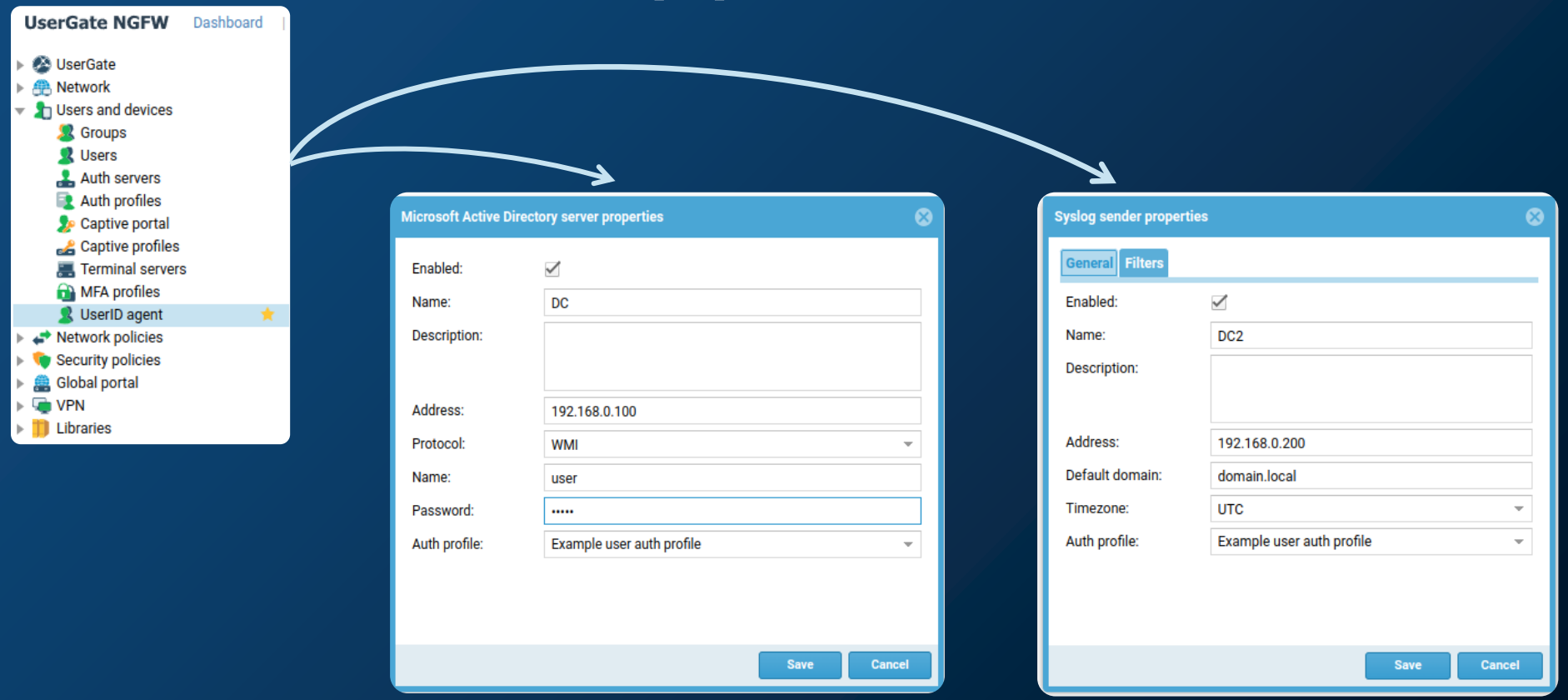
UserGate
7.1



Вариант исполнения: NGFW + LogAn/SIEM с активными агентами

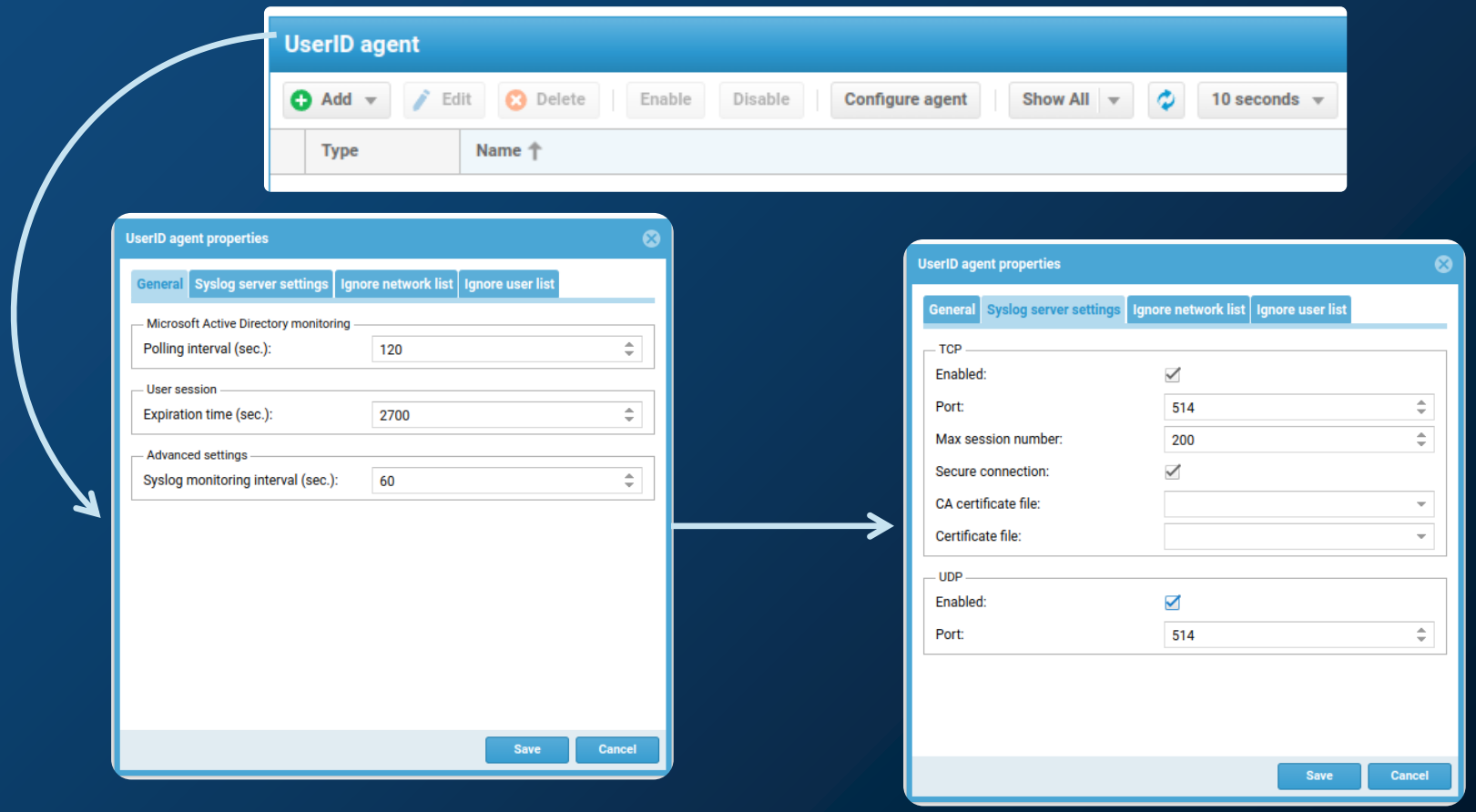
UserGate 7.1

GUI. Добавление агента



UserGate 7.1

GUI. Конфигурирование агента

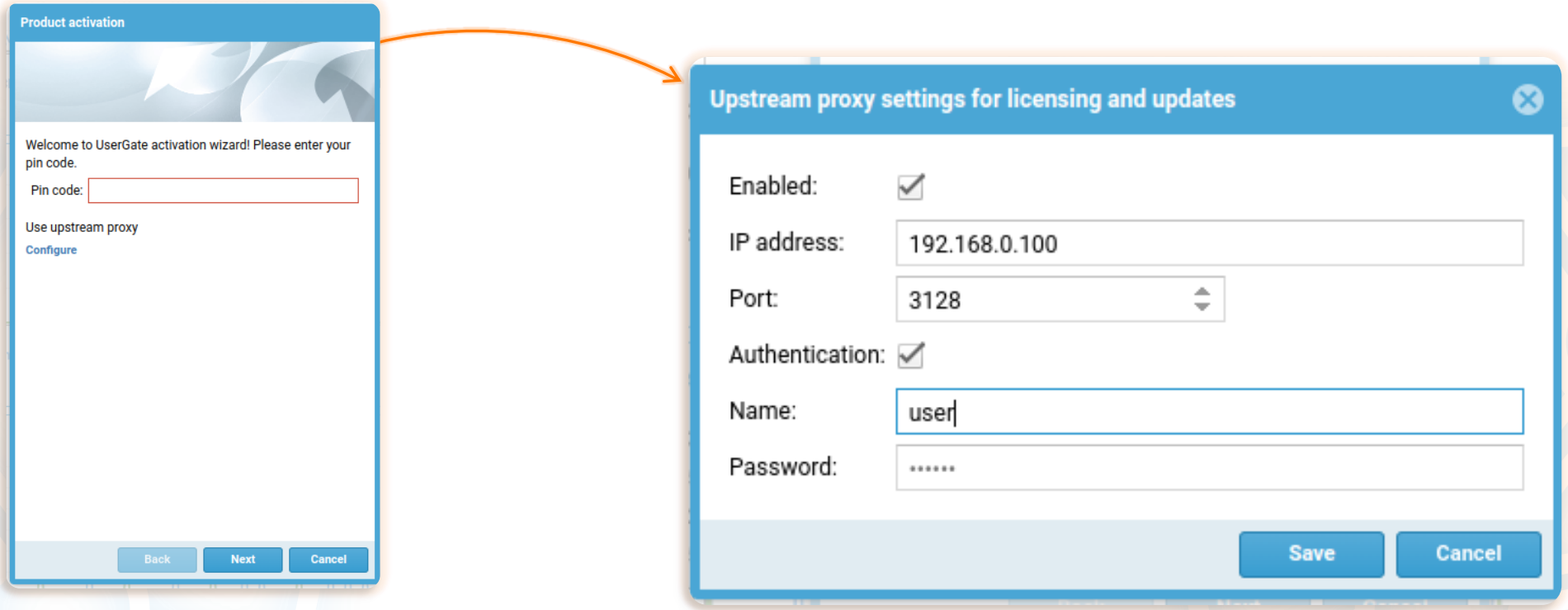


UserGate
7.1

Upstream Proxy

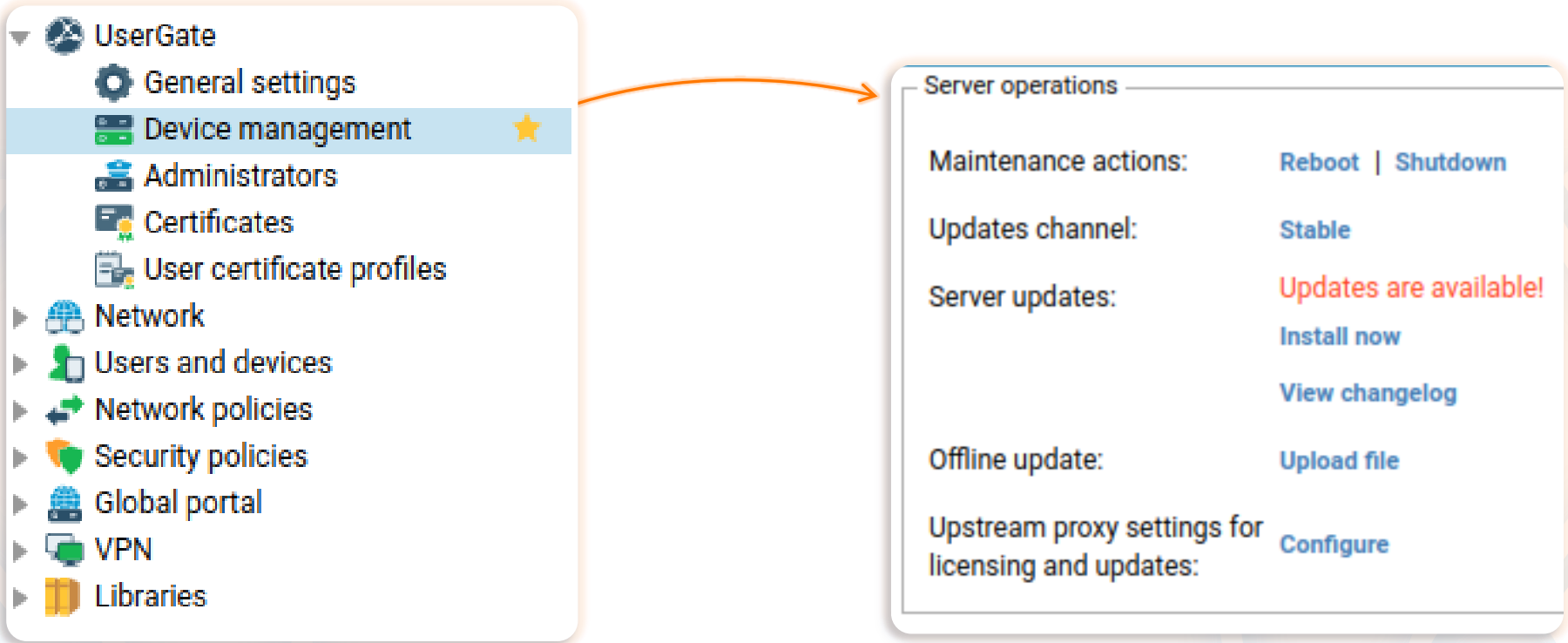
UserGate
7.1

GUI. Настройка. Лицензия и обновления



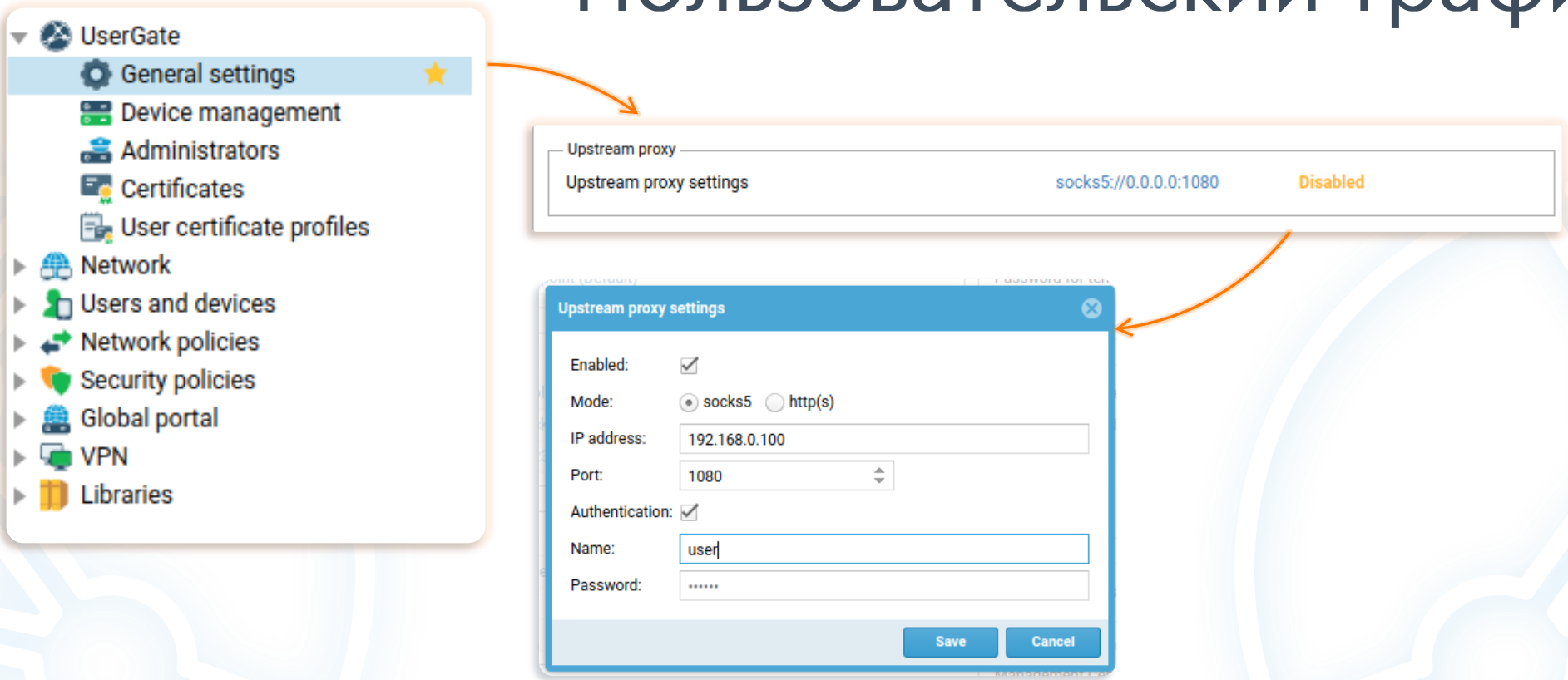
UserGate
7.1

GUI. Реконфигурация. Лицензия и обновления



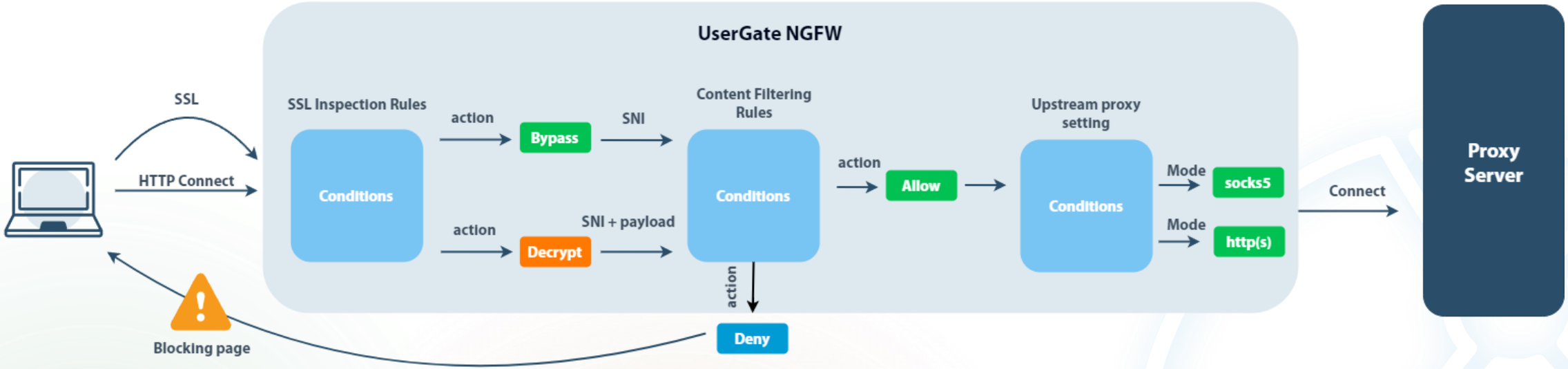
UserGate
7.1

GUI. Настройка. Пользовательский трафик



UserGate 7.1

Upstream Proxy flow



UserGate
7.1

UserGate Endpoint Client

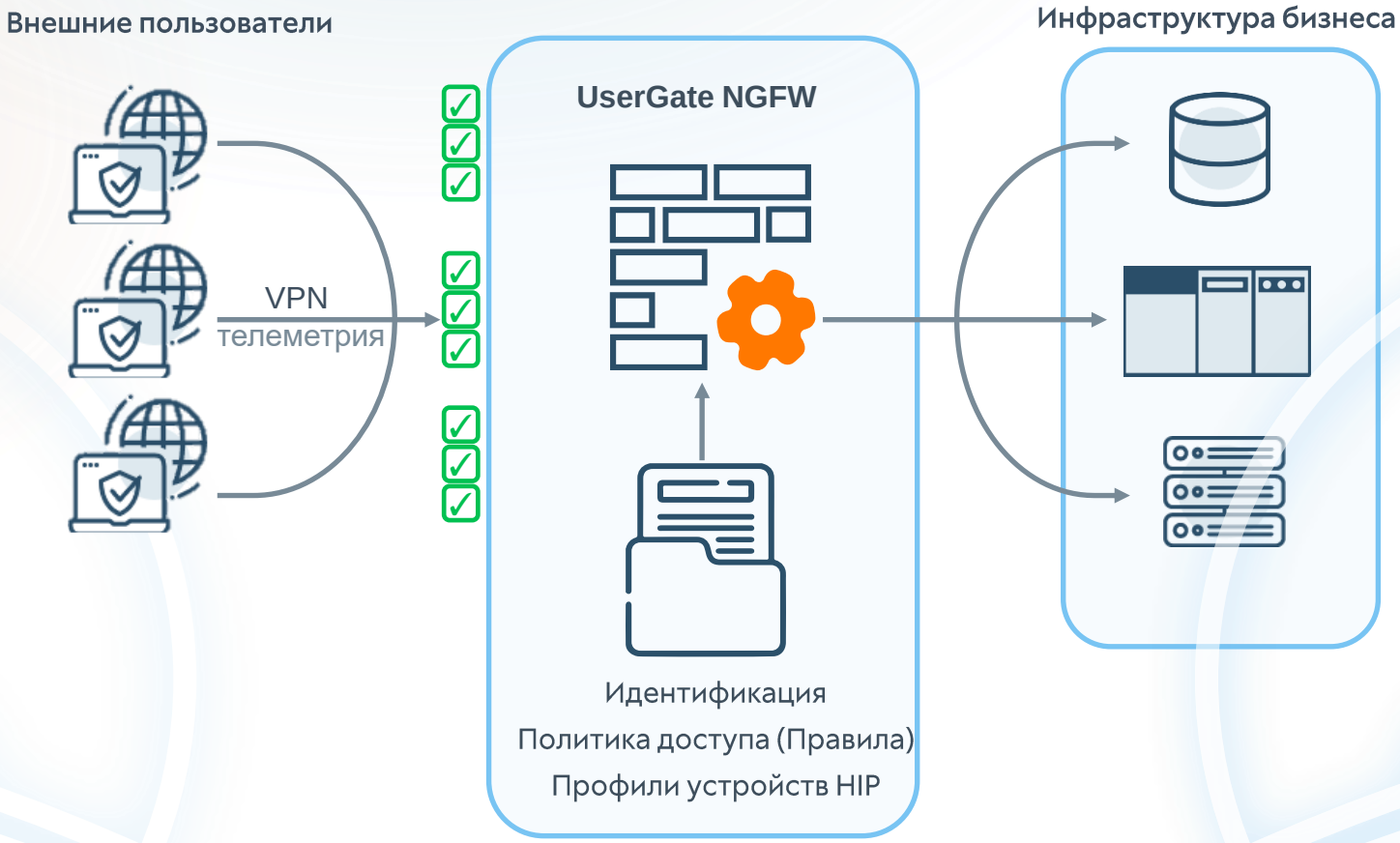
UserGate 7.1

UserGate Client – агент SUMMA

- Режимы работы UserGate Client
- VPN
- HIP, проверка состояния
- Управление
- Мониторинг событий
- Аналитика и реагирование

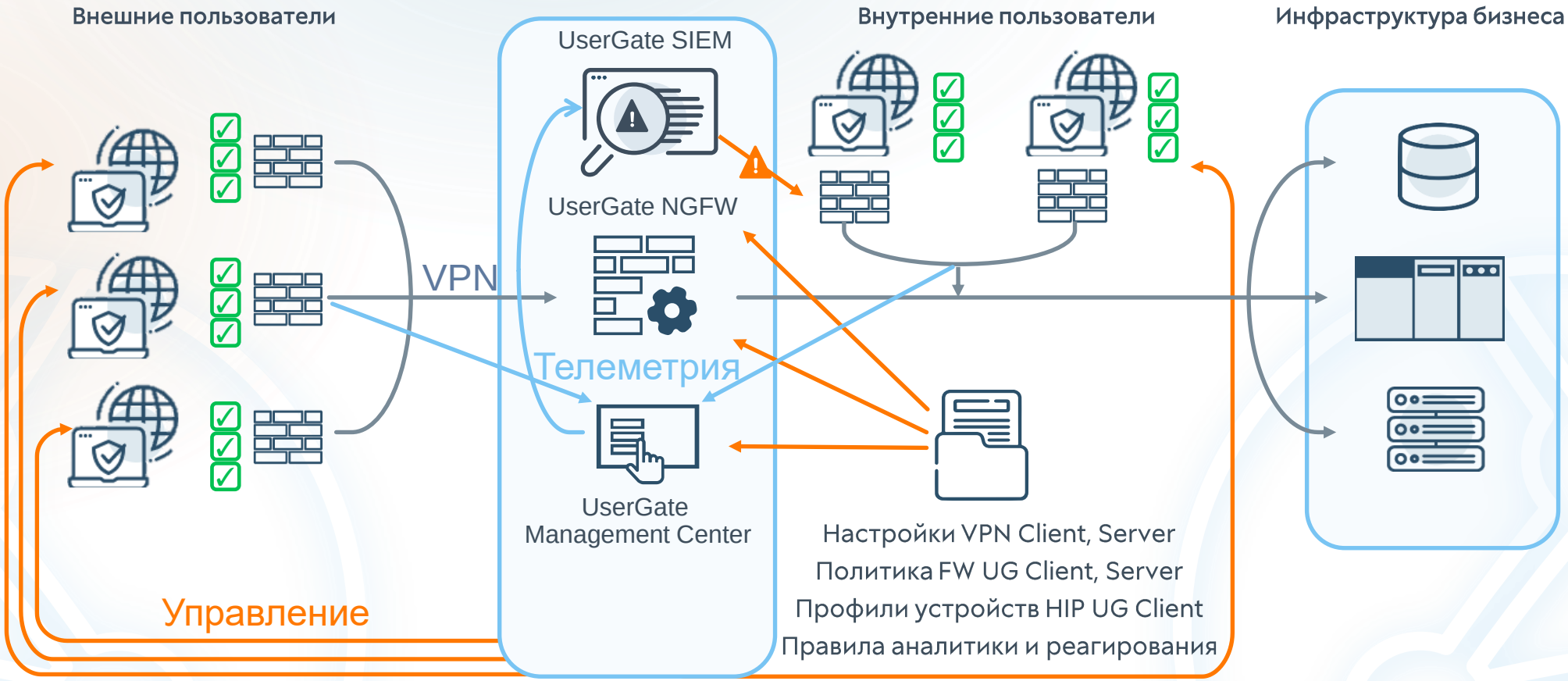
Режим NGFW

UserGate 7.1



Режим МС

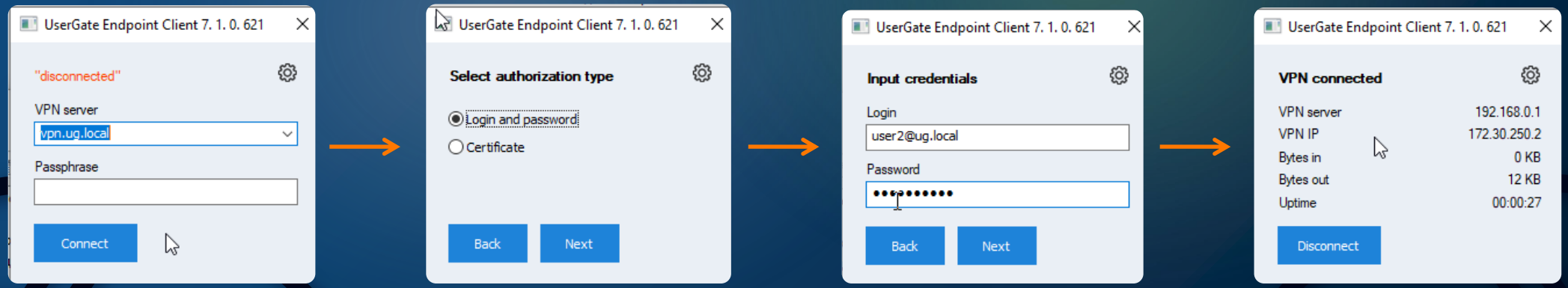
UserGate 7.1



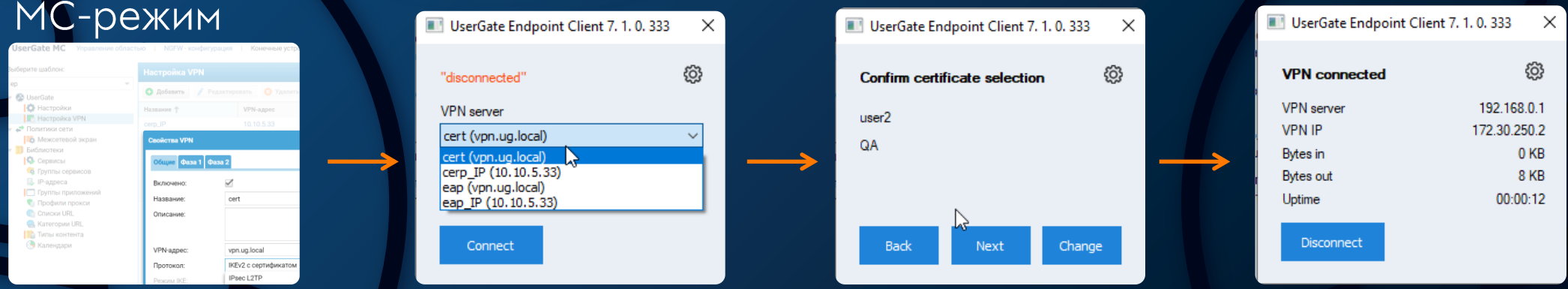
UserGate 7.1

VPN – процесс подключения

NGFW-режим (автонастройка)

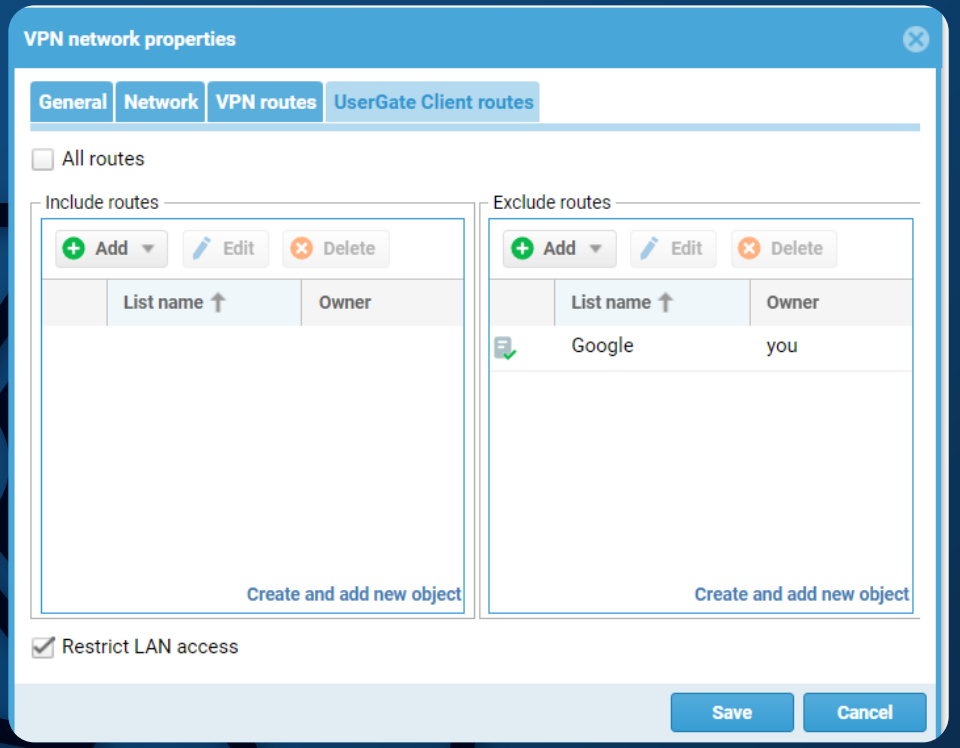


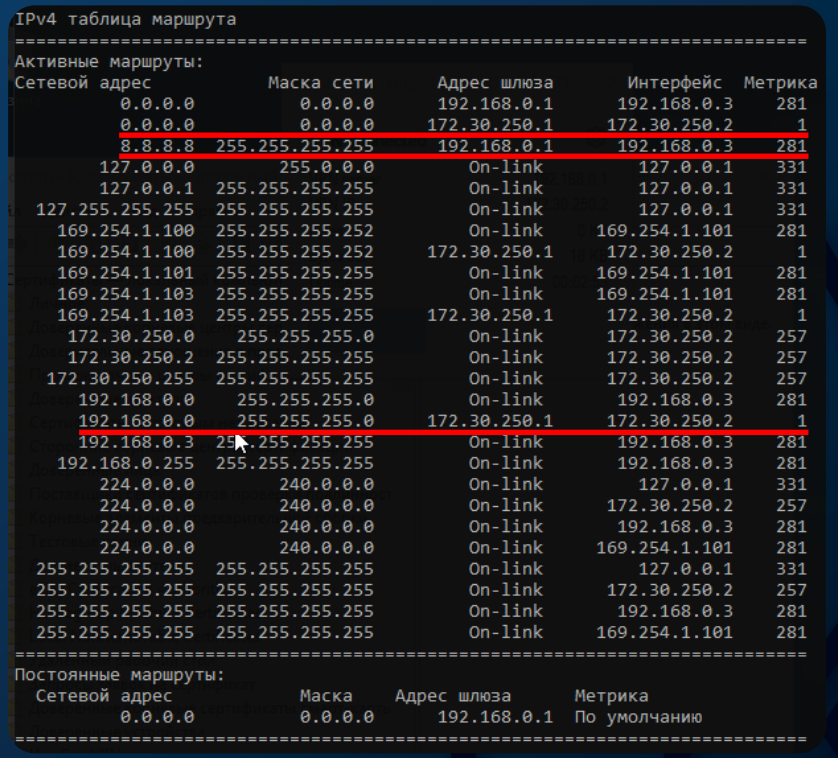
MC-режим



UserGate 7.1

VPN – Split tunneling

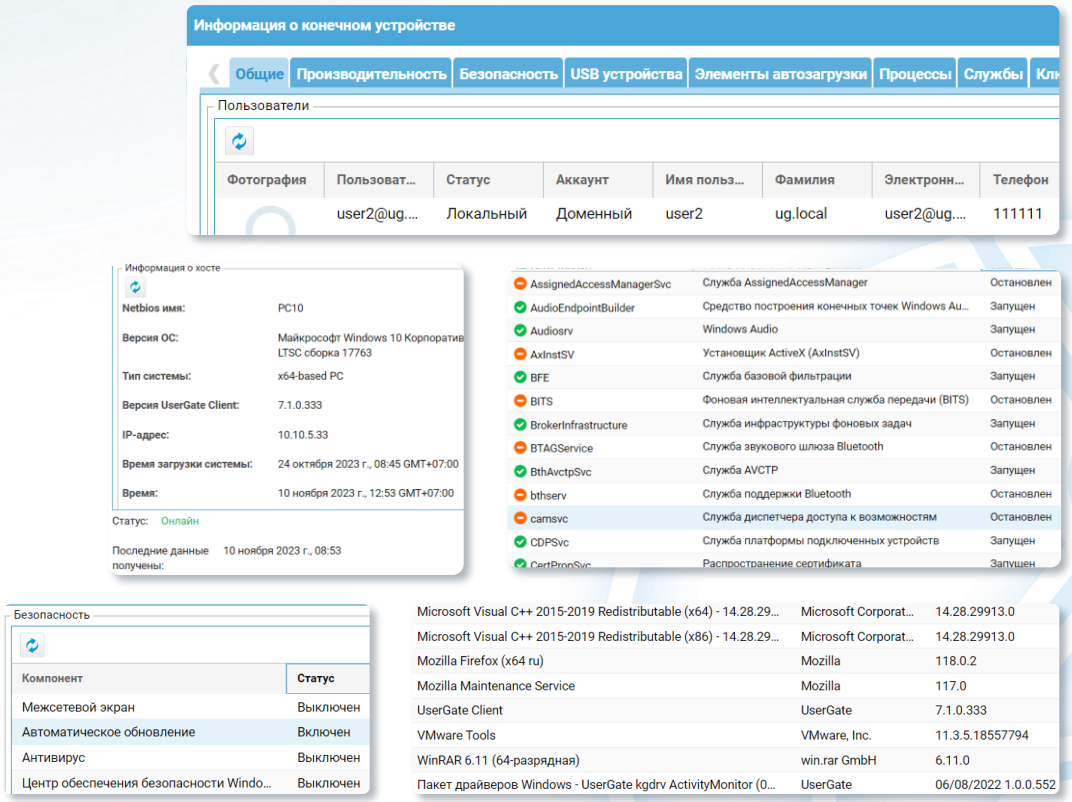




UserGate 7.1

HIP– сбор информации с устройства

- Состояние, производительность
- Безопасность
- USB-устройства
- Элементы автозагрузки
- Процессы
- Службы
- Ключи реестра
- Программное обеспечение
- Установленные обновления

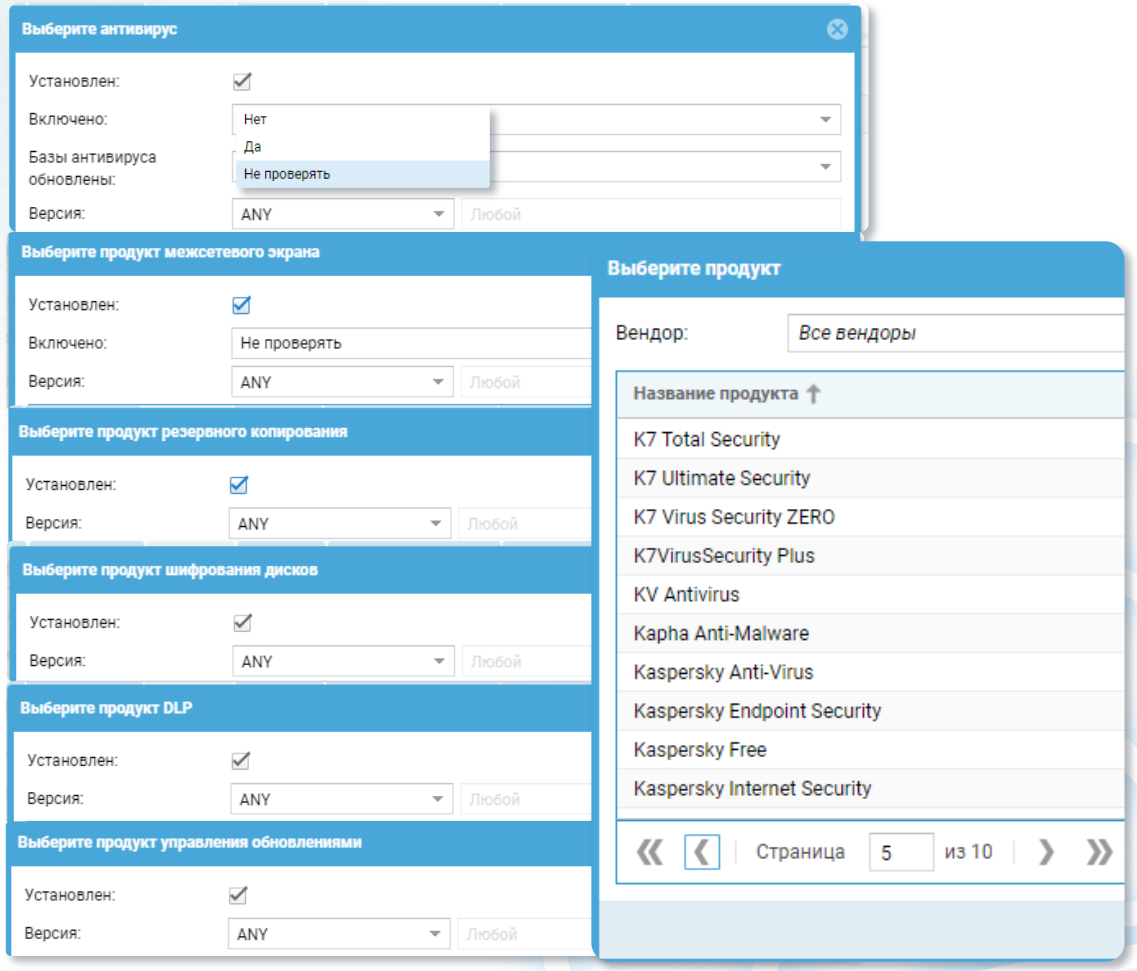


UserGate 7.1

HIP – настройка

В проверке установленных продуктов доступно:

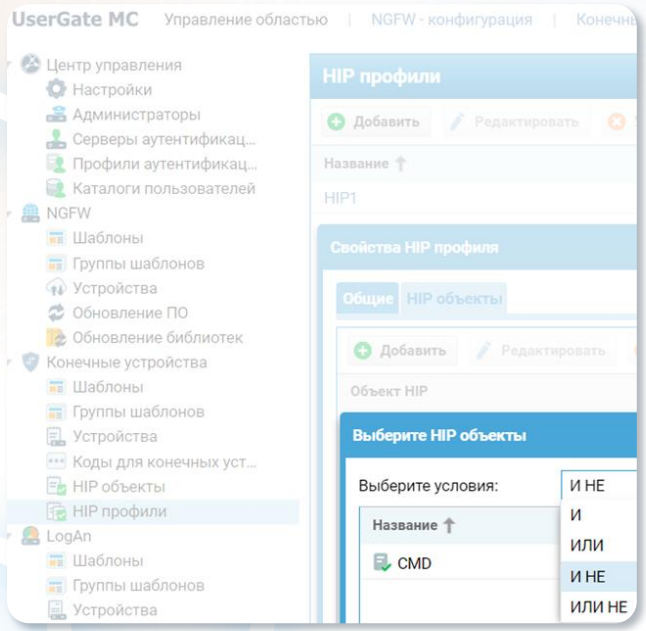
- антивирус (более 500)
- межсетевой экран (более 250)
- резервное копирование (более 220)
- шифрование диска (более 100)
- DLP (более 25)
- управление обновлениями



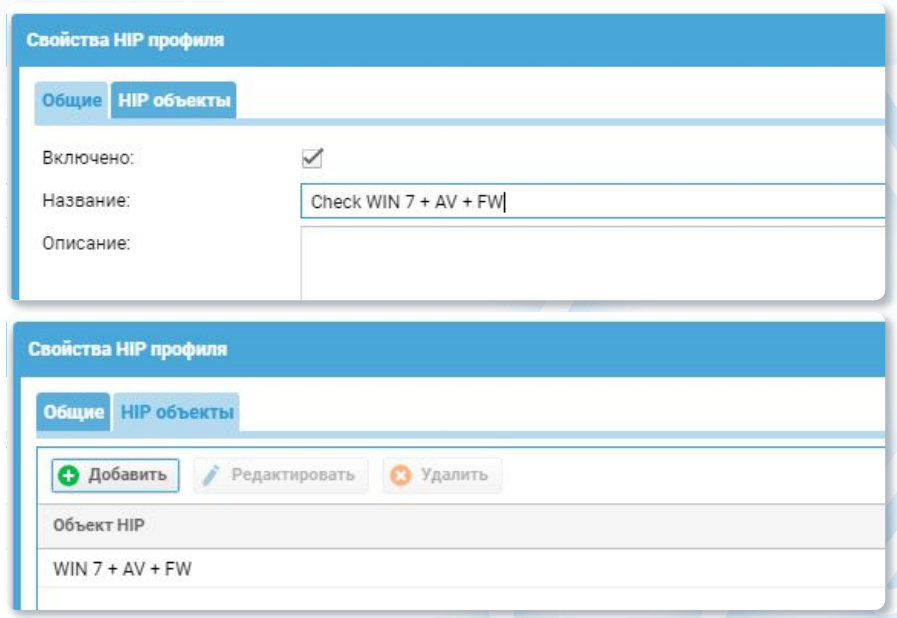
UserGate 7.1

HIP – настройка

В HIP-профиле агрегируем всю информацию по объектам

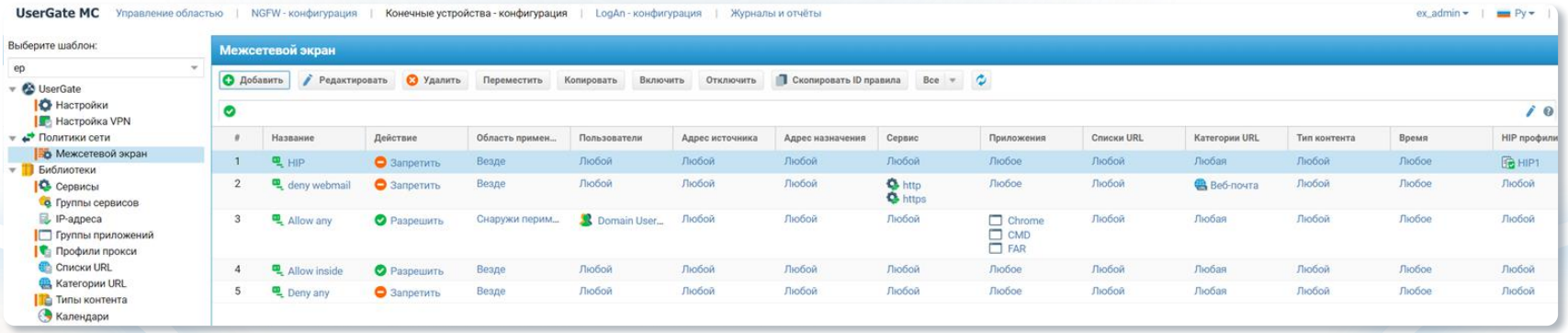


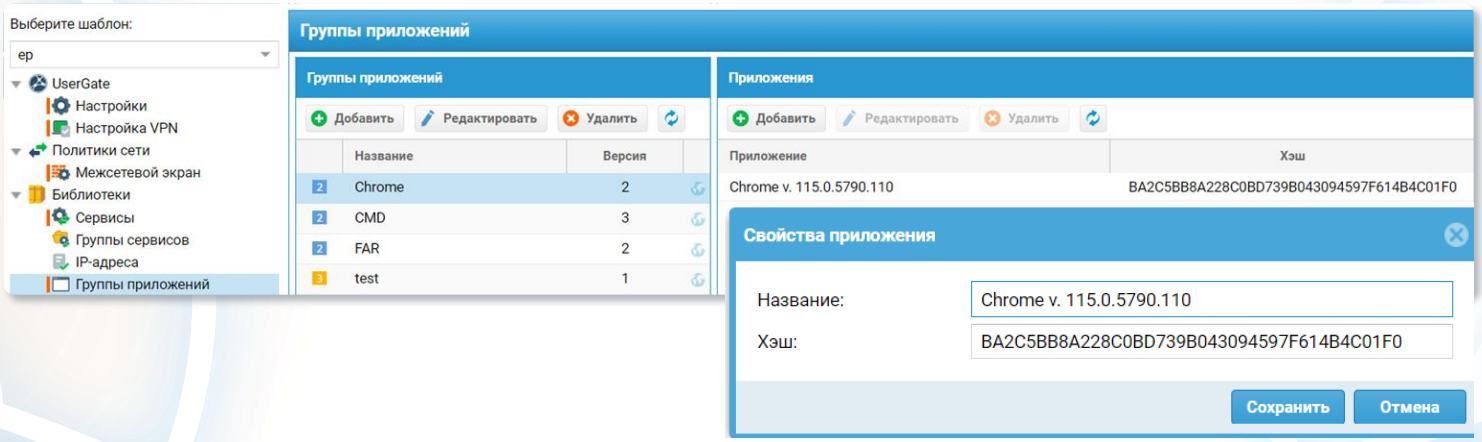
В одном HIP-профиле может быть несколько объектов HIP



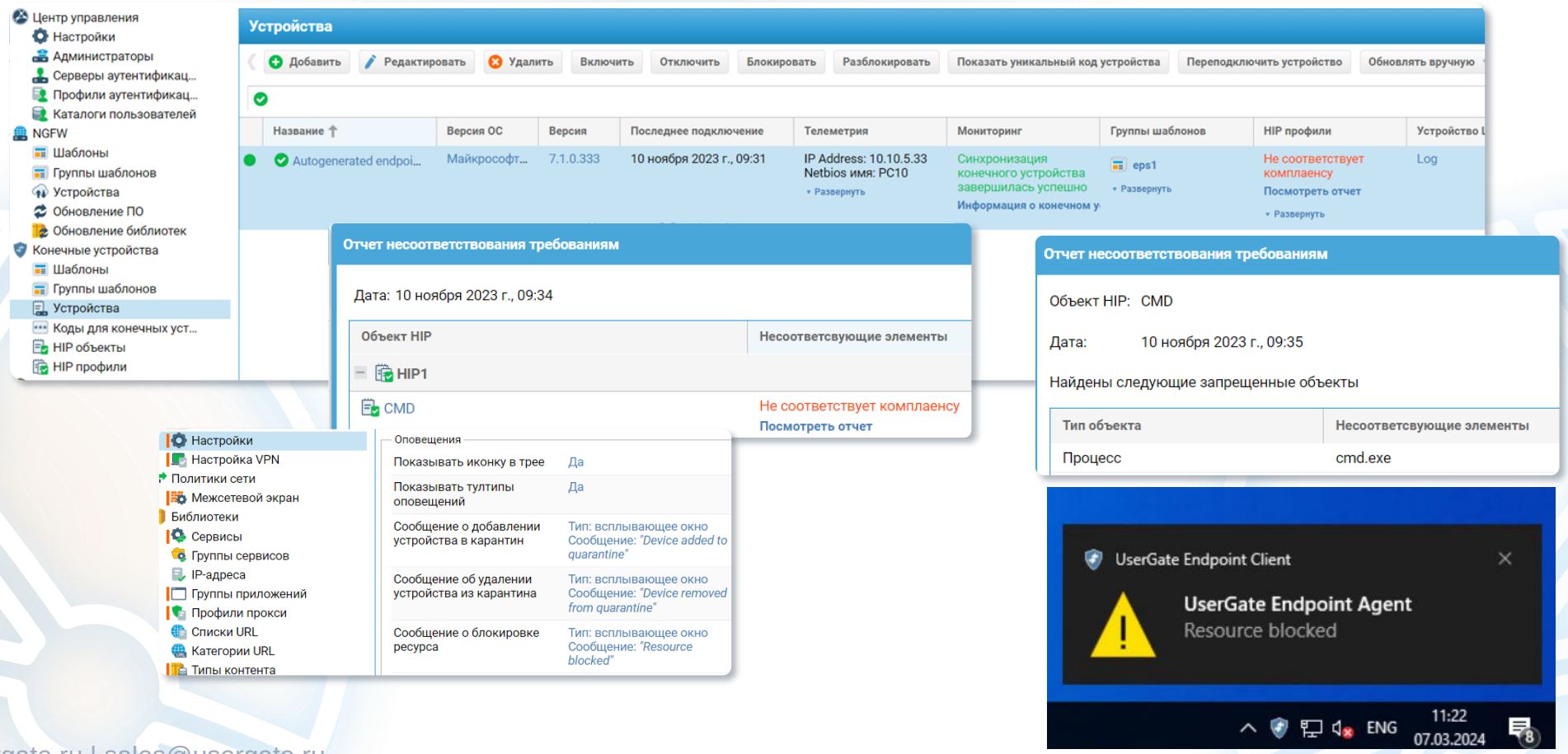
UserGate
7.1

HIP – правила FW





HIP – нотификация



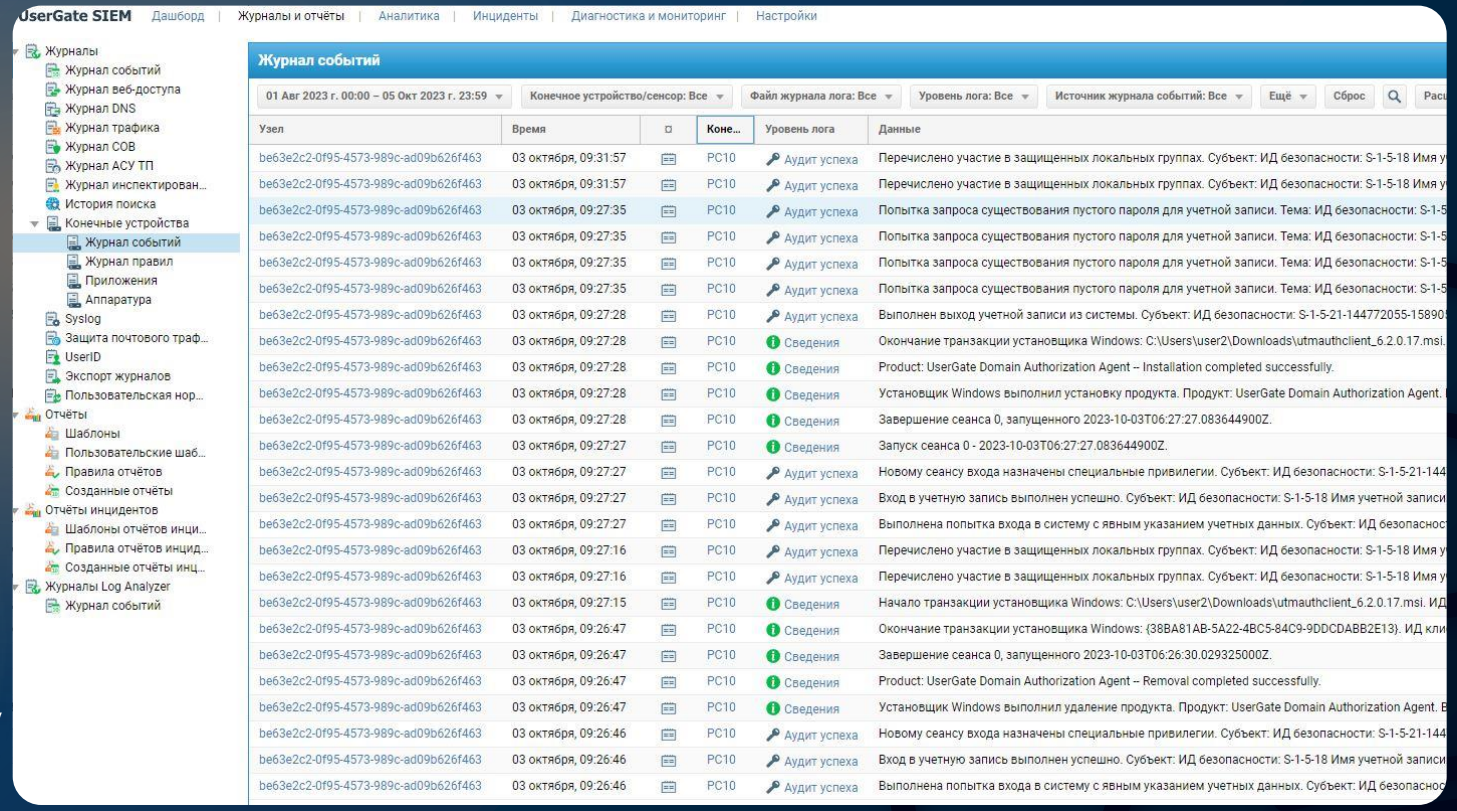
UserGate 7.1

Мониторинг событий

Журнал событий:

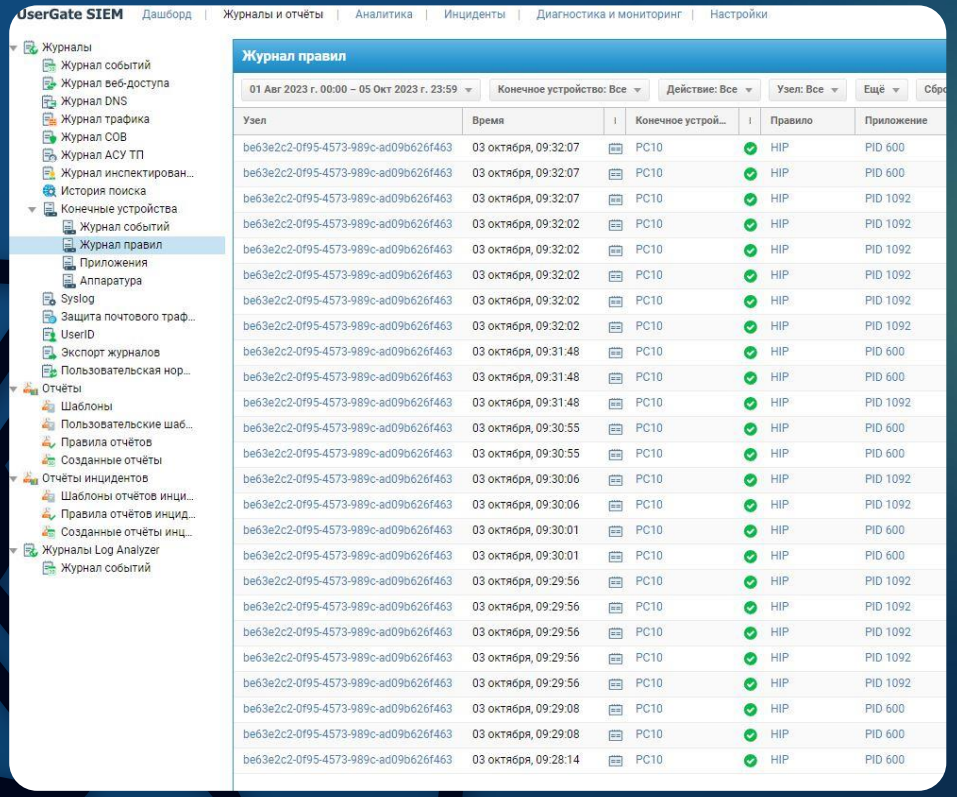
В журнале событий конечных устройств отражены события, получаемые от конечных устройств, контролируемых с использованием программного обеспечения UserGate Client.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, важность, тип события и т.п.



UserGate 7.1

Мониторинг событий



Журнал правил конечных устройств

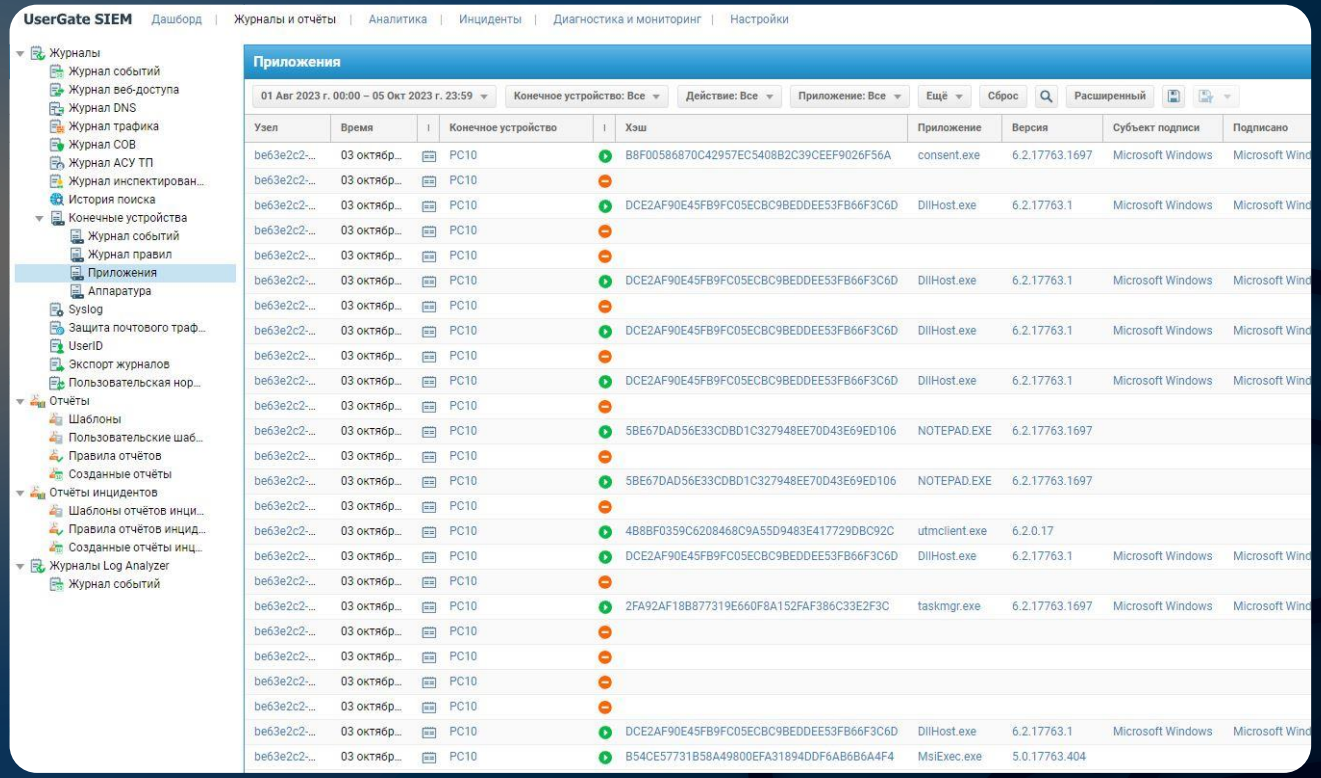
отображает события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включена функция ЖУРНАЛИРОВАНИЕ

UserGate 7.1

Мониторинг событий

Приложения конечных устройств:

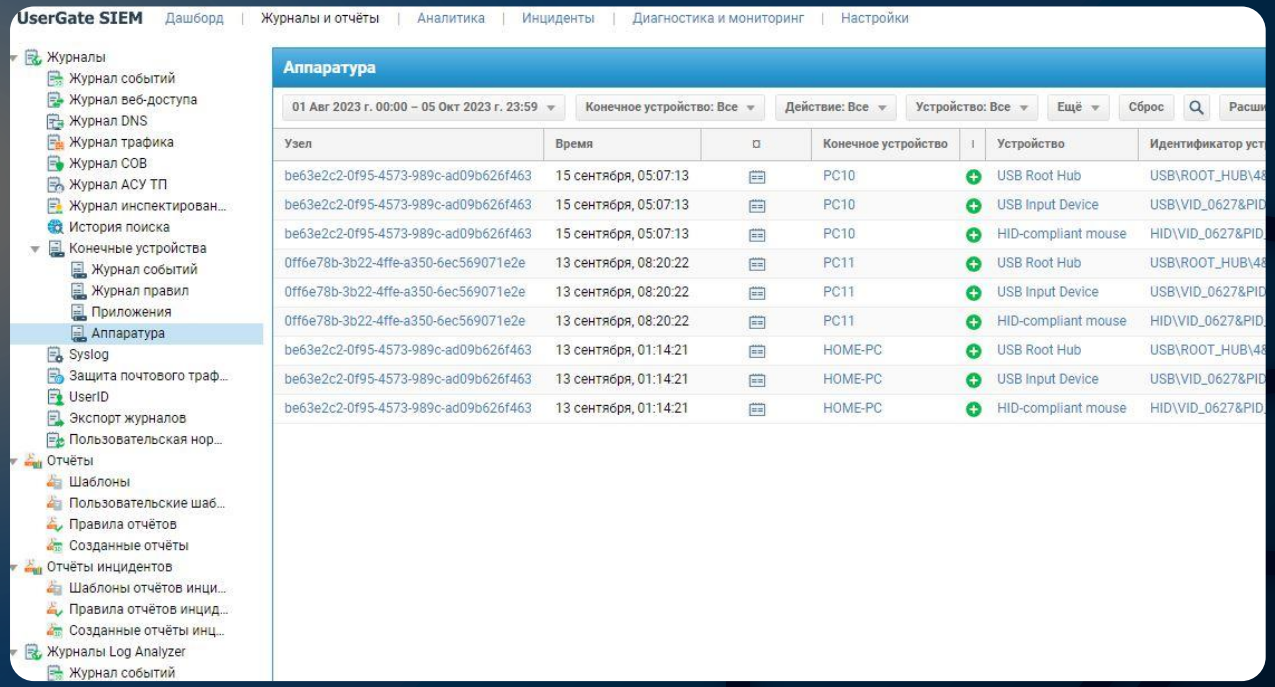
отображает приложения, которые запускались на конечных устройствах



Мониторинг событий

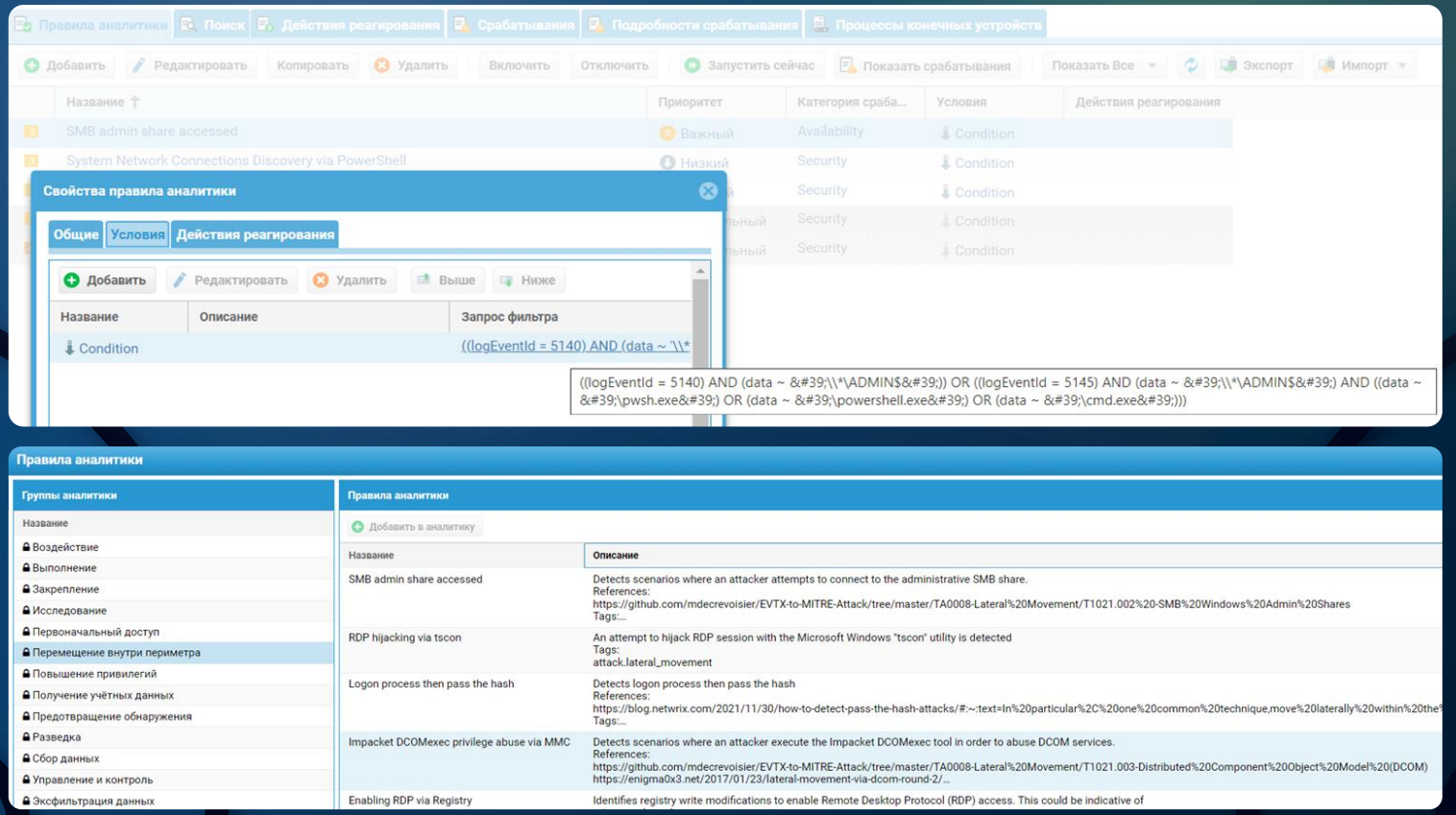
Аппаратура конечных устройств:

данный журнал содержит информацию об устройствах, подключаемых к конечным устройствам с установленным UserGate Client



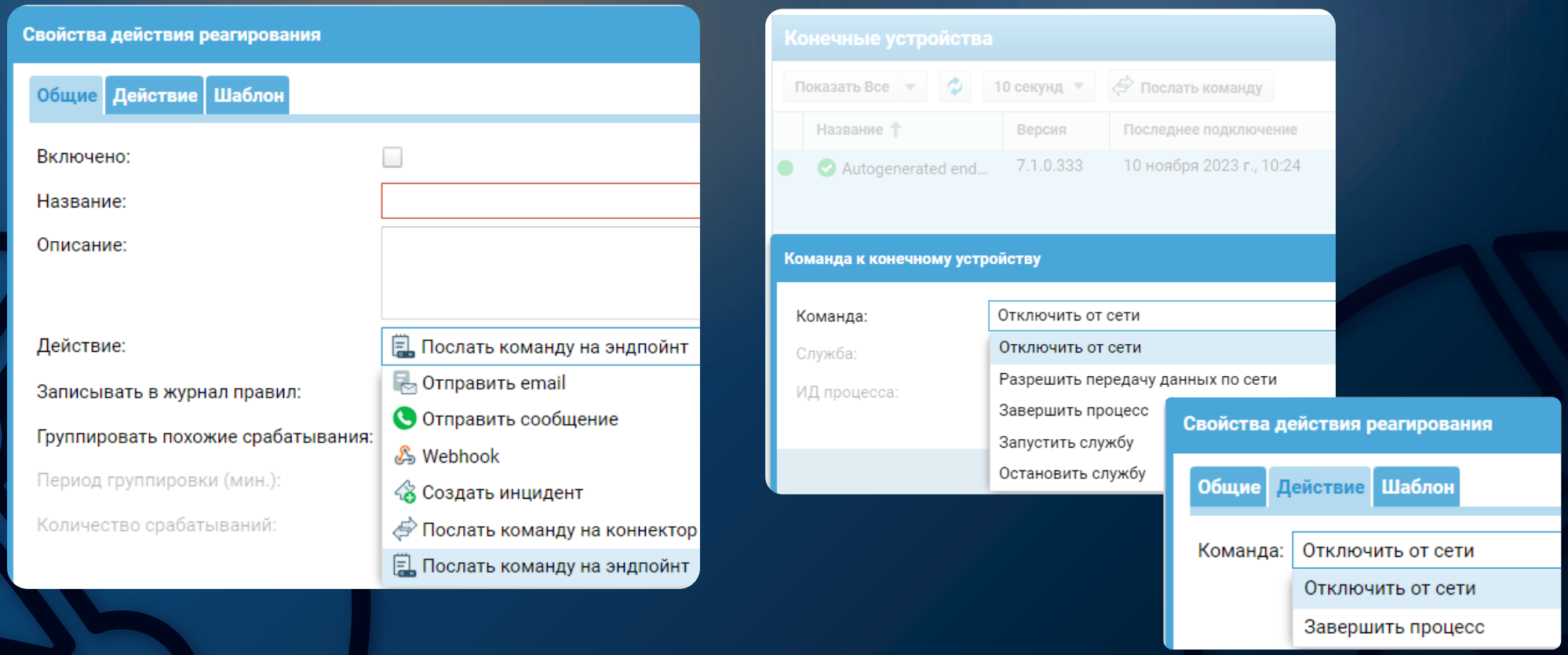
UserGate 7.1

Аналитика



UserGate 7.1

Реагирование



UserGate
7.1

SIEM

UserGate 7.1

UGOS 6.X: Log Analyzer
UGOS 7.0: Log Analyzer + SIEM
UGOS 7.1: Log Analyzer или SIEM

Изменения в UserGate SIEM

- UserGate LogAnalyzer – продукт с базовой лицензией
- UserGate SIEM – полноценная лицензируемая SIEM-система
- UserGate SIEM Expert – подписка на обновляемые правила аналитики от вендора

UserGate 7.1

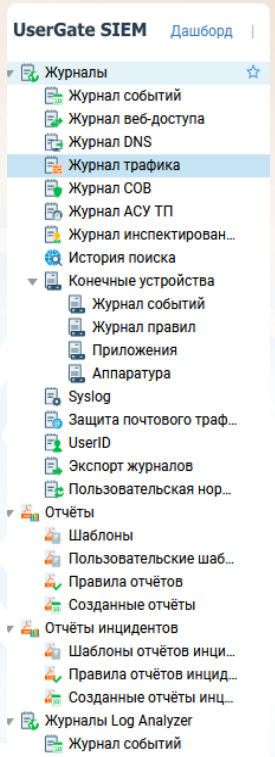
UserGate LogAnalyzer 6.X

ЖУРНАЛЫ:

- событий
- веб-доступа
- трафика
- СОВ
- АСУ ТП
- инспектирования SSH

UserGate 7.1

Журналы UserGate SIEM:



- Журналы UserGate NGFW
- APM Windows – UG Client
- Серверы Windows – протокол WMI
- Syslog-журналы
- Почтовый трафик
- UserID

UserGate 7.1

UserGate SIEM

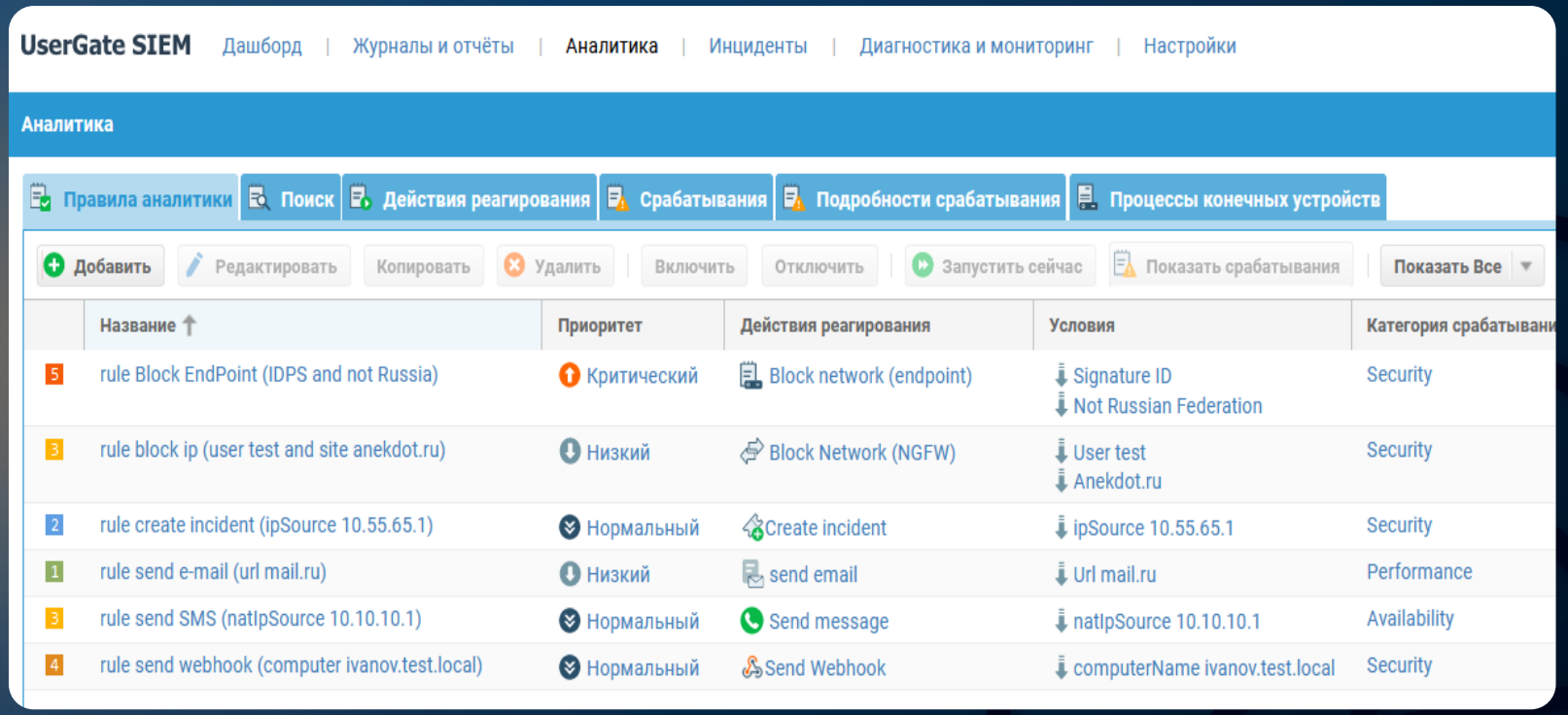
Основные функции:

- функционал LogAnalyzer 6.x
- Дополнительные источники журналов
- Правила аналитики
- Правила нормализации событий
- Экспертиза вендора в создании правил аналитики
- Автоматическая реакция на срабатывания правил аналитики
- Работа с инцидентами информационной безопасности

UserGate 7.1

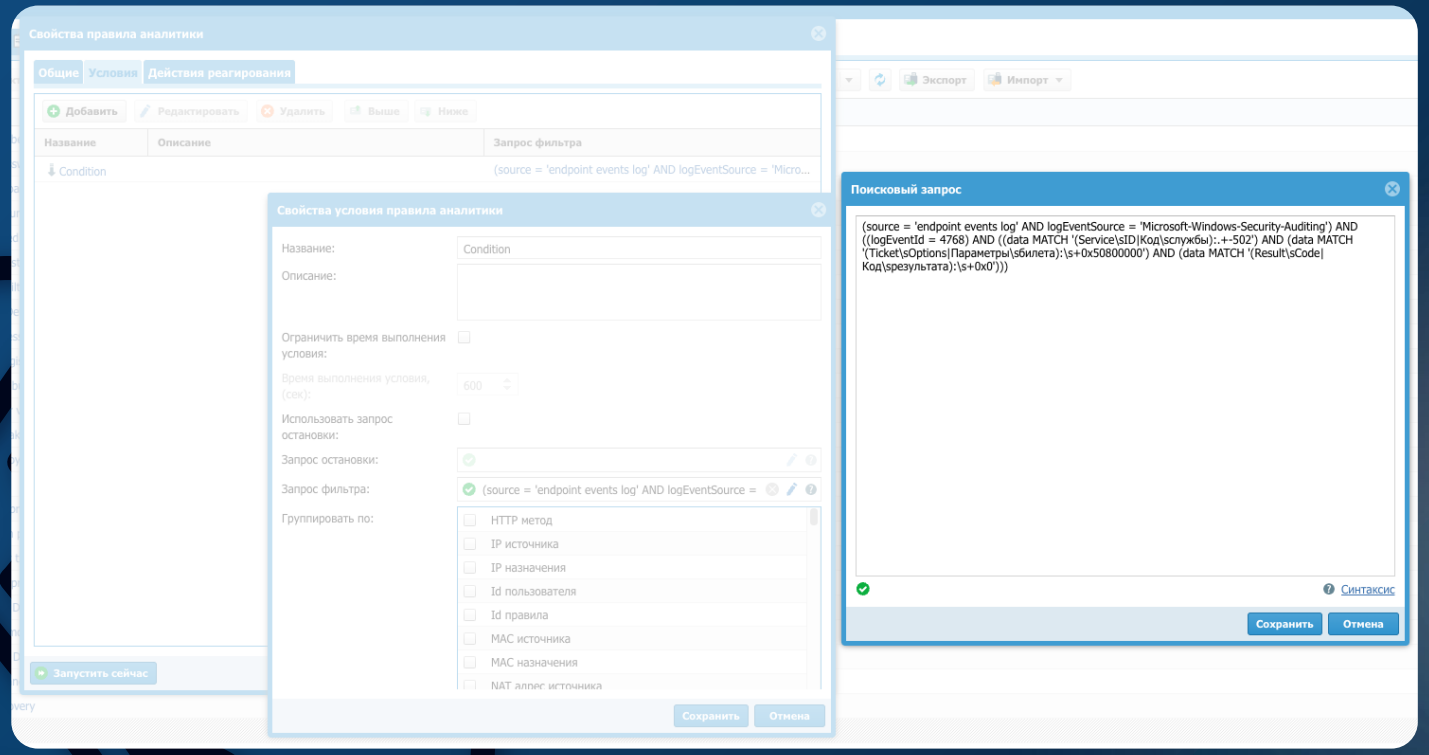
UserGate SIEM: **АНАЛИТИКА**

Правила аналитики: настройки по любому полю журналов



UserGate 7.1

UserGate SIEM: **АНАЛИТИКА**

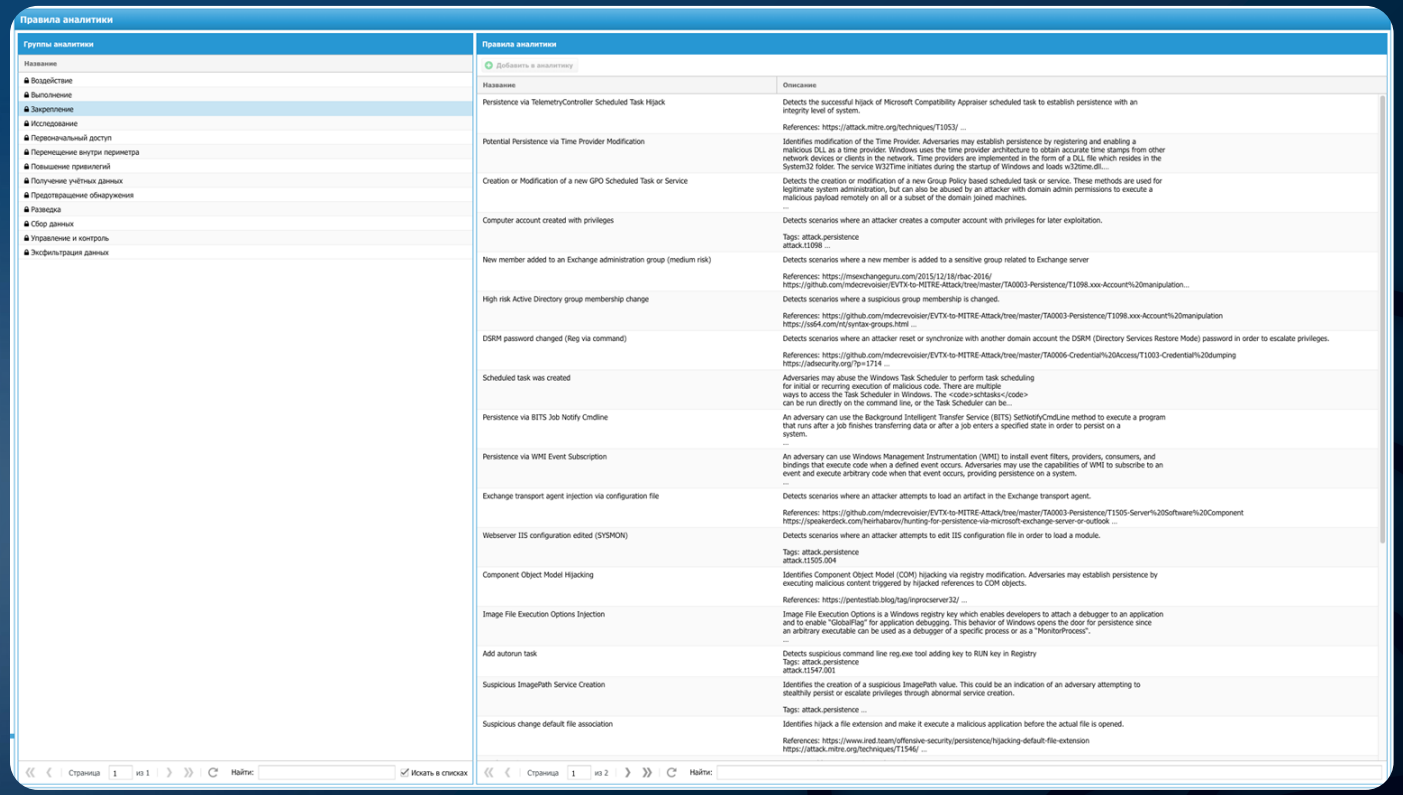


Условия срабатывания: произвольная логика запросов

UserGate 7.1

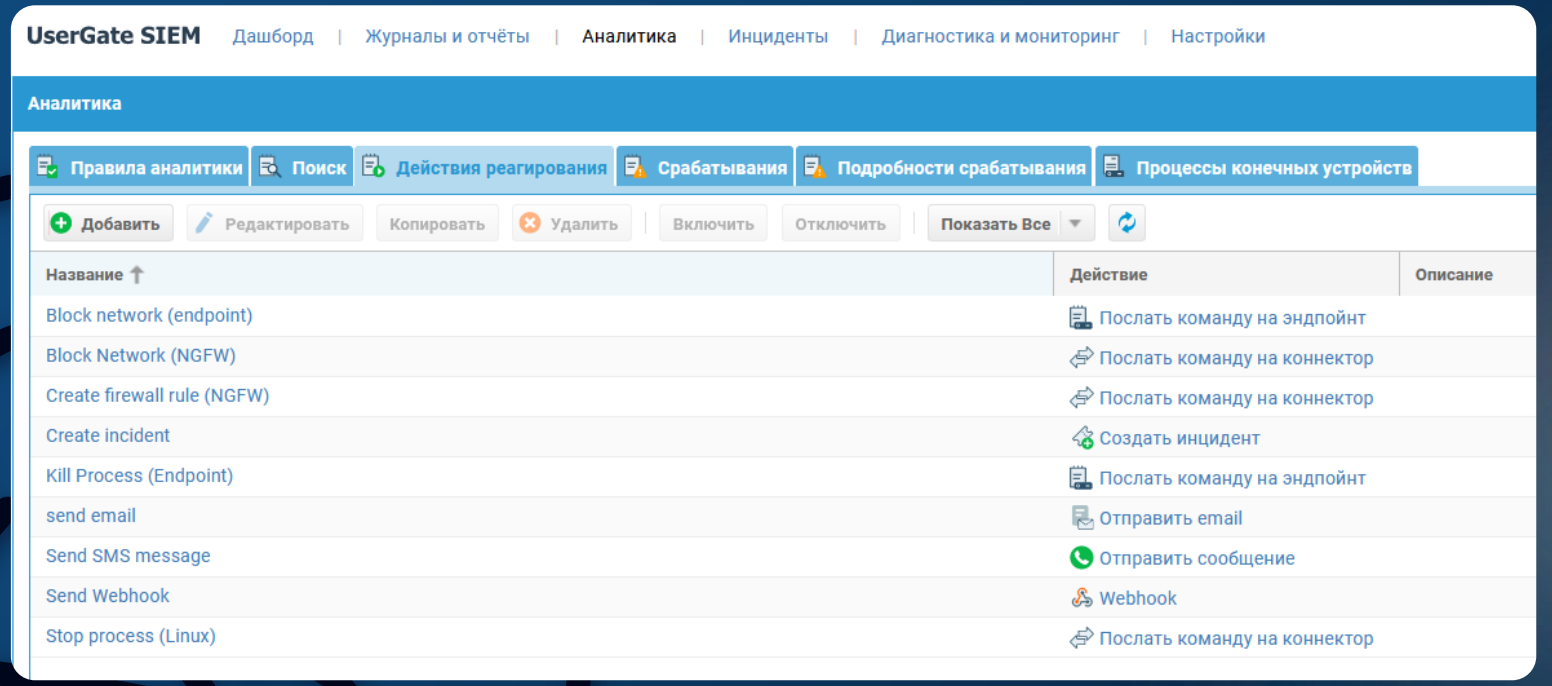
UserGate SIEM: **АНАЛИТИКА**

Правила аналитики:
база правил
аналитики
по подписке



UserGate 7.1

UserGate SIEM: **АНАЛИТИКА**

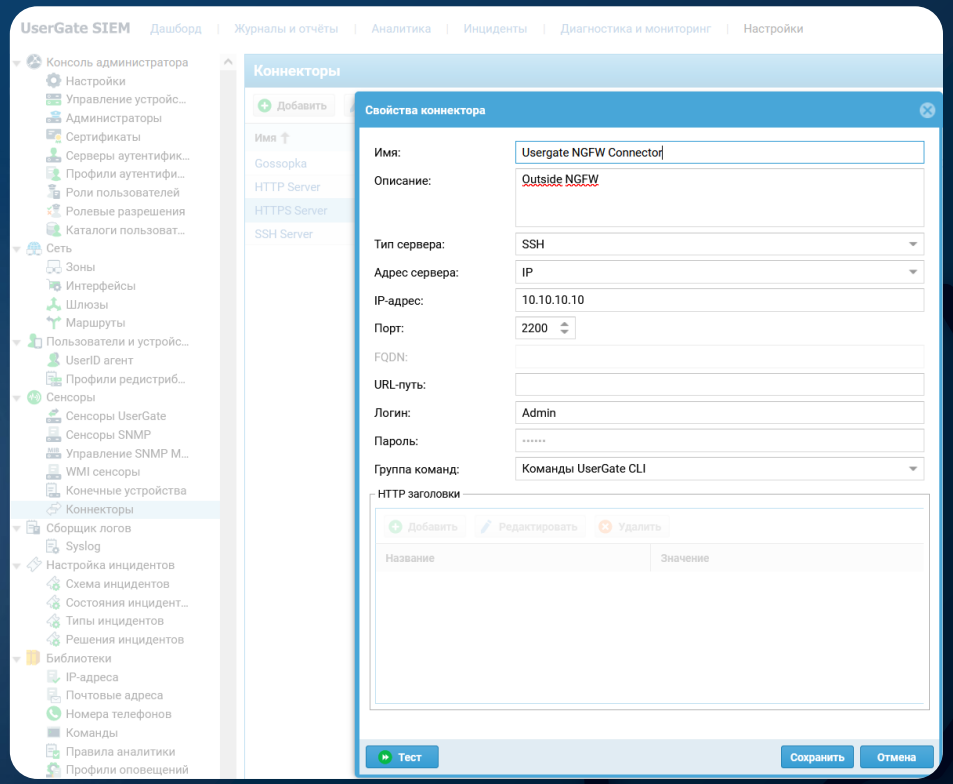


Действия реагирования: информирование инженеров и команды управляемым устройствам

UserGate 7.1

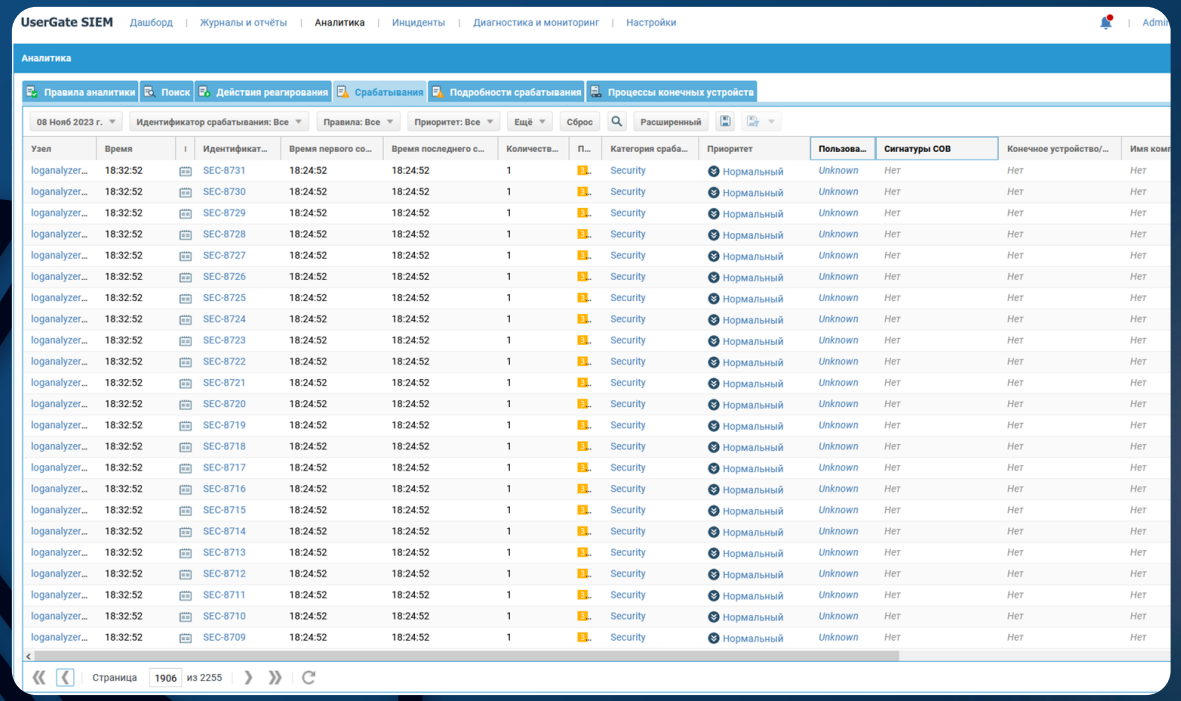
UserGate SIEM: **КОННЕКТОРЫ**

Поддержка устройств по протоколам SSH, HTTP, HTTPS



UserGate 7.1

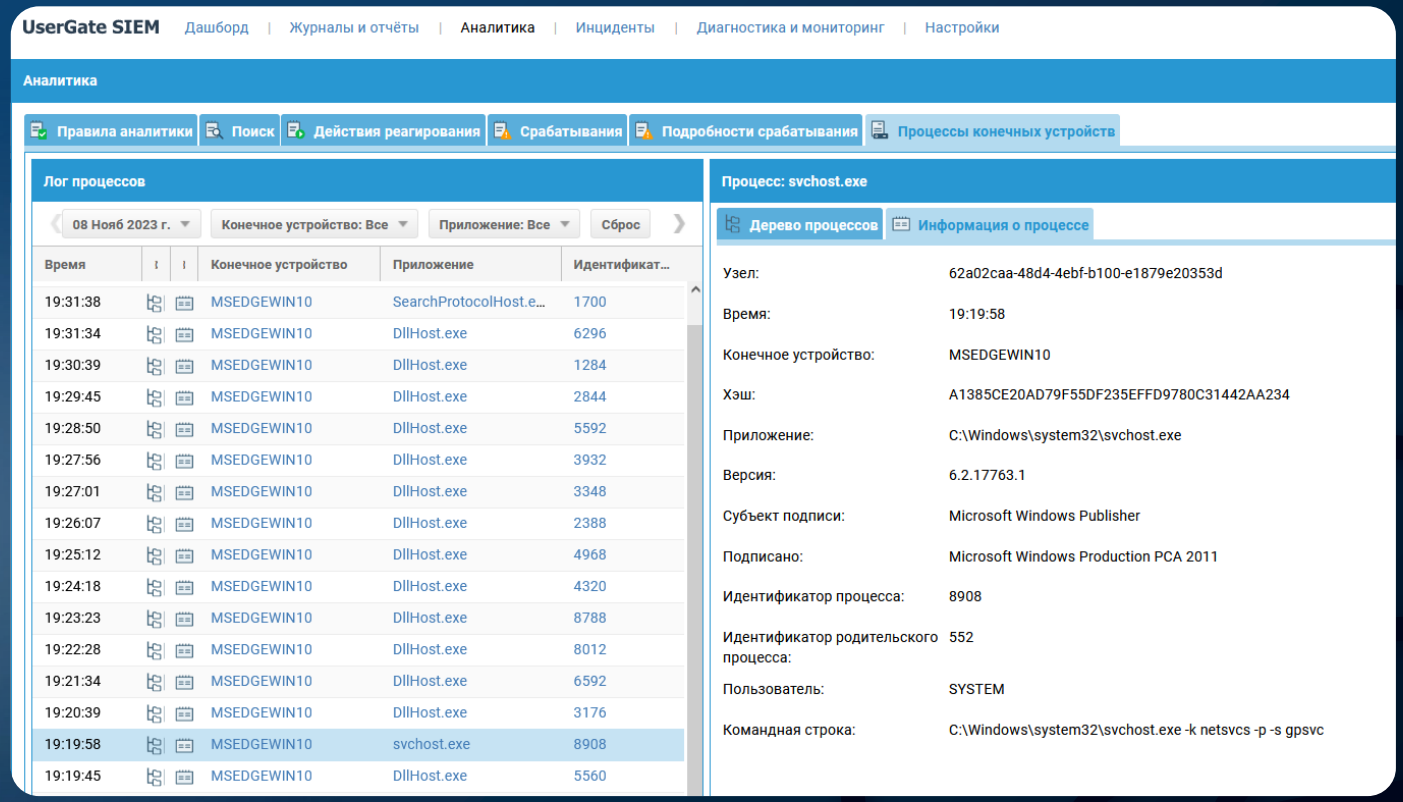
UserGate SIEM: **АНАЛИТИКА**



Срабатывания правил аналитики: ничто не останется вне внимания

UserGate 7.1

UserGate SIEM: АНАЛИТИКА

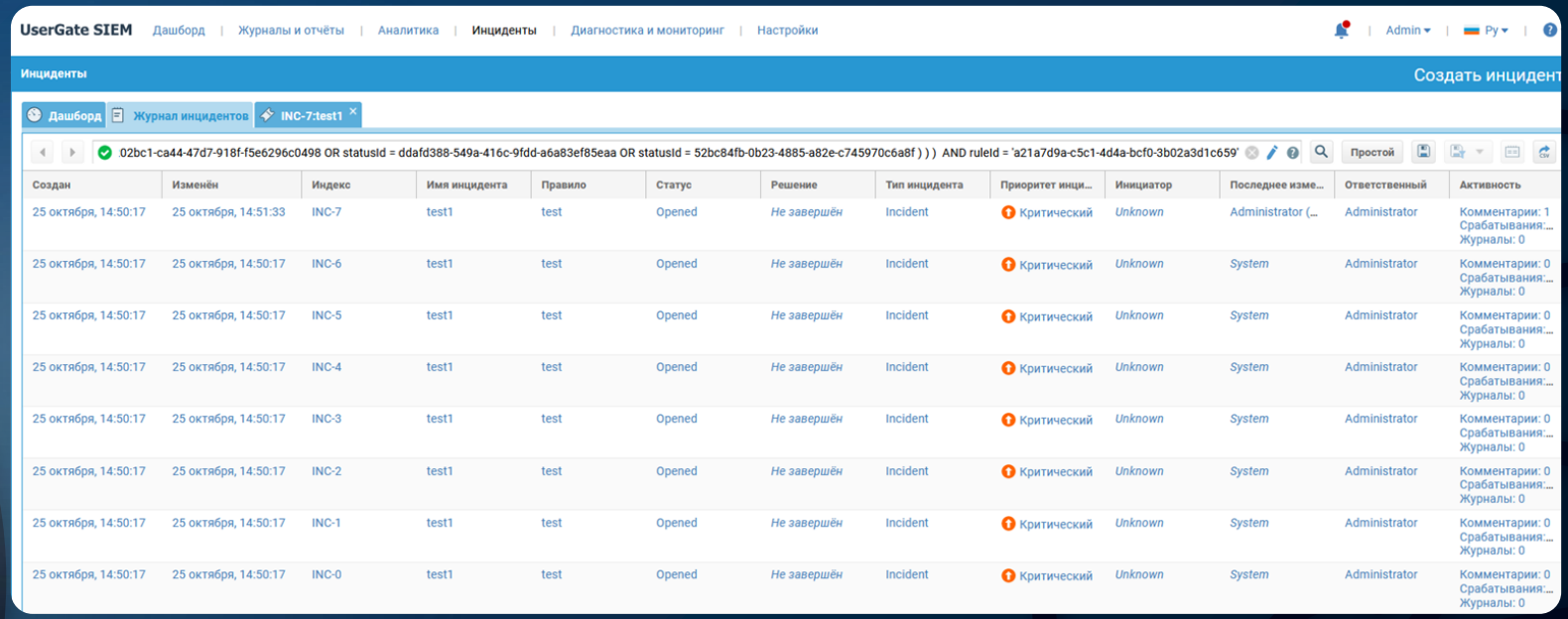


Процессы конечных устройств: полная информация

UserGate 7.1

UserGate SIEM: ИНЦИДЕНТЫ

Журнал инцидентов: информация обо всех инцидентах

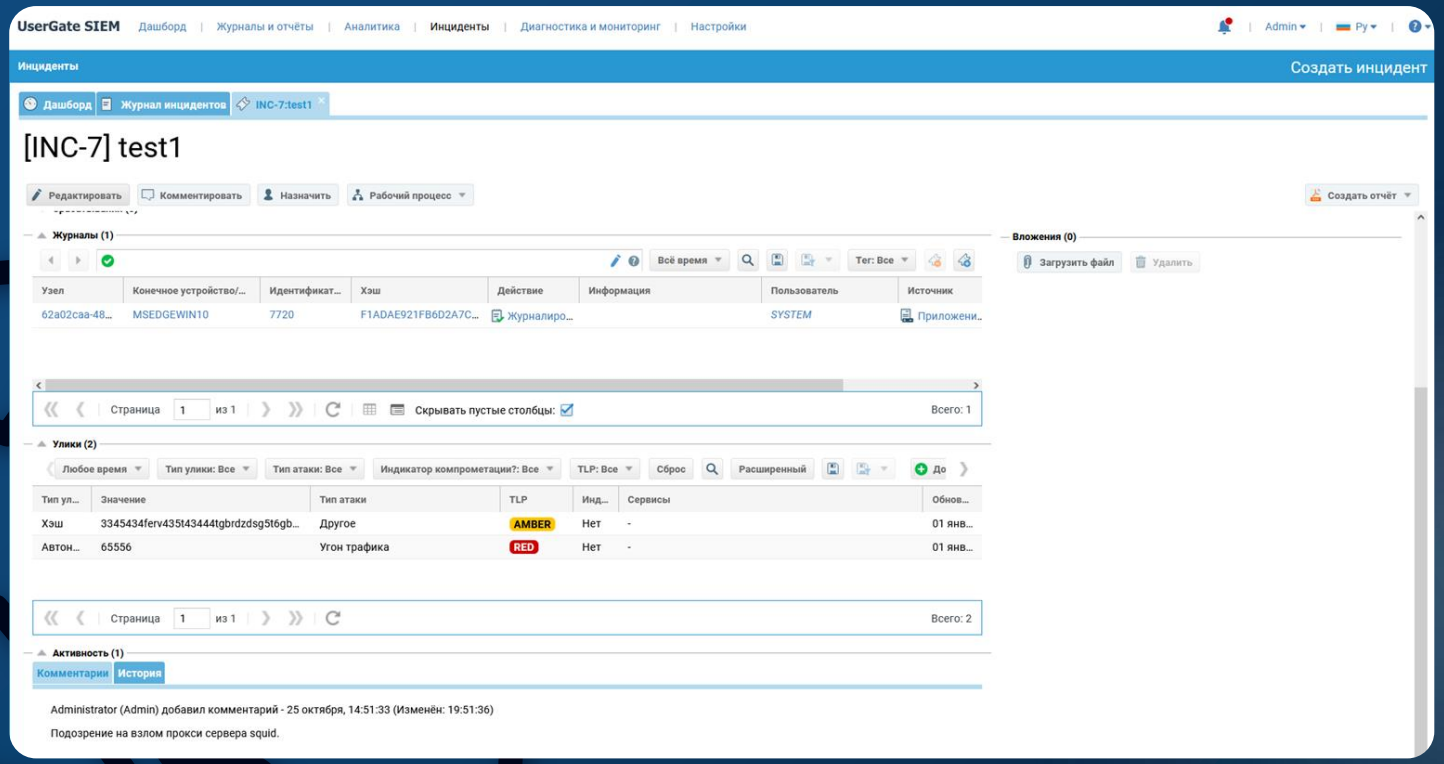


UserGate 7.1

UserGate SIEM:
ЗАЧЕМ?

UserGate 7.1

UserGate SIEM: ИНЦИДЕНТЫ



Работа с инцидентом: одновременная работа с инцидентом множества участников

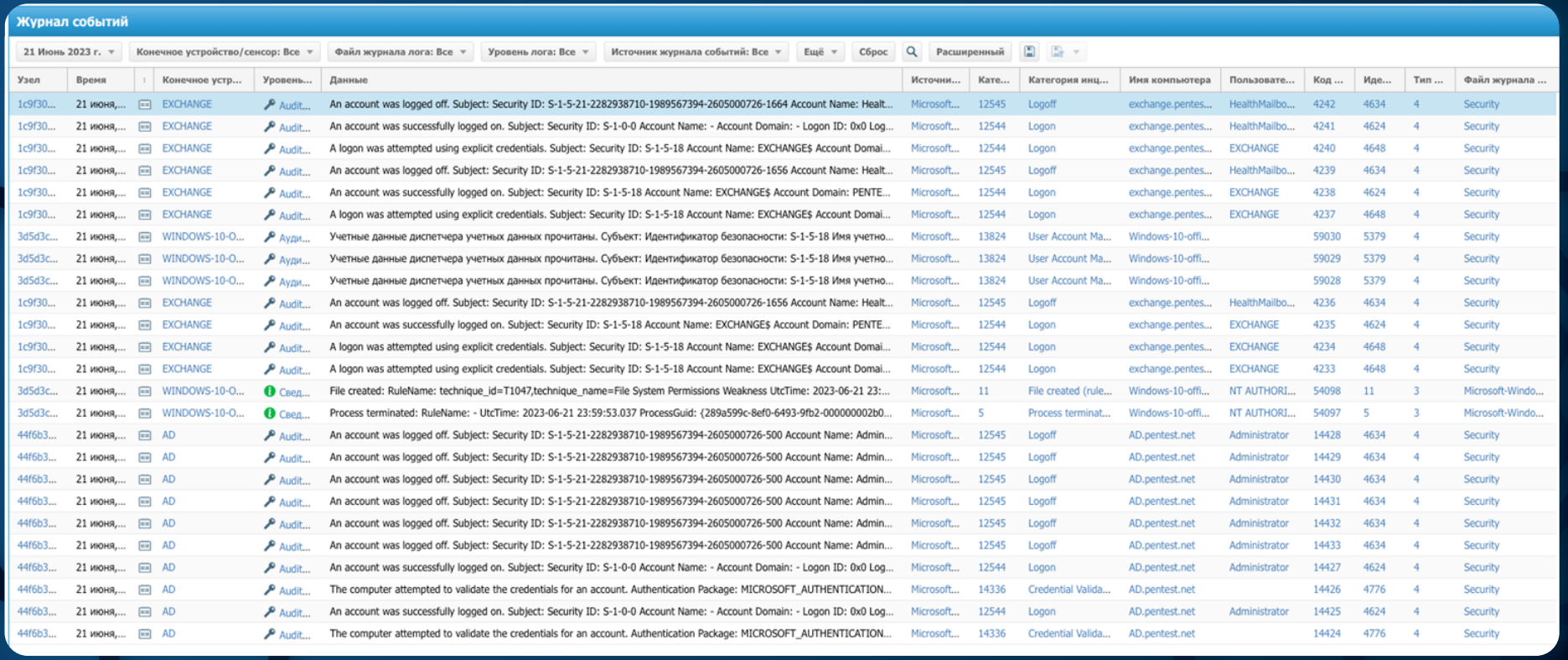
UserGate SIEM: **ЗАЧЕМ?**

- **Анализ и реагирование**
- **Рекомендации UserGate: применять UserGate SIEM при наличии 5-ти и более сетевых устройств**

UserGate 7.1

UserGate SIEM: **ИНЦИДЕНТЫ**

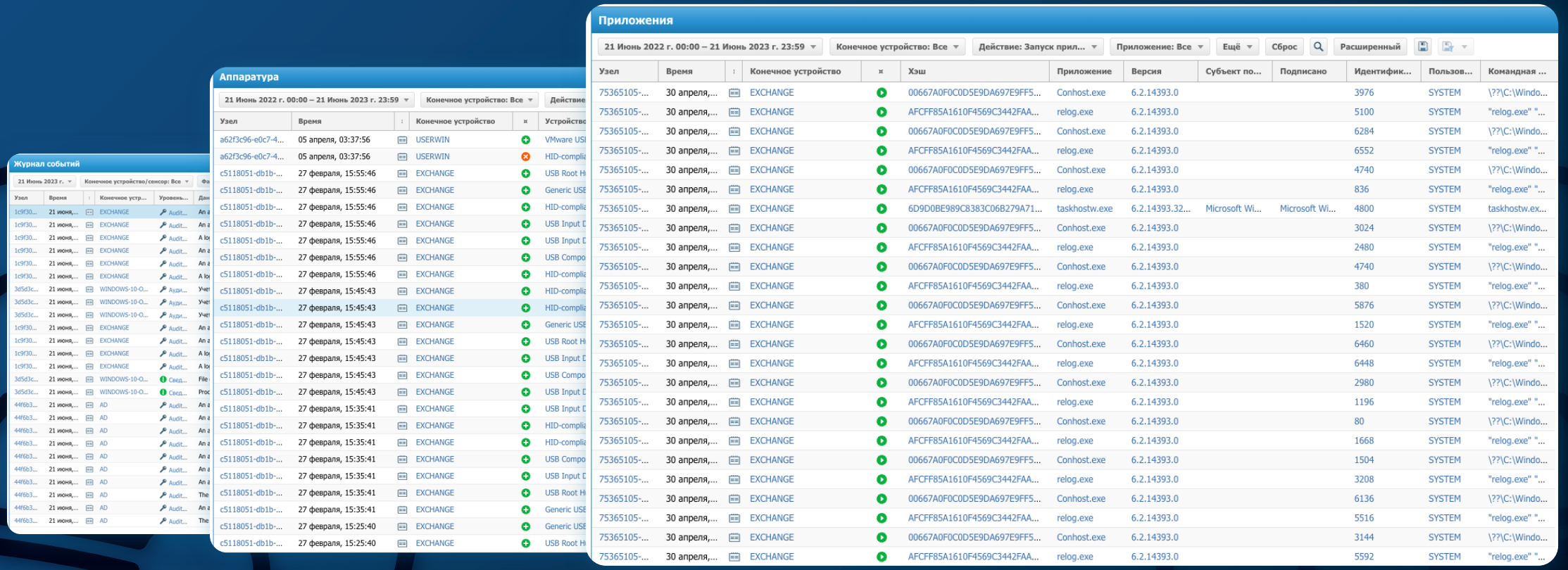
События ИТ



UserGate 7.1

UserGate SIEM: **ИНЦИДЕНТЫ**

События ИТ



UserGate 7.1

UserGate SIEM: **ЗАЧЕМ**

Мы позволяем:

- сократить время реакции на событие ИБ
- расследовать инцидент
- выполнить автоматическую реакцию на инцидент

UserGate 7.1

UserGate SIEM: **ЗАЧЕМ**

Мы позволяем:

не допустить последствий инцидента:

- утечка данных;
- потеря доступа к данным;
- остановка процессов

и многое-многое другое

Регистрация на конференцию

Оффлайн

Онлайн

UserGate

7.1

Спасибо за внимание!

Игорь Шефер
Ведущий инженер UserGate