UserGate

7.1

БОЛЬШОЕ ОБНОВЛЕНИЕ

Игорь Шефер

Ведущий инженер UserGate

UserGate 7.1

IPSv3

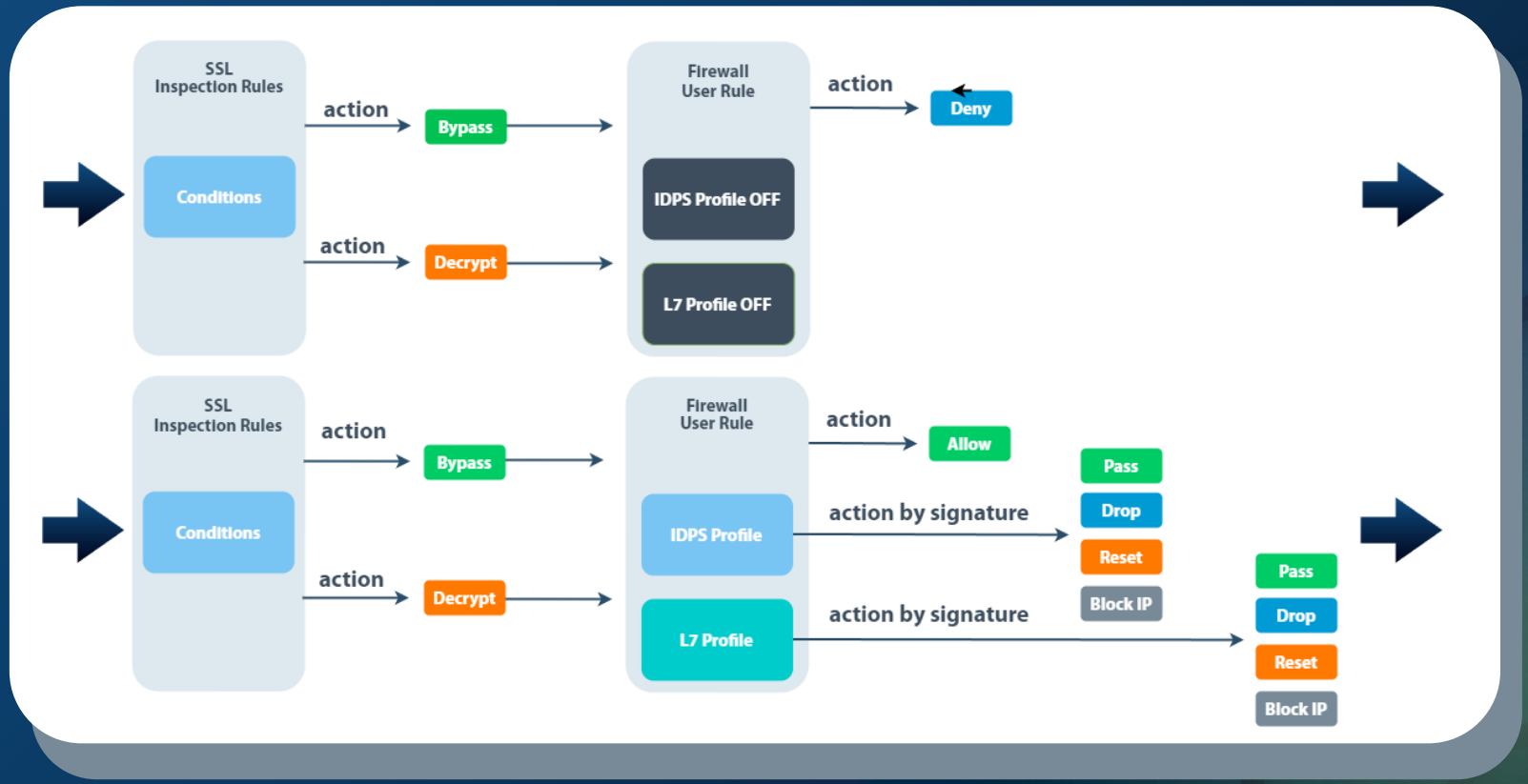
Движок

UserGate 7.1

- 3 версия движка
- поддержка обработки расшифрованного SSL
- возможность описывать свои 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



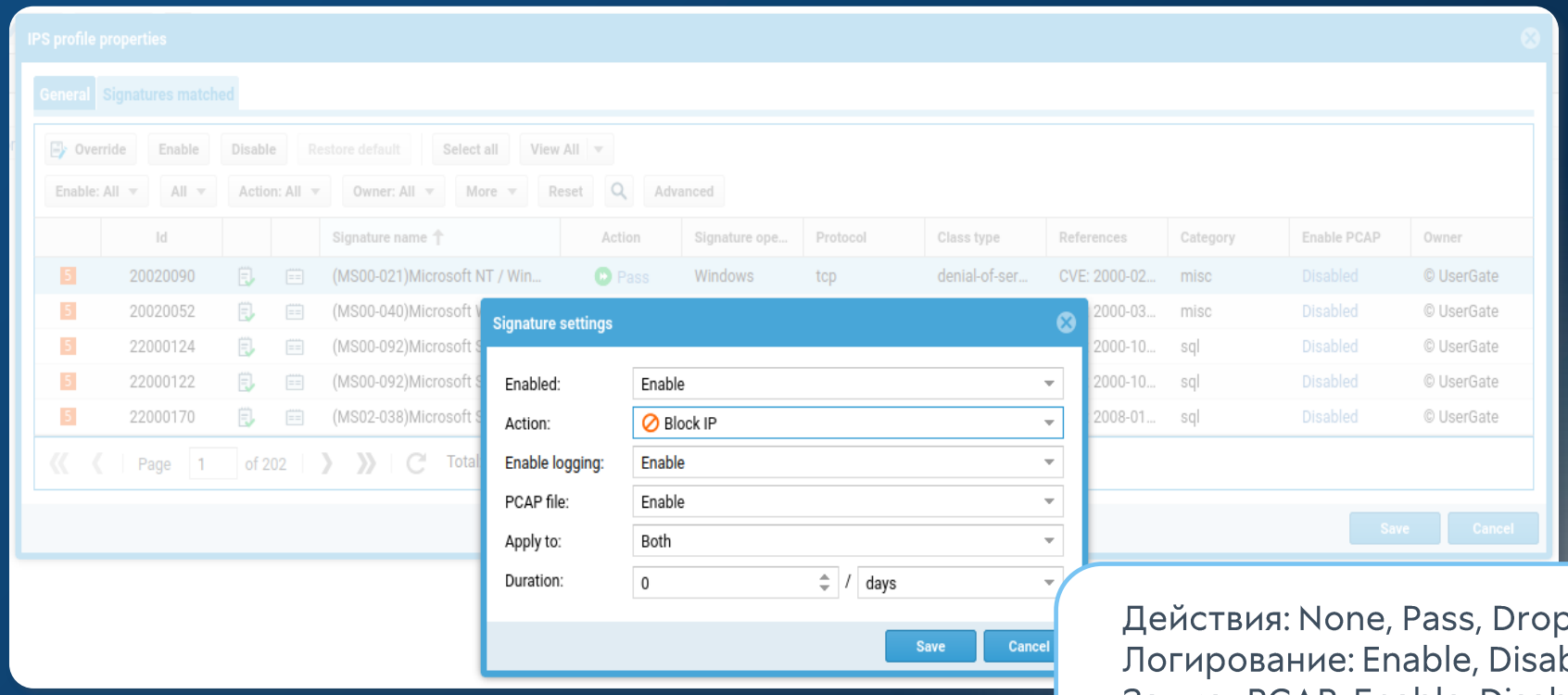
Новые кейсы

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

GUI. IPS-профиль

UserGate 7.1

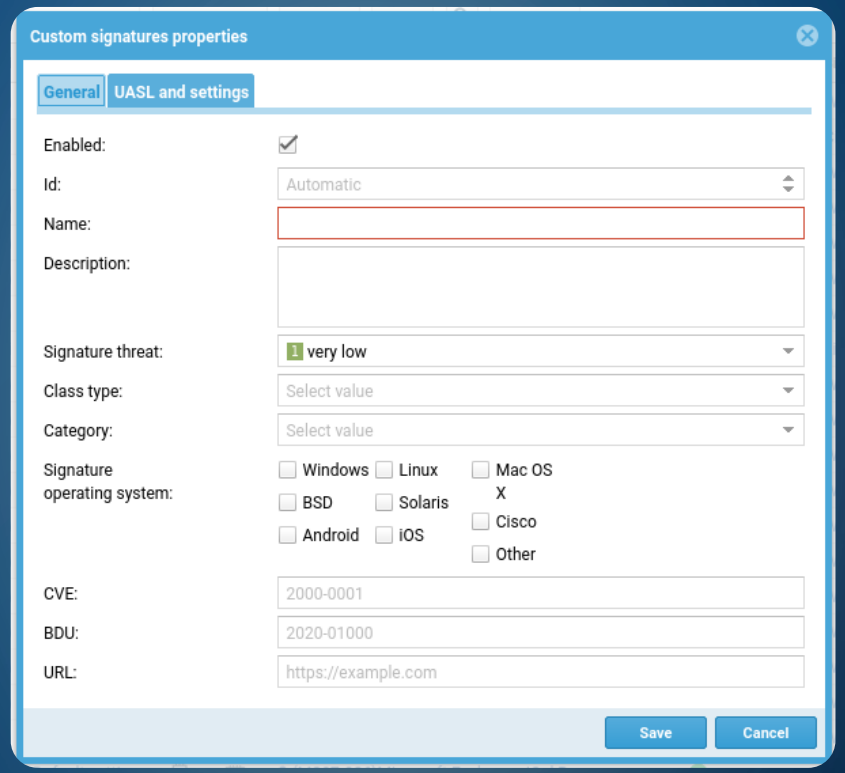


Действия: None, Pass, Drop, Reset, Block IP
Логирование: Enable, Disable
Запись PCAP: Enable, Disable
Применить к: Src, Dst, Both (активно при Reset и Block IP)
Продолжительность: days, hours, minutes

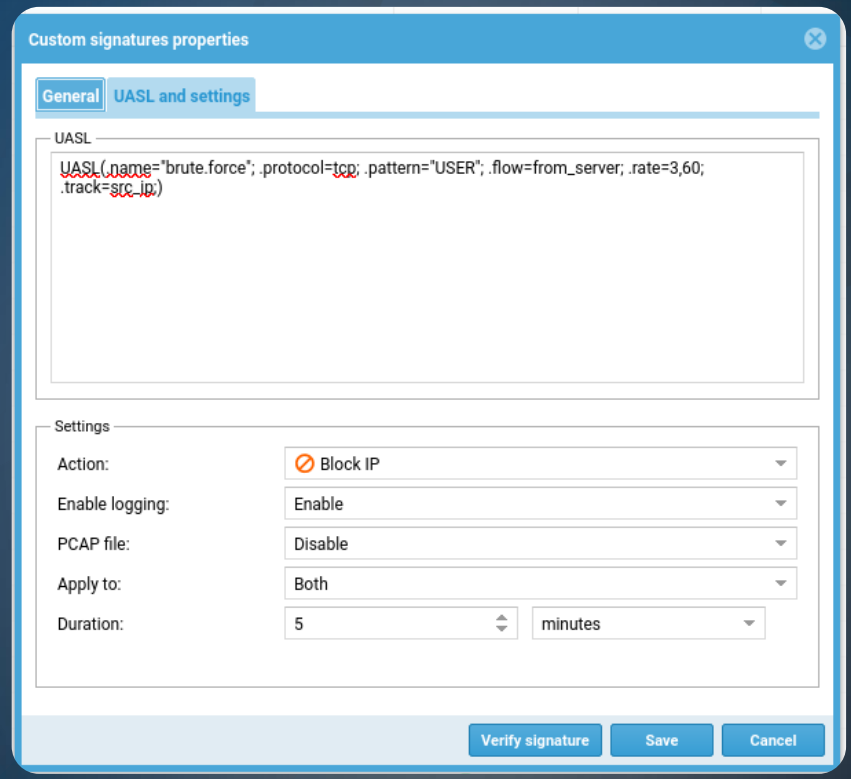
GUI. IPS-сигнатура Создание

UserGate 7.1

Шаг 1



Шаг 2



GUI. UASL

UserGate 7.1

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

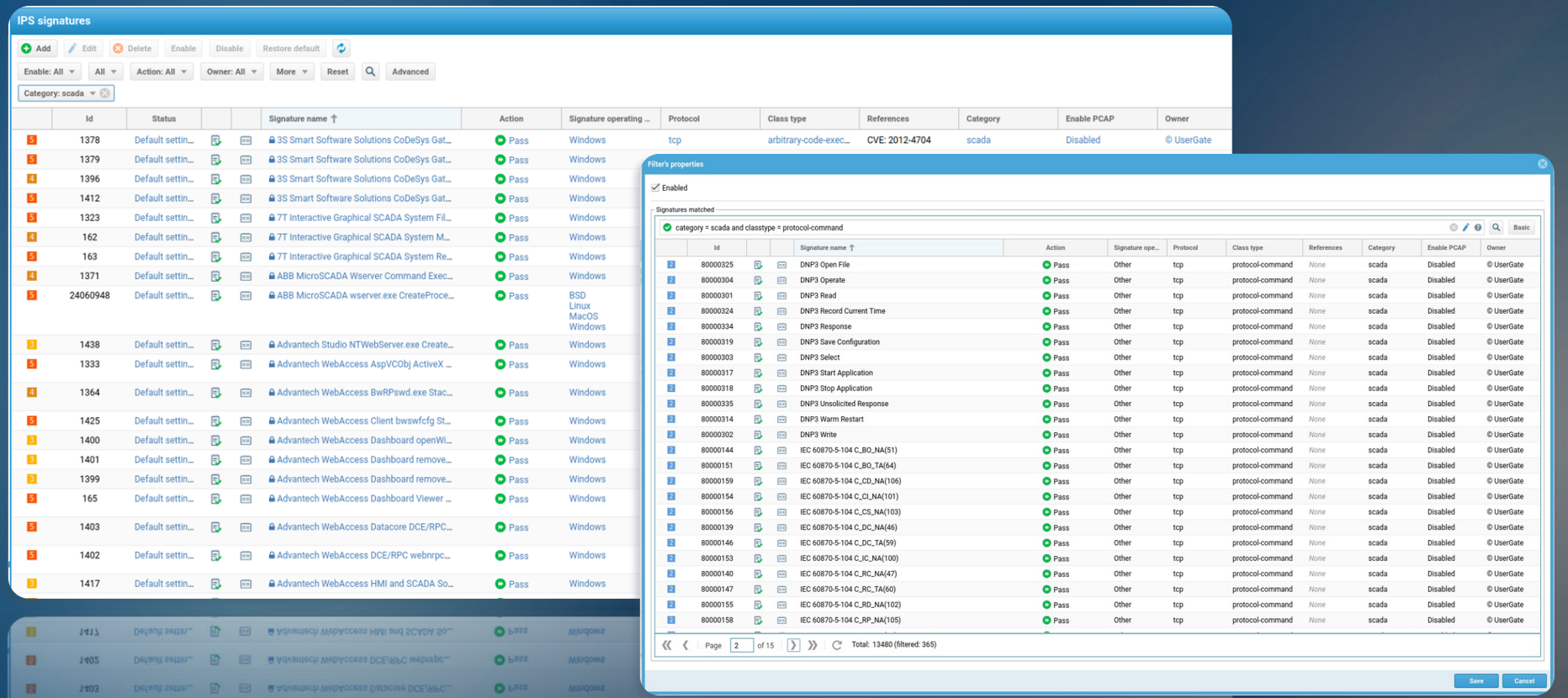
Матчинг бинарных данных
- byte_test, byte_jump

Пример:

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

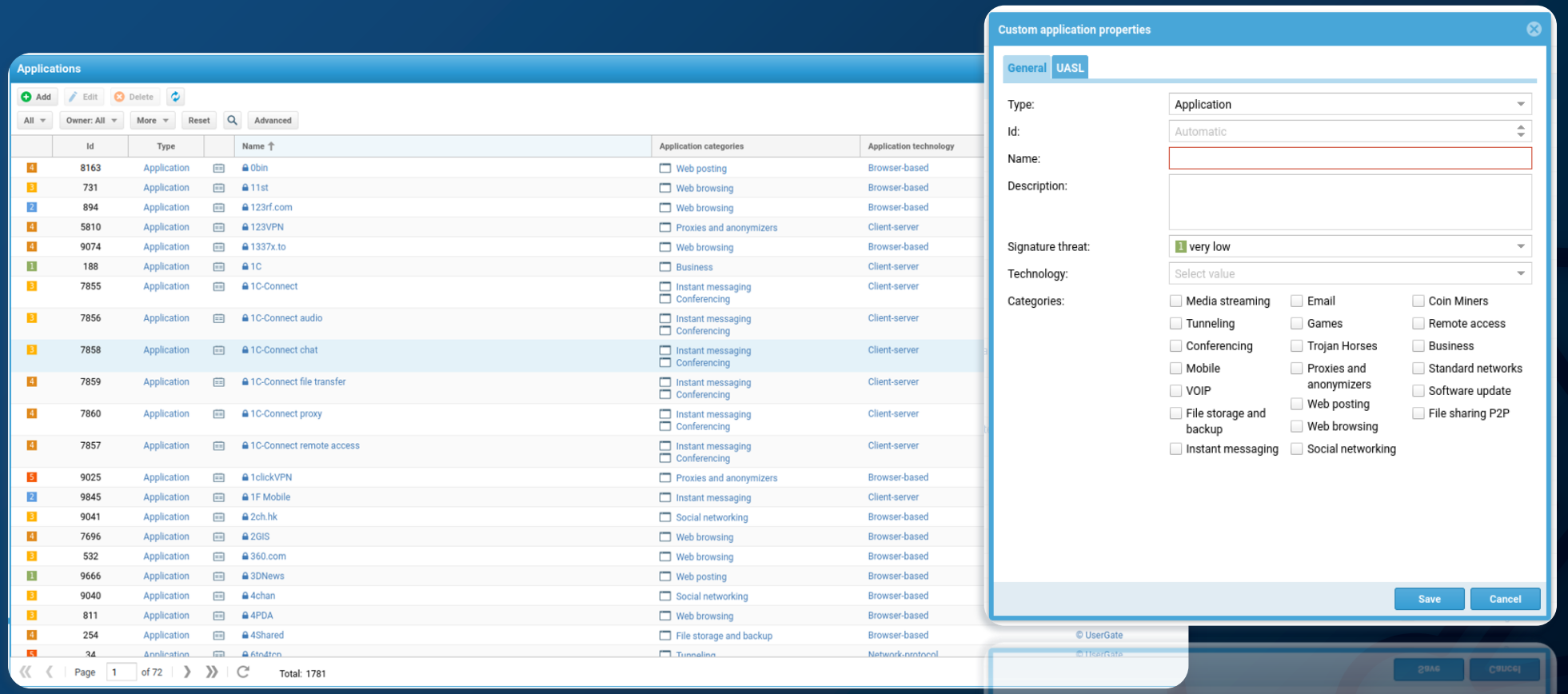
GUI. SCADA

UserGate 7.1



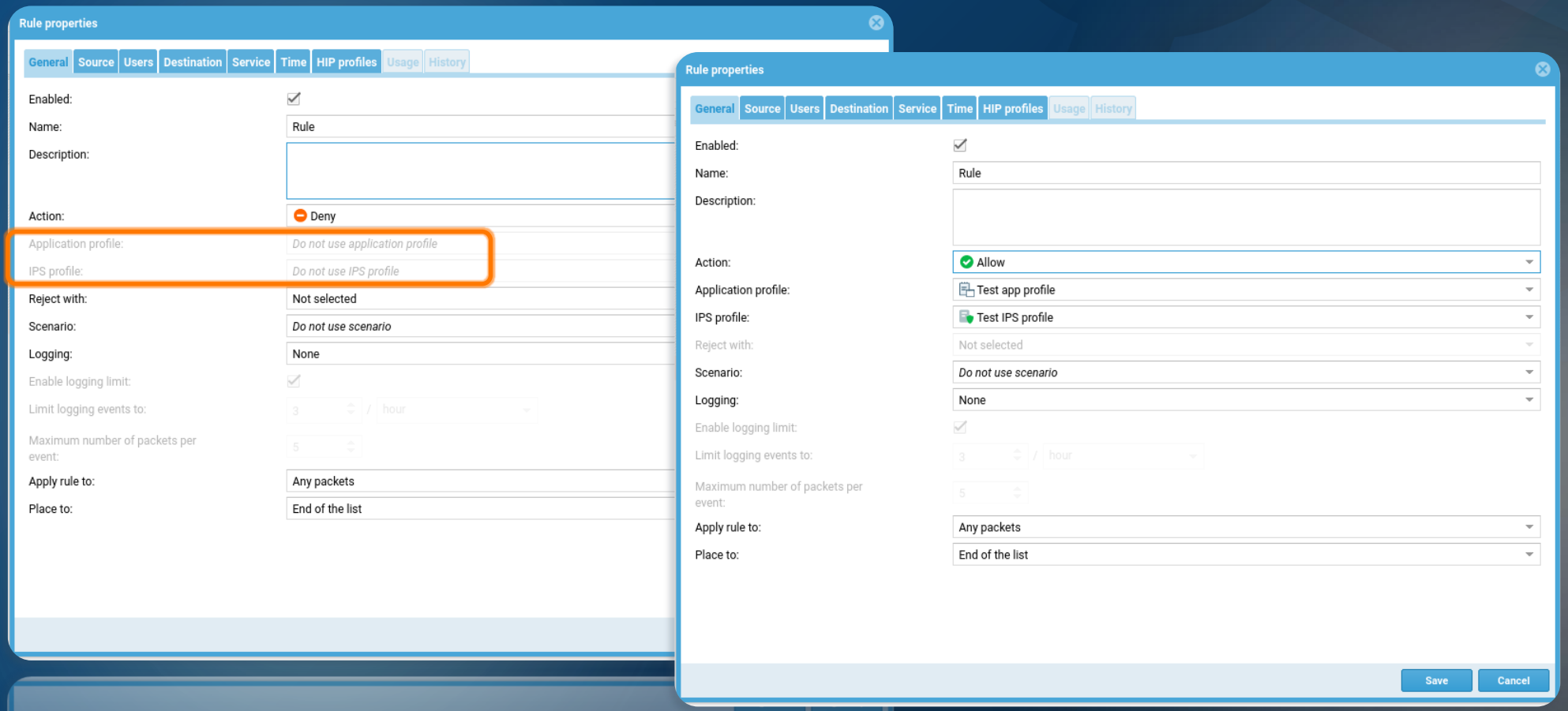
GUI. Сигнатуры L7

UserGate 7.1



GUI. Правила МЭ

UserGate 7.1



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)

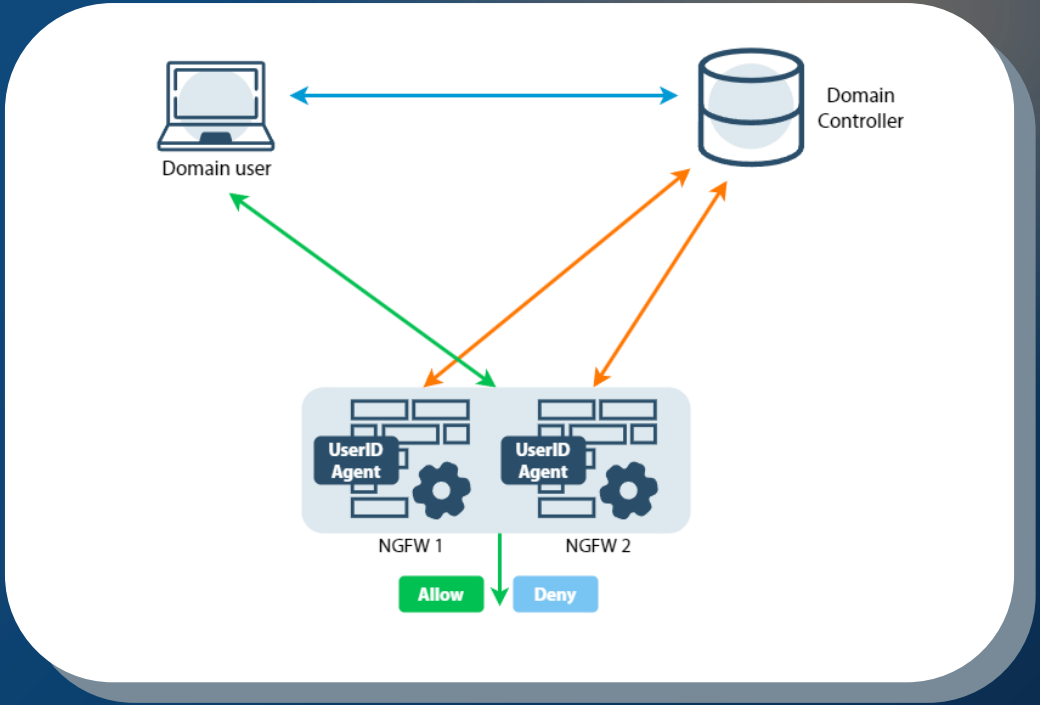
UserGate 7.1

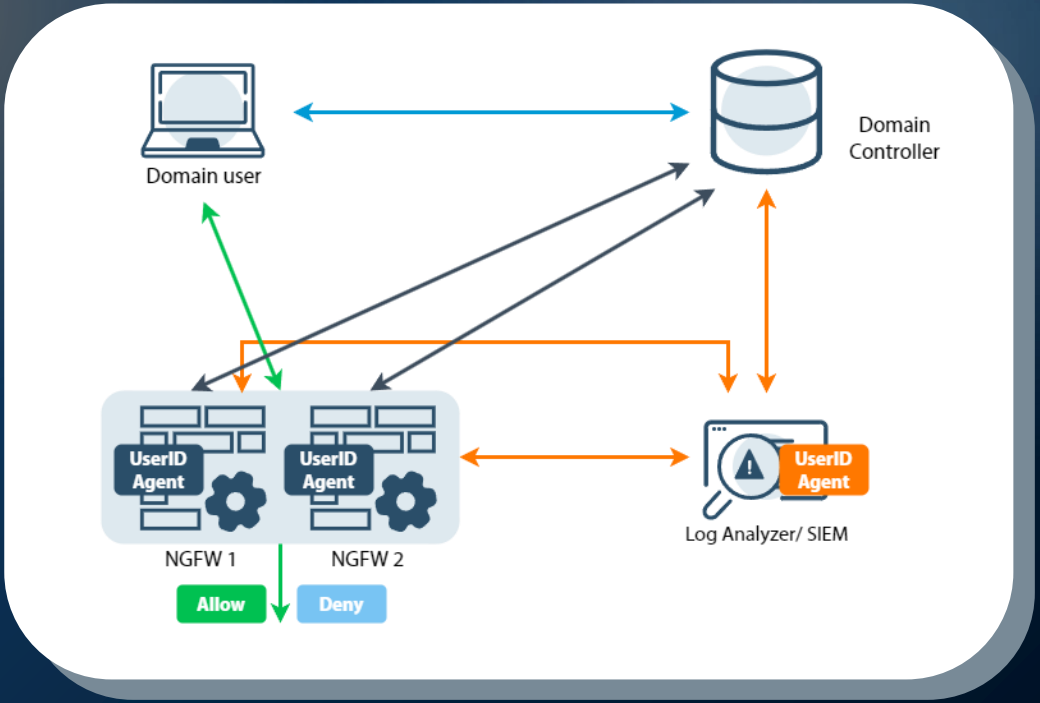
UserID. Возможности

- 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

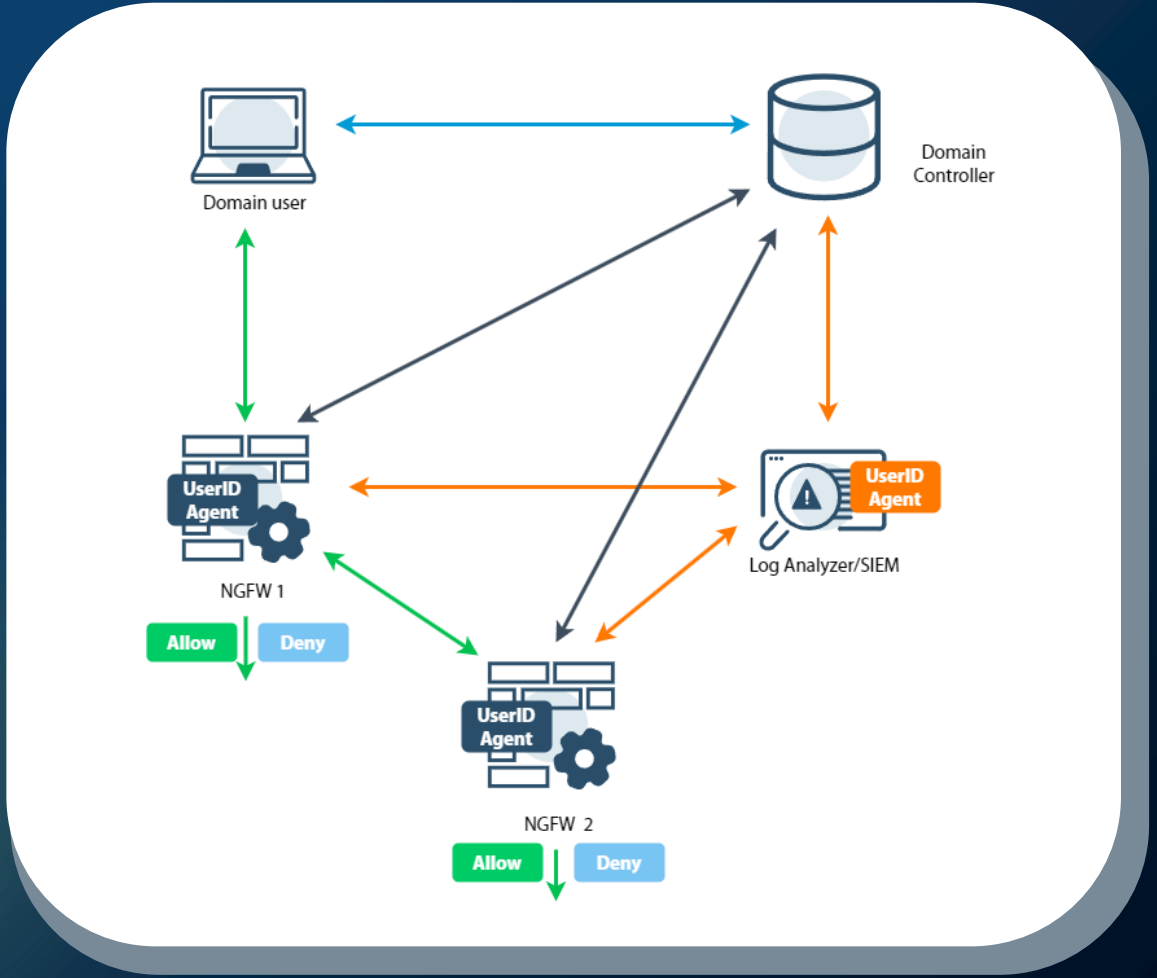
Вариант исполнения: Cluster NGFW



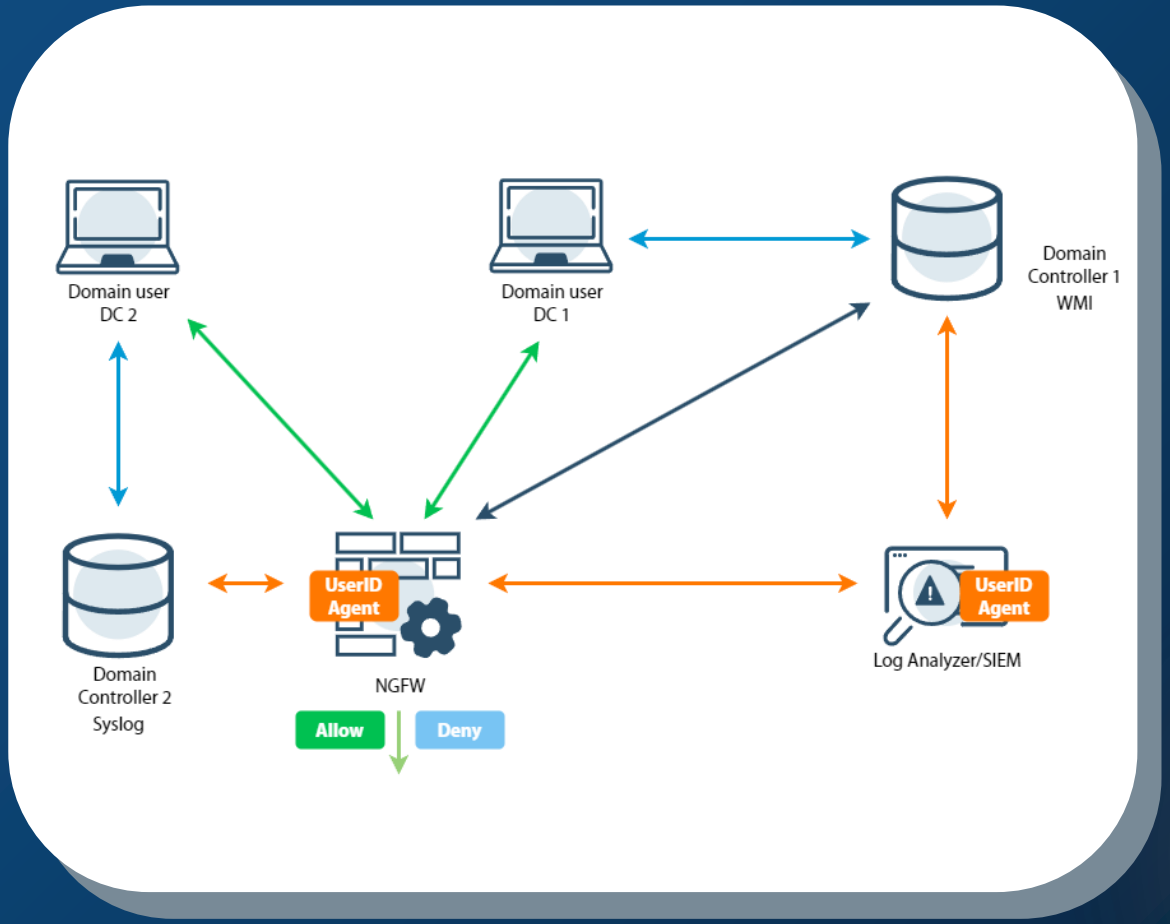


UserGate
7.1

Вариант исполнения: NGFW + LogAn/ SIEM Дистрибуция



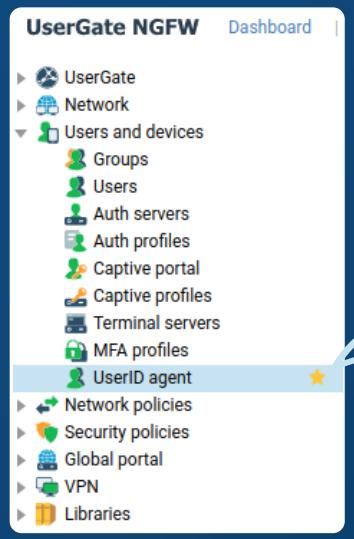
UserGate
7.1

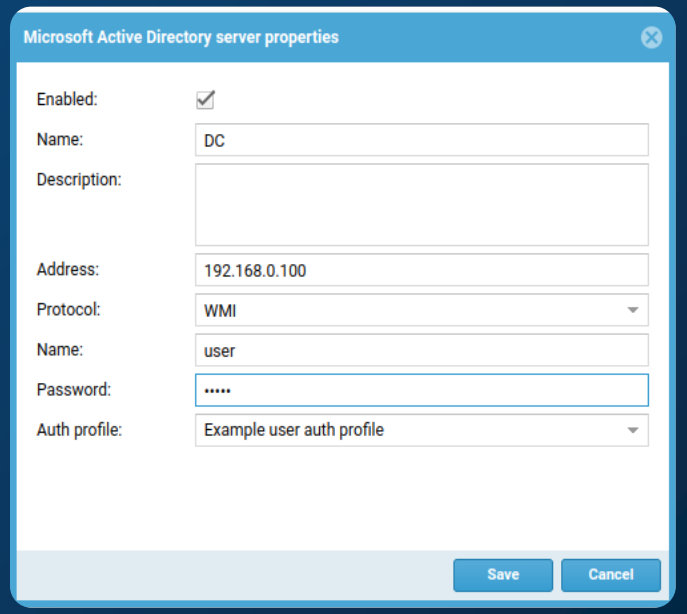


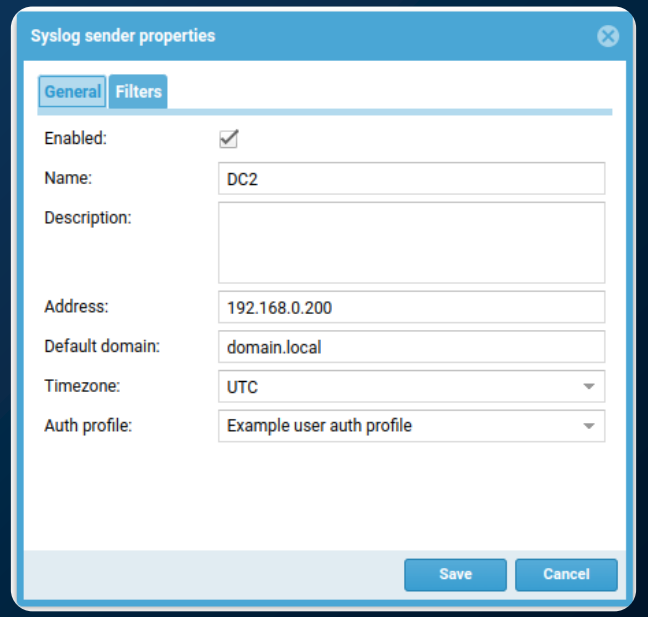
Вариант исполнения: NGFW + LogAn/SIEM с активными агентами

UserGate
7.1

GUI. Добавление агента

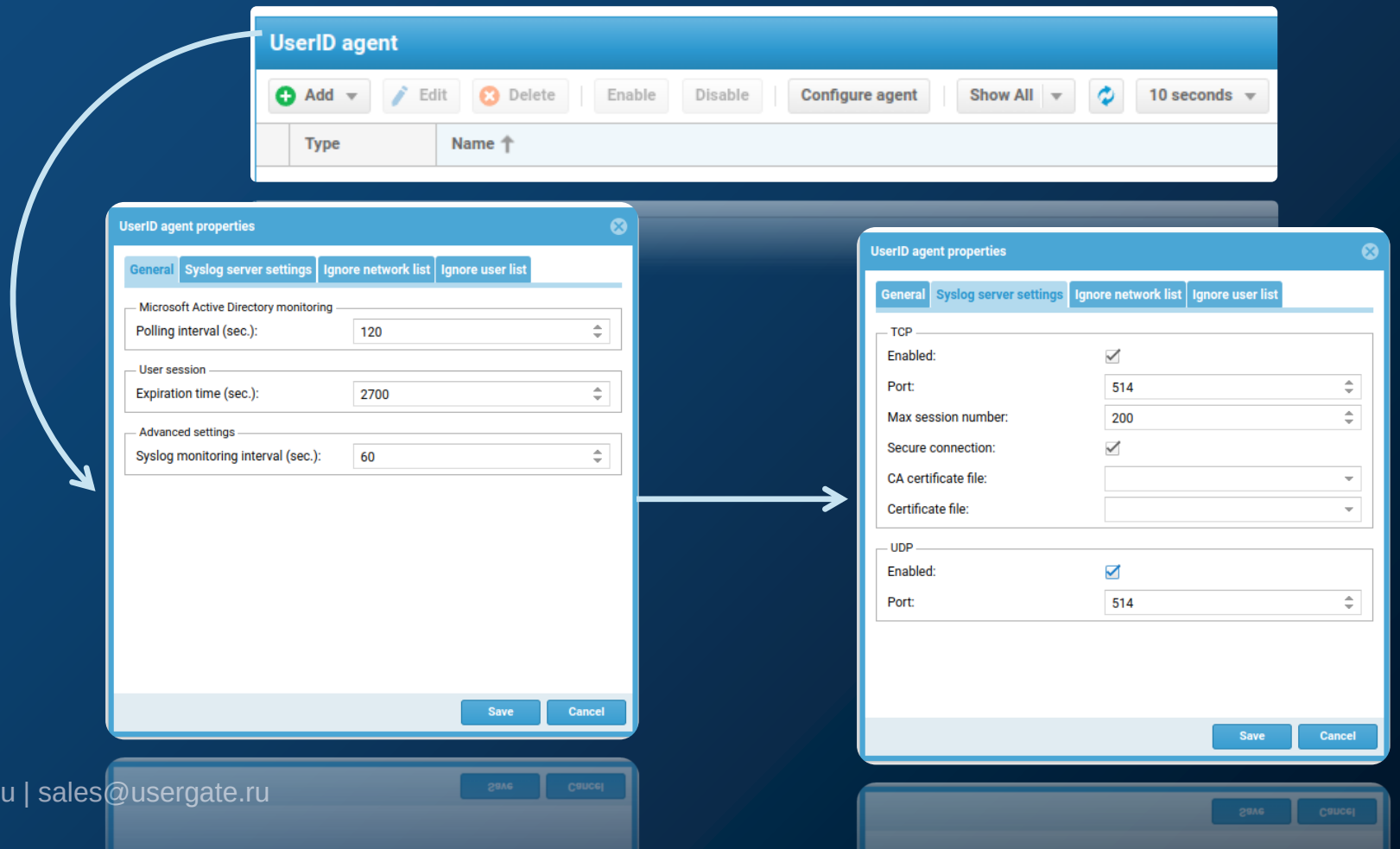






UserGate 7.1

GUI. Конфигурирование агента

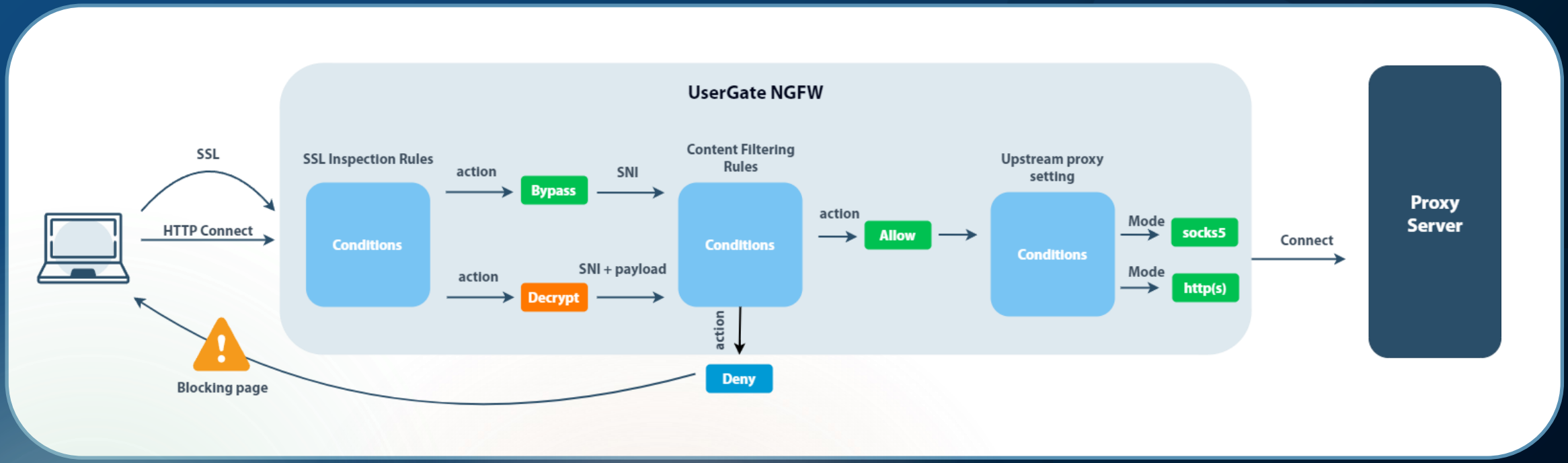


UserGate
7.1

Upstream Proxy

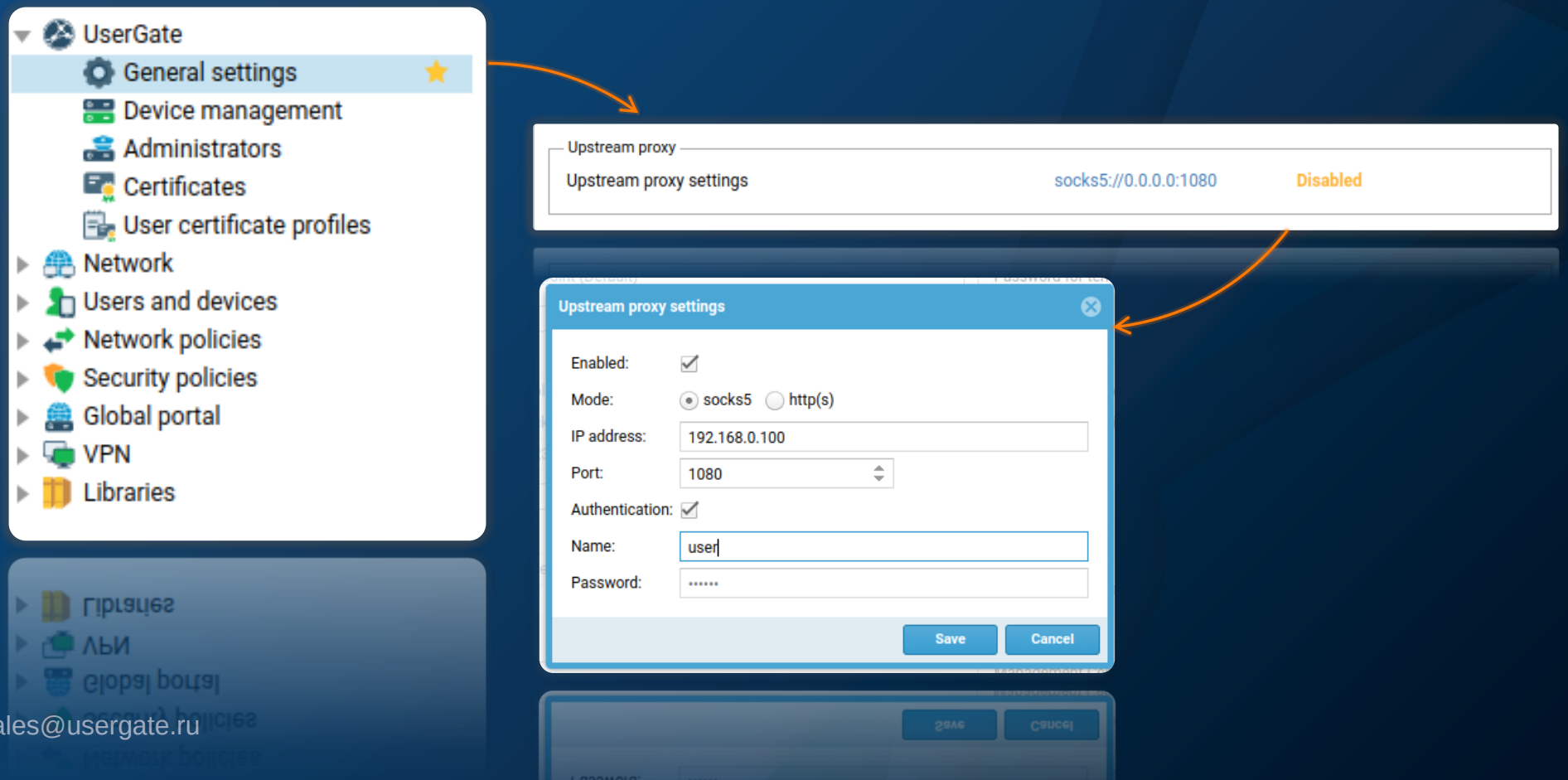
UserGate 7.1

Upstream Proxy flow



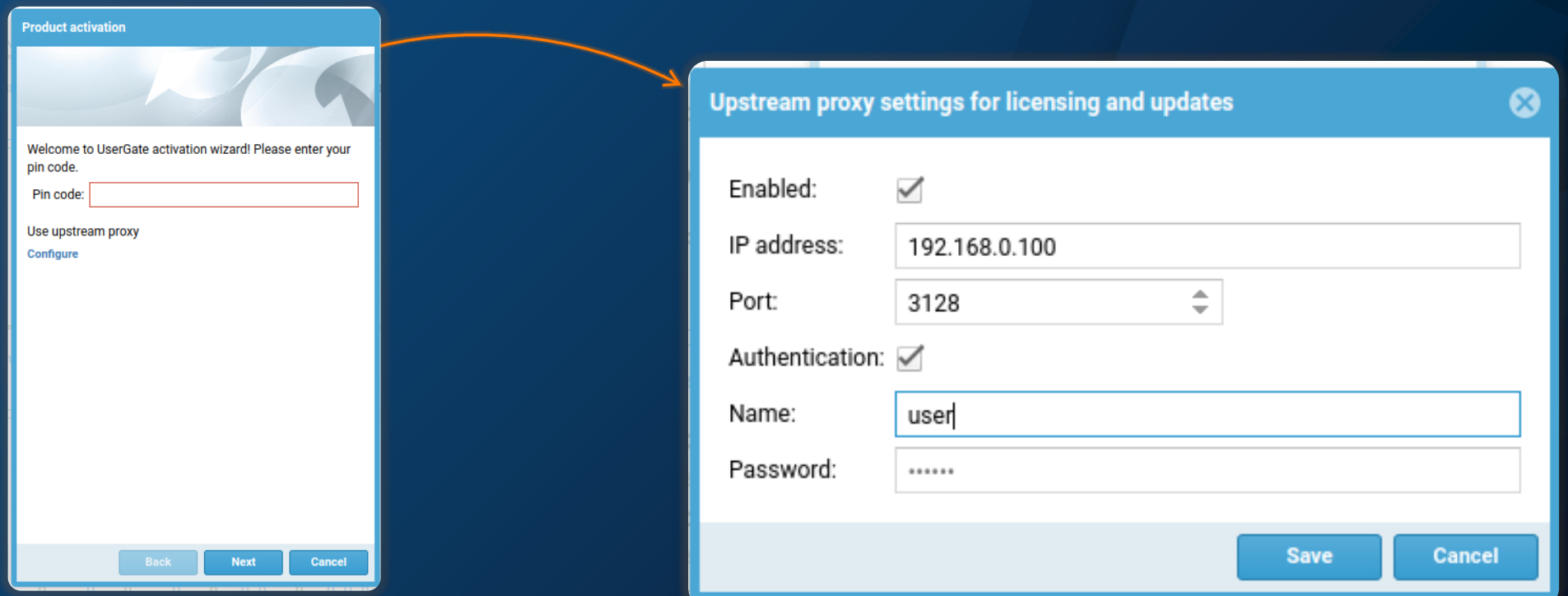
GUI. Настройка. Пользовательский трафик

UserGate 7.1



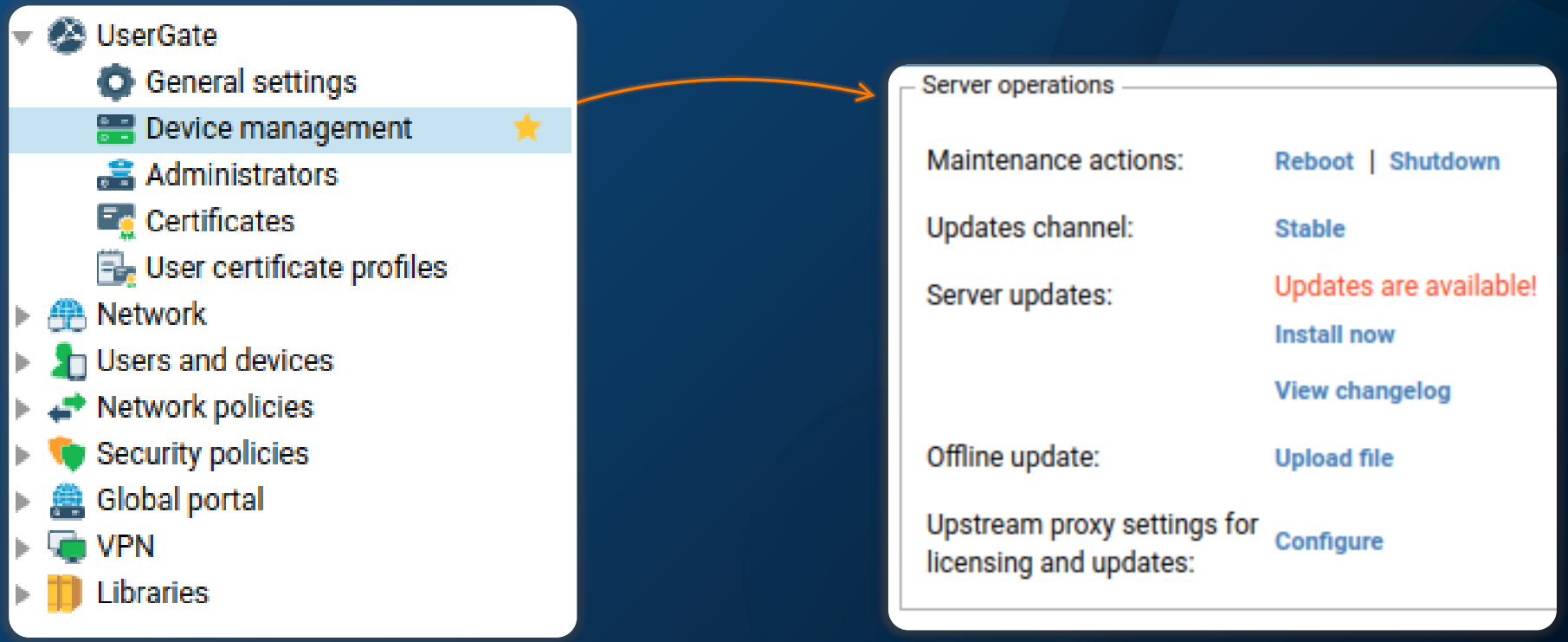
GUI. Настройка. Лицензия и обновления

UserGate 7.1



GUI. Реконфигурация
Лицензия и обновления

UserGate 7.1



UserGate 7.1

Endpoint Client

UserGate 7.1

Client – агент SUMMA

Режимы работы UserGate Client

VPN

HIP, проверка состояния

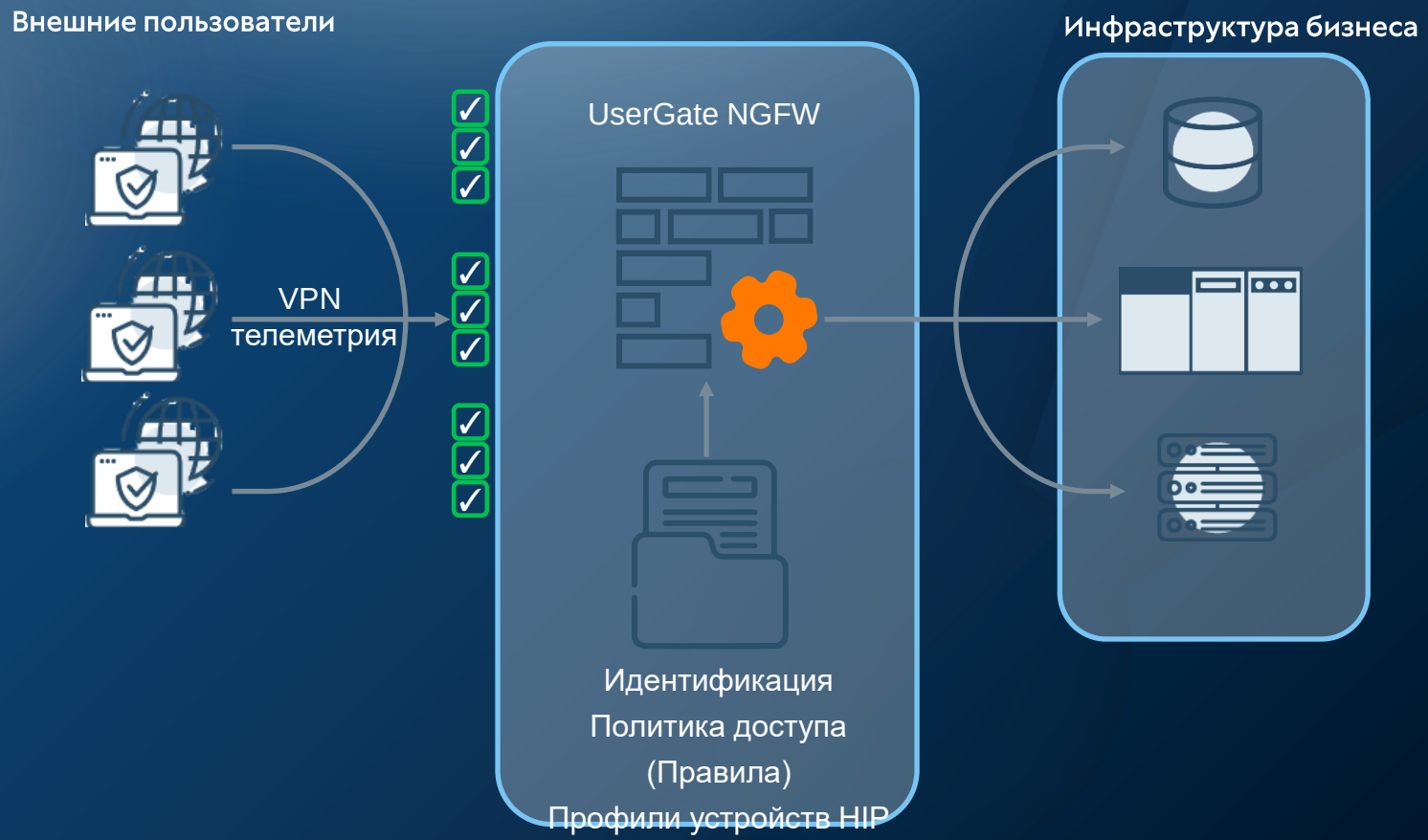
Управление

Мониторинг событий

Аналитика и реагирование

UserGate 7.1

Режим NGFW



UserGate 7.1

Режим МС

UserGate Client –

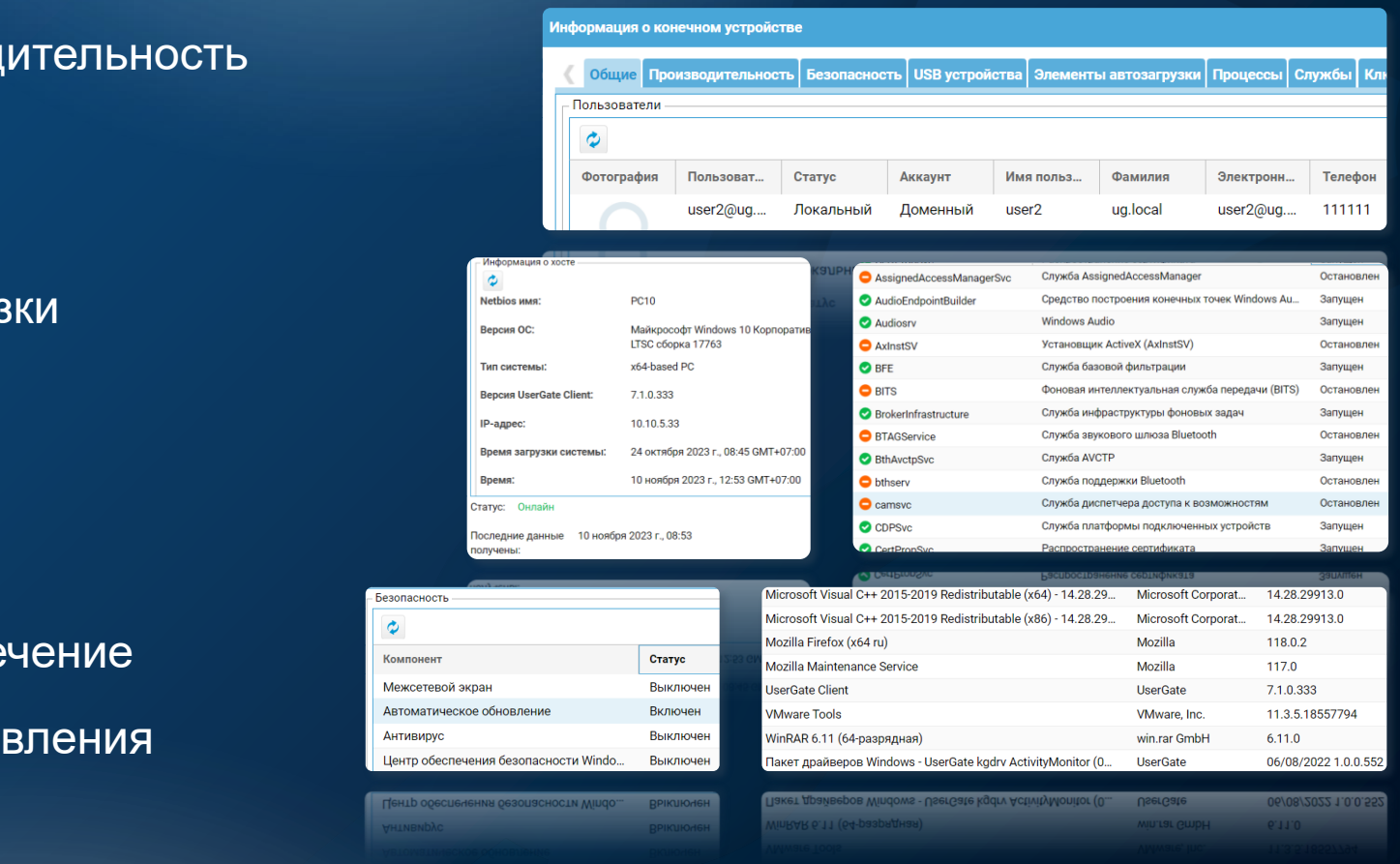
UserGate 7.1

Функции		UG client (MC режим)	UG client (NGFW режим)	Сторонние VPN клиенты (Win, Android, etc.)
VPN		**Endpoint лицензия MC Лицензия пользователя в NGFW**	**Лицензия пользователя NGFW**	**Лицензия пользователя NGFW**
IKEv1	Аутентификация L2TP	✓	✓	✓
IKEv2	Аутентификация по сертификатам	✓	✓	✓
	Аутентификация EAP MS-CHAPv2	✓	✓	✓
	MFA	✓	✓	
	Split-tunneling	✓	✓	
HIP		**Endpoint лицензия MC NAC подписка MC**	**Лицензия пользователя NGFW NAC подписка NGFW**	
	Блокировка на клиенте	✓		
	Блокировка на NGFW		✓	
	Поддержка работы из-за NAT	✓		
Локальный FW на клиенте		**Endpoint лицензия MC**		
Мониторинг логов клиента		**Sensor лицензия Logan**		
Аналитика и реагирование		**SIEM лицензия Logan**		
Пред-настроенные правила аналитики		**Подписка на экспертизу SIEM**		

UserGate 7.1

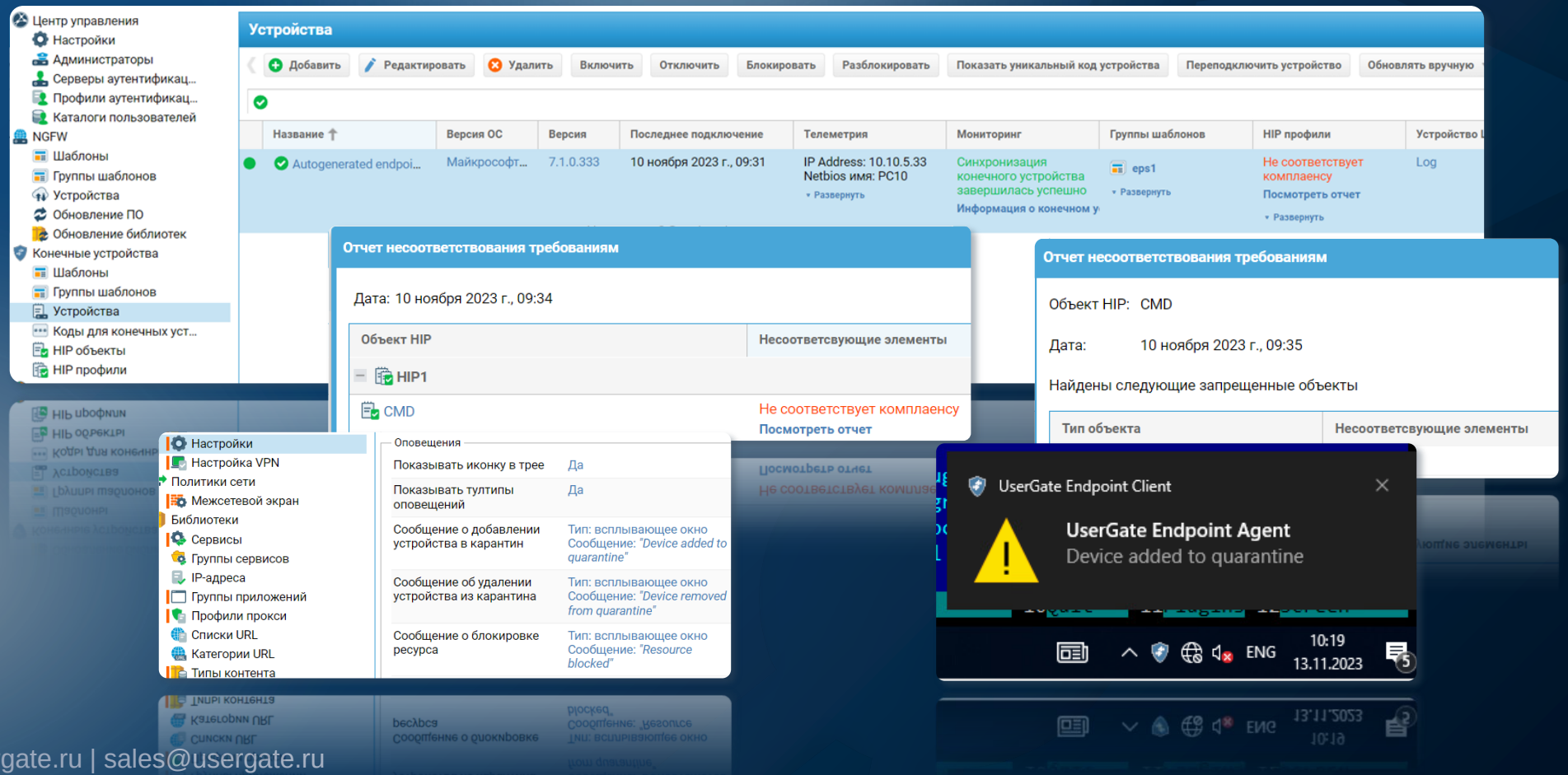
HIP - сбор информации с устройства

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



UserGate 7.1

HIP - нотификация



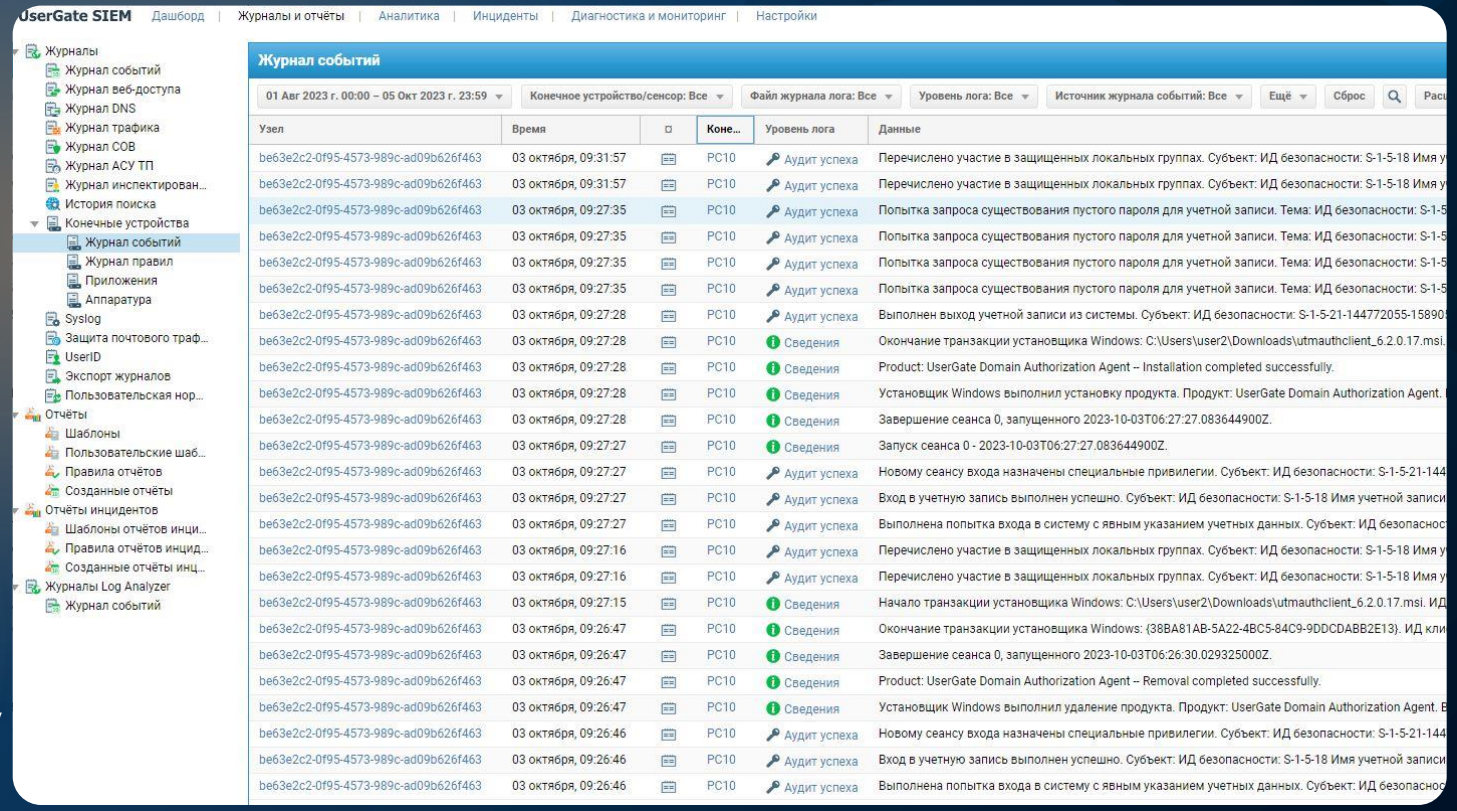
UserGate 7.1

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, важности, типу события и т.п.

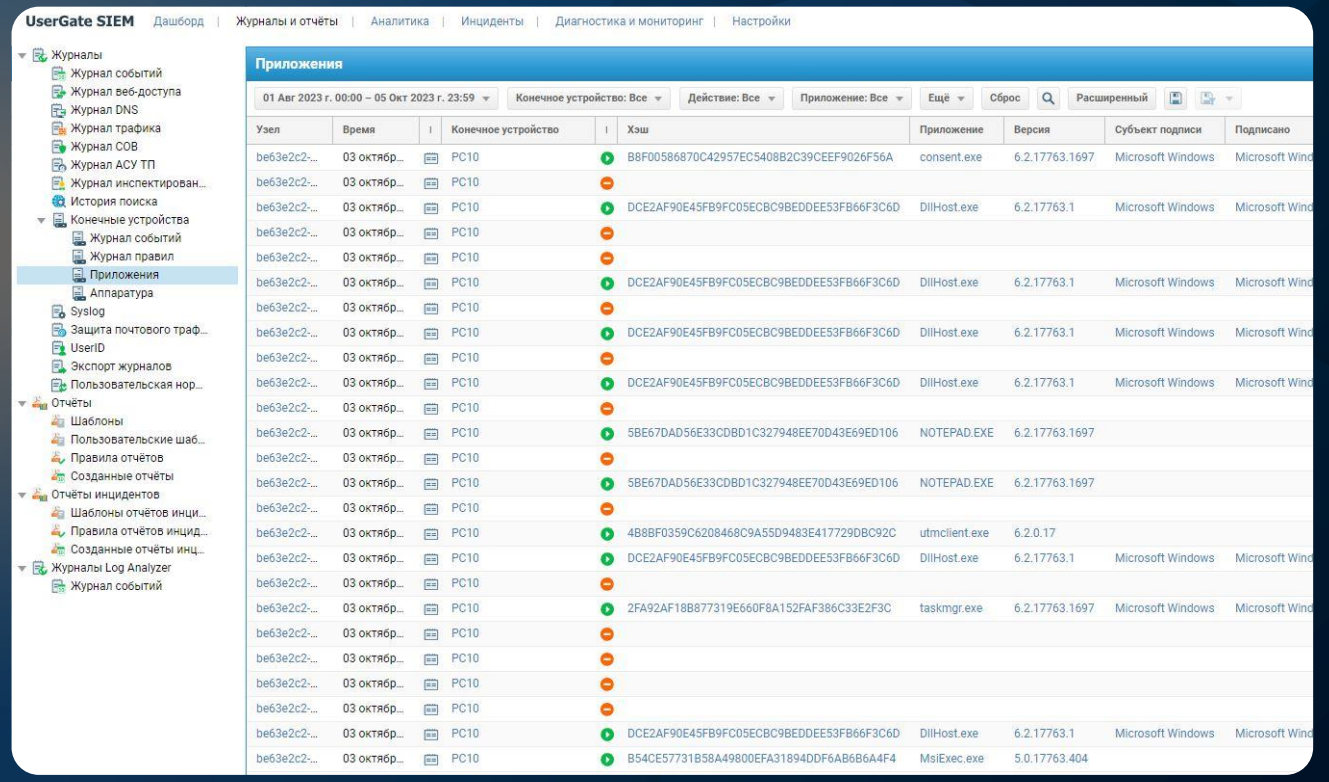


UserGate 7.1

Мониторинг событий

Приложения конечных устройств:

Отображает приложения, которые запускались на конечных устройствах

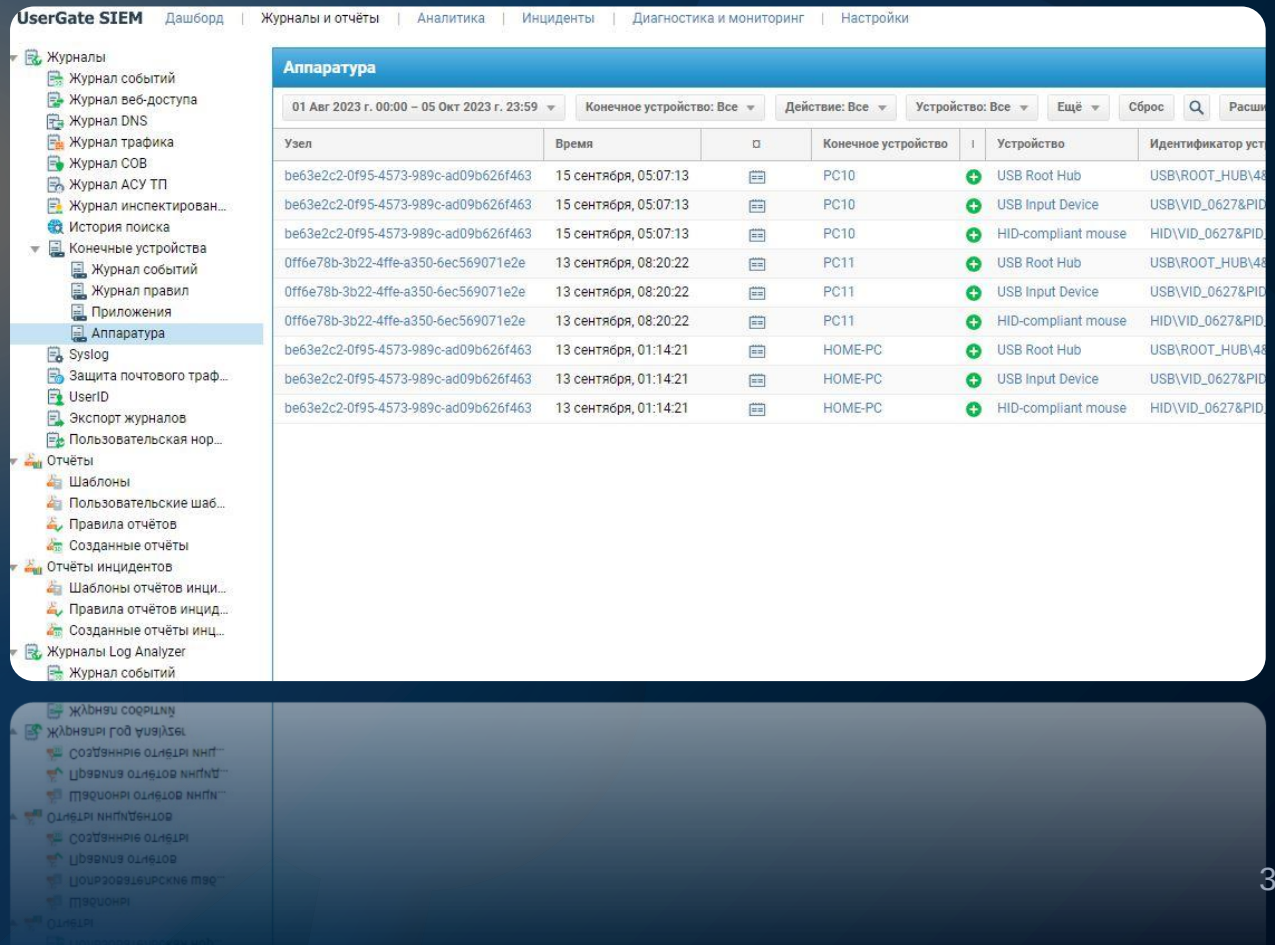


UserGate 7.1

Мониторинг событий

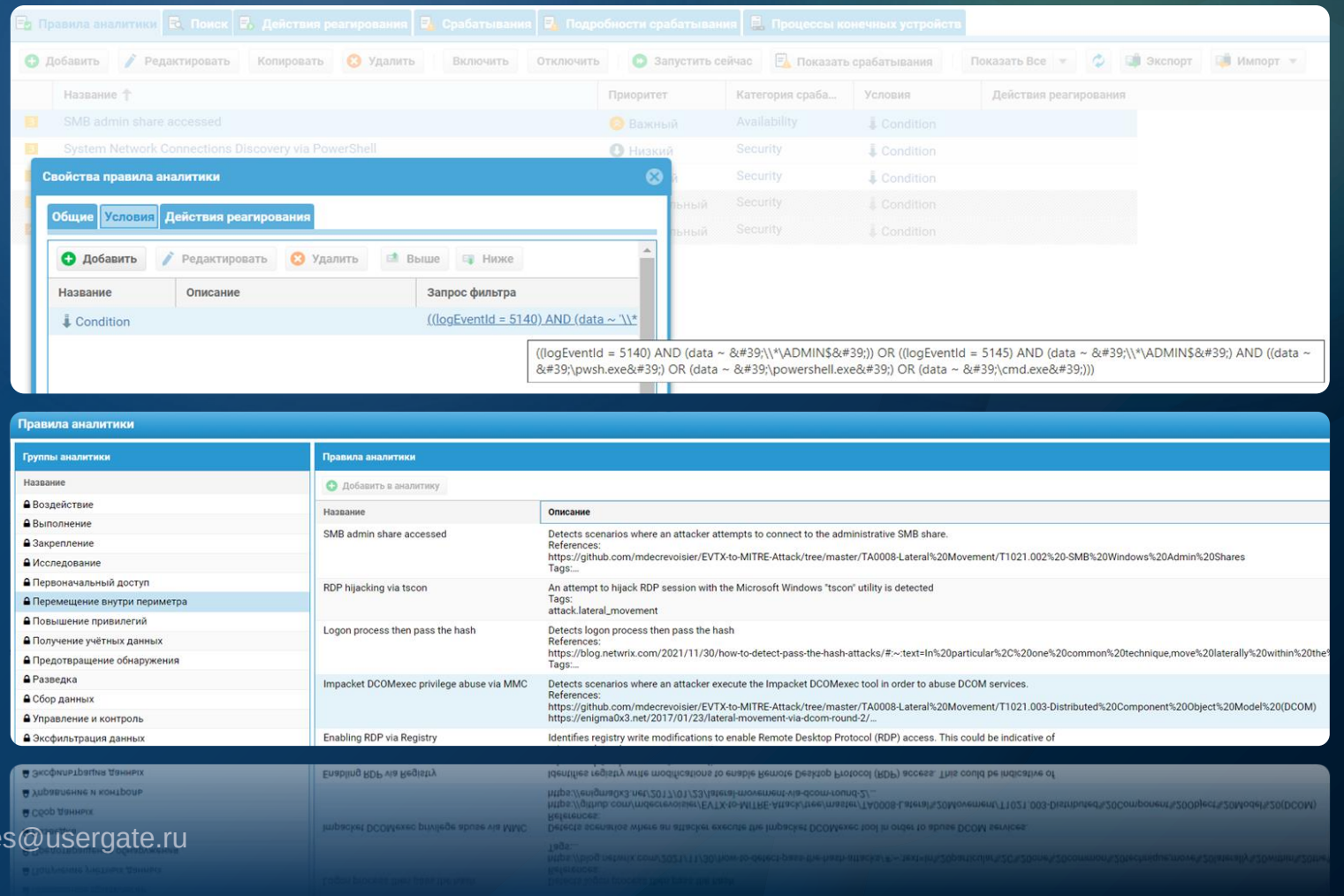
Аппаратура конечных устройств:

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



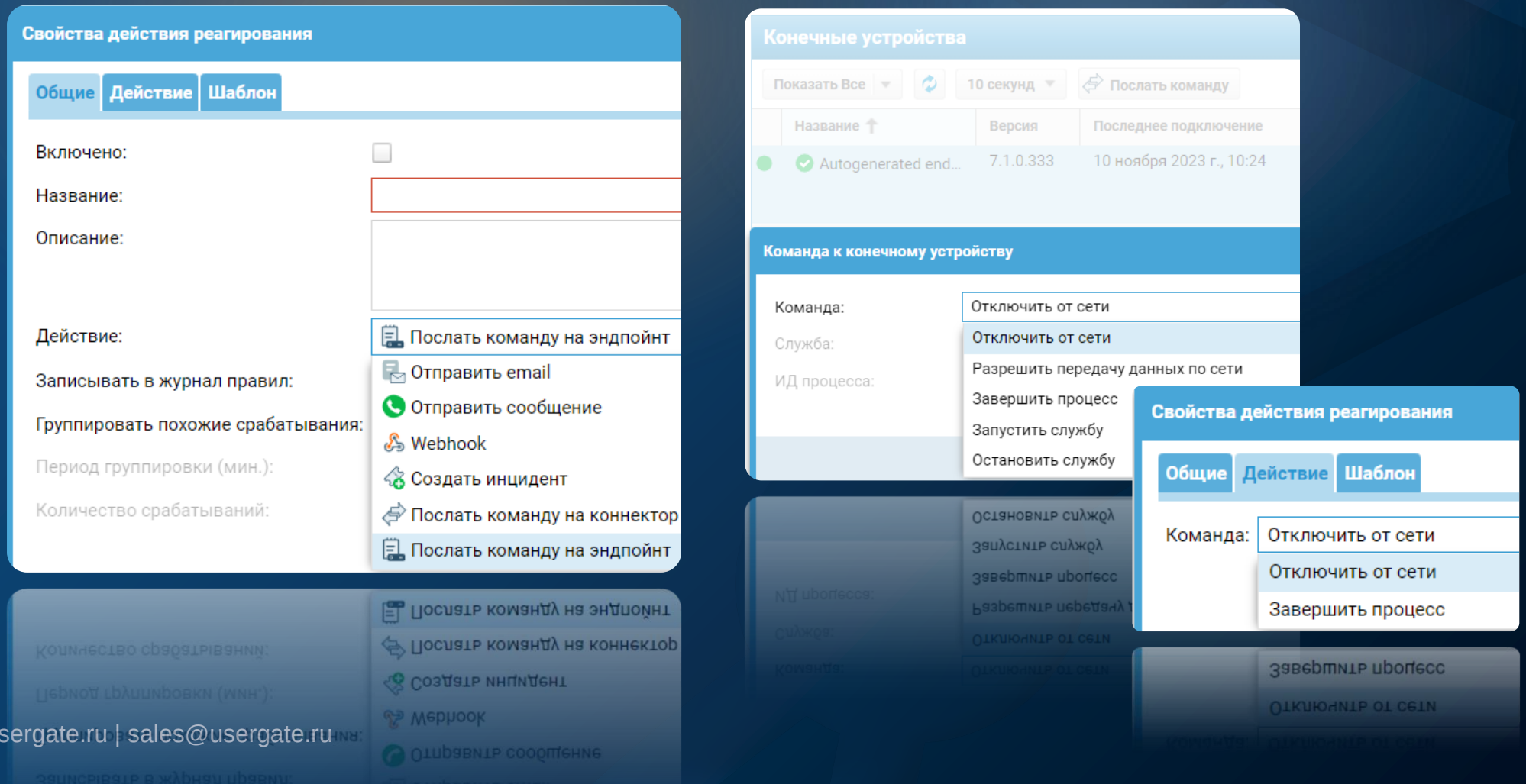
UserGate 7.1

Аналитика



UserGate 7.1

Реагирование



UserGate

7.1

Q&A?!

Игорь Шефер
Ведущий инженер UserGate