UserGate

Экосистема UserGate

8 800 500 4032
sales@usergate.ru

Содержание

Важные даты UserGate

2001 — запуск первой версии UserGate Proxy

2009 — начало разработки первого российского NGFW UserGate

2010 — создан внутренний стартап, в рамках которого началась разработка новой платформы

2012 — UserGate – резидент Академпарка в Новосибирске

2015 — UserGate – резидент Сколково

2016 — выпуск нового UserGate как решения класса UTM

Сертификация новой платформы по требованиям ФСТЭК России

2018 — создание экспертной лаборатории и начало разработки собственных аппаратных платформ

2019 — открытие первого московского офиса UserGate

2020 — открытие офиса UserGate в Хабаровске

2020 — начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

2021 — выход на рынок экосистемы безопасности UserGate SUMMA

2022 — открытие офиса в Санкт-Петербурге

2023 — релиз UG OS 7.0

Наш офис разработки находится в Технопарке Новосибирского Академгородка,
в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

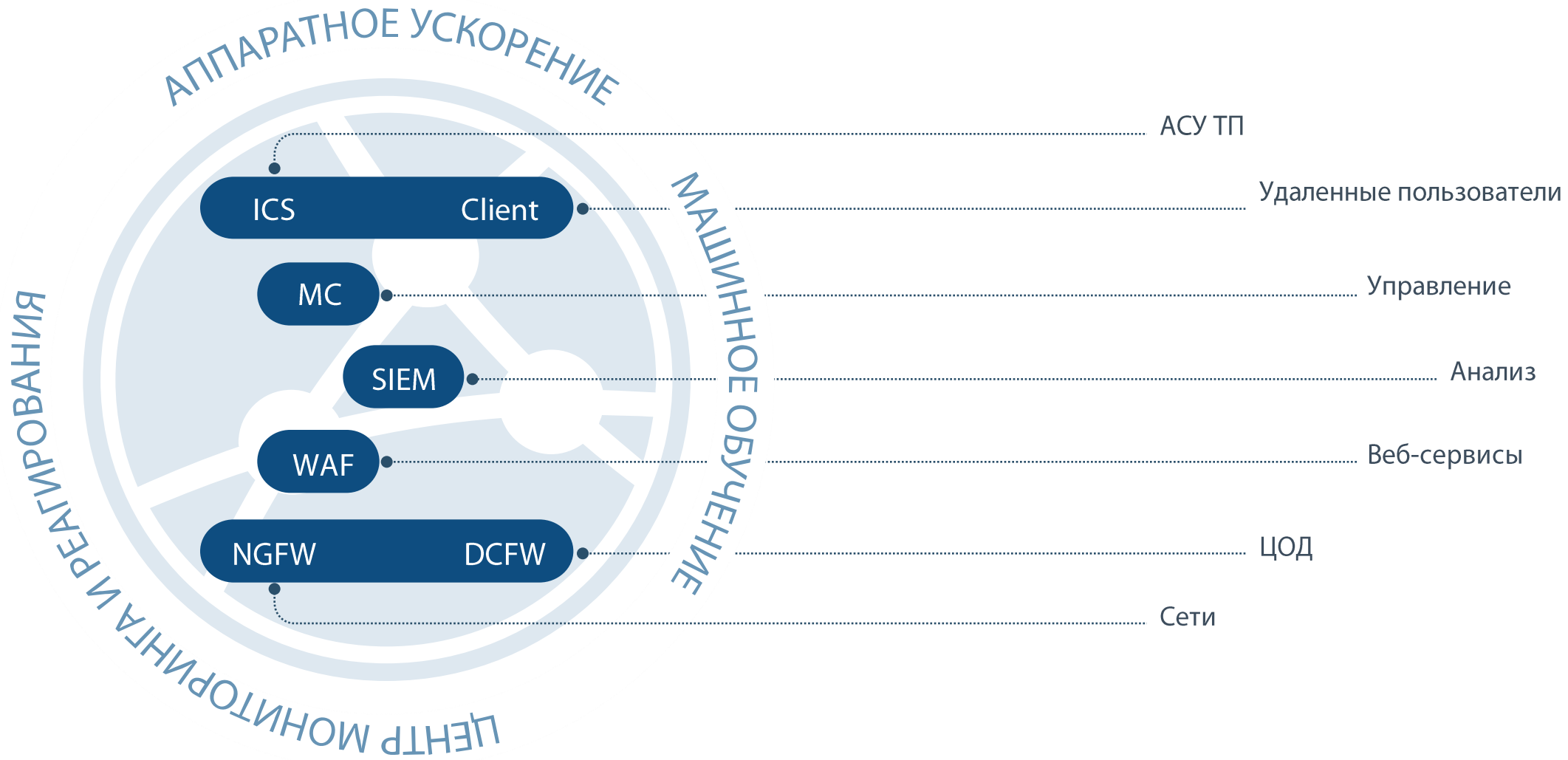
Фронт-офис
в г. Москве расположен
в БЦ «ФилиГрад»

Новый офис разработки
и сопровождения продаж
в «Санкт-Петербург Плаза»

Еще один офис продаж
и технического
сопровождения расположен
в Хабаровске

UserGate SUMMA

100% видимость событий безопасности



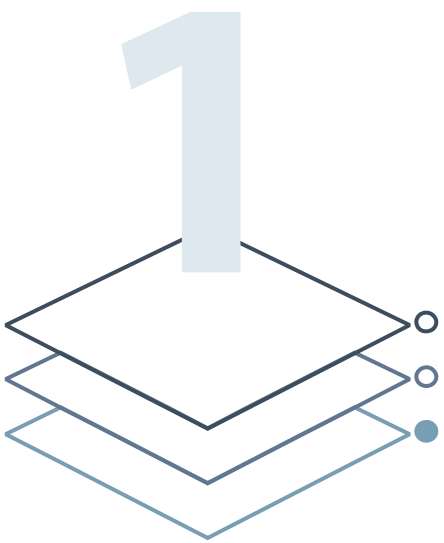
UserGate NGFW

Межсетевой экран следующего поколения

13 лет разработки

1 уровень

«Для тех, кто вообще ничего не умеет»

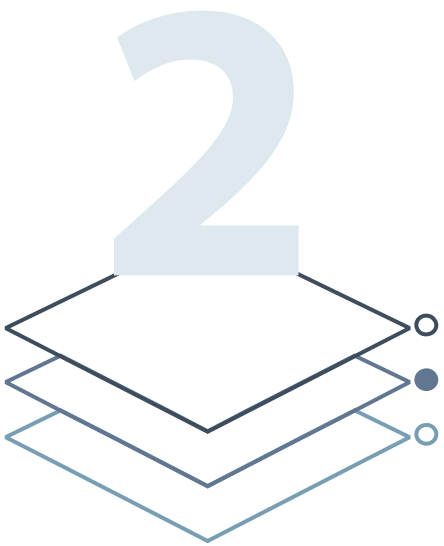


Готовые продукты:

- pfSense
- OPNSense
- M0n0wall
- IPCop
- …

2 уровень

«Для тех, кто сам научился собирать образы»

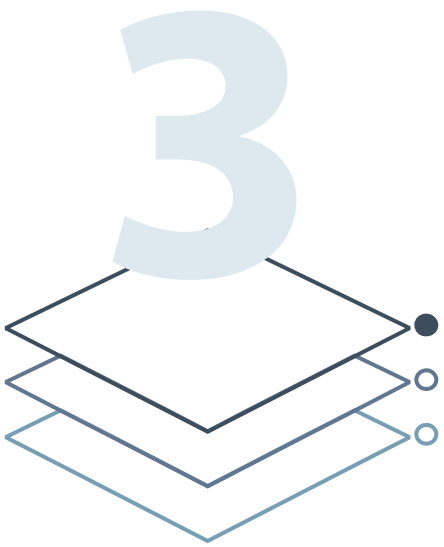


Готовые продукты:

- Suricata
- Snort
- nDPI
- Squid
- OpenVPN
- OpenSSL
- …

3 уровень

«Для профессионалов»

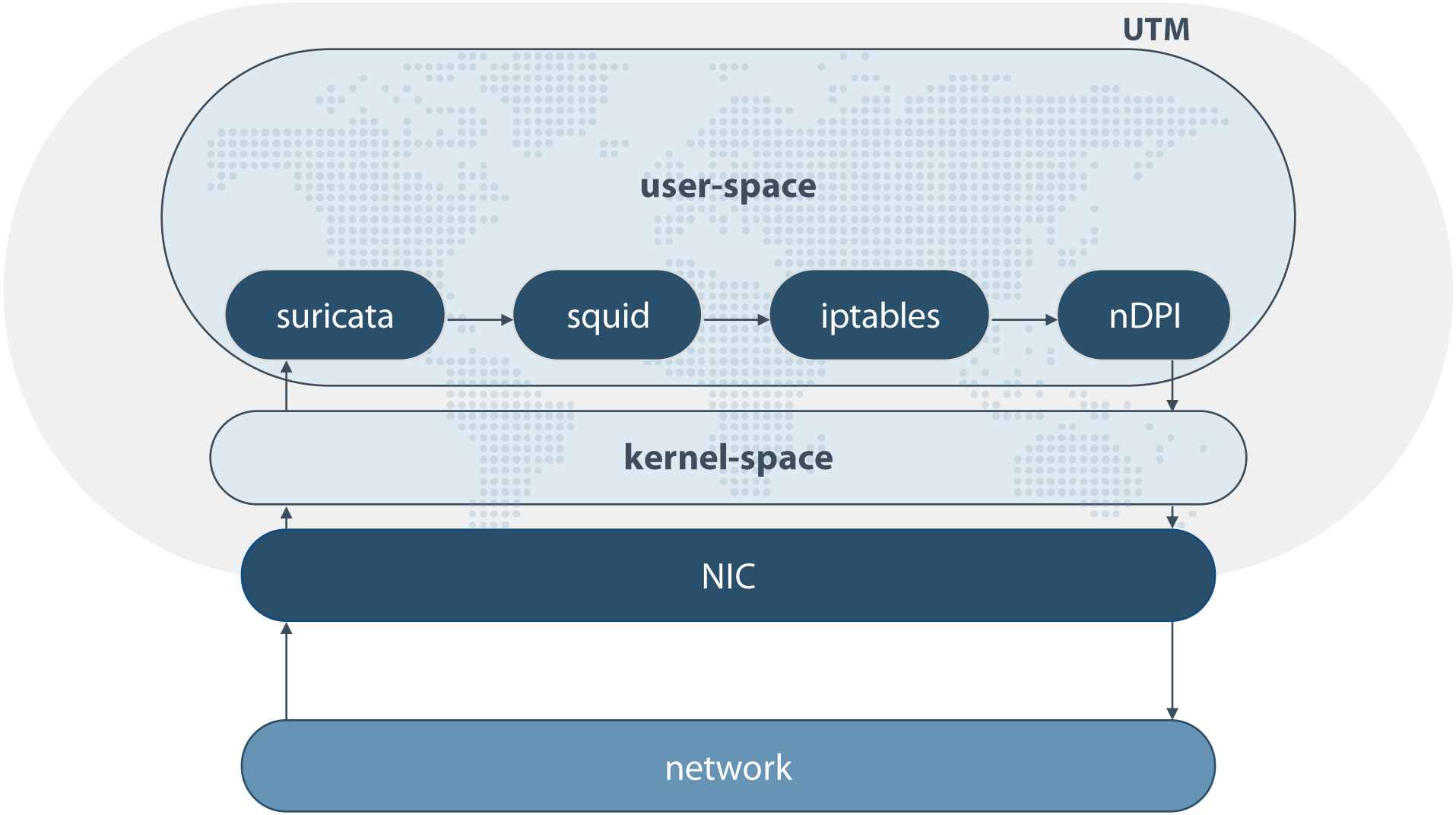


Низкоуровневые библиотеки:

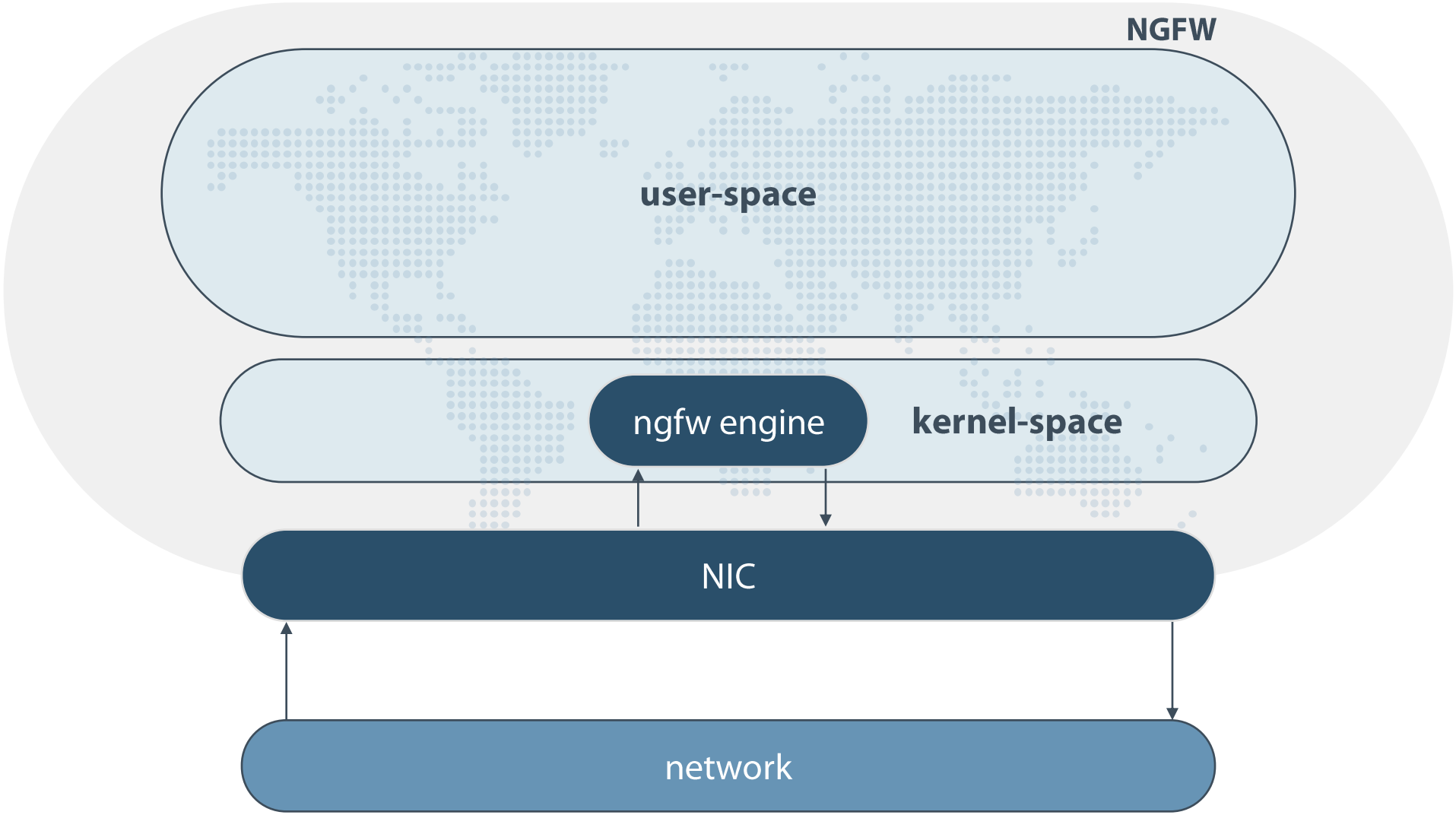
- Curl
- Python
- Apache
- Bash
- telnet-server
- их сотни

NGFW vs UTM

UTM


UTM
user-space
suricata
squid
iptables
nDPI
kernel-space
NIC
network

NGFW



	Чужие платформы	Свои платформы
Проприетарное ПО		
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО		CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	CHECK POINT	CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	CHECK POINT	CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

	Чужие платформы	Свои платформы
Проприетарное ПО	UserGate CHECK POINT	UserGate CISCO HUAWEI paloalto NETWORKS FORTINET
Open-source		

Выбор правильного пути развития вендора

Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

CHECK POINT

UserGate

CISCO

HUAWEI

paloalto NETWORKS

FORTINET

	Чужие платформы	Свои платформы
Проприетарное ПО	CHECK POINT	UserGate, CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

NGFW


PORT 80
PORT 443
SSL
kaspersky
Gmail
by Google
Yandex
Viber
Яндекс.Диск
zoom
eset
@mail.ru
Microsoft
OfficeUpdate
ssh
COMMUNICATIONS SECURITY
AMMYY
JUST DO IT REMOTELY
SSL

Преимущества UserGate NGFW

- высокая скорость обработки трафика;
- идентификация пользователей;
- применение гибких политик к пользователям;
- контроль приложений на L7 уровне по всем портам;
- интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и поддержкой TLS ГОСТ;
- инспекция SSH;
- защита от DoS-атак.

Операционная система UGOS

Новое в UGOS 7.0

- CLI;
- система бэкапов;
- SSL Forwarding;
- UserGate Policy Language;
- Cloud-init;
- новая архитектура процессоров – новые платформы;
- новый движок IPS.

CLI

- теперь в CLI можно конфигурировать абсолютно все и даже немного больше, чем в веб-версии;
- добавлены новые инструменты диагностики.

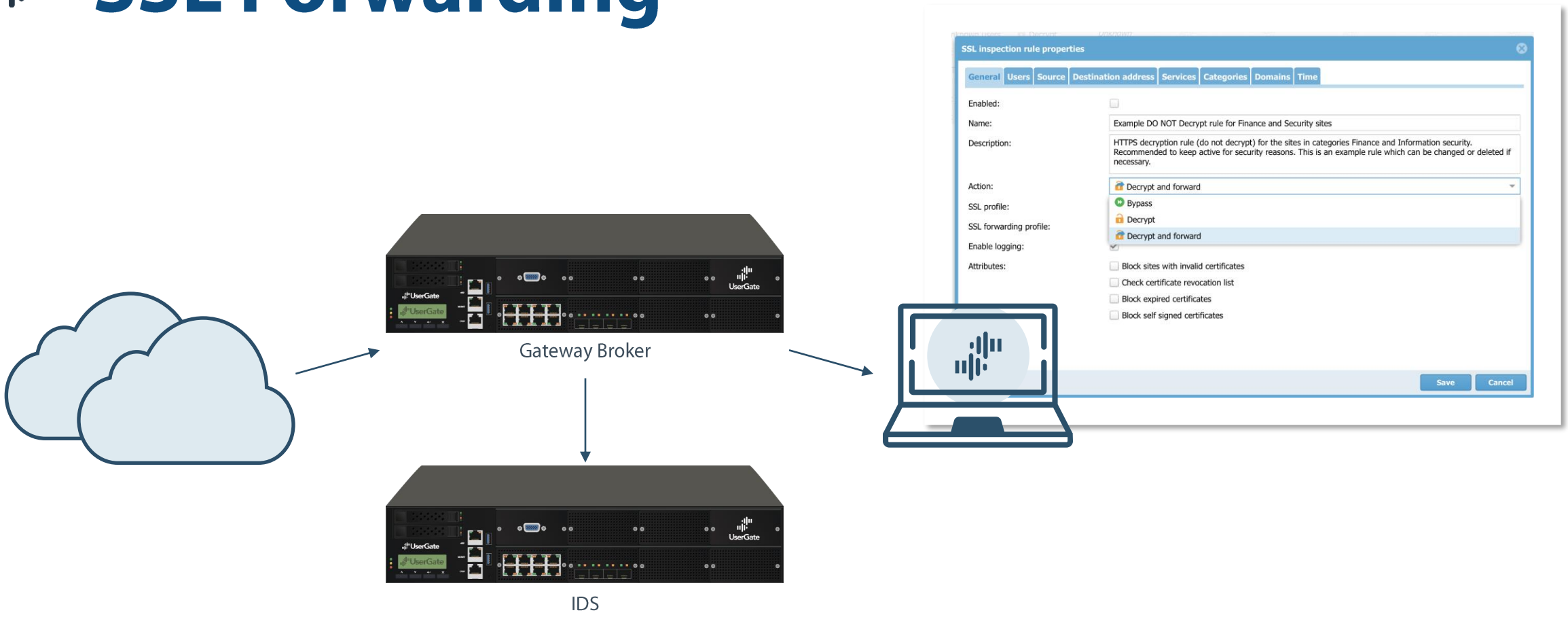
```
Admin@UGOS>

+ traceroute      Print the route packets trace to network host
+ shutdown        Shutdown
+ show            Show
+ clear           Clear
+ ping            Ping
+ reboot          Reboot
+ date            Display date
+ exit            Logout
+ netcheck        Check HTTP/HTTPS connection
+ configure       Configuration mode
+ dig             Query domain name server
```

Система бэкапов

- уменьшен размер образа;
- проведение бэкапов без перезагрузки;
- хранение бэкапов в памяти устройства.

SSL Forwarding



UserGate Policy Language

- Новый синтаксис написания правил безопасности;
- мощный инструмент для создания политик.

```
Admin@UGOS> configure
Admin@UGOS# create

+ security-policy      Security Policy level
+ network              Network level
+ settings             Settings level
+ global-portal        Global Portal level
+ libraries            Libraries level
+ network-policy       Network policies level
+ vpn                  VPN configuration
+ users                Users level

Admin@UGOS# create _
```

Cloud-init

- удобное разворачивание образов в виртуальных средах с параметрами конфигурирования.

Новые платформы

FG

C150

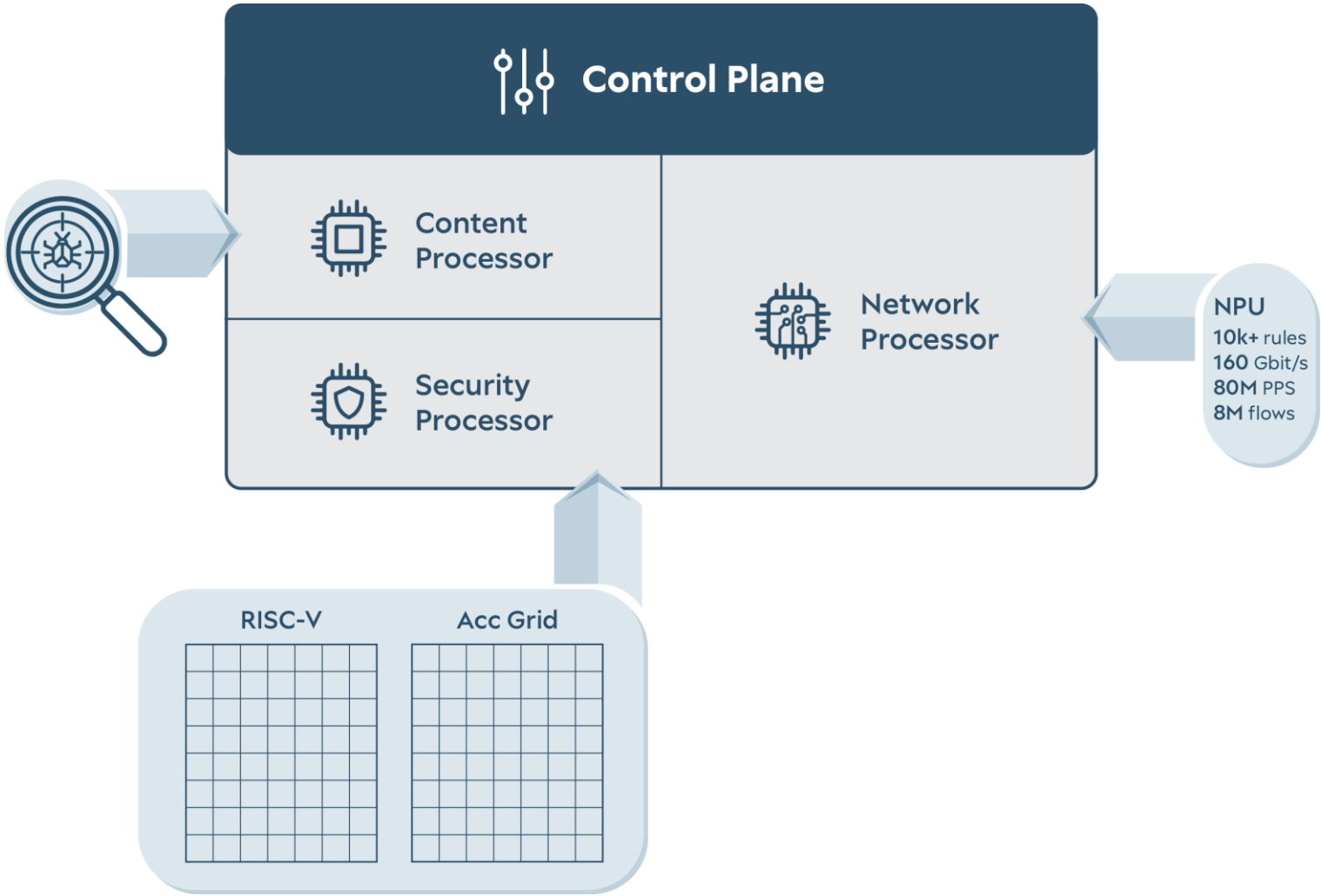
B50

UserGate FG

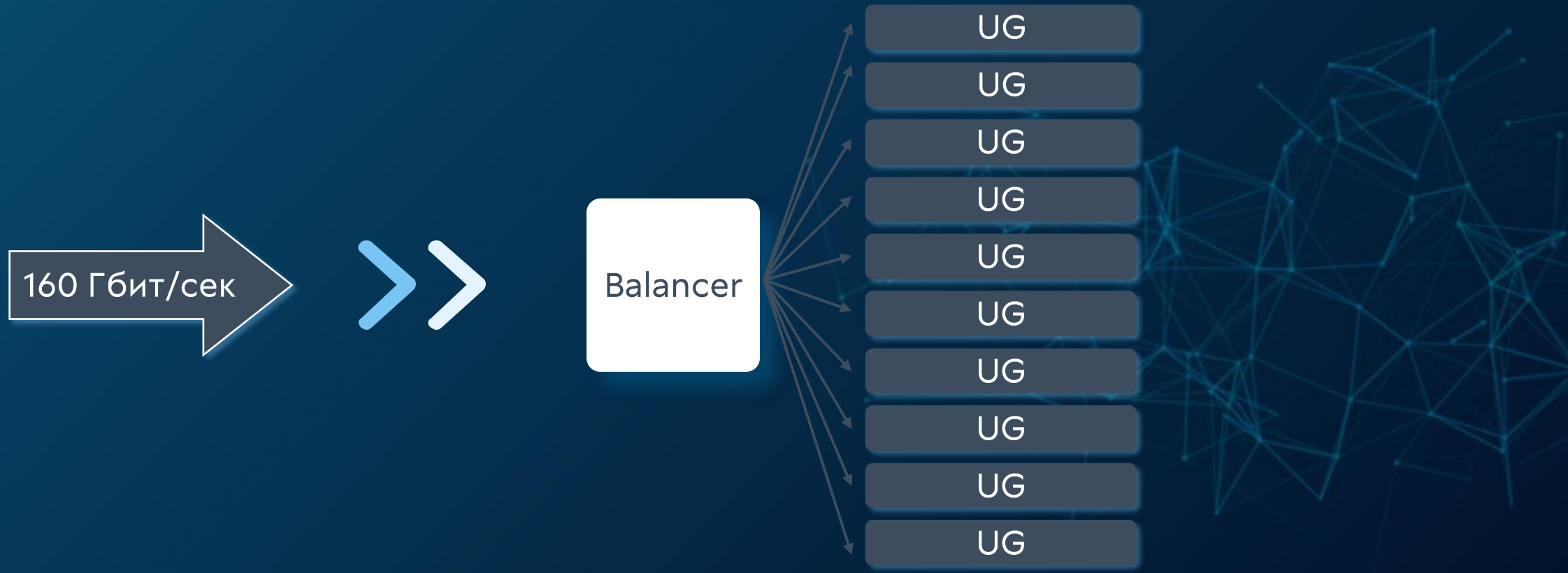
2x100 + 16x10, wirespeed

- CPS - 80 000 сессий в секунду
- CC - 11 000 000 TCP сессий
- UDP 1518 byte - 150+ гбит/с
- EMIX - 65 гбит/с (цифра из ограничения тестового стенда, CPS - 35 000, 10 000 правил)
- 80M PPS

Как это работает



Стекирование

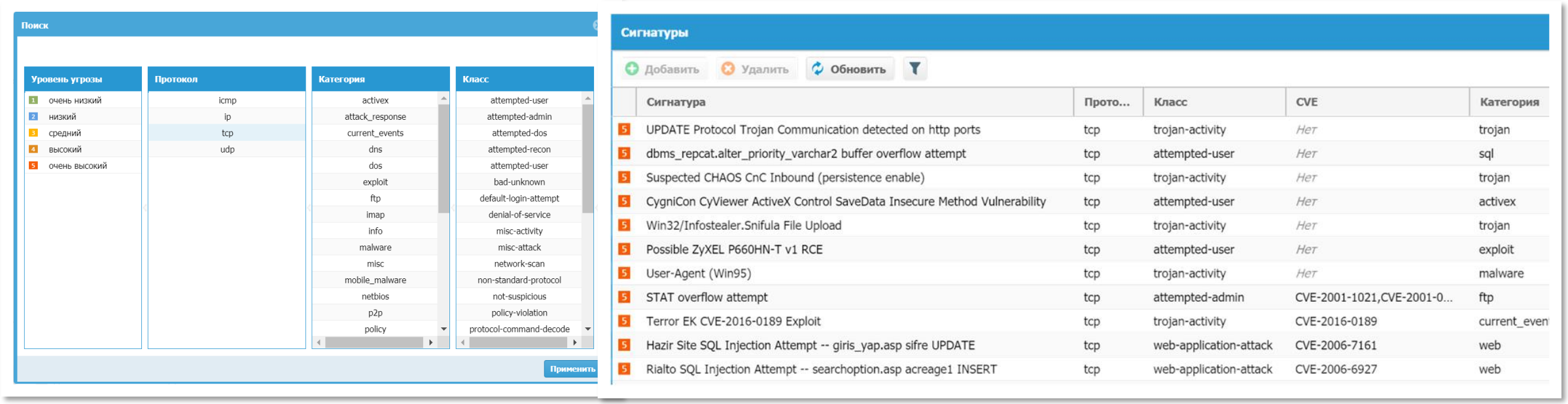

160 Гбит/сек
Balancer
UG
UG
UG
UG
UG
UG
UG
UG
UG
UG

UserGate IDPS (СОВ)

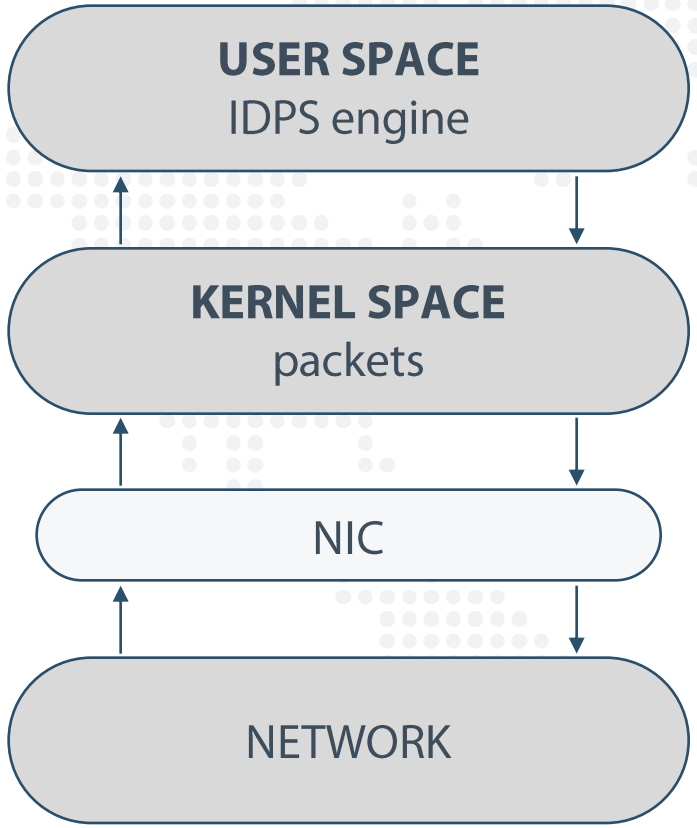
Модуль в составе UserGate NGFW

Система обнаружения вторжений

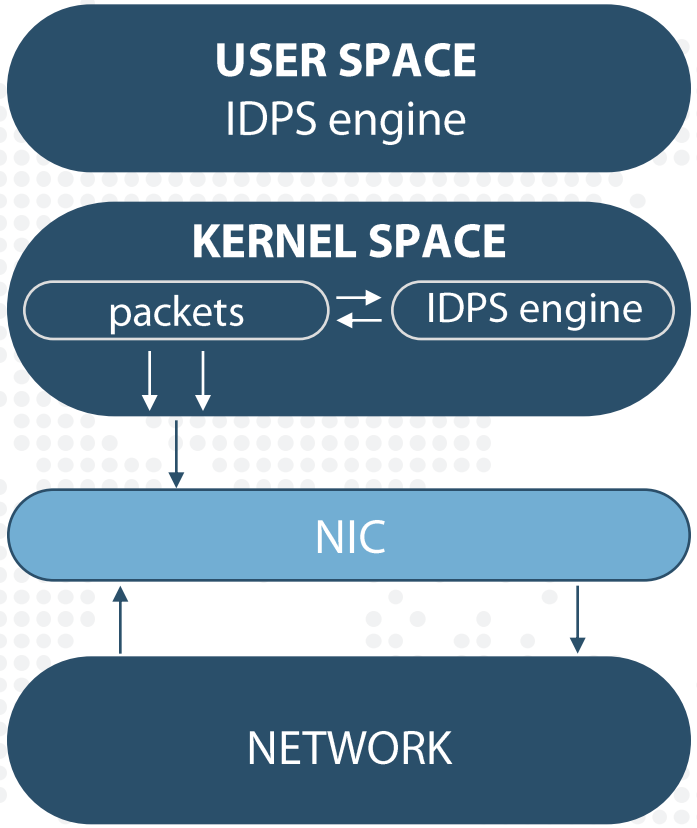
Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.



IDPS работает в Kernel Mode

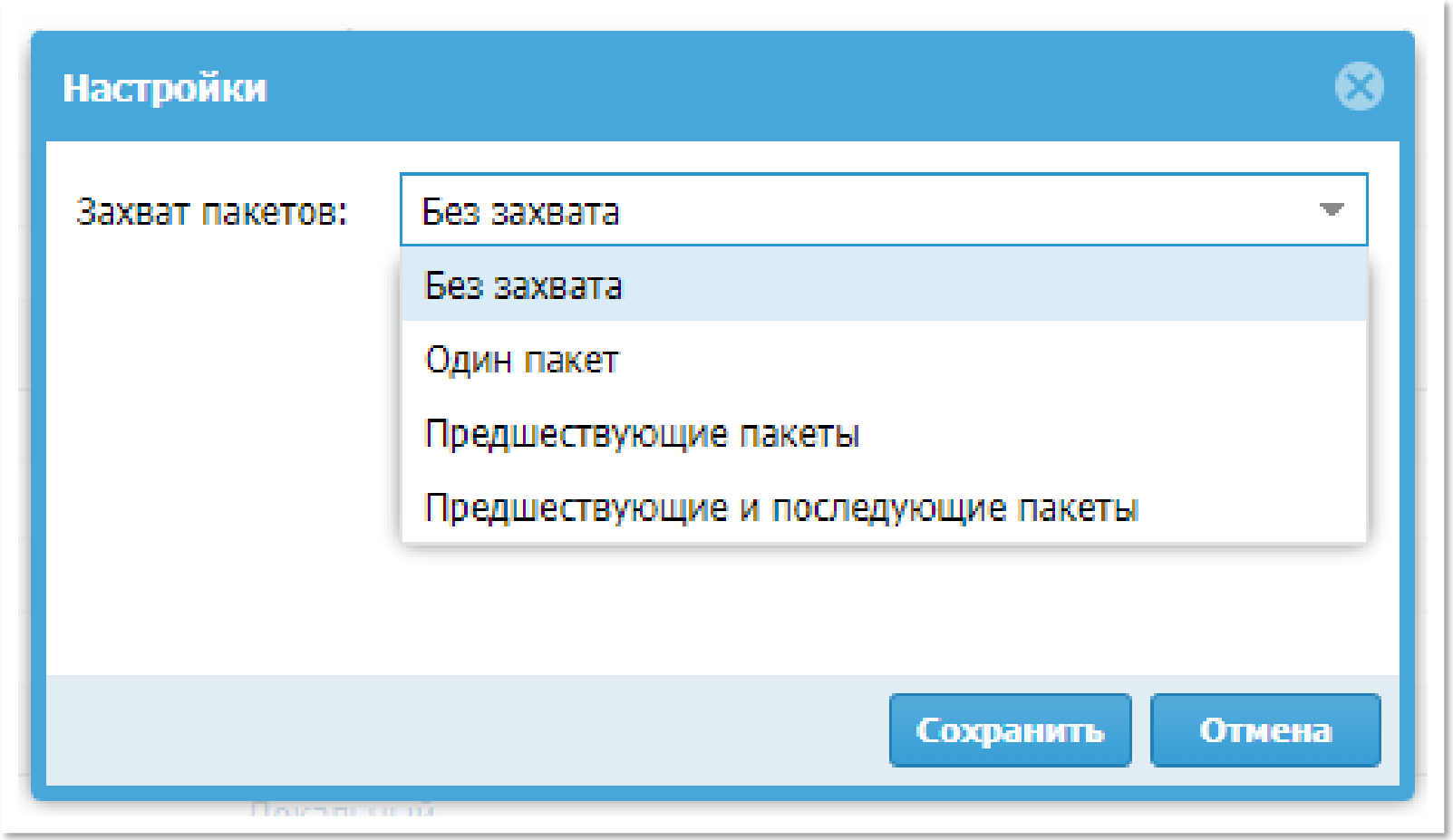


БЫЛО



СТАЛО

Запись трафика в PCAP



Чек-лист по безопасности

Контент-фильтрация

Модуль в составе UserGate NGFW

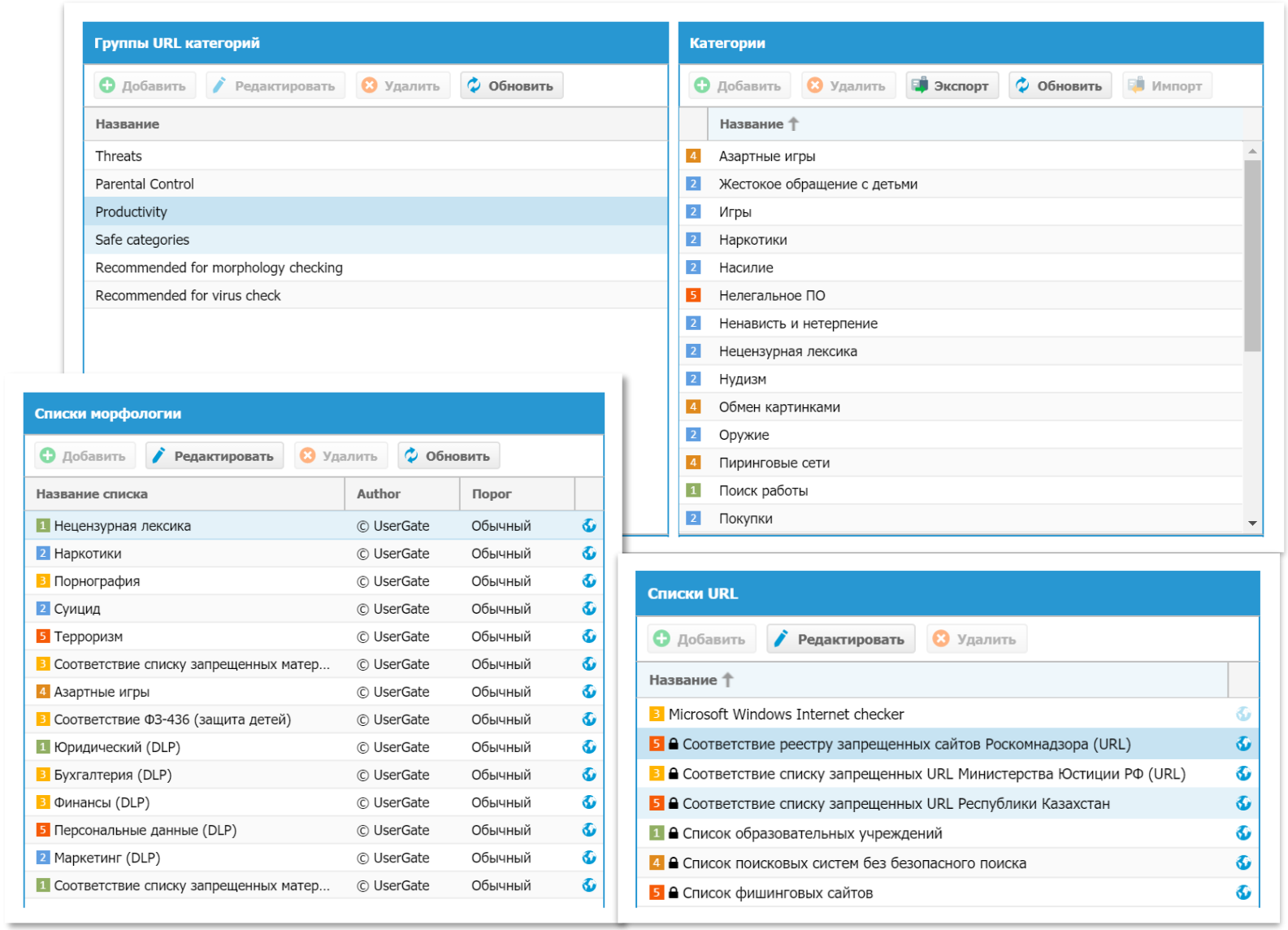
Механизмы фильтрации

- фильтрация по категориям;
- морфологический анализ;
- безопасный поиск;
- белые и черные списки;
- блокировка контекстной рекламы;
- запрет загрузки определенных видов файлов;
- антивирусная проверка трафика;
- интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и TLS ГОСТ.

Механизмы фильтрации

- крупнейшая база электронных ресурсов
  – более **600** миллионов сайтов;
- **80+** категорий;
- ежедневное обновление списка сайтов;
- повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории.

Механизмы фильтрации

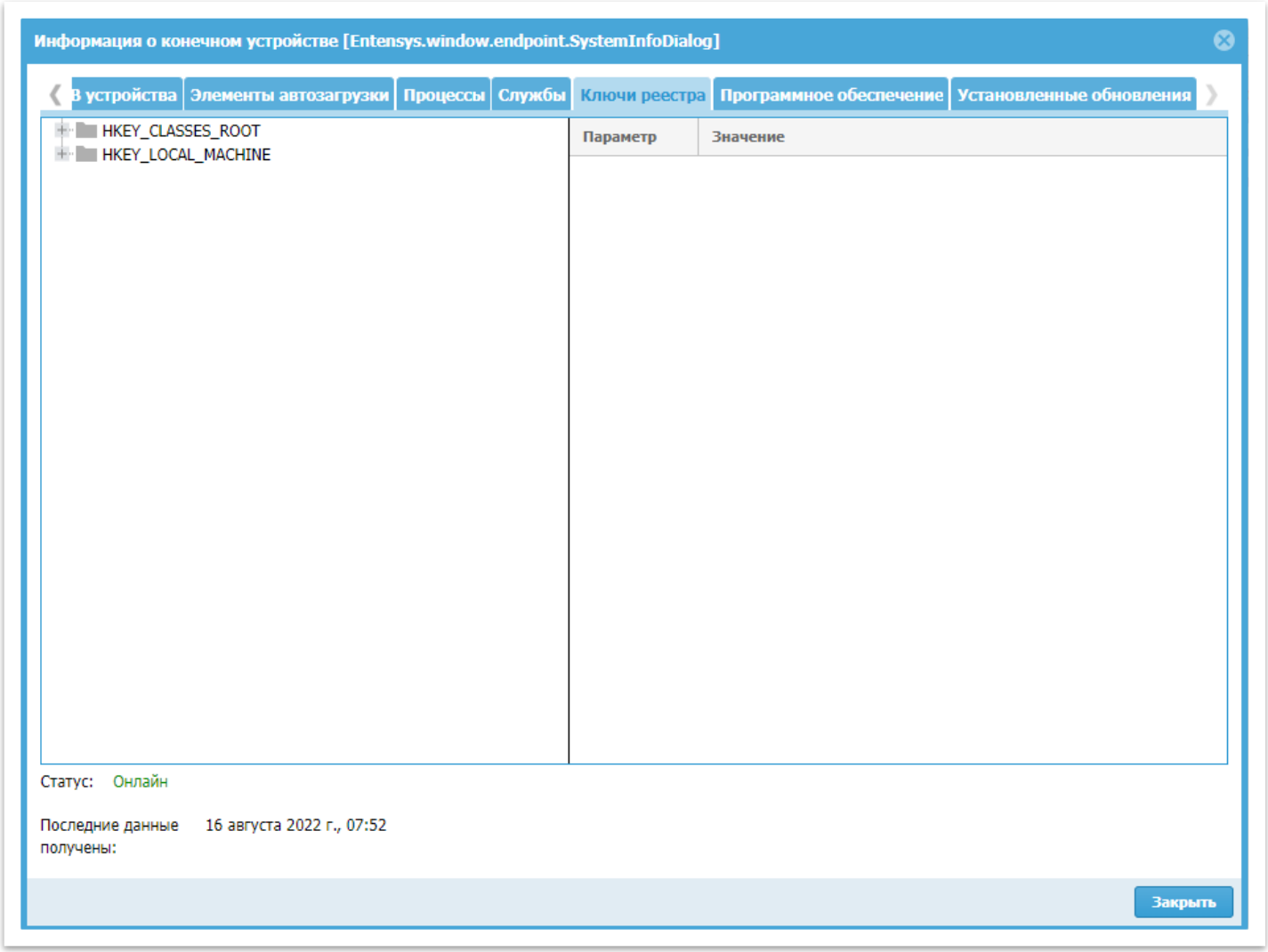


UserGate Client

UserGate Client – агент SUMMA

- видимость событий безопасности;
- контроль устройства;
- доступ с нулевым доверием.

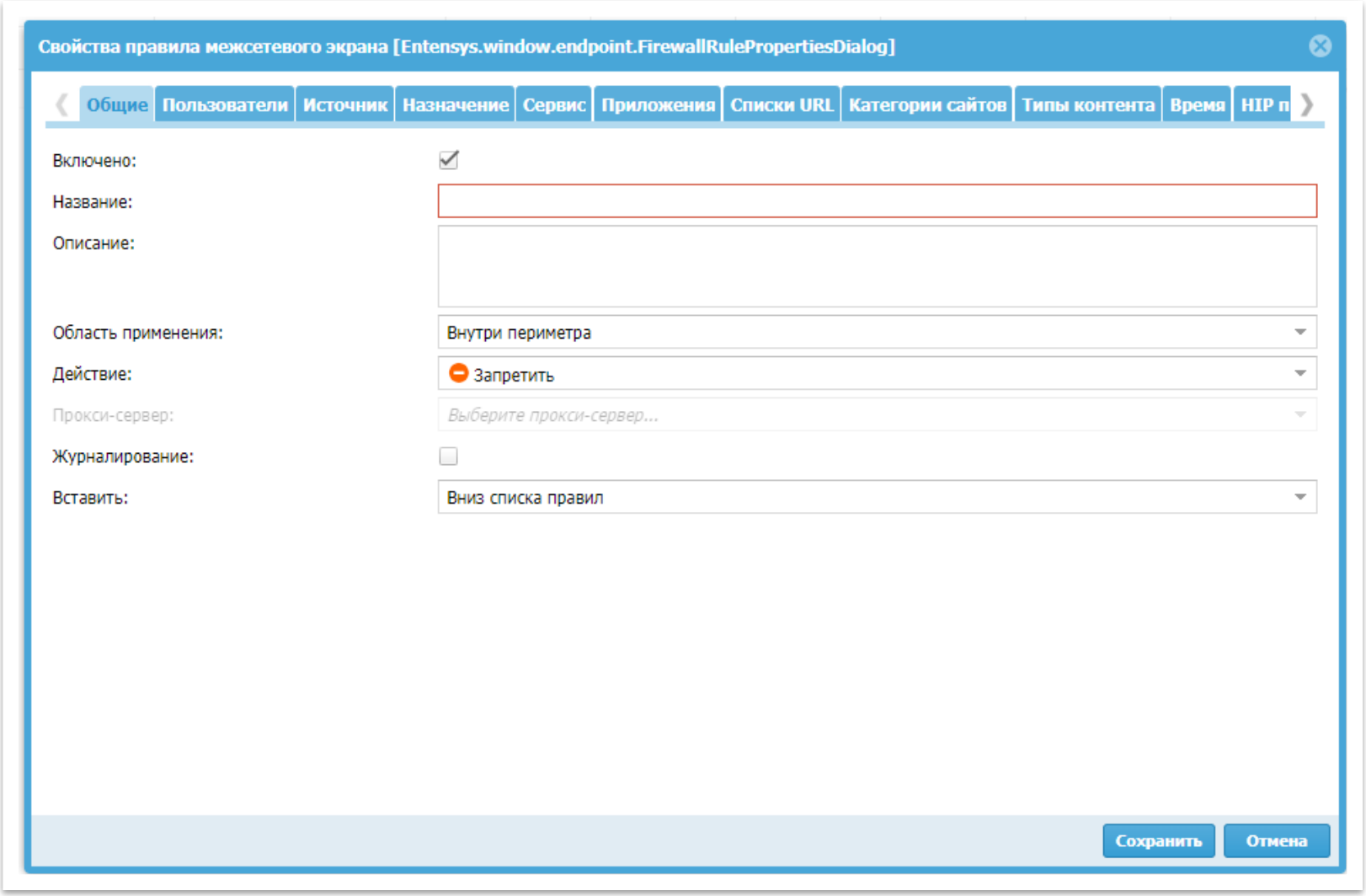
Сбор информации с устройства



Сбор информации с устройства

- состояние, память и производительность;
- безопасность;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- службы;
- ключи реестра;
- программное обеспечение;
- установленные обновления.

Персональный межсетевой экран



NAC

Профили устройств:

- продукт;
- процесс;
- запущенная служба;
- ключи реестра;
- установленные обновления.

VPN

- Client2Site – IPSec/L2TP, IKEv2;
- SSL VPN;
- «принудительный» VPN.

Экспертиза, IoC

Данные из логов, которые можно обогатить и найти следы компрометации:

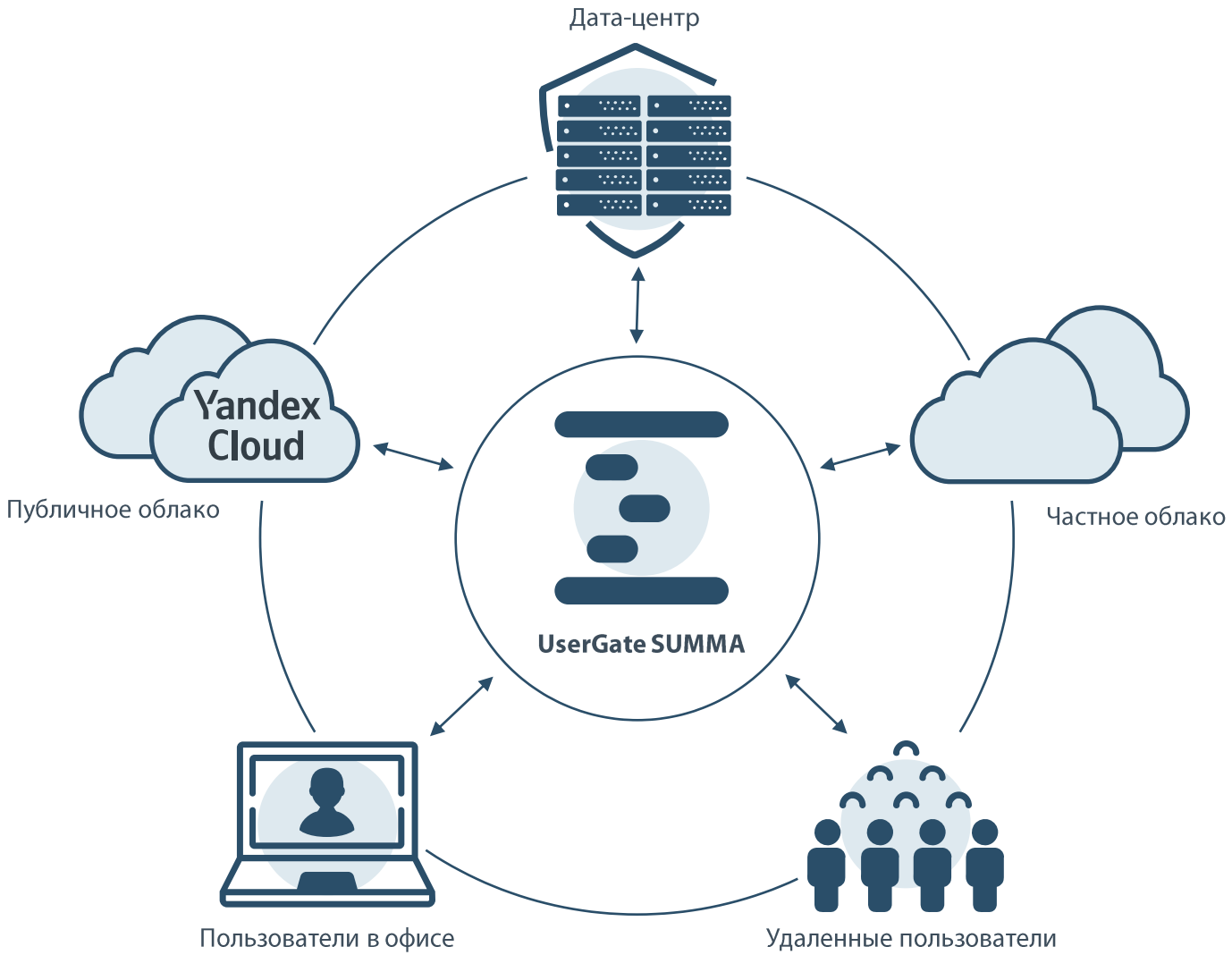
- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

В рамках UserGate SUMMA

EDR/XDR


Extended
Detection
Response
Сети
Облака
Устройства
UserGate Log Analyzer
SOC
Cloud Protection
UserGate Client
Proxy
UserGate NGFW
WAF

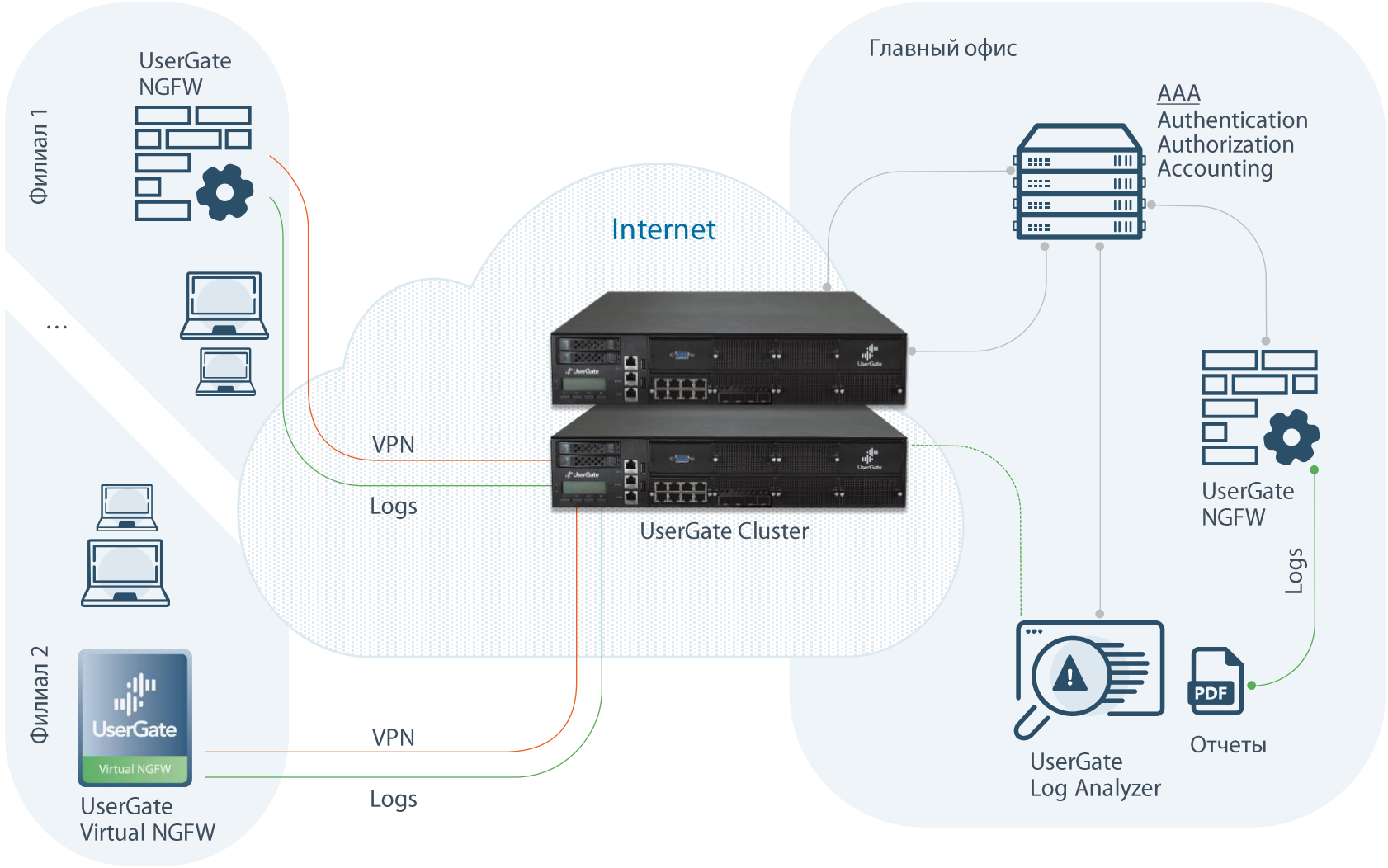
ZTNA


Дата-центр
Yandex Cloud
Публичное облако
UserGate SUMMA
Частное облако
Пользователи в офисе
Удаленные пользователи

Log Analyzer

1. Анализ

Примеры использования



192.168.95.248:8010

UserGate

Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin

Аналитика

Правила аналитики | Поиск | Правила действий | Срабатывания | Подробности срабатывания

source='traffic log' AND dayOfWeek=2

Добавить правило | Добавить условие | Добавить в тикет

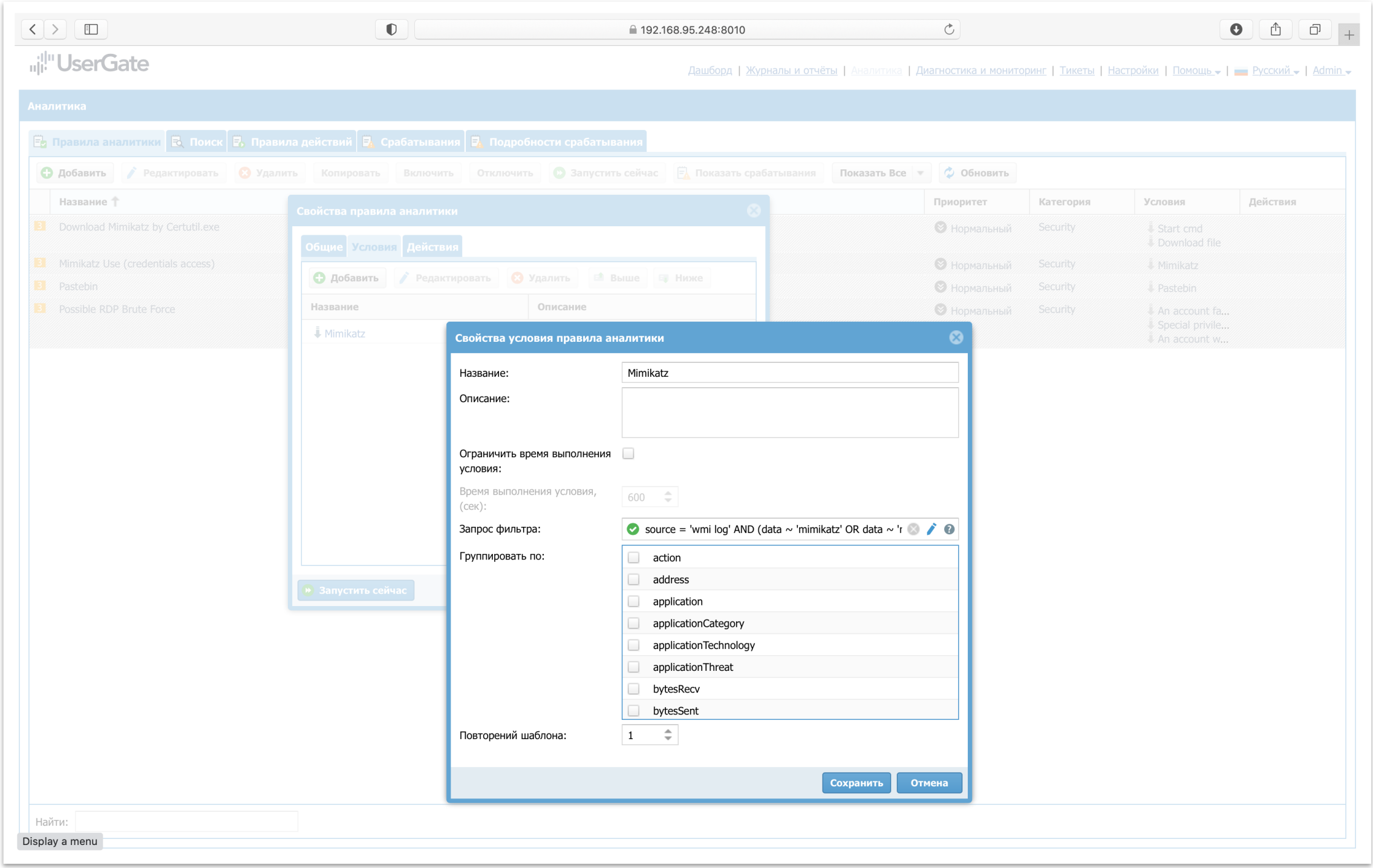
Время	Узел	Источ...	Имя пользо...	Правило	Действие	При...	Прот...	Зона источ...	IP источника	Порт...	Зона назна...	IP назначе...	Порт...	NAT адрес ...	NAT ...	NAT адрес ...	NAT ...	Б
17:08:29	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57036	Trusted	192.168....	80		0		0	6
17:08:29	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57042	Trusted	192.168....	80		0		0	6
17:08:28	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56132	Unknown	192.168....	8010	192.168.95.2...	56132	192.168.2.101	8010	6
17:08:24	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57040	Trusted	192.168....	80		0		0	6
17:08:23	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57034	Trusted	192.168....	80		0		0	6
17:08:16	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.116	60077	Trusted	192.168....	7680		0		0	5
17:08:16	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57032	Trusted	192.168....	80		0		0	6
17:08:14	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.129	62676	Trusted	192.168....	7680		0		0	5
17:08:14	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57036	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57034	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57030	Trusted	192.168....	80		0		0	6
17:08:07	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57028	Trusted	192.168....	80		0		0	6
17:08:00	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57032	Trusted	192.168....	80		0		0	6
17:08:00	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57026	Trusted	192.168....	80		0		0	6
17:07:54	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56128	Unknown	192.168....	8010	192.168.95.2...	56128	192.168.2.101	8010	6
17:07:54	utmcor...	Журнал	Unknown	To Logan	DNAT		TCP	External	192.168.95.245	56127	Unknown	192.168....	8010	192.168.95.2...	56127	192.168.2.101	8010	6
17:07:53	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57024	Trusted	192.168....	80		0		0	6
17:07:52	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57030	Trusted	192.168....	80		0		0	6
17:07:51	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57028	Trusted	192.168....	80		0		0	6
17:07:45	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57026	Trusted	192.168....	80		0		0	6
17:07:44	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57018	Trusted	192.168....	80		0		0	6
17:07:38	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57016	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57024	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57022	Trusted	192.168....	80		0		0	6
17:07:37	utmcor...	Журнал	Unknown	Allow all	Разрешить		TCP	External	192.168.95.55	57020	Trusted	192.168....	80		0		0	6

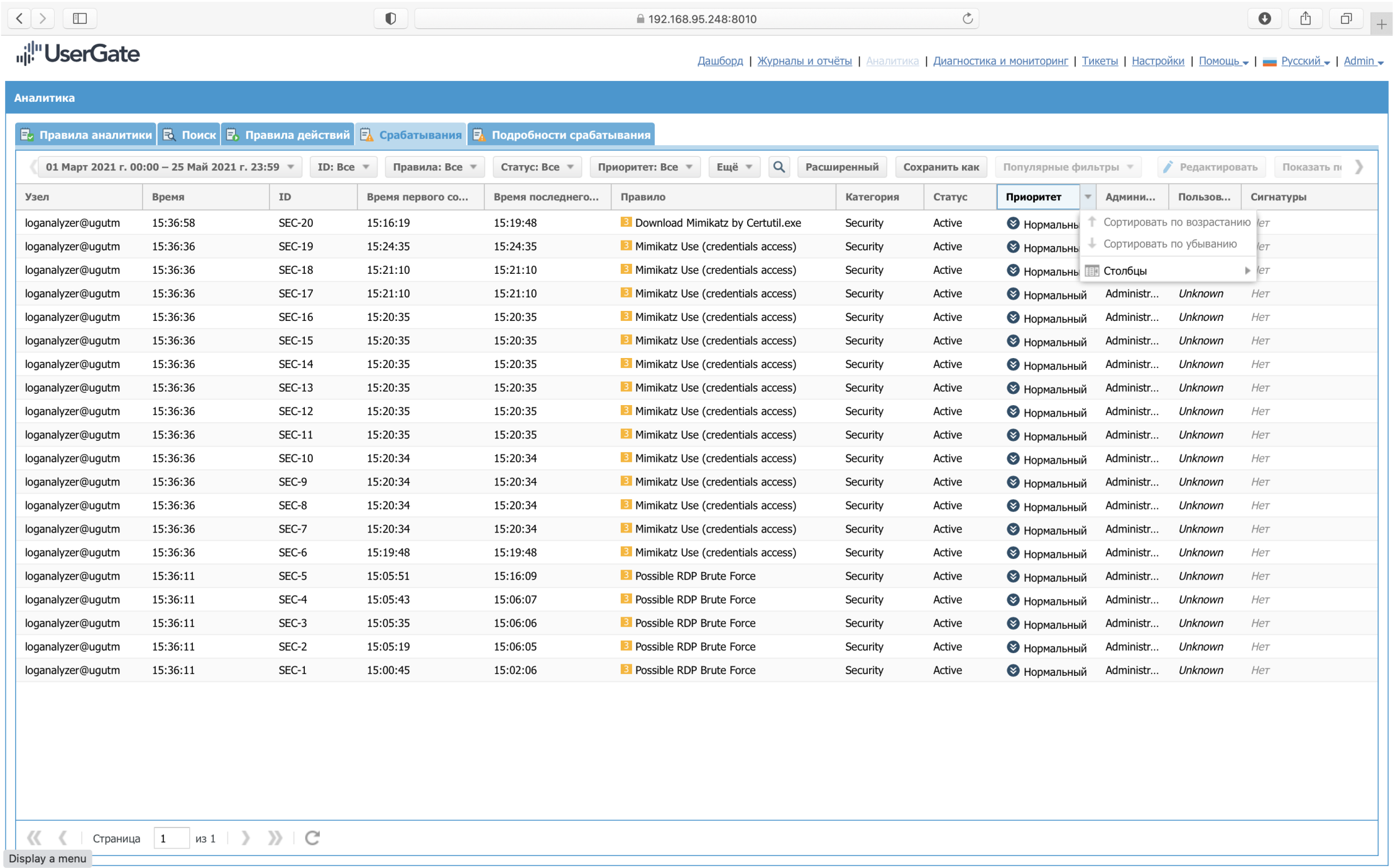
Страница 1 из 5104

Display a menu

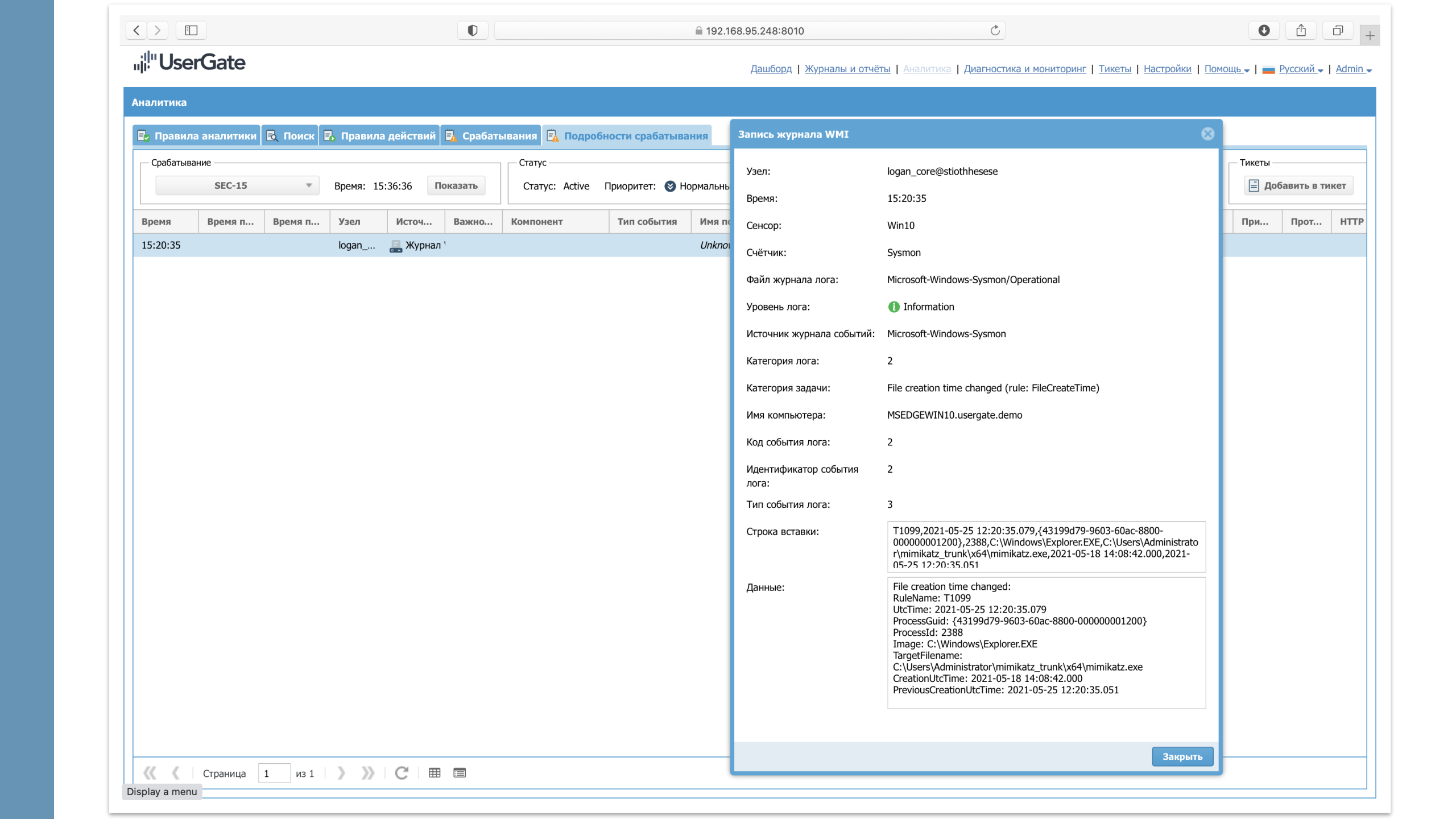
Log Analyzer

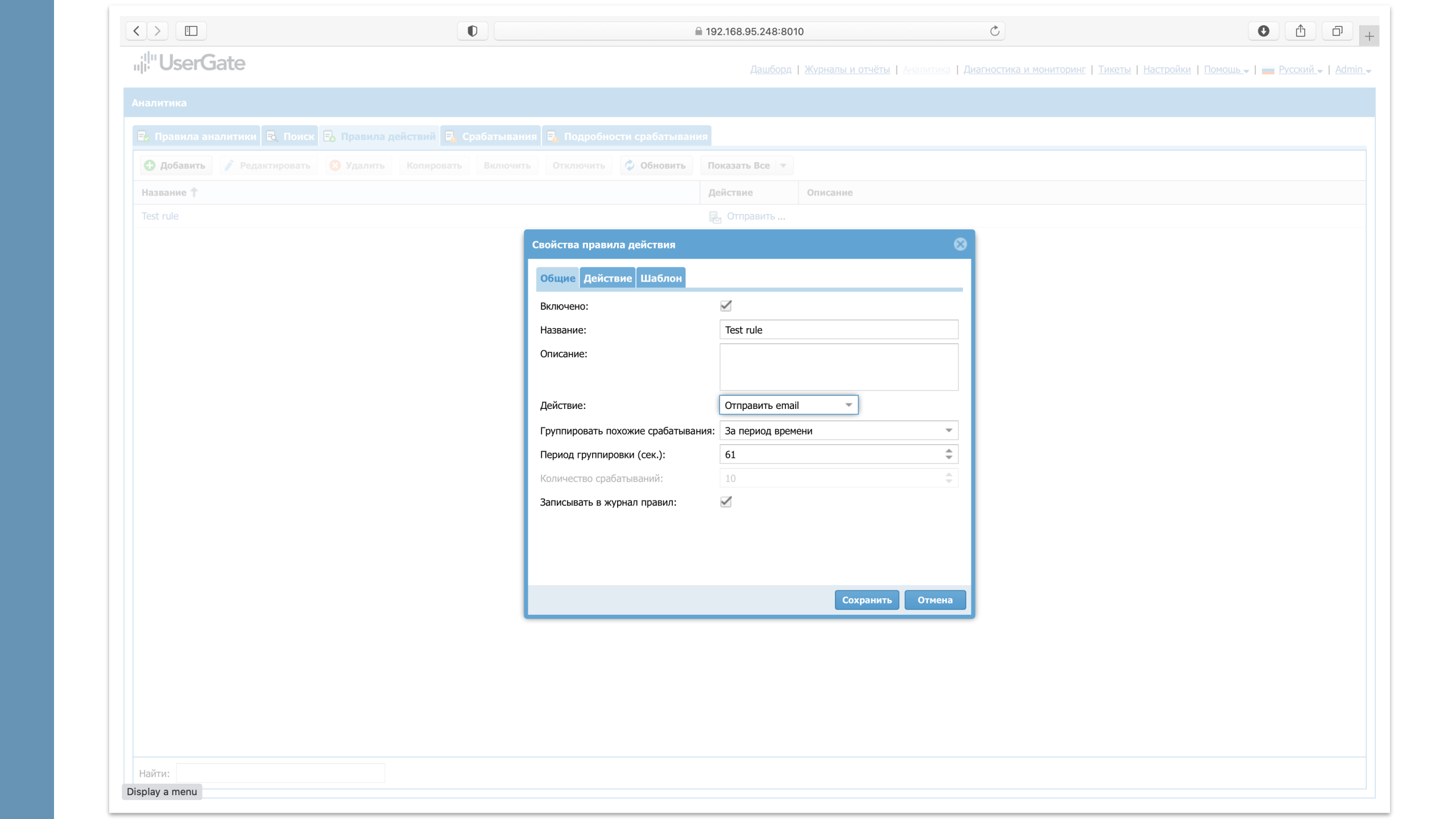
1. Анализ
2. Реагирование

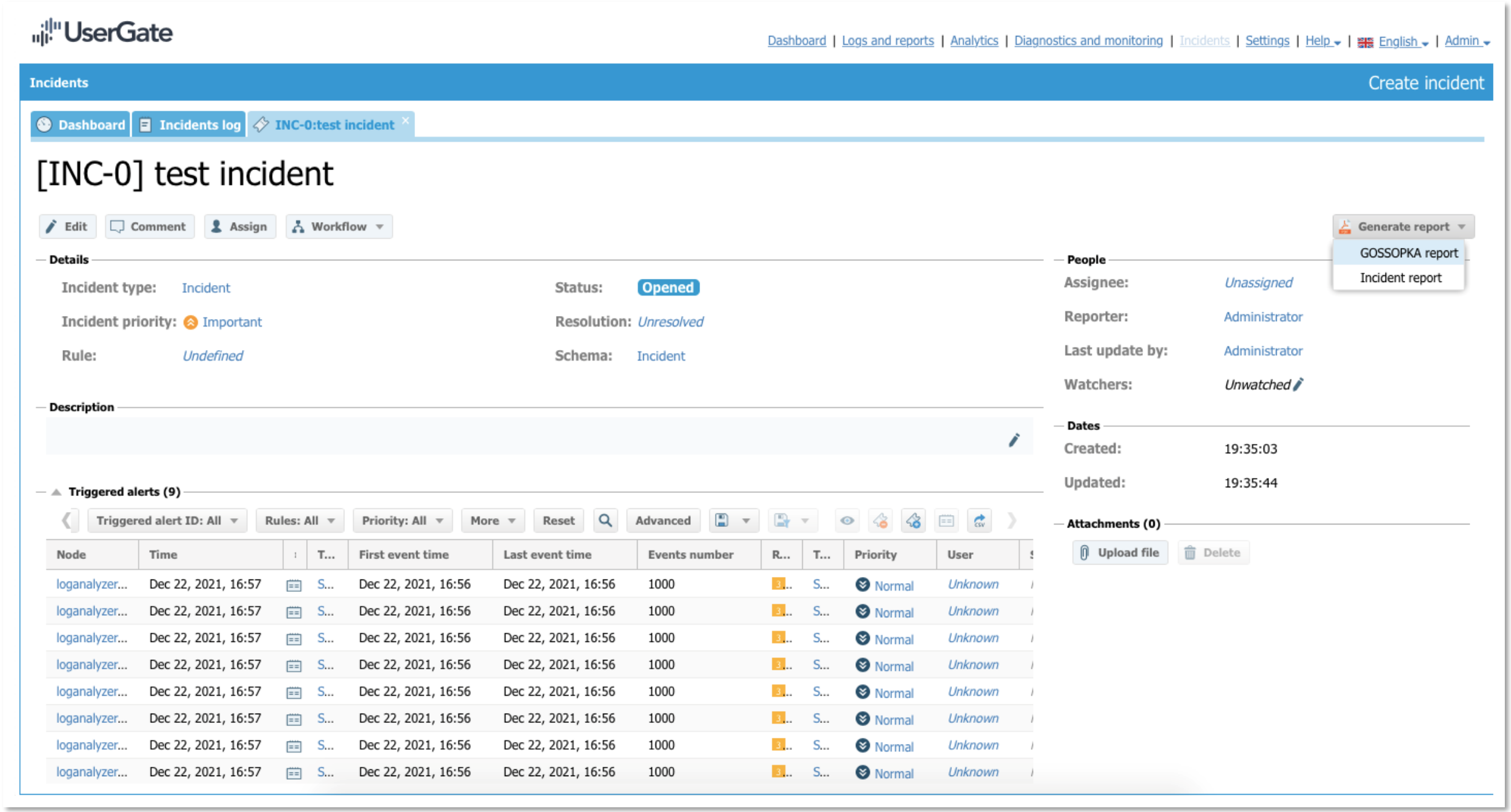

192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Запустить сейчас
Показать срабатывания
Показать Все
Обновить
Название
Приоритет
Категория
Условия
Действия
Download Mimikatz by Certutil.exe
Нормальный
Security
Start cmd
Download file
Mimikatz Use (credentials access)
Нормальный
Security
Mimikatz
Pastebin
Нормальный
Security
Pastebin
Possible RDP Brute Force
Нормальный
Security
An account fa...
Special privile...
An account w...
Свойства правила аналитики
Общие
Условия
Действия
Добавить
Редактировать
Удалить
Выше
Ниже
Название
Описание
Mimikatz
Запустить сейчас
Свойства условия правила аналитики
Название:
Mimikatz
Описание:
Ограничить время выполнения условия:
Время выполнения условия, (сек):
600
Запрос фильтра:
source = 'wmi log' AND (data ~ 'mimikatz' OR data ~ 'r
Группировать по:
action
address
application
applicationCategory
applicationTechnology
applicationThreat
bytesRecv
bytesSent
Повторений шаблона:
1
Сохранить
Отмена
Найти:
Display a menu



Узел	Время	ID	Время первого со...	Время последнего...	Правило	Категория	Статус	Приоритет	Админи...	Пользов...	Сигнатуры
loganalyzer@ugutm	15:36:58	SEC-20	15:16:19	15:19:48	Download Mimikatz by Certutil.exe	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-19	15:24:35	15:24:35	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-18	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальны			Нет
loganalyzer@ugutm	15:36:36	SEC-17	15:21:10	15:21:10	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-16	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-15	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-14	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-13	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-12	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-11	15:20:35	15:20:35	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-10	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-9	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-8	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-7	15:20:34	15:20:34	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:36	SEC-6	15:19:48	15:19:48	Mimikatz Use (credentials access)	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-5	15:05:51	15:16:09	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-4	15:05:43	15:06:07	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-3	15:05:35	15:06:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-2	15:05:19	15:06:05	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет
loganalyzer@ugutm	15:36:11	SEC-1	15:00:45	15:02:06	Possible RDP Brute Force	Security	Active	Нормальный	Administr...	*Unknown*	Нет


192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Срабатывание
SEC-15
Время: 15:36:36
Показать
Статус
Статус: Active
Приоритет:
Тикеты
Добавить в тикет
Время
Время п...
Время п...
Узел
Источ...
Важно...
Компонент
Тип события
Имя по
При...
Прот...
HTTP
15:20:35
logan_...
Журнал '
Unknow
Страница 1 из 1
Display a menu
Запись журнала WMI
Узел: logan_core@stiothhesese
Время: 15:20:35
Сенсор: Win10
Счётчик: Sysmon
Файл журнала лога: Microsoft-Windows-Sysmon/Operational
Уровень лога: Information
Источник журнала событий: Microsoft-Windows-Sysmon
Категория лога: 2
Категория задачи: File creation time changed (rule: FileCreateTime)
Имя компьютера: MSEDGEWIN10.usergate.demo
Код события лога: 2
Идентификатор события лога: 2
Тип события лога: 3
Строка вставки: T1099,2021-05-25 12:20:35.079,{43199d79-9603-60ac-8800-000000001200},2388,C:\Windows\Explorer.EXE,C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe,2021-05-18 14:08:42.000,2021-05-25 12:20:35.051
Данные: File creation time changed:
RuleName: T1099
UtcTime: 2021-05-25 12:20:35.079
ProcessGuid: {43199d79-9603-60ac-8800-000000001200}
ProcessId: 2388
Image: C:\Windows\Explorer.EXE
TargetFilename:
C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe
CreationUtcTime: 2021-05-18 14:08:42.000
PreviousCreationUtcTime: 2021-05-25 12:20:35.051
Закрыть

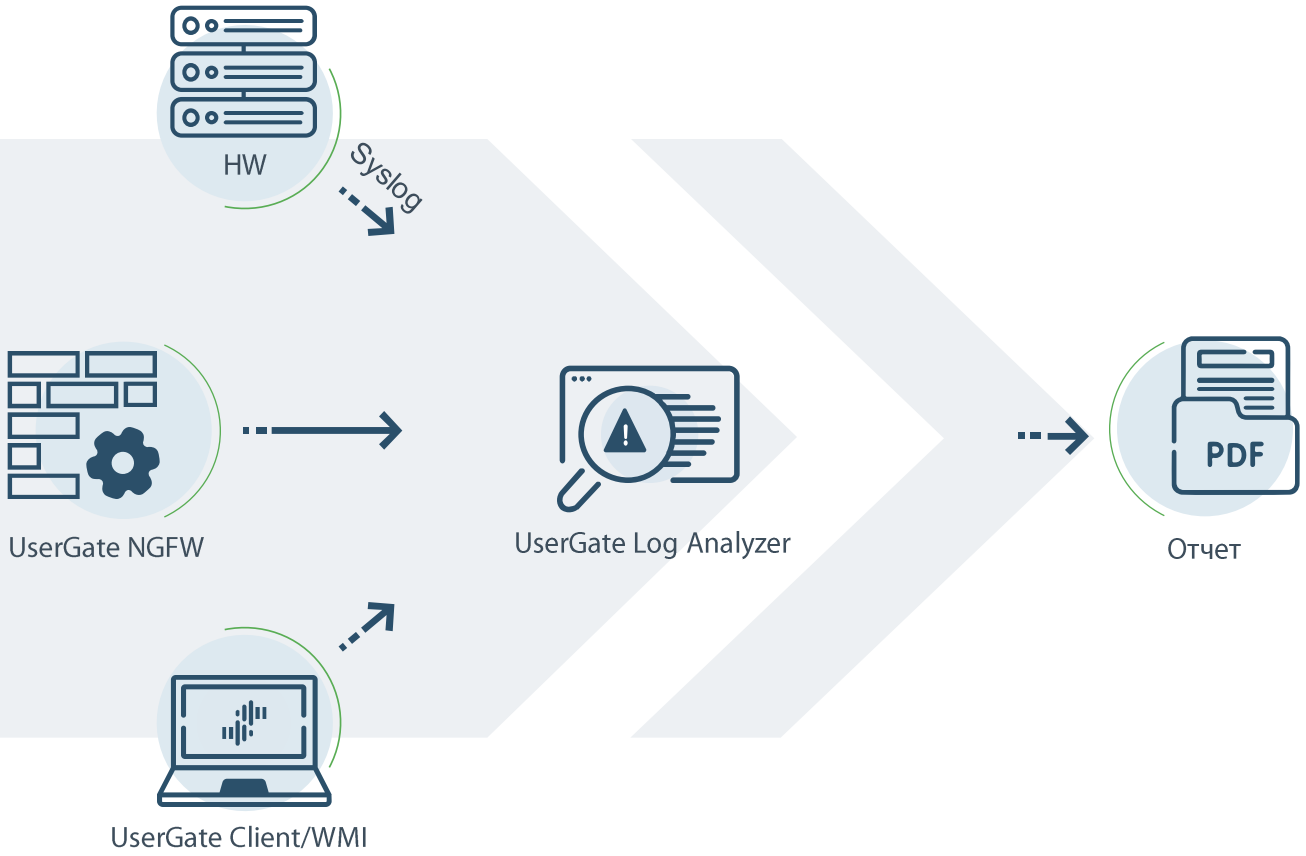

192.168.95.248:8010
UserGate
Дашборд | Журналы и отчёты | Аналитика | Диагностика и мониторинг | Тикеты | Настройки | Помощь | Русский | Admin
Аналитика
Правила аналитики
Поиск
Правила действий
Срабатывания
Подробности срабатывания
Добавить
Редактировать
Удалить
Копировать
Включить
Отключить
Обновить
Показать Все
Название
Действие
Описание
Test rule
Отправить ...
Свойства правила действия
Общие
Действие
Шаблон
Включено:
Название:
Test rule
Описание:
Действие:
Отправить email
Группировать похожие срабатывания:
За период времени
Период группировки (сек.):
61
Количество срабатываний:
10
Записывать в журнал правил:
Сохранить
Отмена
Найти:
Display a menu


UserGate
Dashboard | Logs and reports | Analytics | Diagnostics and monitoring | Incidents | Settings | Help | English | Admin
Incidents
Create incident
Dashboard
Incidents log
INC-0:test incident
[INC-0] test incident
Edit
Comment
Assign
Workflow
Generate report
GOSSOPKA report
Incident report
Details
Incident type: Incident
Incident priority: Important
Rule: Undefined
Status: Opened
Resolution: Unresolved
Schema: Incident
People
Assignee: Unassigned
Reporter: Administrator
Last update by: Administrator
Watchers: Unwatched
Description
Dates
Created: 19:35:03
Updated: 19:35:44
Triggered alerts (9)
Triggered alert ID: All
Rules: All
Priority: All
More
Reset
Advanced
Attachments (0)
Upload file
Delete
Node
Time
First event time
Last event time
Events number
Priority
User
loganalyzer...
Dec 22, 2021, 16:57
Dec 22, 2021, 16:56
1000
Normal
Unknown

Log Analyzer

1. Анализ
2. Реагирование
3. Глобальный мониторинг

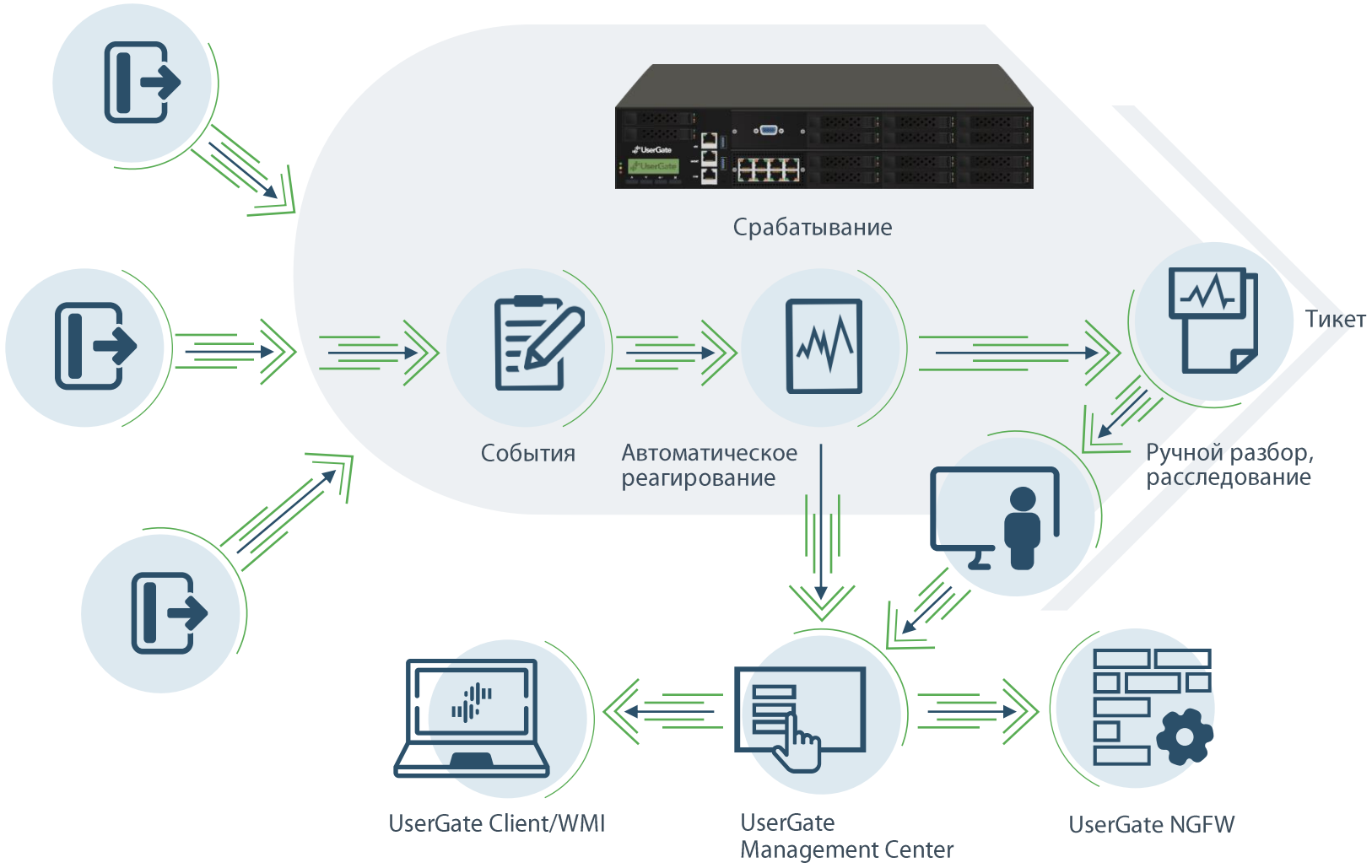
Платформы


HW
Syslog
UserGate NGFW
UserGate Log Analyzer
PDF
Отчет
UserGate Client/WMI

Log Analyzer

1. Анализ
2. Реагирование
3. Глобальный мониторинг
4. Унифицированная платформа

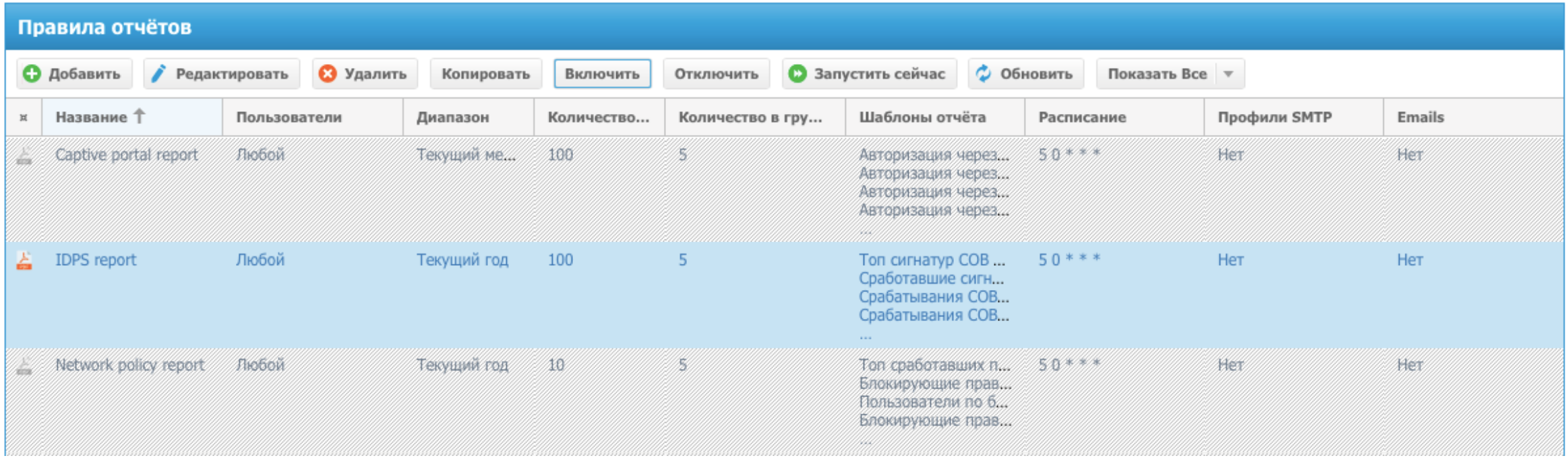
Архитектура продукта



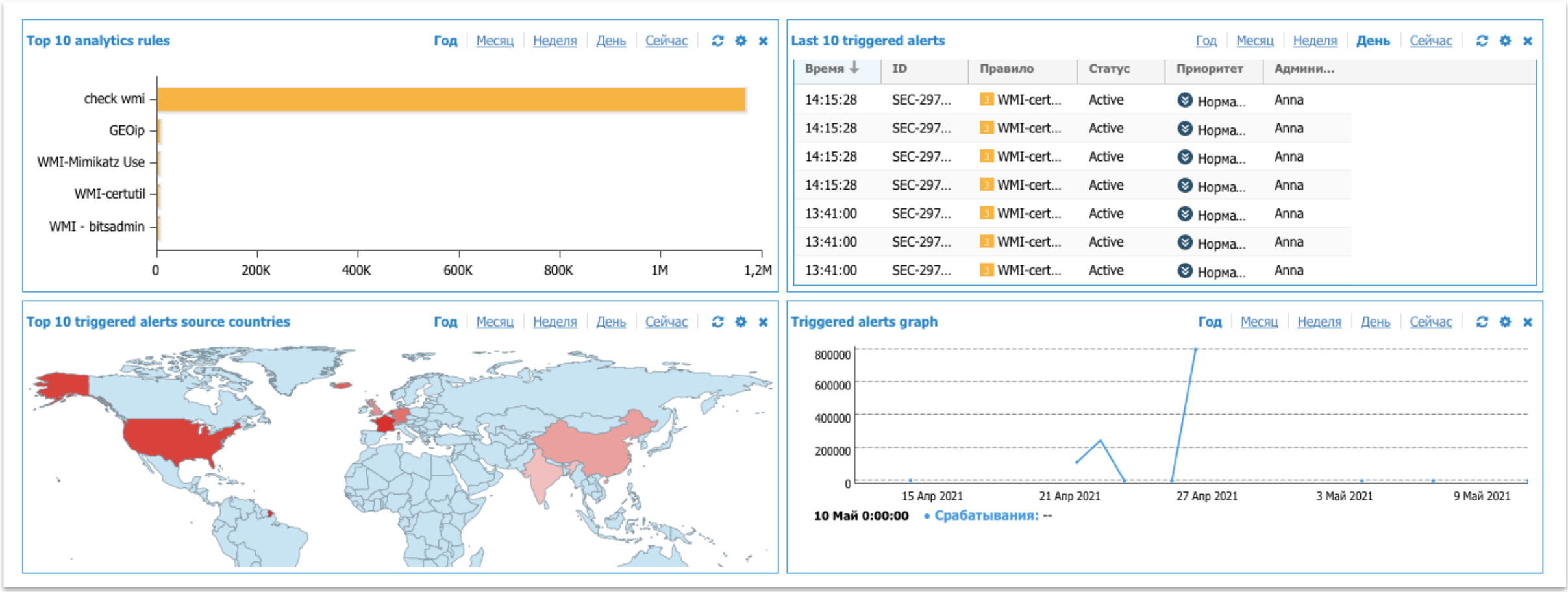
Log Analyzer

1. Анализ
2. Реагирование
3. Глобальный мониторинг
4. Унифицированная платформа
5. Систематизация

Правила отчетов

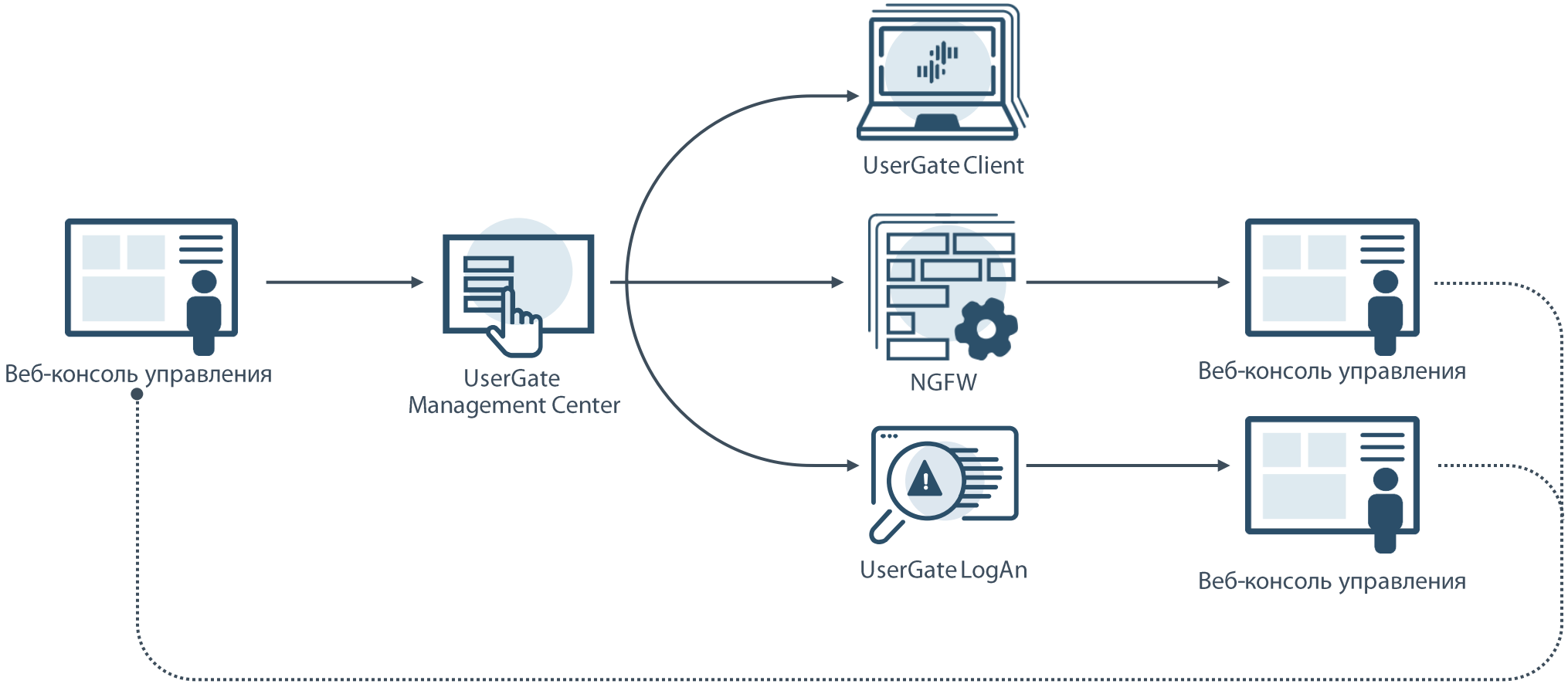


Дашборд


Top 10 analytics rules
Год | Месяц | Неделя | День | Сейчас
check wmi
GEOip
WMI-Mimikatz Use
WMI-certutil
WMI - bitsadmin
0
200K
400K
600K
800K
1M
1,2M
Last 10 triggered alerts
Год | Месяц | Неделя | День | Сейчас
Время | ID | Правило | Статус | Приоритет | Админи...
14:15:28 SEC-297... WMI-cert... Active Норма... Anna
14:15:28 SEC-297... WMI-cert... Active Норма... Anna
14:15:28 SEC-297... WMI-cert... Active Норма... Anna
14:15:28 SEC-297... WMI-cert... Active Норма... Anna
13:41:00 SEC-297... WMI-cert... Active Норма... Anna
13:41:00 SEC-297... WMI-cert... Active Норма... Anna
13:41:00 SEC-297... WMI-cert... Active Норма... Anna
Top 10 triggered alerts source countries
Год | Месяц | Неделя | День | Сейчас
Triggered alerts graph
Год | Месяц | Неделя | День | Сейчас
800000
600000
400000
200000
0
15 Апр 2021
21 Апр 2021
27 Апр 2021
3 Май 2021
9 Май 2021
10 Май 0:00:00 • Срабатывания: --

Management Center

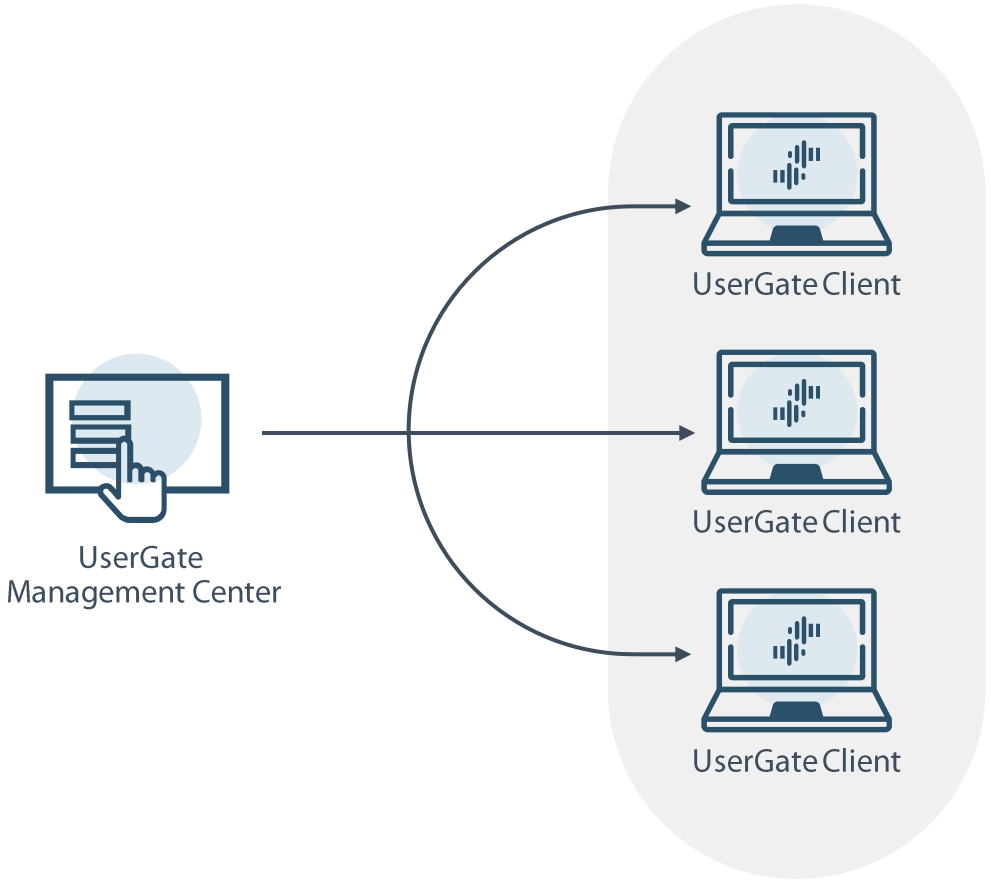
Веб-консоль управления



UserGate Management Center – зачем?

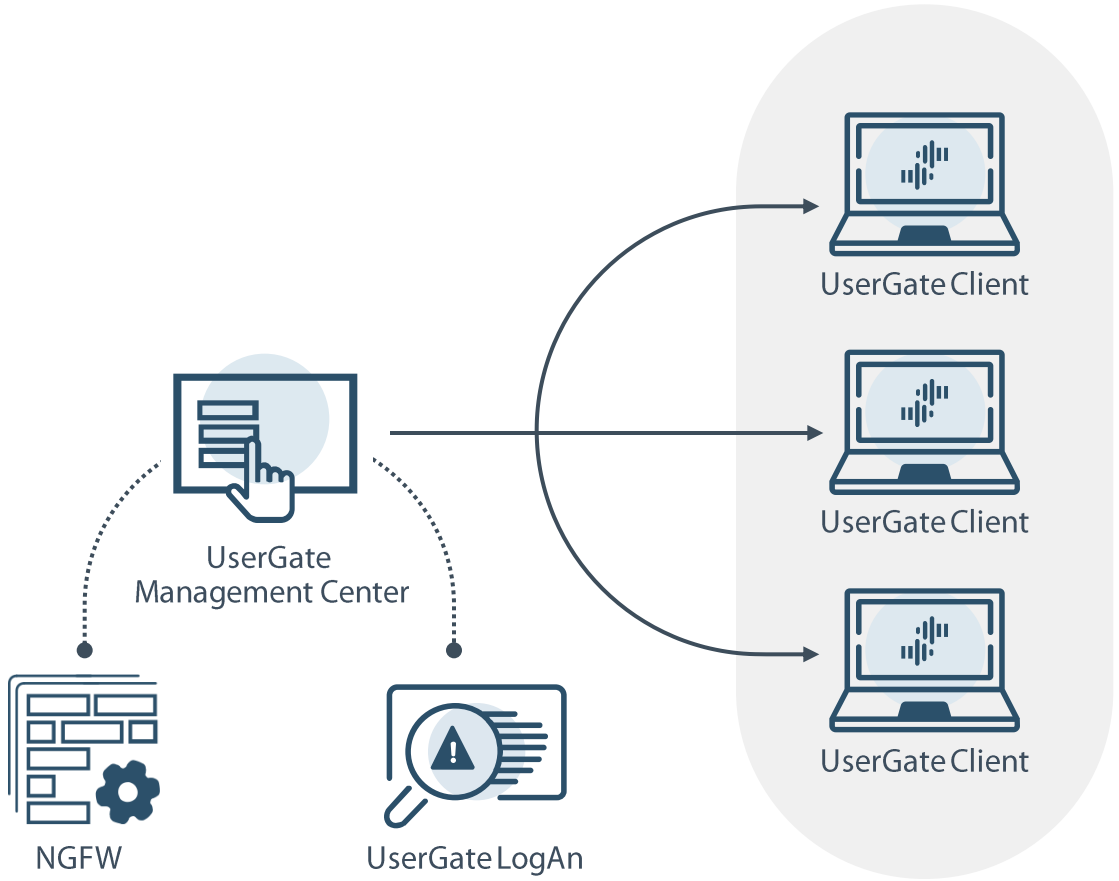
- упрощение администрирования большим парком продуктов UserGate (управление списками объектов: IP-адреса, URL-адреса, морфология, типы контента и т.д.);
- централизованное управление политиками безопасности и шаблонами политик безопасности;
- ролевая модель доступа к управлению;
- создание мультитенантной среды.

Схемы использования MC



Management Center – необходимый компонент для управления UserGate Client

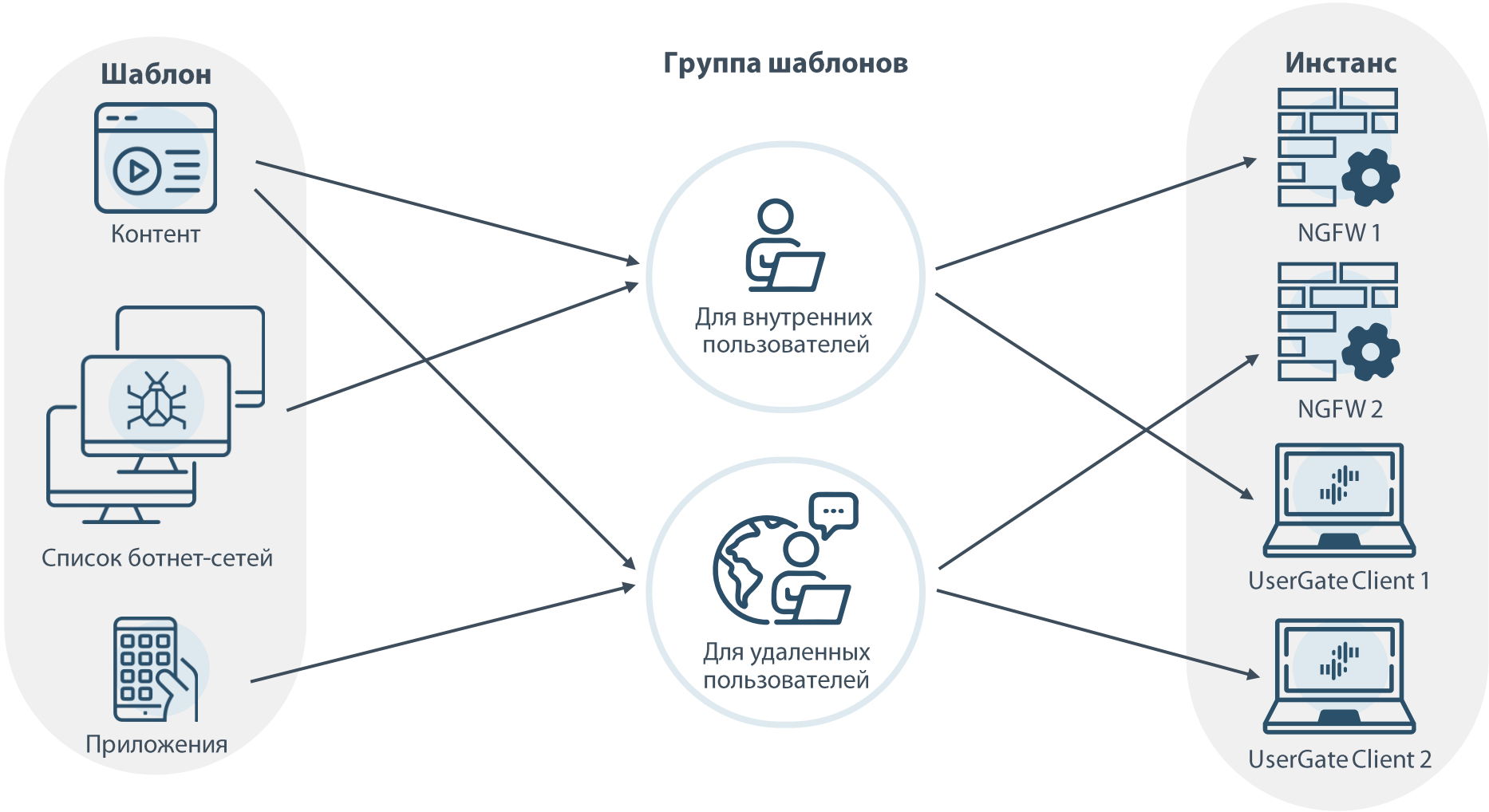
Схемы использования MC



Management Center – необязательный элемент для управления остальными компонентами;

Management Center можно собирать в кластер.

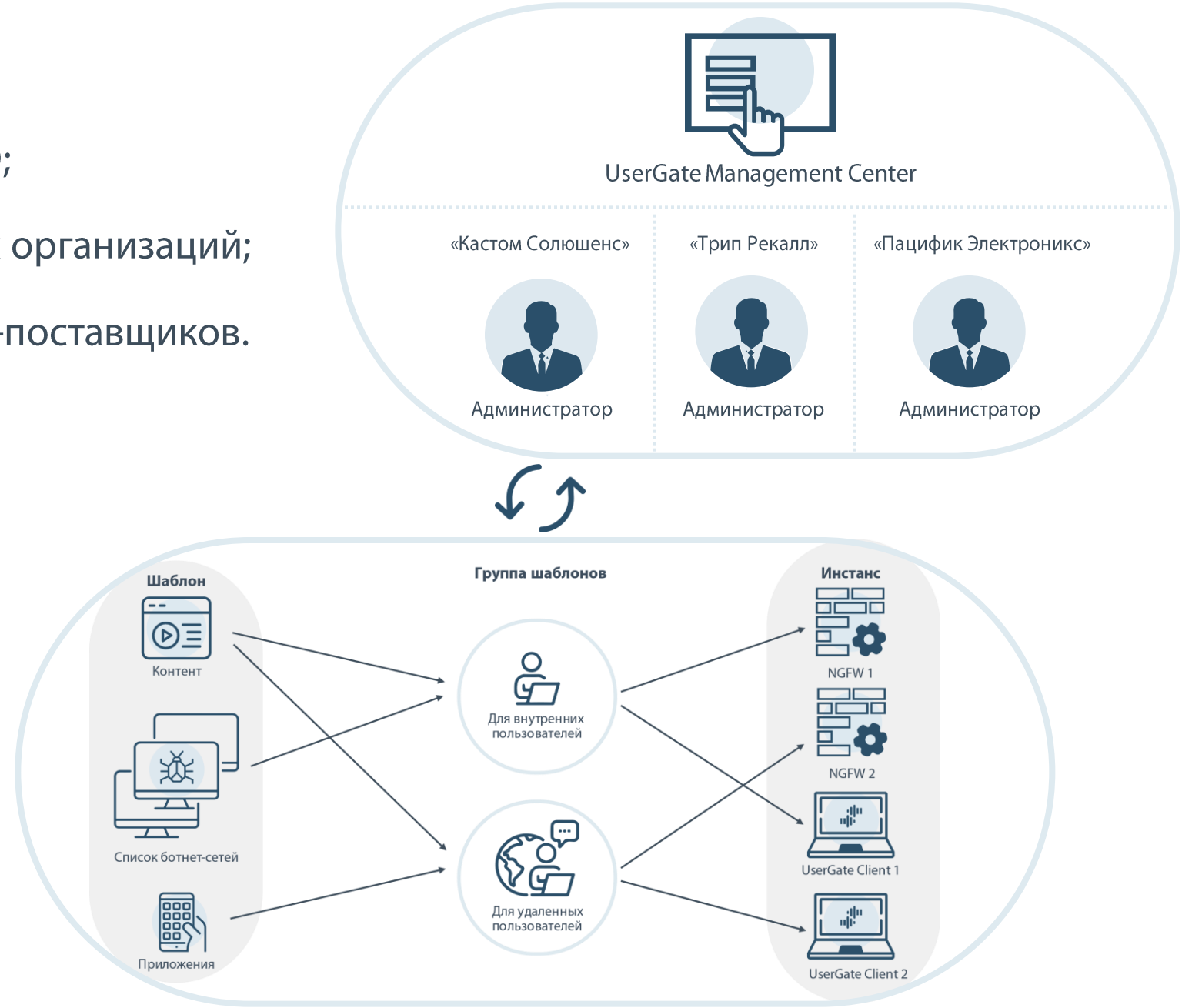
Шаблоны



Management Center позволяет создавать шаблоны политик безопасности.

Области

- для управления ДЗО;
- для обслуживающих организаций;
- для облачных/MSSP-поставщиков.



Пользователи

Администратор МС

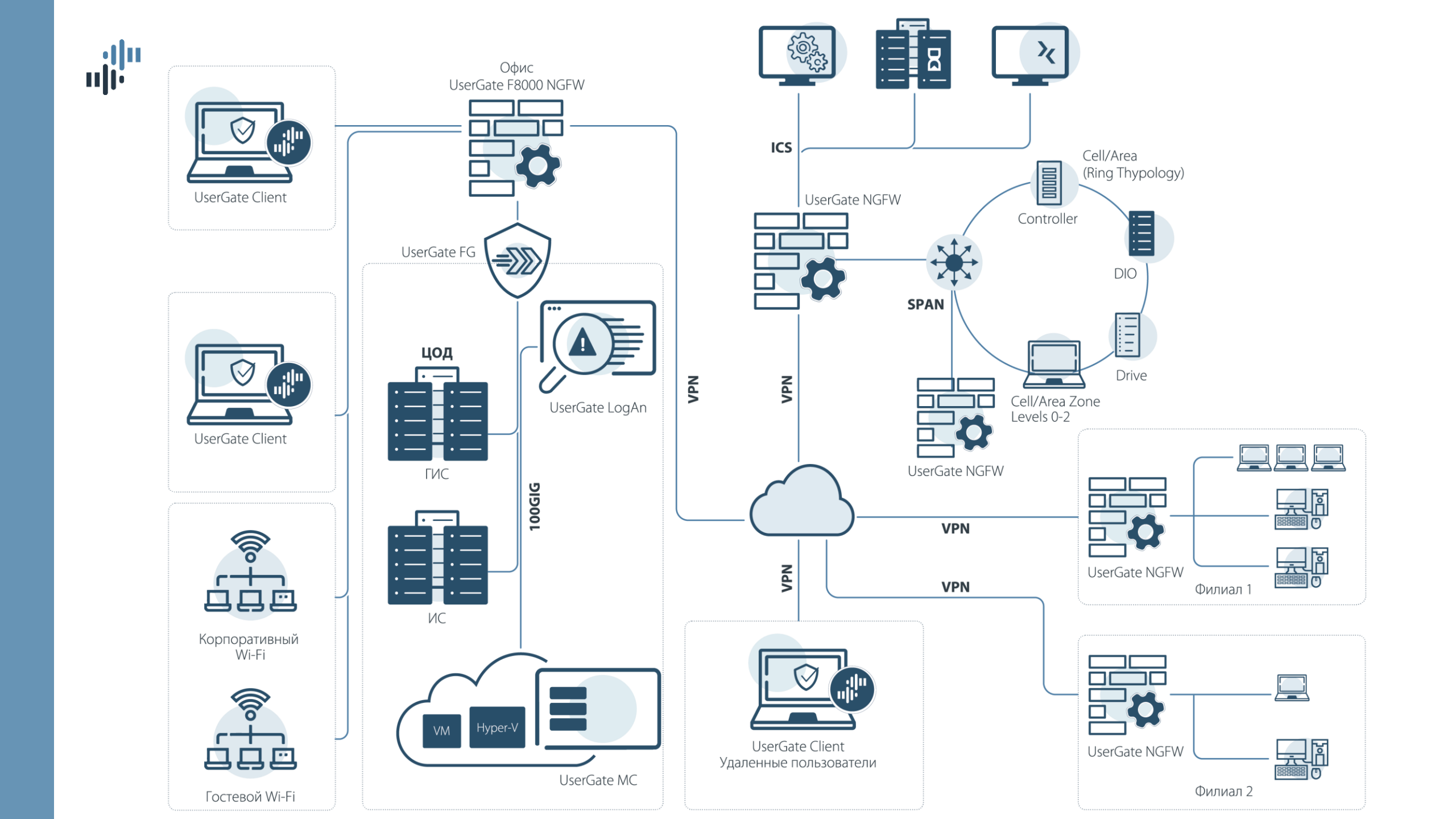
- настраивает устройство МС;
- не имеет доступа к областям;

Корневой администратор области
(создается администратором МС)

- настраивает области;
- не имеет доступа к настройкам устройства МС;
- не имеет доступа к другим областям;

Администратор области
(создается корневым администратором области)

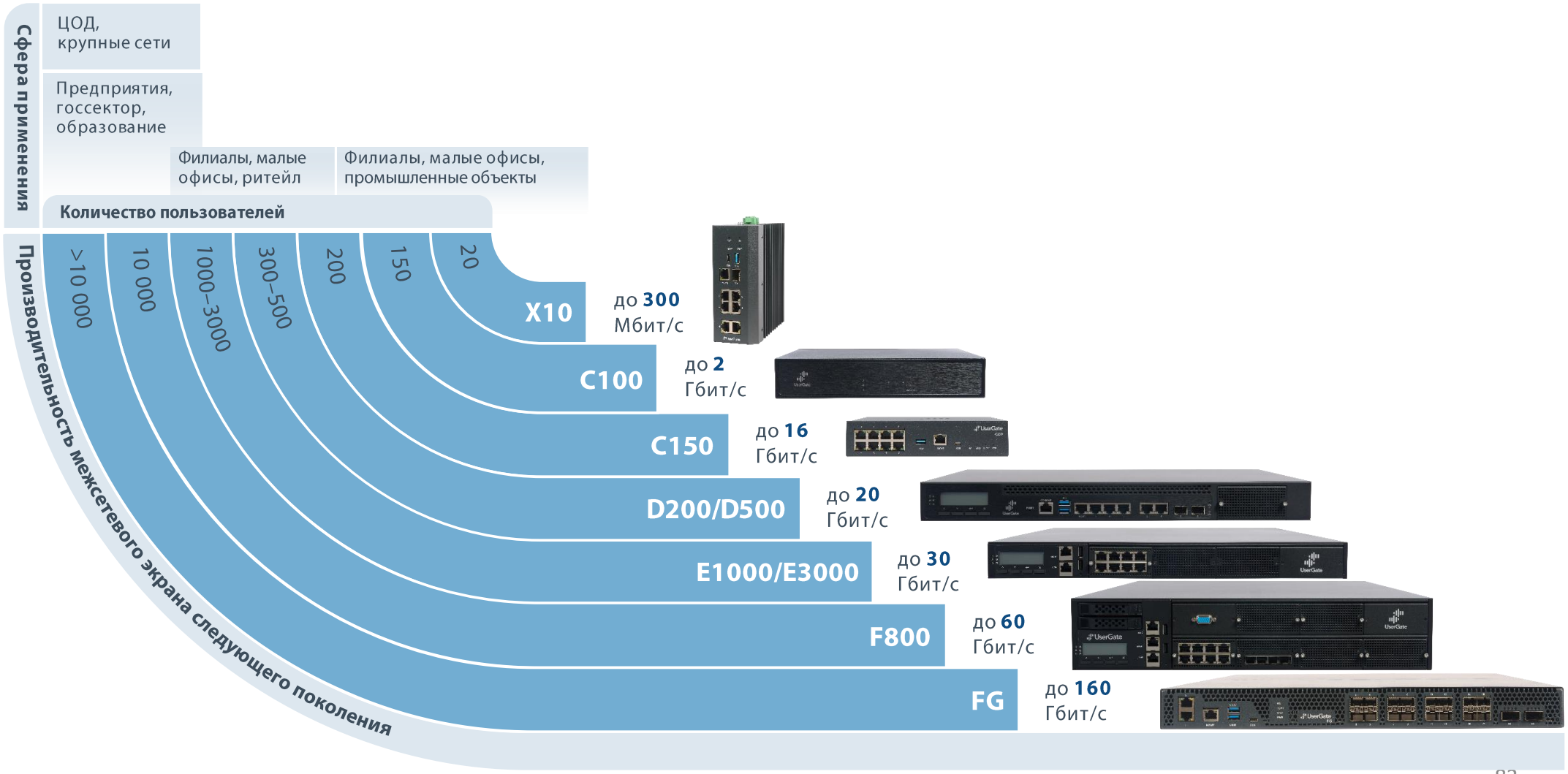
- может быть привязан к Active Directory;
- управляет политиками на устройстве;
- может быть настроен гранулярно, по профилю.


Офис
UserGate F8000 NGFW
UserGate Client
UserGate Client
Корпоративный Wi-Fi
Гостевой Wi-Fi
UserGate FG
ЦОД
ГИС
ИС
UserGate LogAn
100GIG
VM
Hyper-V
UserGate MC
VPN
ICS
UserGate NGFW
SPAN
Cell/Area
(Ring Thypology)
Controller
DIO
Drive
Cell/Area Zone
Levels 0-2
UserGate NGFW
VPN
VPN
VPN
VPN
UserGate Client
Удаленные пользователи
UserGate NGFW
Филиал 1
UserGate NGFW
Филиал 2

Платформы

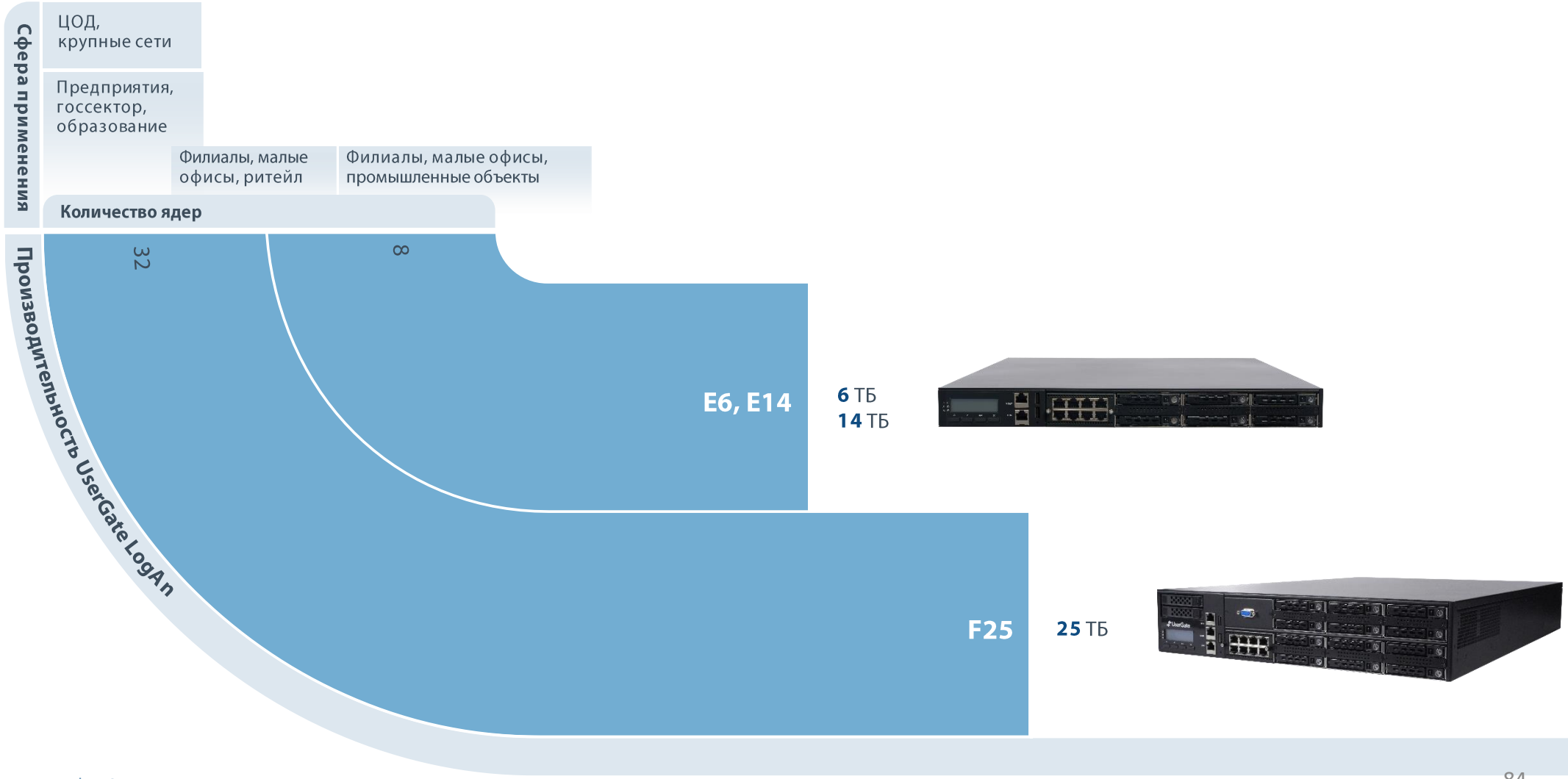
UserGate NGFW

Модельный ряд аппаратных платформ



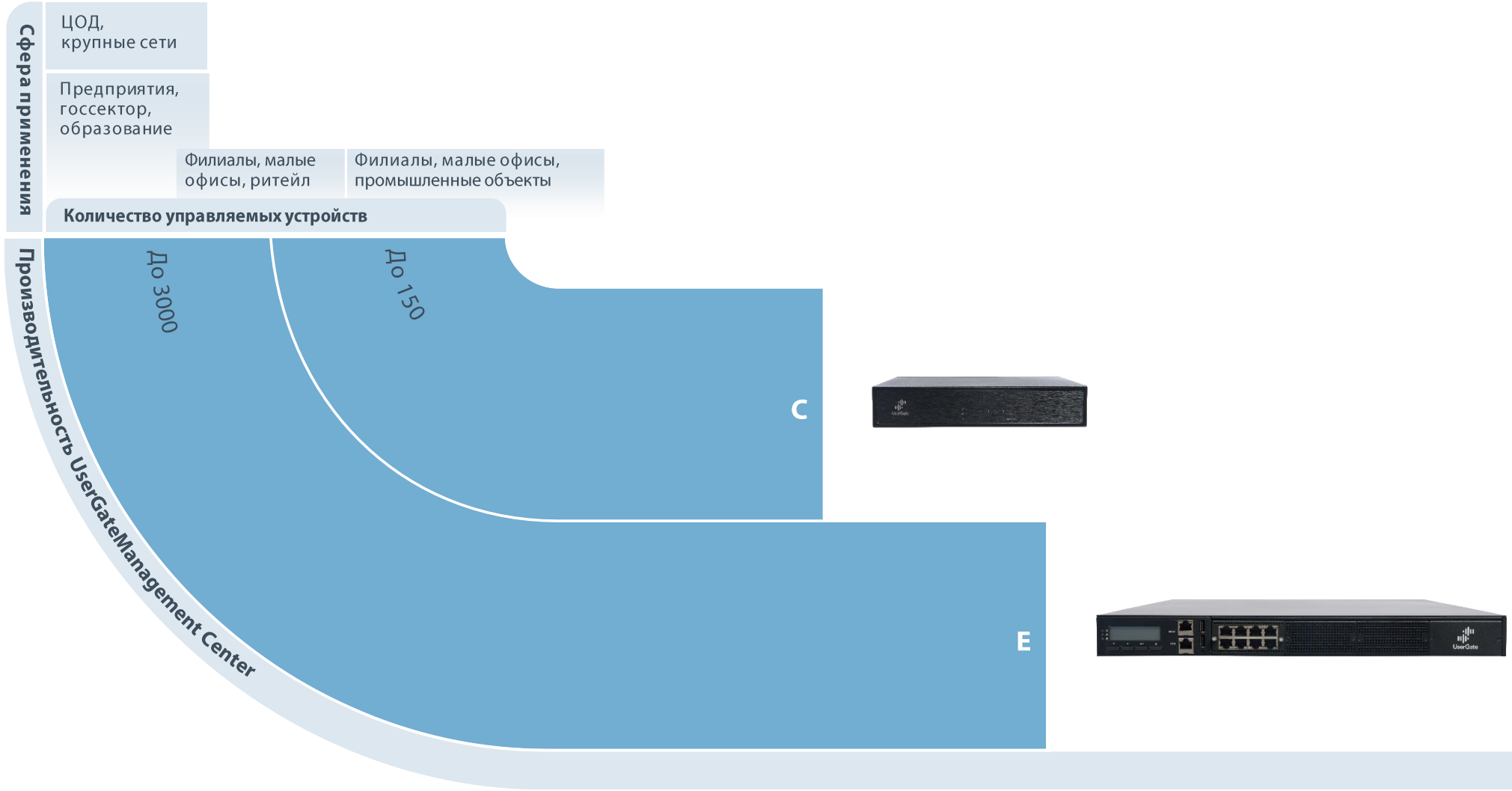
UserGate Log Analyzer

Модельный ряд аппаратных платформ

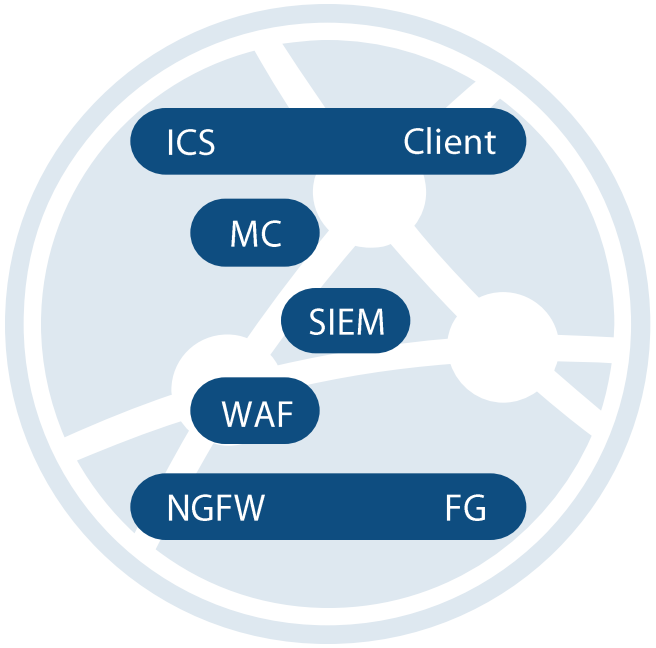


UserGate Management Center

Модельный ряд аппаратных платформ



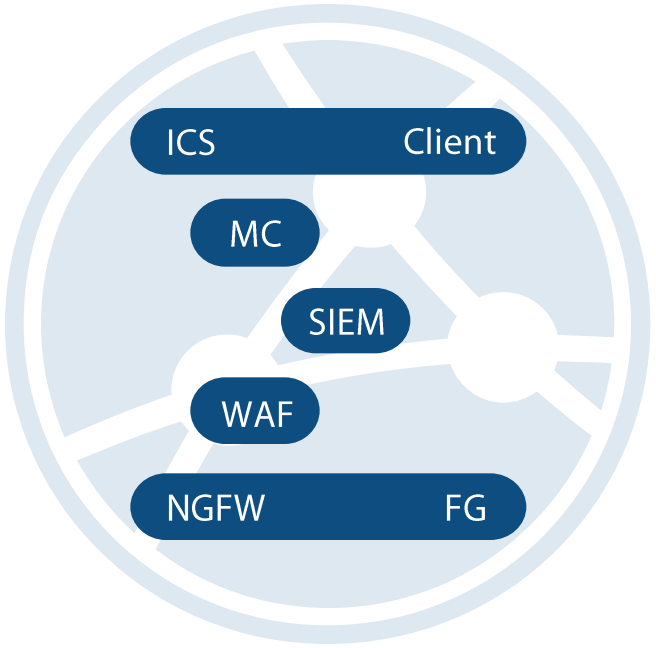
Все продукты UserGate SUMMA доступны в виртуальном исполнении



Гипервизоры:

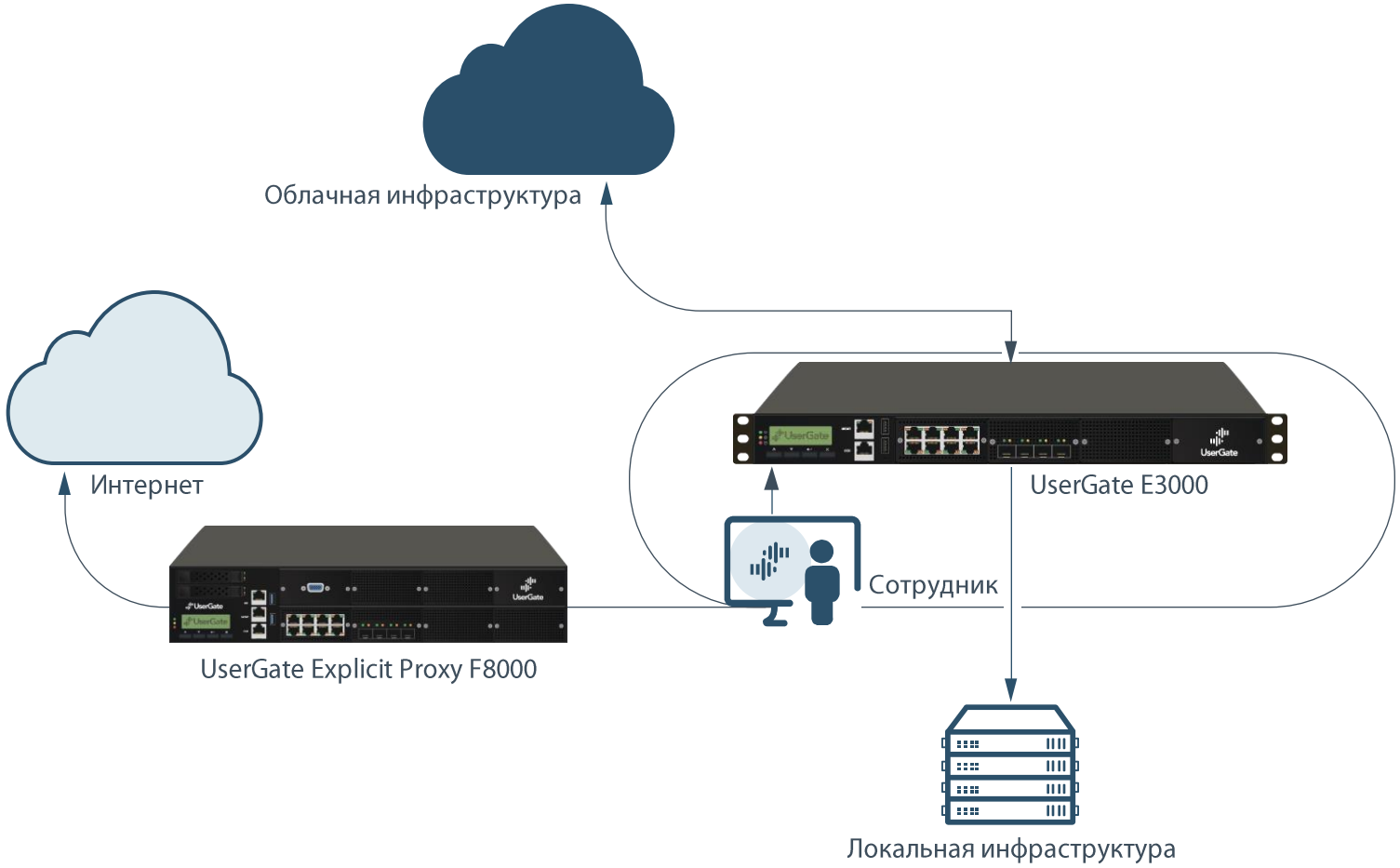
Xen
vmware
Hyper-V
БРЕСТ
ROS ПЛАТФОРМА
base alt
VirtualBox
openstack.
РЕД ВИРТУАЛИЗАЦИЯ
KVM
ГОРИЗОНТ-ВС ЦИФРОВОЕ БУДУЩЕЕ НАЧИНАЕТСЯ СЕГОДНЯ
zVirt

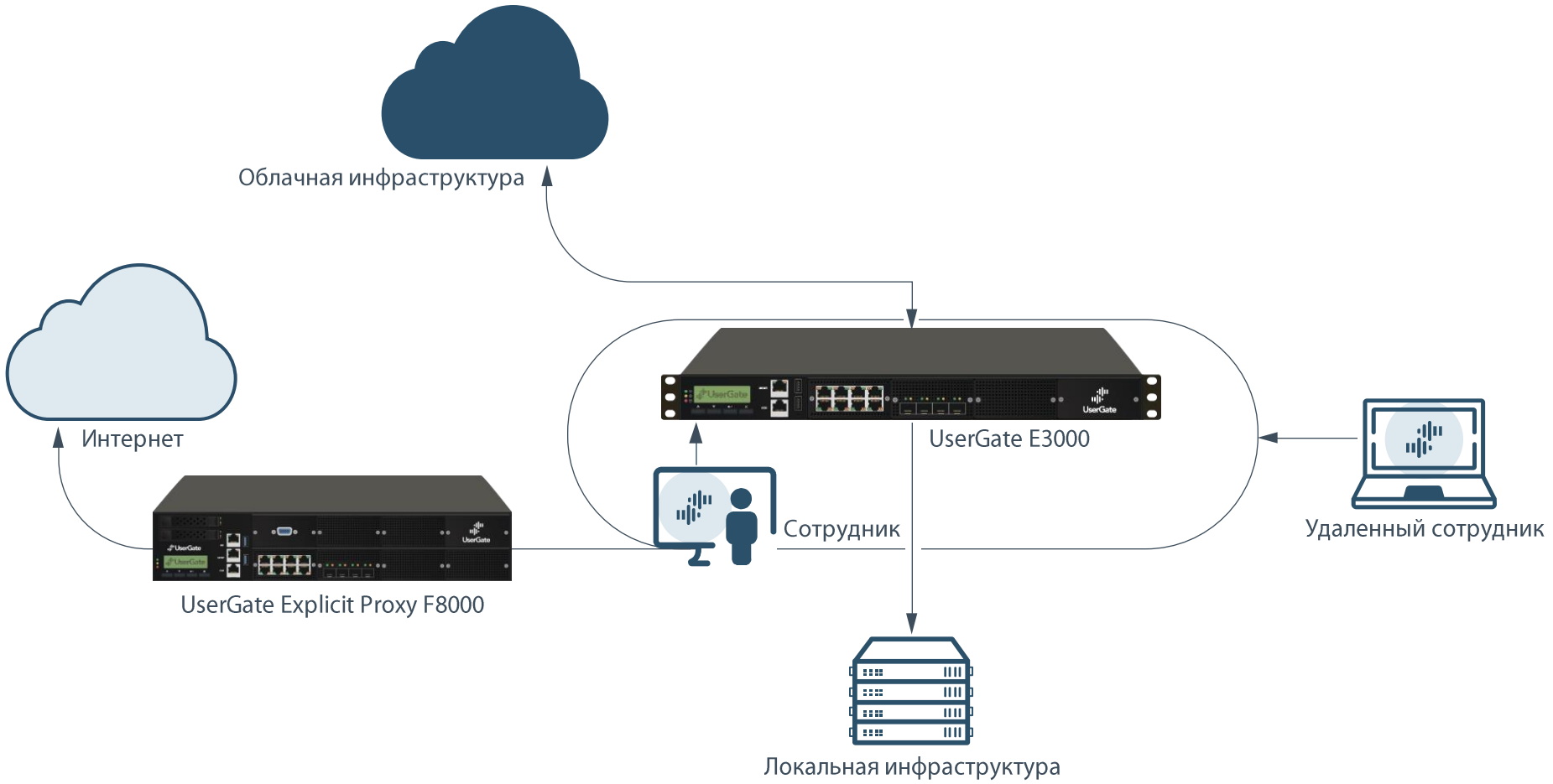
Все продукты UserGate SUMMA доступны в облачном исполнении

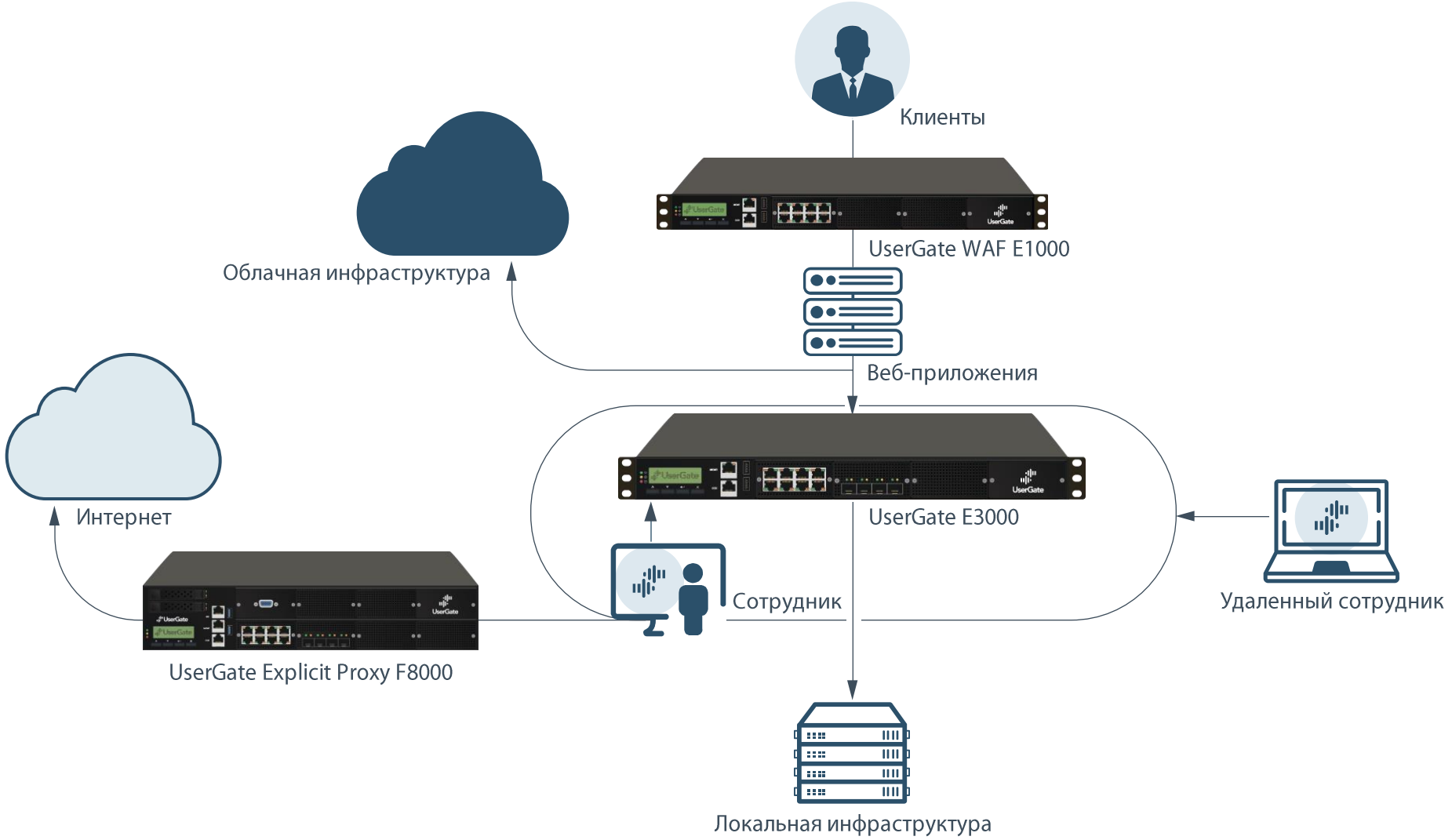


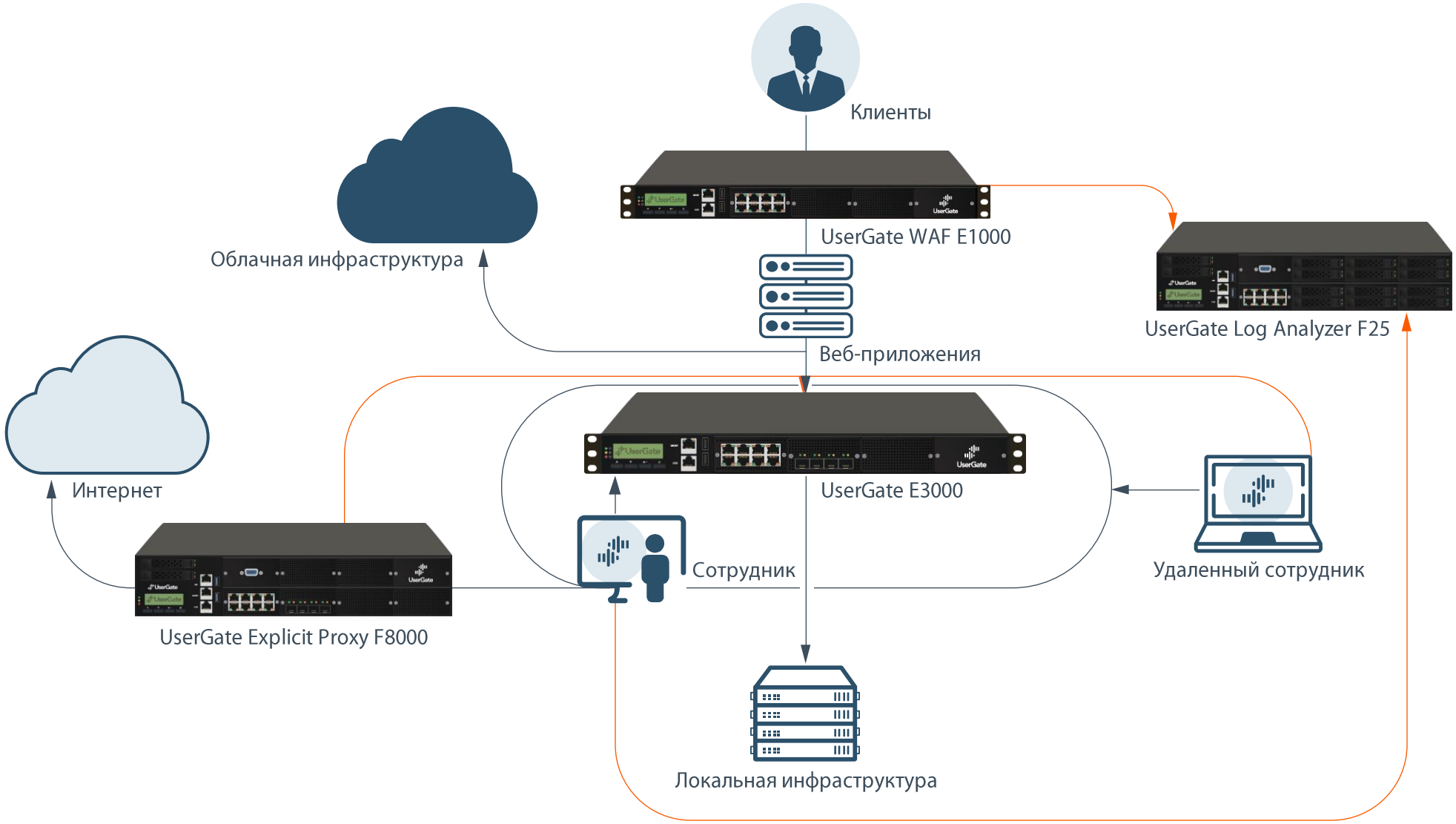
Yandex Cloud

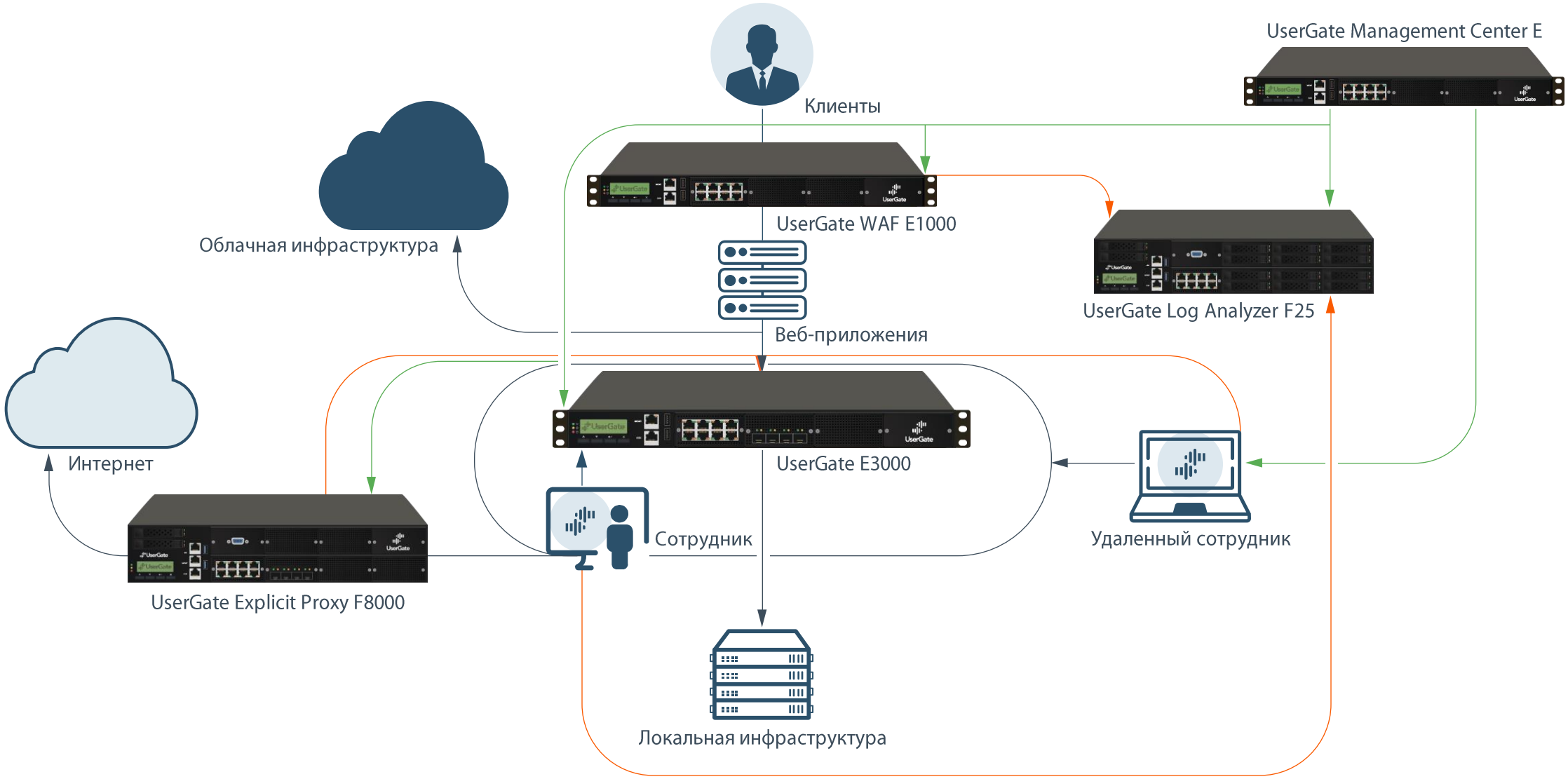
UserGate SUMMA


Облачная инфраструктура
Интернет
UserGate E3000
Сотрудник
UserGate Explicit Proxy F8000
Локальная инфраструктура


Облачная инфраструктура
Интернет
UserGate E3000
Удаленный сотрудник
Сотрудник
UserGate Explicit Proxy F8000
Локальная инфраструктура


Клиенты
Облачная инфраструктура
UserGate WAF E1000
Веб-приложения
Интернет
UserGate E3000
Сотрудник
Удаленный сотрудник
UserGate Explicit Proxy F8000
Локальная инфраструктура


Клиенты
Облачная инфраструктура
UserGate WAF E1000
UserGate Log Analyzer F25
Веб-приложения
Интернет
UserGate E3000
Сотрудник
Удаленный сотрудник
UserGate Explicit Proxy F8000
Локальная инфраструктура


UserGate Management Center E
Клиенты
Облачная инфраструктура
UserGate WAF E1000
UserGate Log Analyzer F25
Веб-приложения
Интернет
UserGate E3000
Сотрудник
Удаленный сотрудник
UserGate Explicit Proxy F8000
Локальная инфраструктура

Network Access Control

современная концепция безопасного доступа

Проблематика

Доступ с устройств к бизнес-инфраструктуре

Глубина проверок:

0 – внутри сети можно всем и везде;

1 – сегментирование на уровне подсетей и пользователей/групп;

2 – сегментирование на уровне приложений.

Проблема:

устройства не проверяются.

Цели и задачи NAC

Цели NAC

Network Access Control (NAC) –
– подход к построению системы защиты:

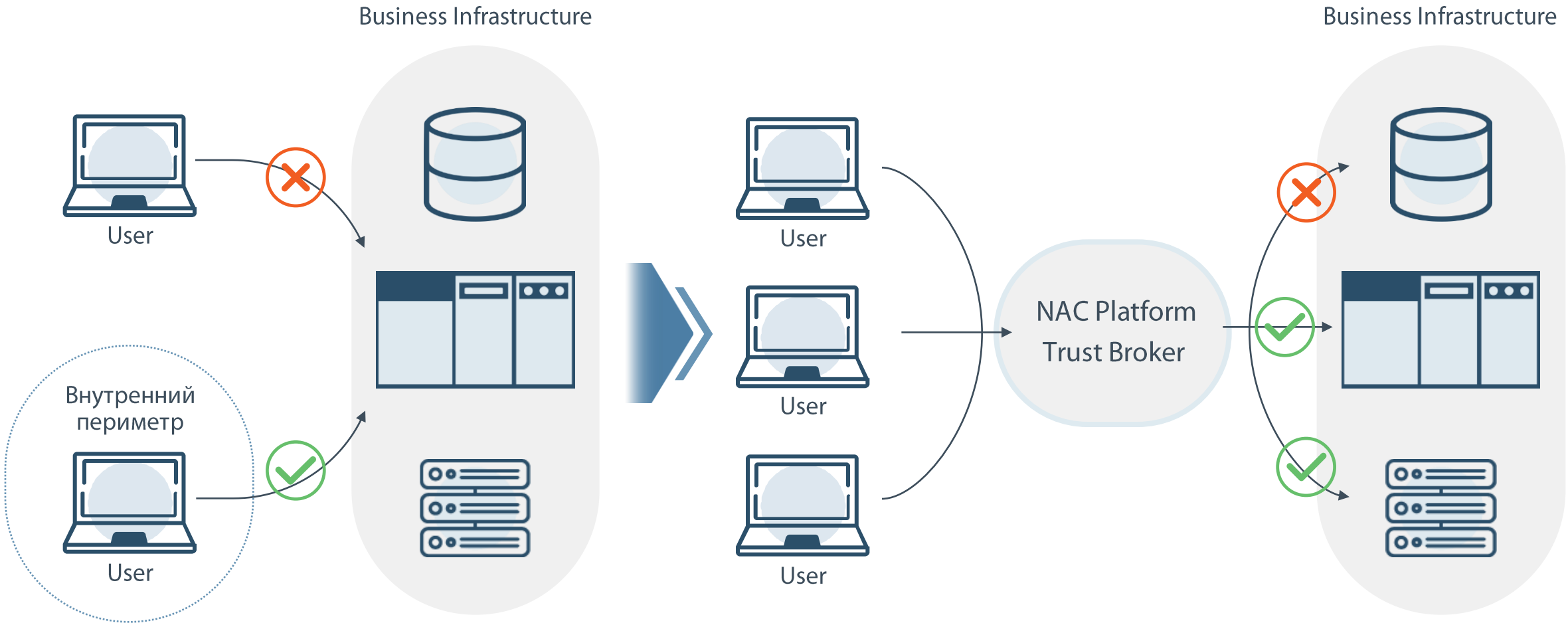
технологии безопасности конечных точек ⊕ аутентификация пользователя ⊕ сетевая безопасность

Цели NAC

- автоматизация с другими инструментами для определения сетевой роли на основе другой информации;
- управление идентификацией и доступом;
- проверка состояния безопасности после аутентификации.

Задача NAC

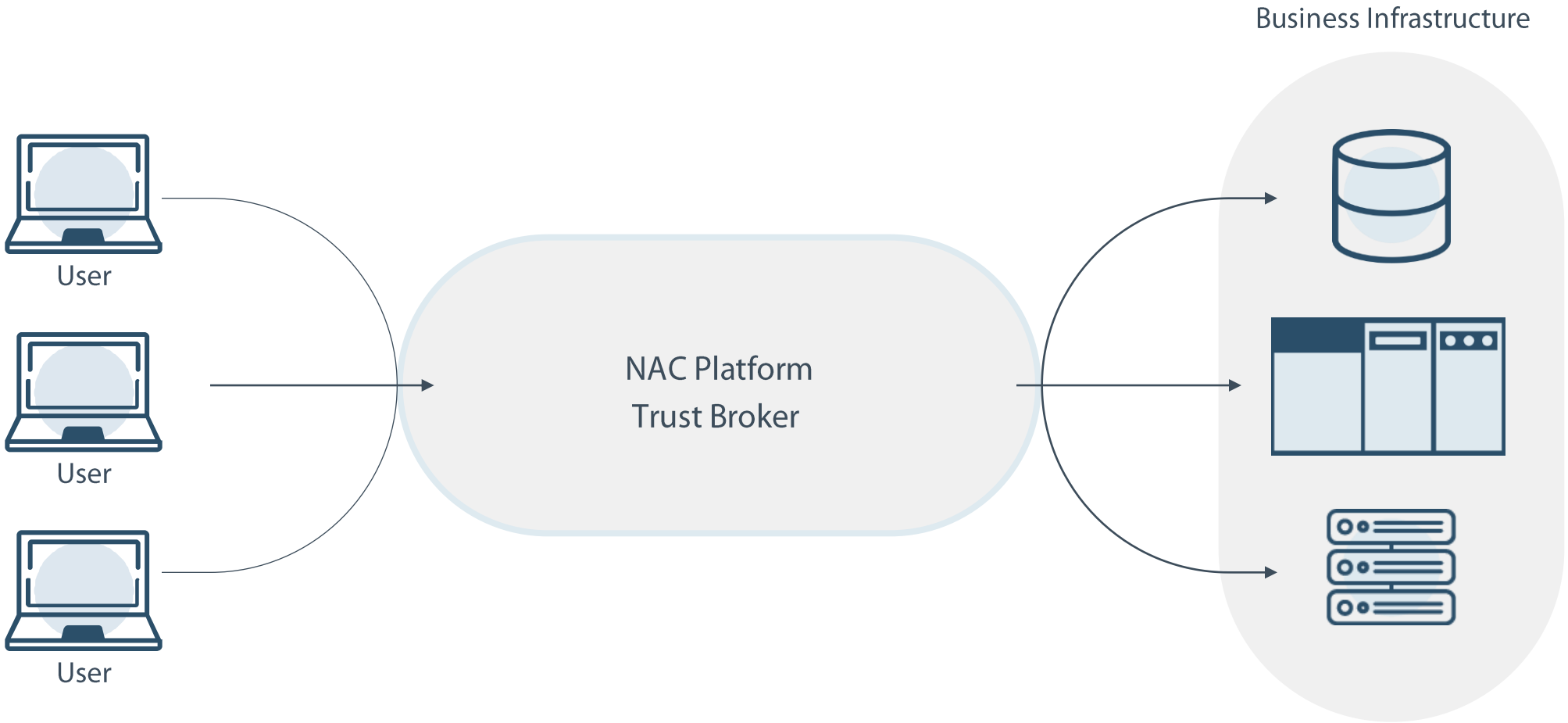
Заменить фактор доверенности нахождения
на фактор доверенности состояния устройства



Фактор доверенности нахождения

Фактор доверенности состояния устройства

Задача NAC


Business Infrastructure
User
User
User
NAC Platform
Trust Broker

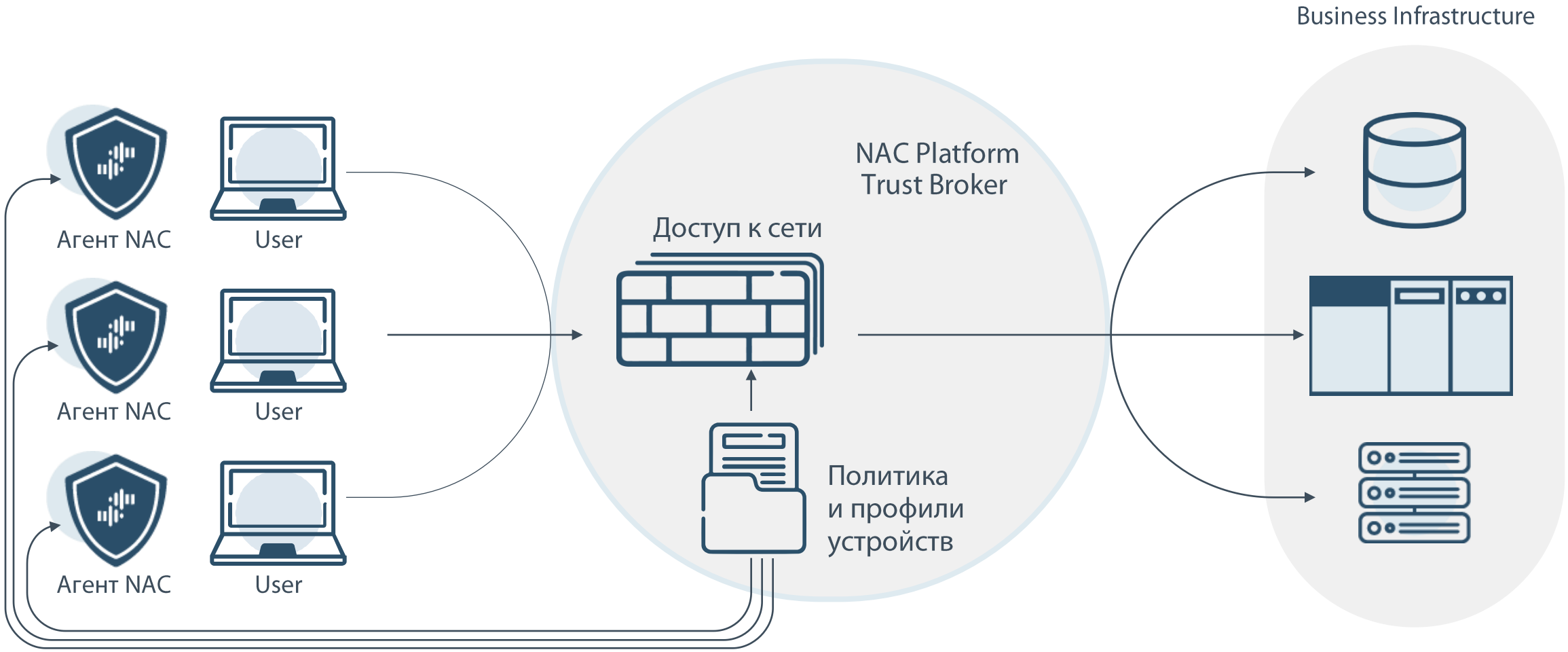
Бизнес-задачи

Разграничение доступа и предотвращение неправомерного доступа

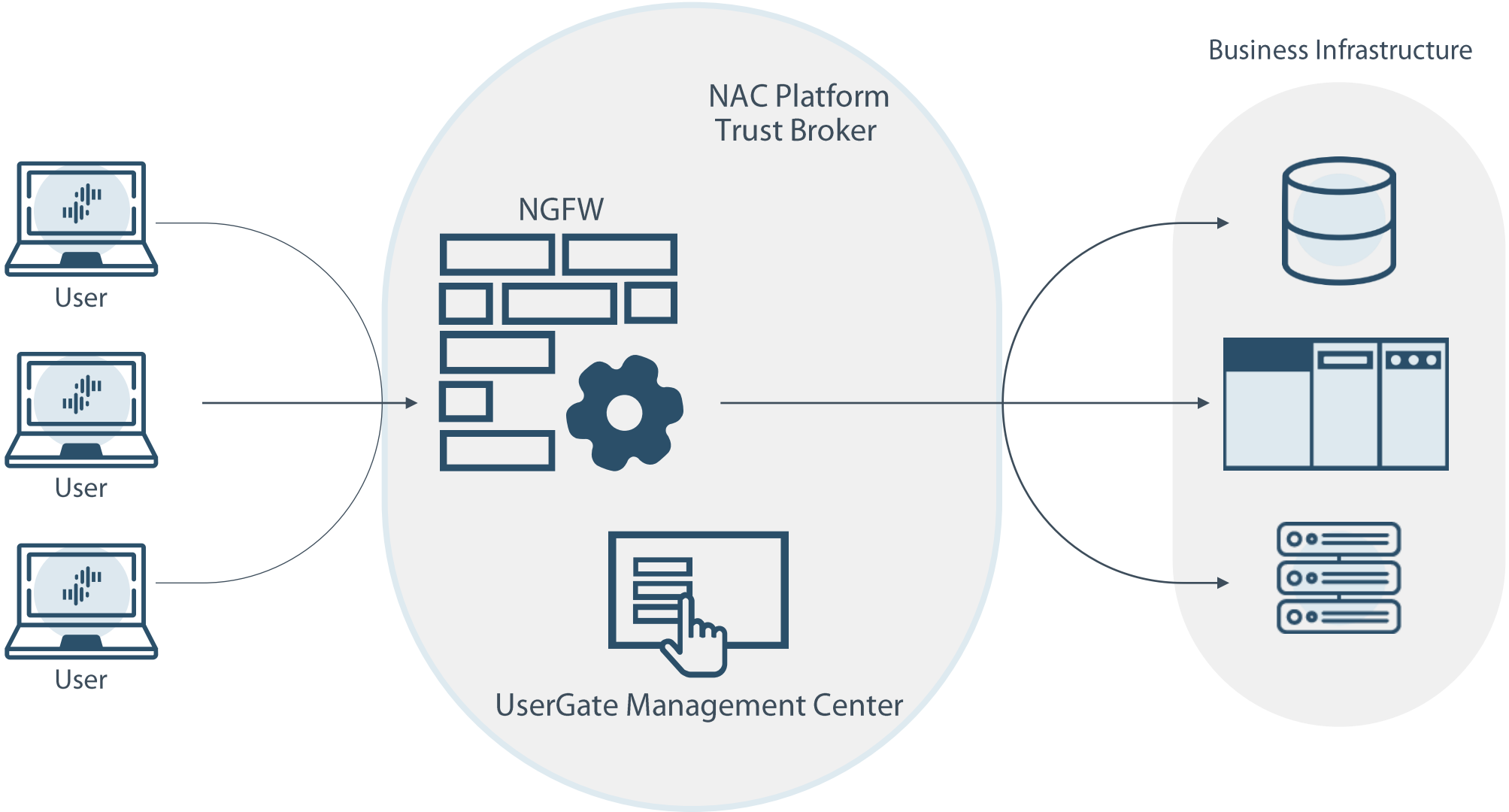
Удаленная работа

Подключение сотрудников к гибридной инфраструктуре

Схема реализации



UserGate SUMMA представляет NAC



ZTNA


NAC
Безопасность устройства
User Identification
Идентификация +
Аутентификация +
Авторизация
ZTNA
Context
Политики безопасности

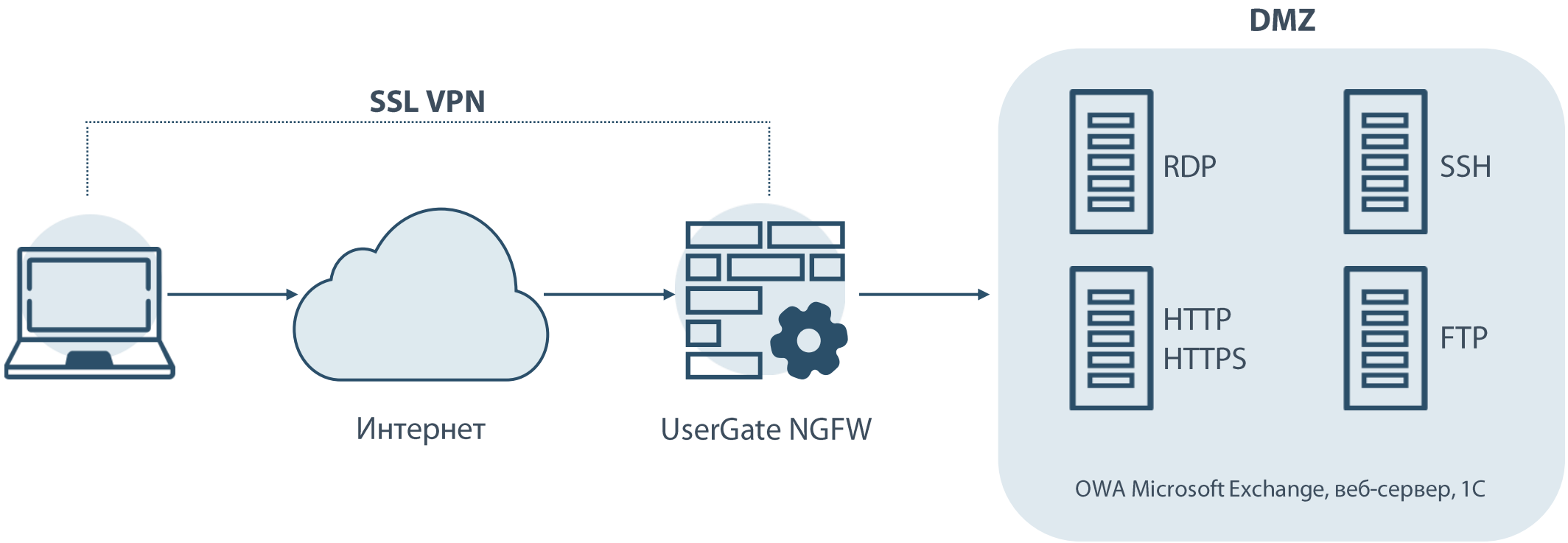
Безопасность удаленной работы

Проблематика

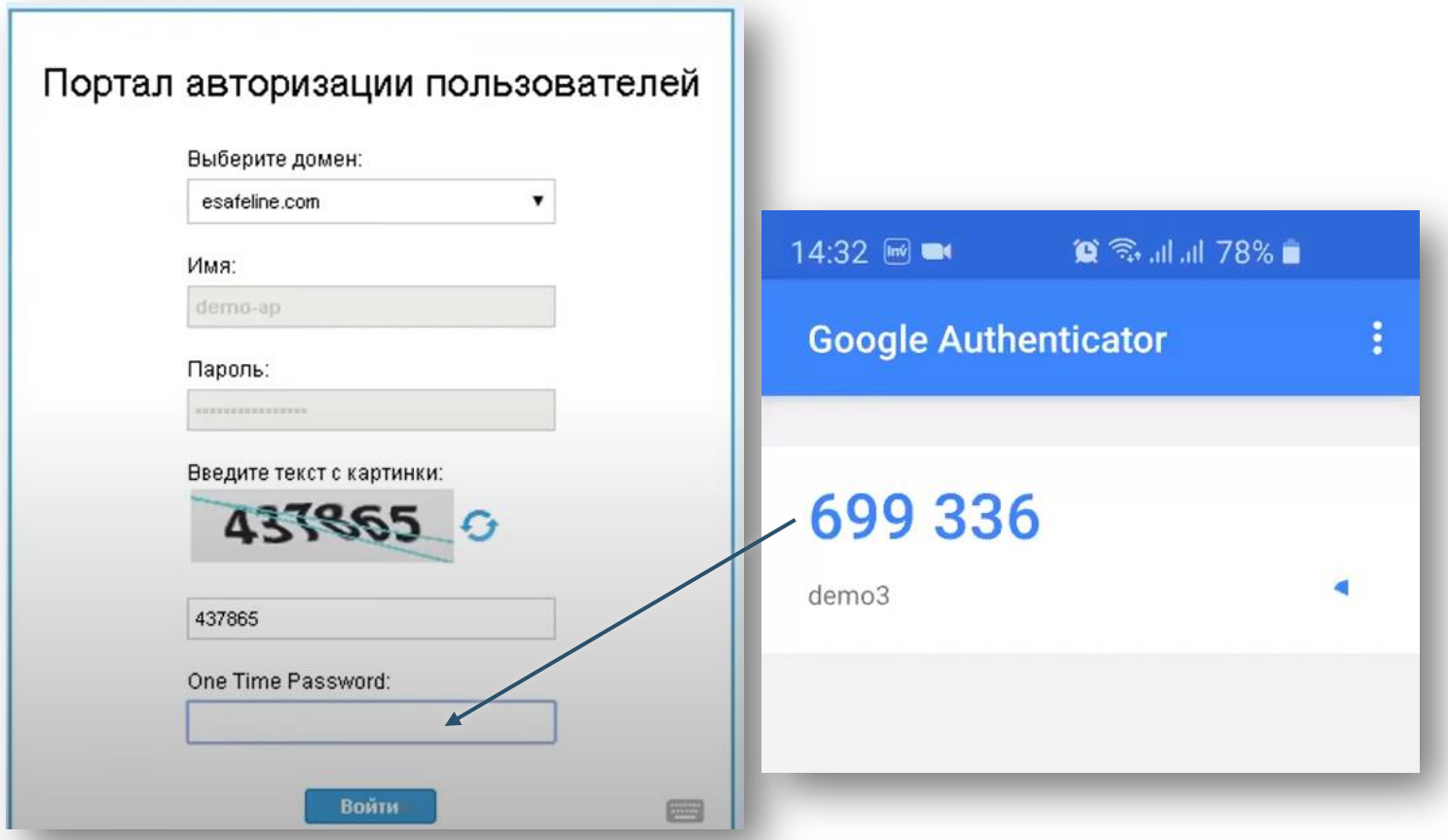
- доверие к удаленному сотруднику;
- неподконтрольность удаленного устройства;
- источник угроз для корпоративной сети.

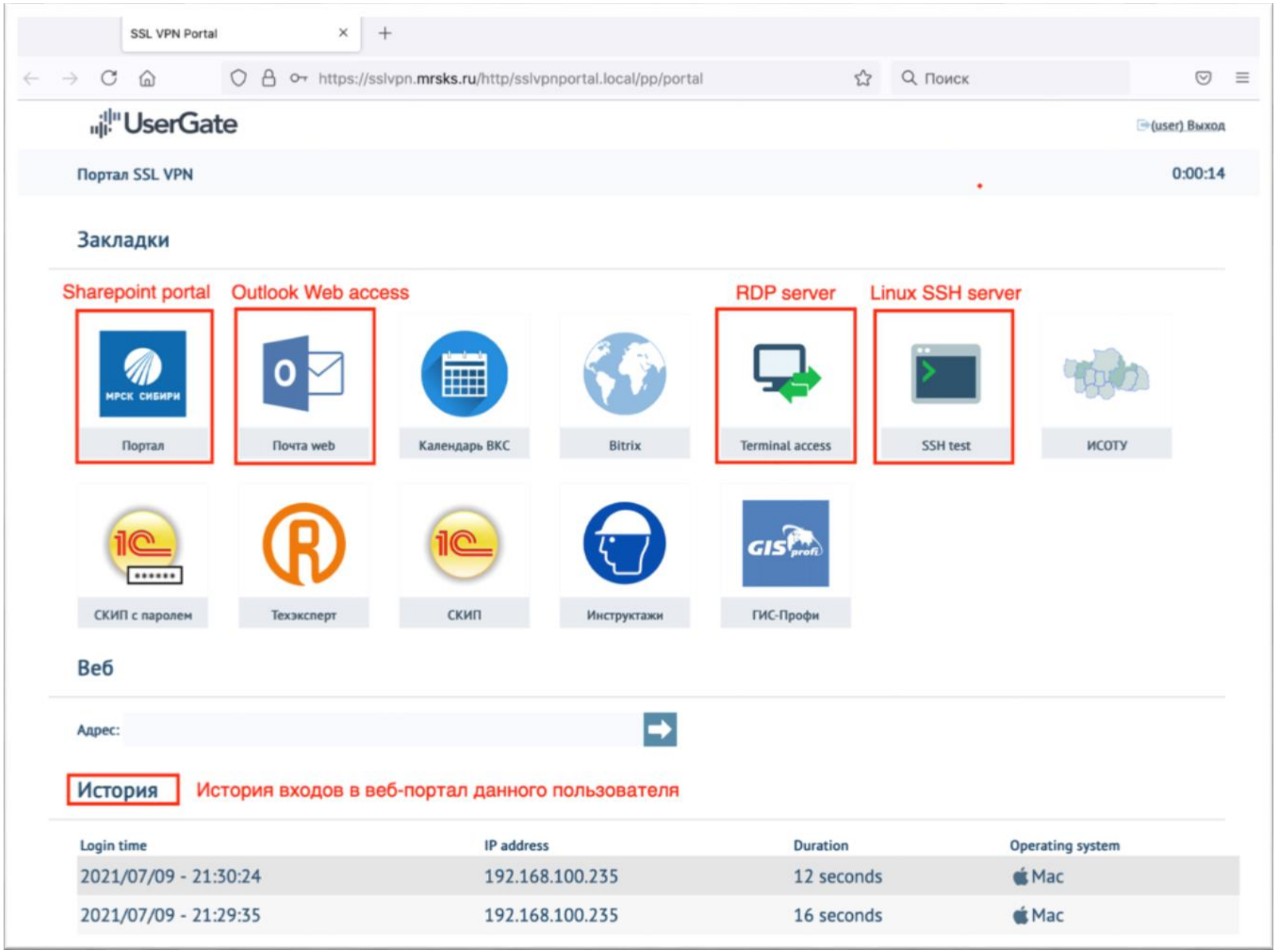
Решение

- сегментирование зоны с удаленными сотрудниками;
- изоляция приложений на уровне сети;
- построение безопасного подключения.


DMZ
SSL VPN
RDP
SSH
HTTP
HTTPS
FTP
Интернет
UserGate NGFW
OWA Microsoft Exchange, веб-сервер, 1С

- MFA (TOTP, SMS, e-mail);
- настройка политик доступа к отдельным сервисам по пользователям и группам;
- доступ через браузер;
- SSO.



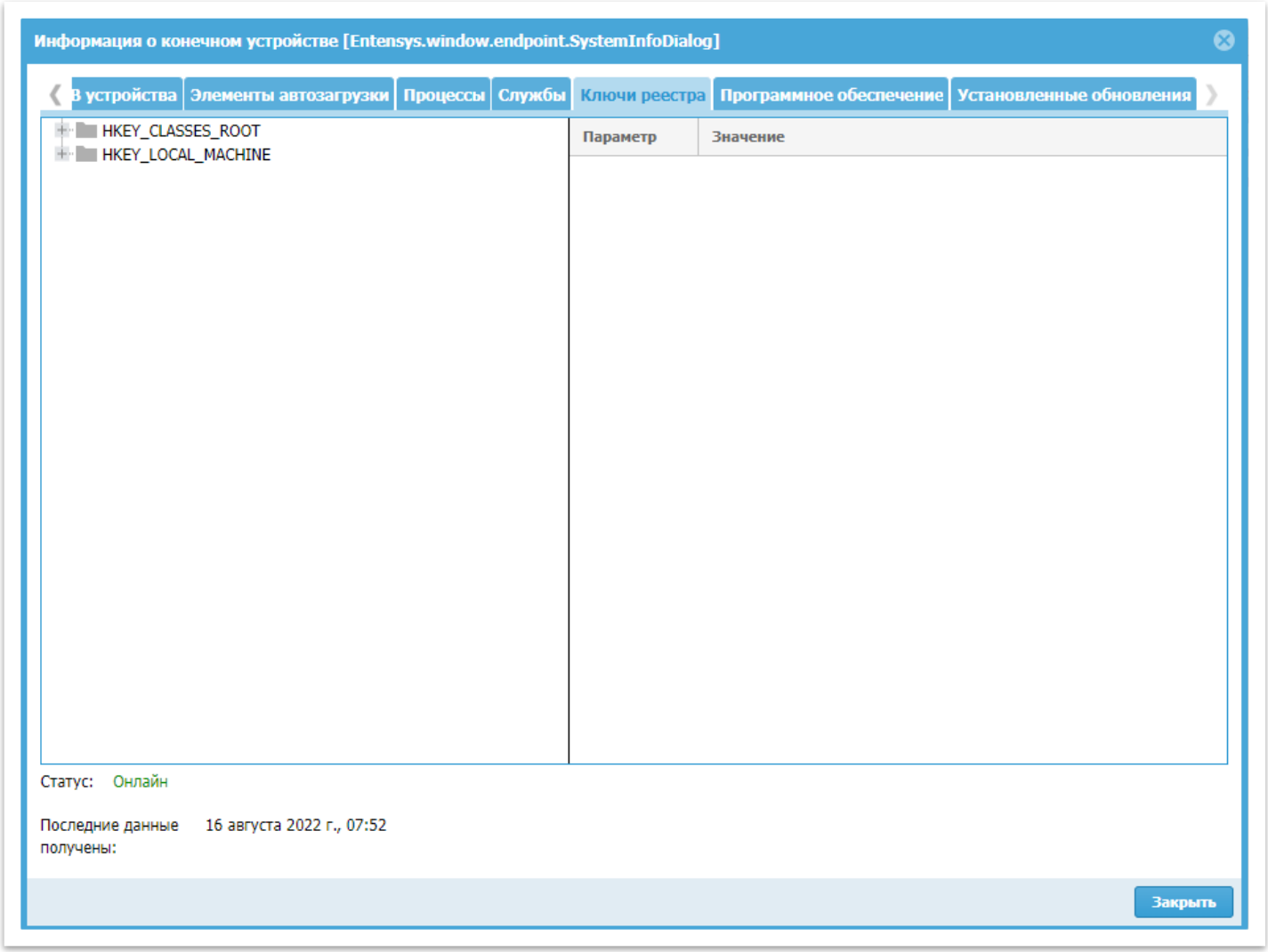

SSL VPN Portal
https://sslvpn.mrsks.ru/http/sslvpnportal.local/pp/portal
Поиск
UserGate
(user) Выход
Портал SSL VPN
0:00:14
Закладки
Sharepoint portal
Outlook Web access
RDP server
Linux SSH server
Портал
Почта web
Календарь ВКС
Bitrix
Terminal access
SSH test
ИСОТУ
СКИП с паролем
Техэксперт
СКИП
Инструктажи
ГИС-Профи
Веб
Адрес:
История
История входов в веб-портал данного пользователя
Login time
IP address
Duration
Operating system
2021/07/09 - 21:30:24
192.168.100.235
12 seconds
Mac
2021/07/09 - 21:29:35
192.168.100.235
16 seconds
Mac

Безопасность удаленного сотрудника

UserGate Client – агент SUMMA

- видимость событий безопасности;
- контроль устройства;
- доступ с нулевым доверием.

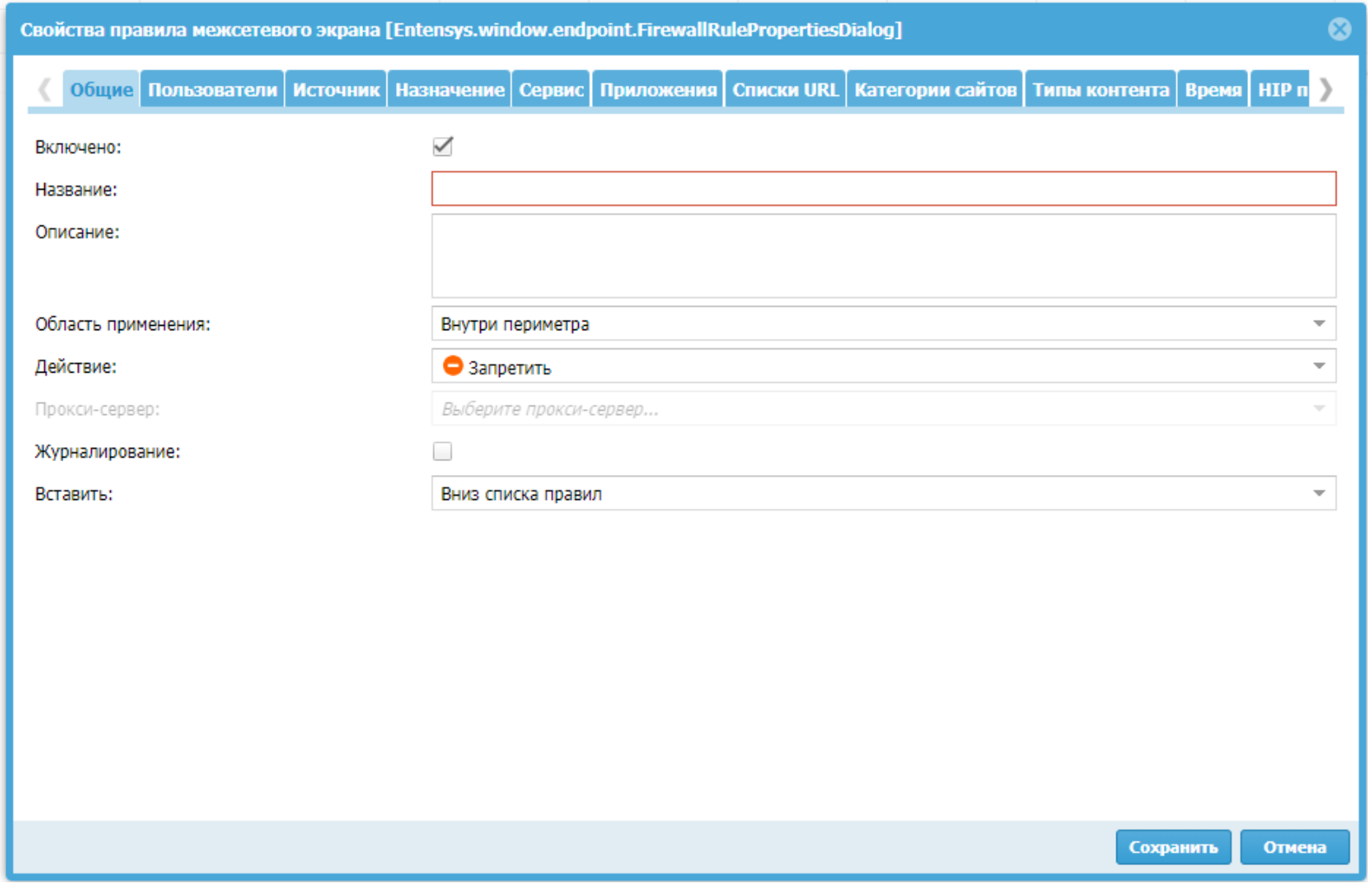
Сбор информации с устройства



Сбор информации с устройства

- состояние, память и производительность;
- безопасность;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- службы;
- ключи реестра;
- программное обеспечение;
- установленные обновления.

Персональный межсетевой экран



NAC

Профили устройств:

- продукт;
- процесс;
- запущенная служба;
- ключи реестра;
- установленные обновления.

VPN

- Client2Site – IPSec/L2TP, IKEv2;
- SSL VPN;
- «принудительный» VPN.

Экспертиза, IoC

Данные из логов, которые можно обогатить и найти следы компрометации:

- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

Нам доверяют








































Пилотирование UserGate

DEMO

Отправьте заявку на пилотирование или
запросите демонстрацию решений UserGate

sales@usergate.ru
8 (800) 500-40-32

UserGate

Спасибо за внимание!

8 800 500 4032
sales@usergate.ru