TechDay

Экосистема UserGate SUMMA

Дмитрий Аловацкий

Ведущий менеджер по работе с корпоративными заказчиками

dalovatsky@usergate.com

+7 (913) 750 63 90

О компании 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

2018
создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2019
открытие первого московского офиса UserGate

2020
открытие офиса UserGate в Хабаровске

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

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»

UserGate SUMMA

100% видимость событий безопасности

- АСУ ТП
- Удаленные пользователи
- Управление
- Анализ
- Веб-сервисы
- ЦОД
- Сети

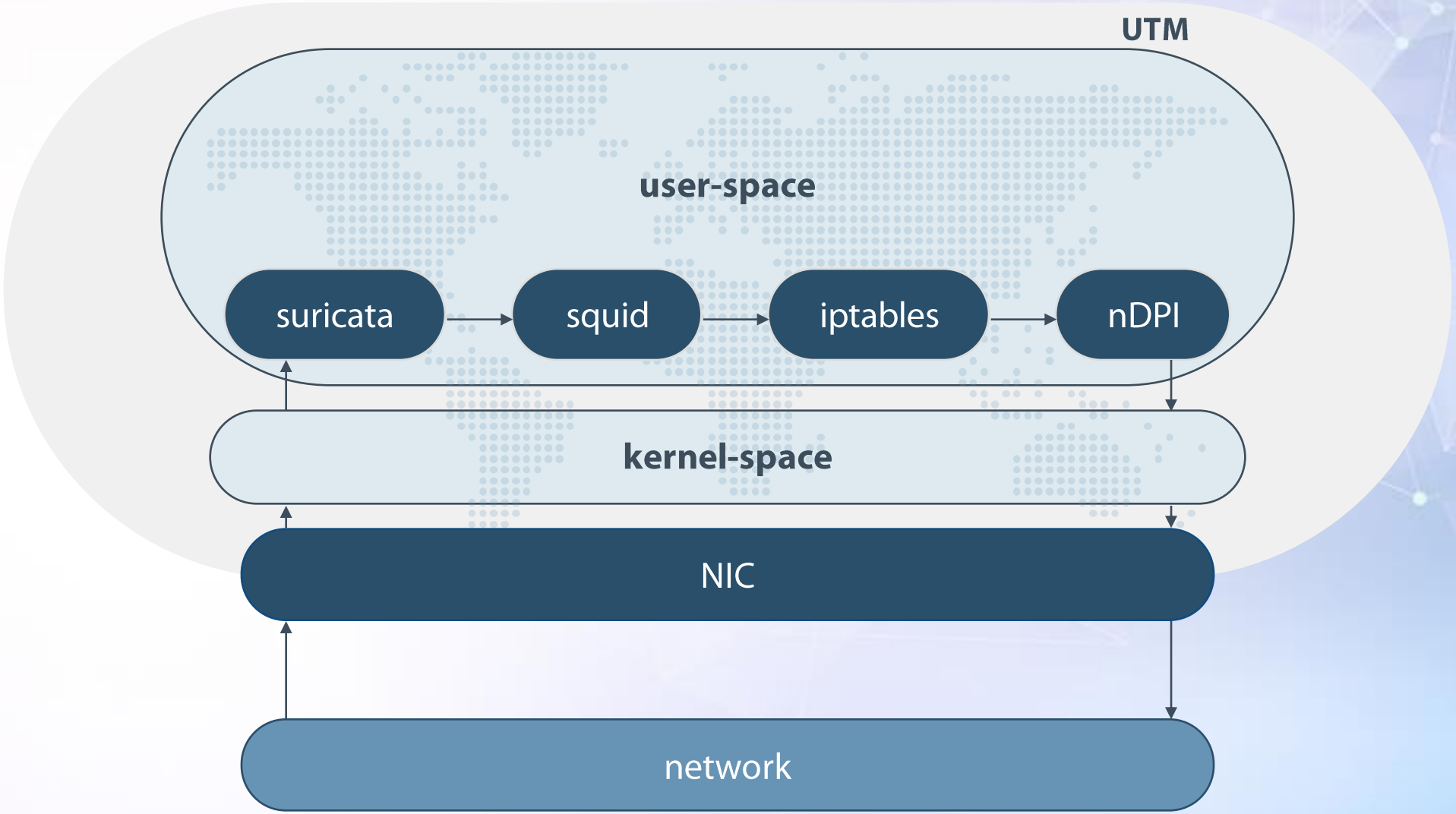
UserGate

TechDay

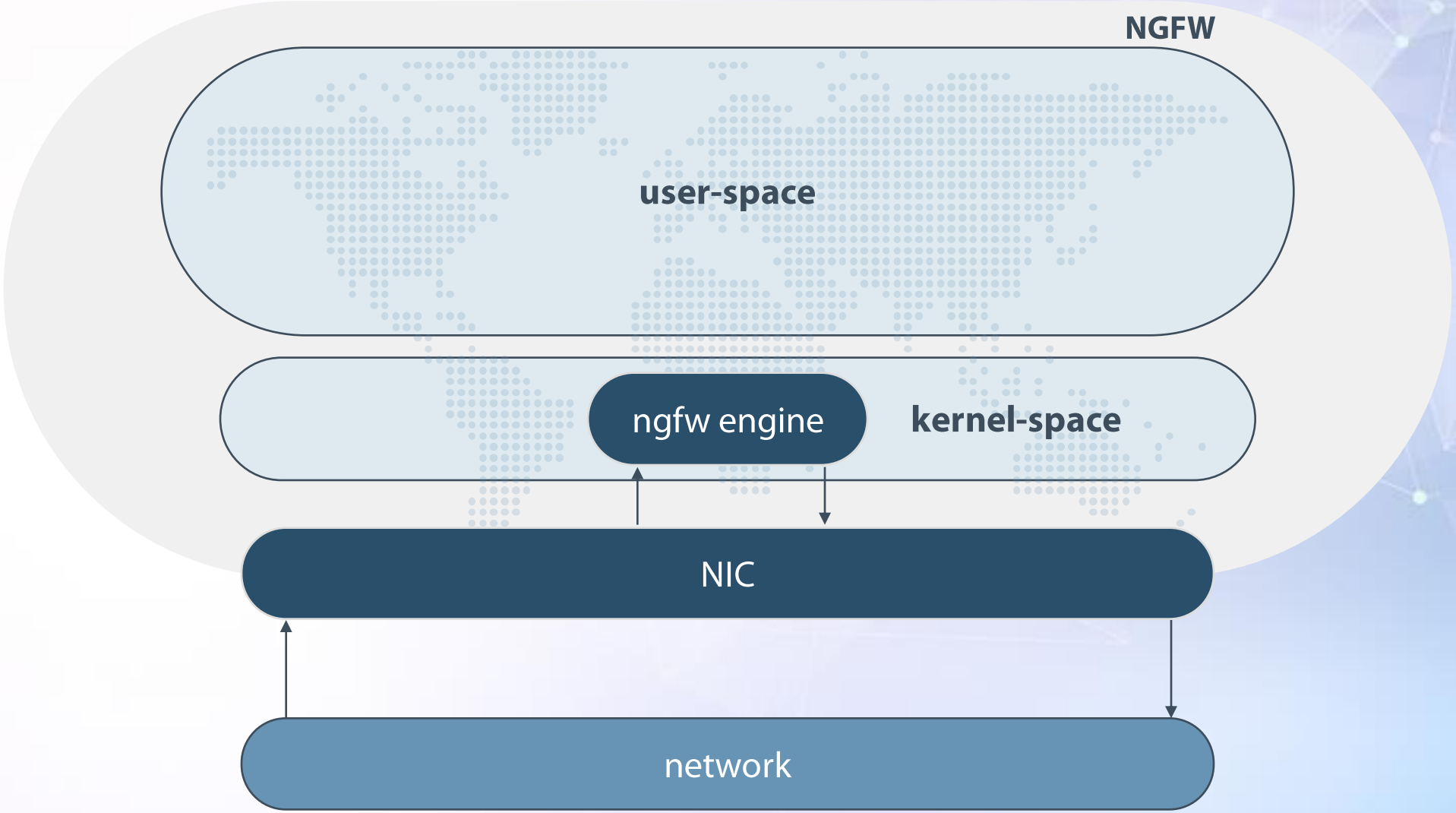
UserGate NGFW

Межсетевой экран следующего поколения

UTM


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

NGFW

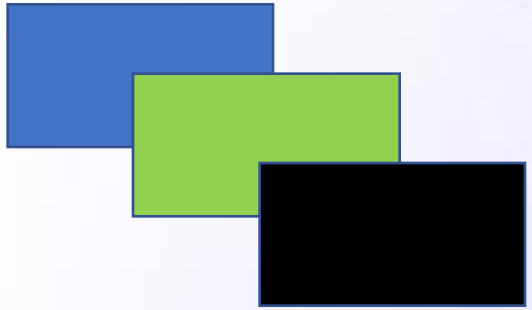


	Чужие платформы	Свои платформы
Проприетарное ПО		
Open-source		

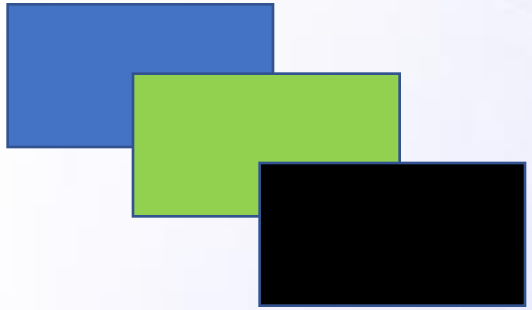
	Чужие платформы	Свои платформы
Проприетарное ПО		CISCO, HUAWEI, paloalto NETWORKS, FORTINET
Open-source		

TECHDAY

	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		

TECHDAY

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

UserGate

TechDay

Выбор правильного пути развития вендора

Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

CHECK POINT

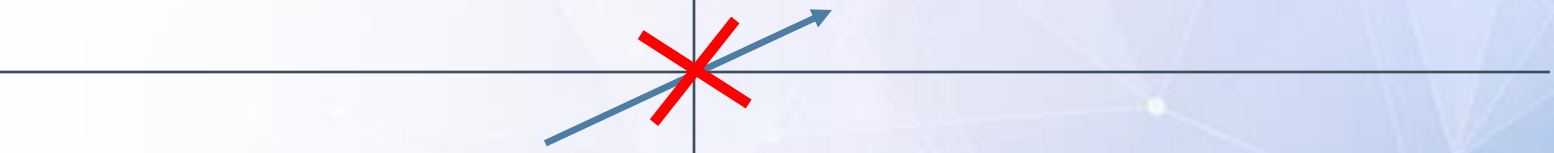
UserGate

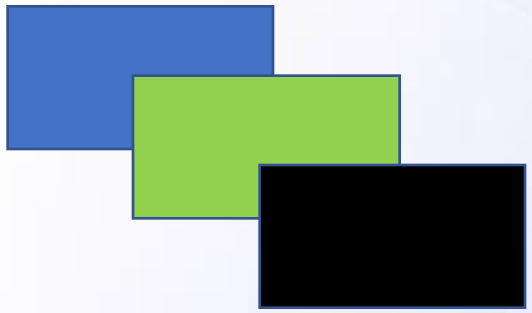
CISCO

HUAWEI

paloalto NETWORKS

FORTINET





TECHDAY

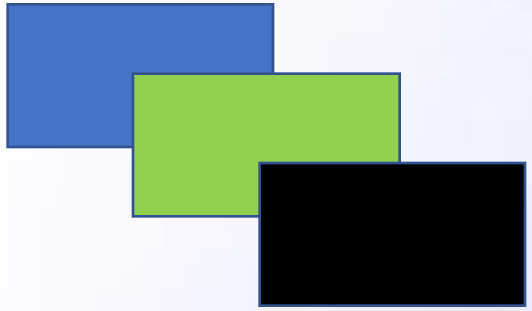
Чужие платформы

Свои платформы

Проприетарное ПО

Open-source

CHECK POINT



UserGate

CISCO

HUAWEI

paloalto NETWORKS

FORTINET

TECHDAY

UserGate

TECHDAY

Новое в 7.0

Новое в 7.0

- CLI
- Новая система бэкапов (без перезагрузки)
- SSL Forwarding
- UserGate Policy Language
- Новая архитектура процессоров - новые платформы
- Новый движок IPS

TECHDAY

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 _
```

Новые платформы

FG

C150

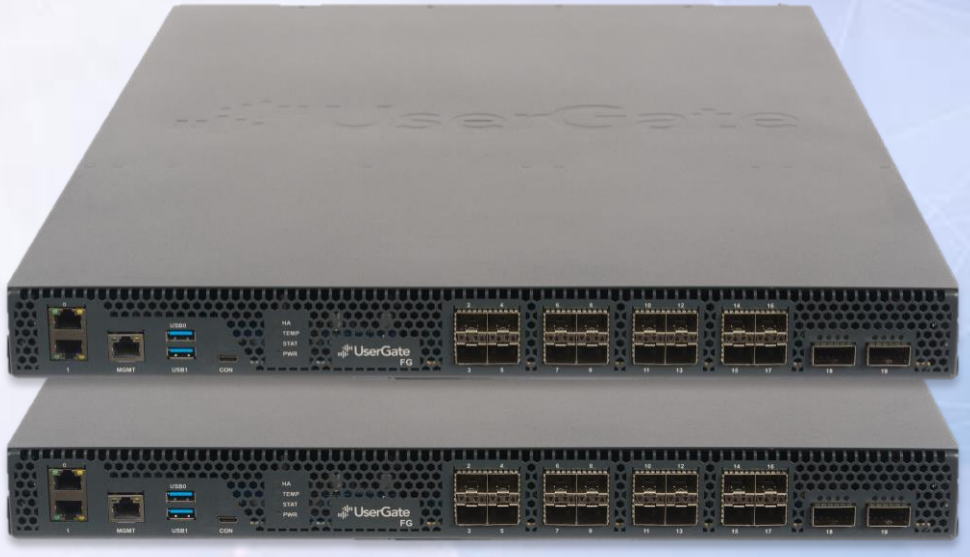
B50

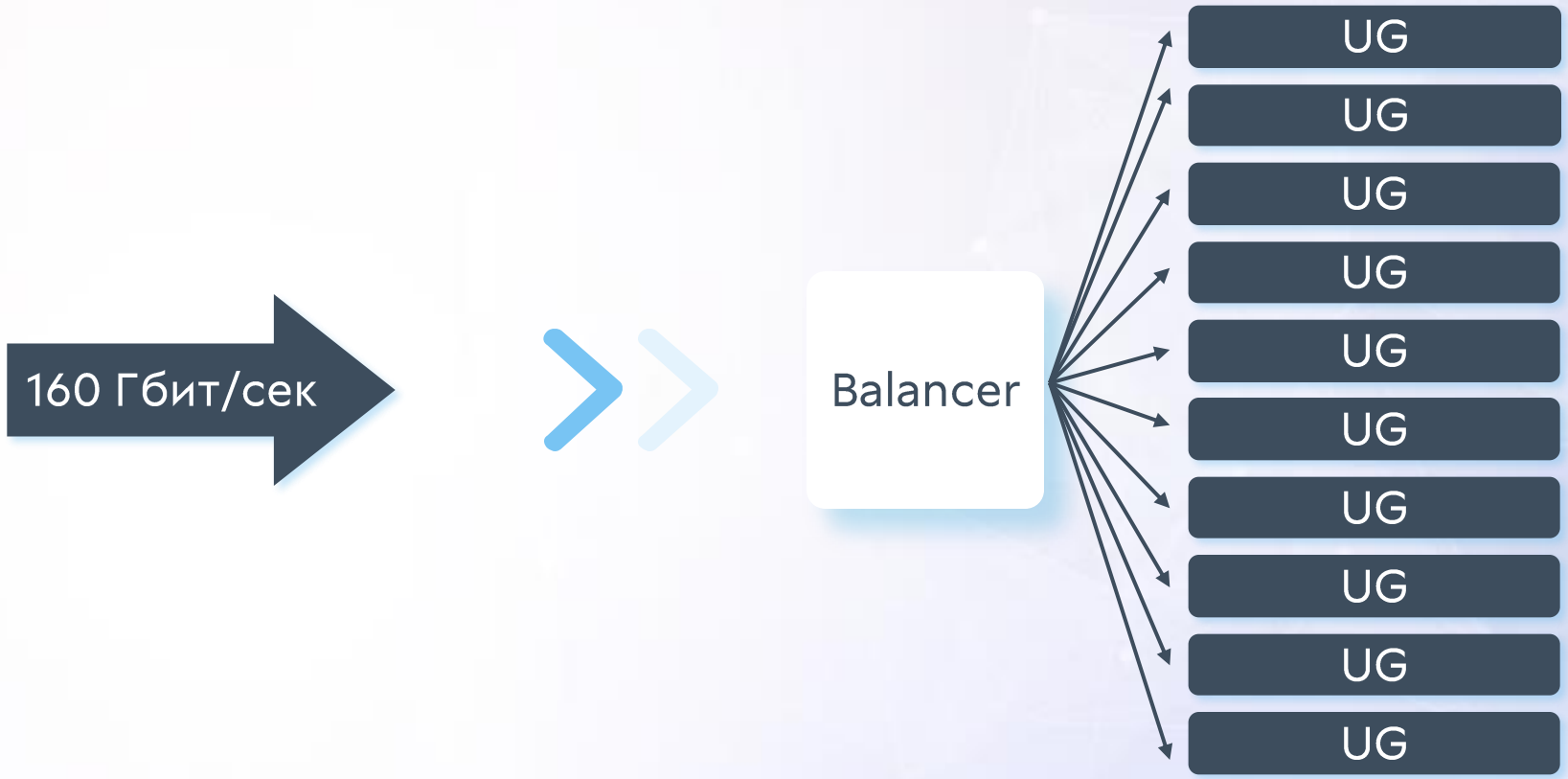
UserGate FG

- 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

2x100 + 16x10, wirespeed

Стекирование



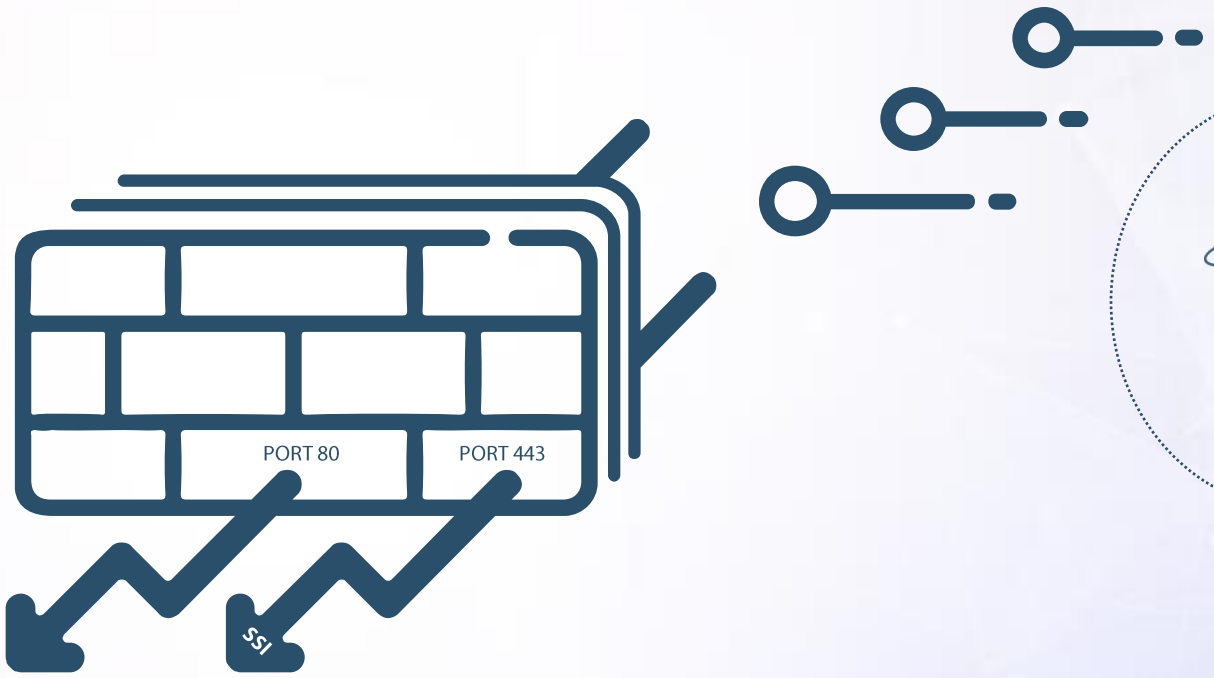

160 Гбит/сек
Balancer
UG
UG
UG
UG
UG
UG
UG
UG
UG
UG

UserGate

TECHDAY

Перейдем от общего к частному

NGFW


PORT 80
PORT 443
SSL


kaspersky
Yandex
Gmail
by Google
Viber
Яндекс.Диск
zoom
eset
@mail.ru
Microsoft
OfficeUpdate
ssh
COMMUNICATIONS SECURITY
AMMYY
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.

UserGate

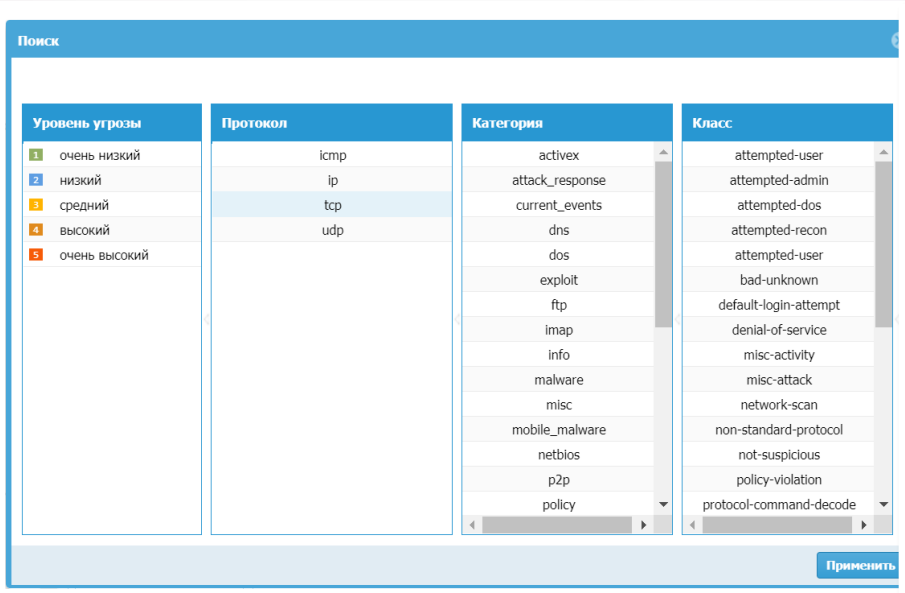
TECHDAY

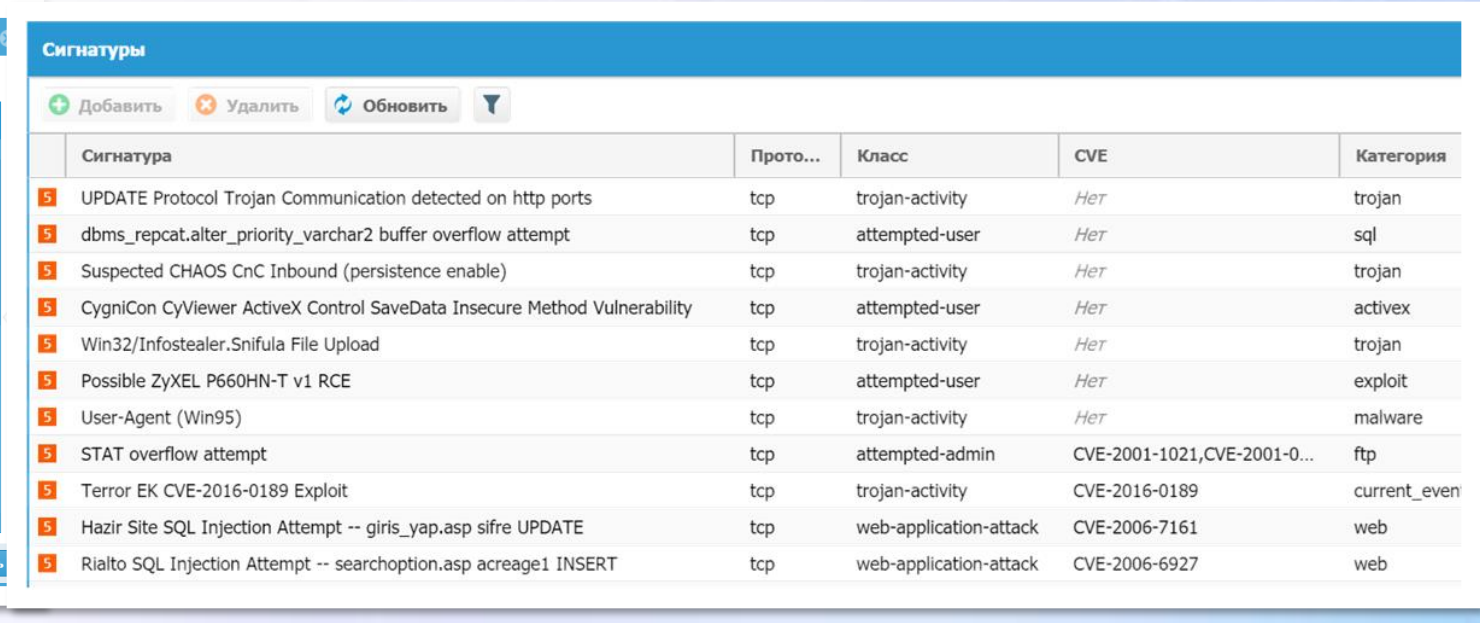
UserGate IDPS (СОВ)

Модуль в составе UserGate NGFW

Система обнаружения вторжений

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





Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon CyViewer ActiveX Control SaveData Insecure Method Vulnerability	tcp	attempted-user	Нет	activex
Win32/Infostealer.Snifula File Upload	tcp	trojan-activity	Нет	trojan
Possible ZyXEL P660HN-T v1 RCE	tcp	attempted-user	Нет	exploit
User-Agent (Win95)	tcp	trojan-activity	Нет	malware
STAT overflow attempt	tcp	attempted-admin	CVE-2001-1021,CVE-2001-0...	ftp
Terror EK CVE-2016-0189 Exploit	tcp	trojan-activity	CVE-2016-0189	current_even
Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UPDATE	tcp	web-application-attack	CVE-2006-7161	web
Rialto SQL Injection Attempt -- searchoption.asp acreage1 INSERT	tcp	web-application-attack	CVE-2006-6927	web

UserGate

TECHDAY

Контент-фильтрация

Модуль в составе UserGate NGFW

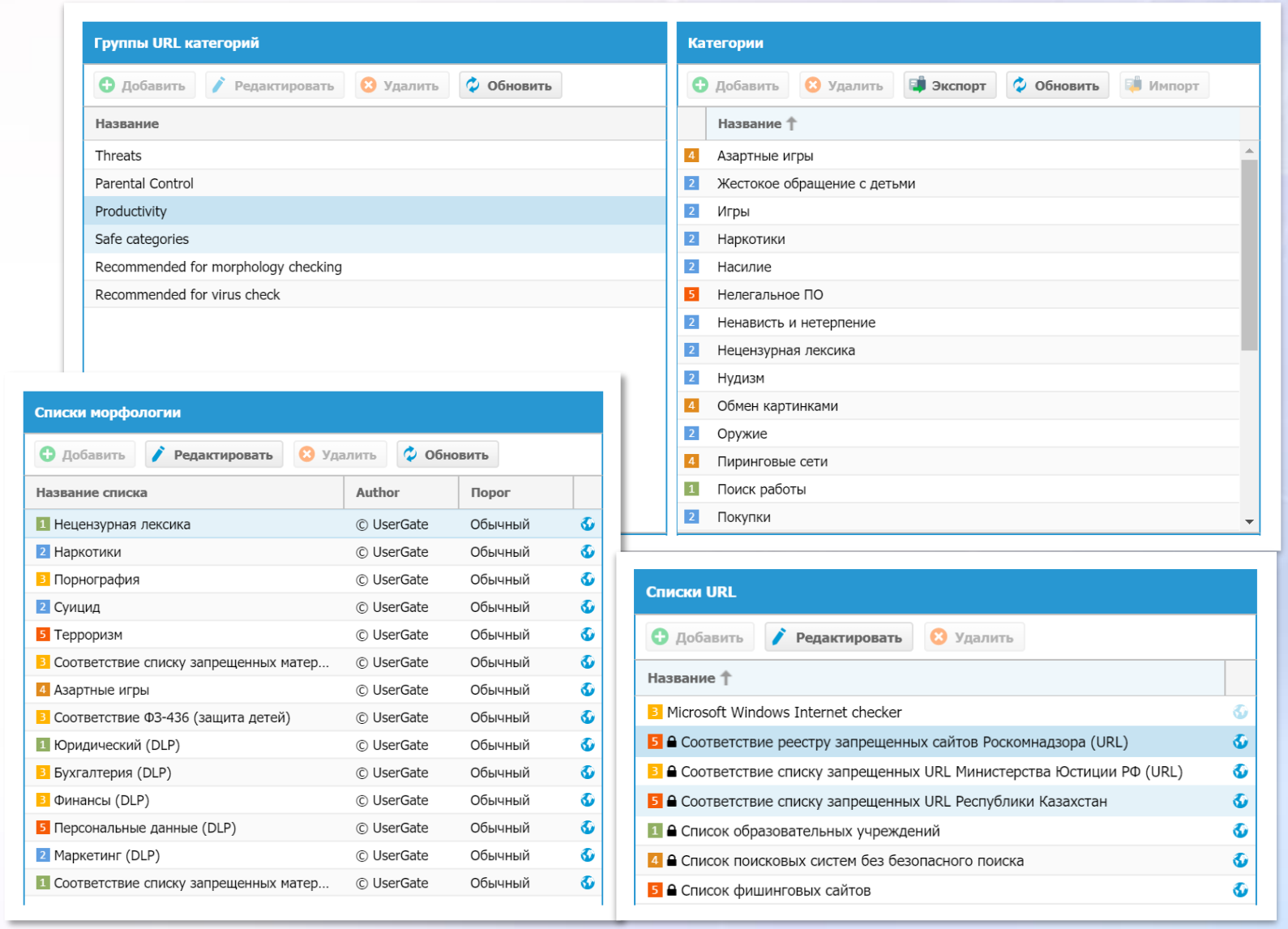
Механизмы фильтрации

- 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

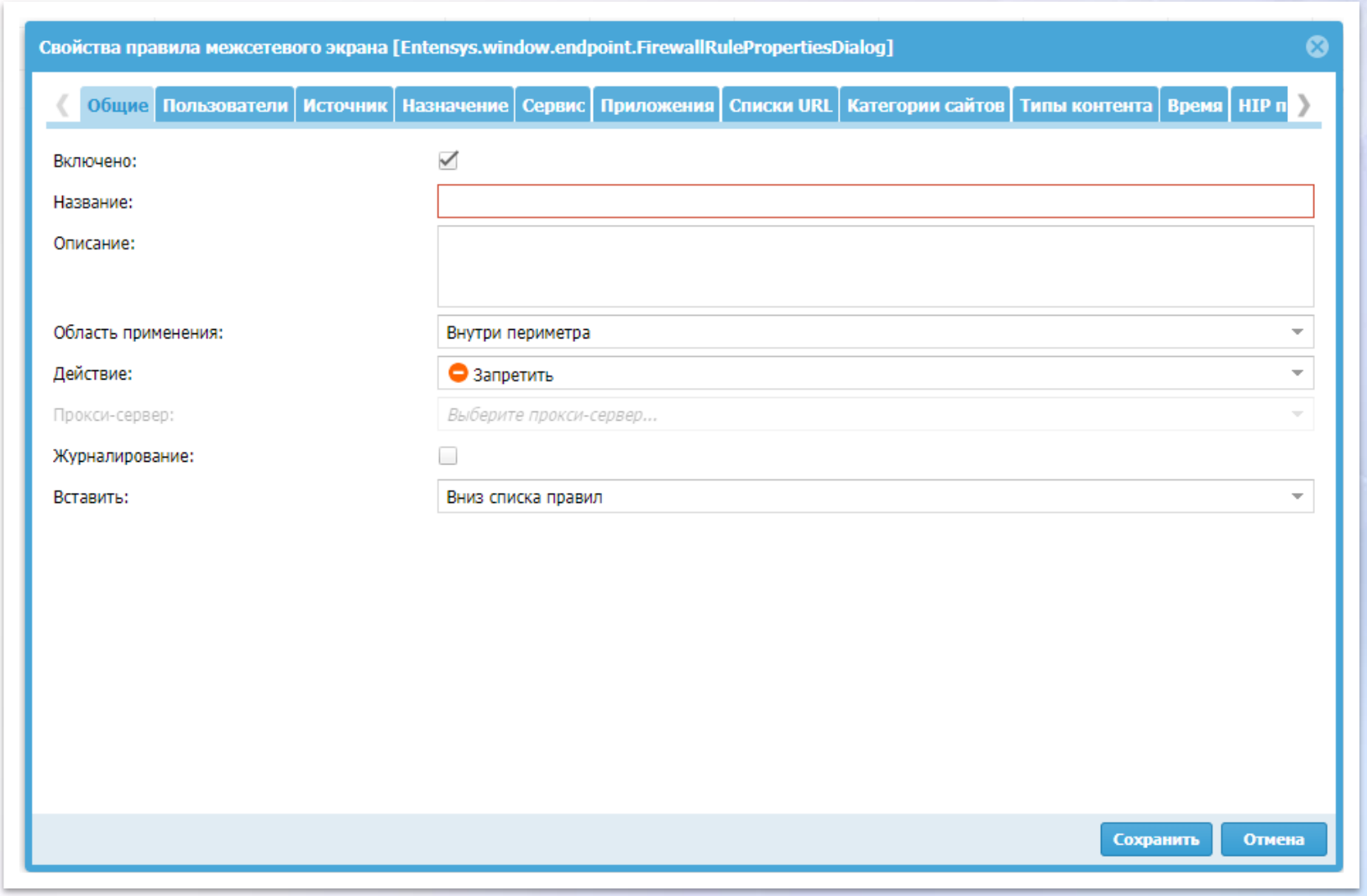
TECHDAY

UserGate Client

Сбор информации с устройства

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

Персональный межсетевой экран



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.

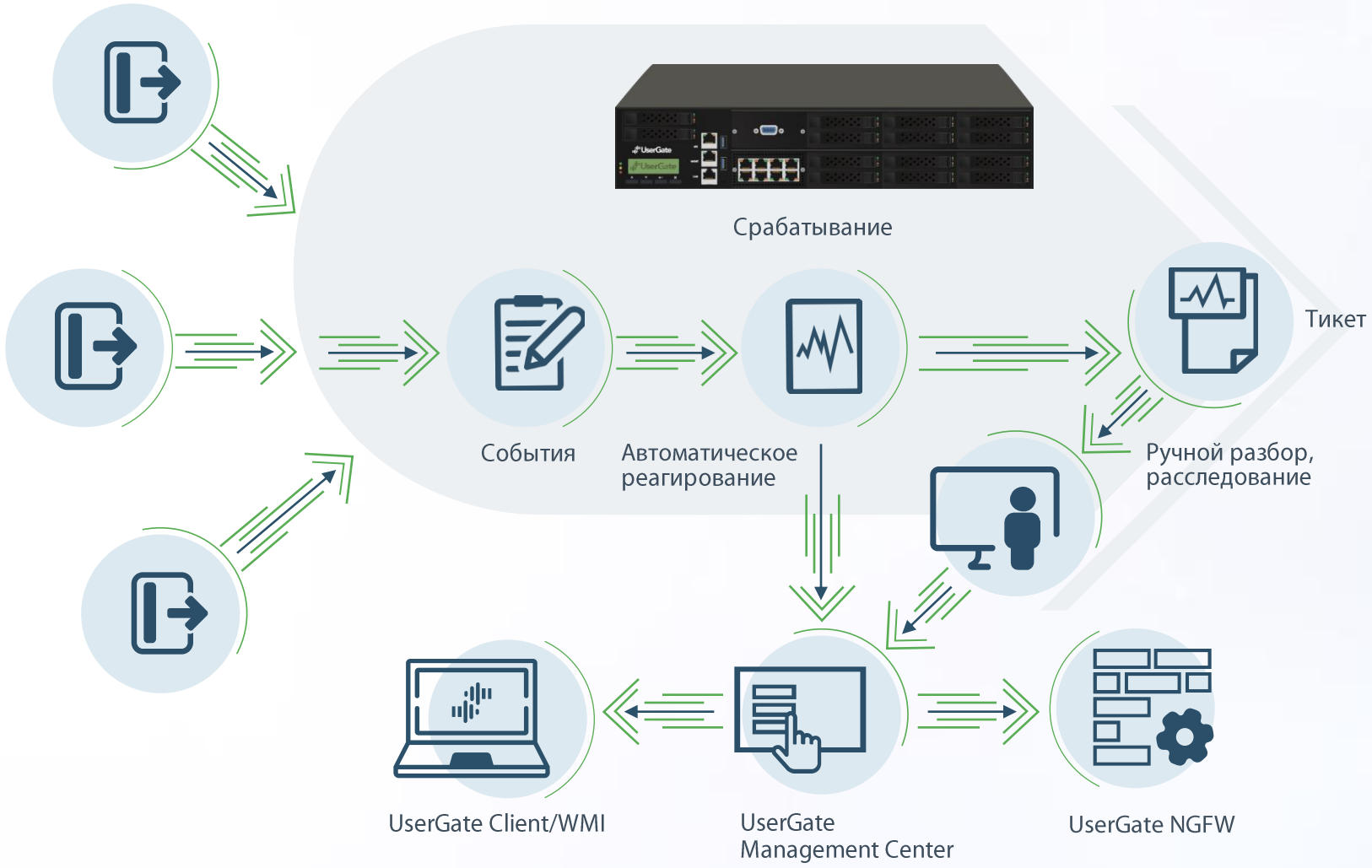
UserGate

TECHDAY

Log Analyzer

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

Архитектура продукта

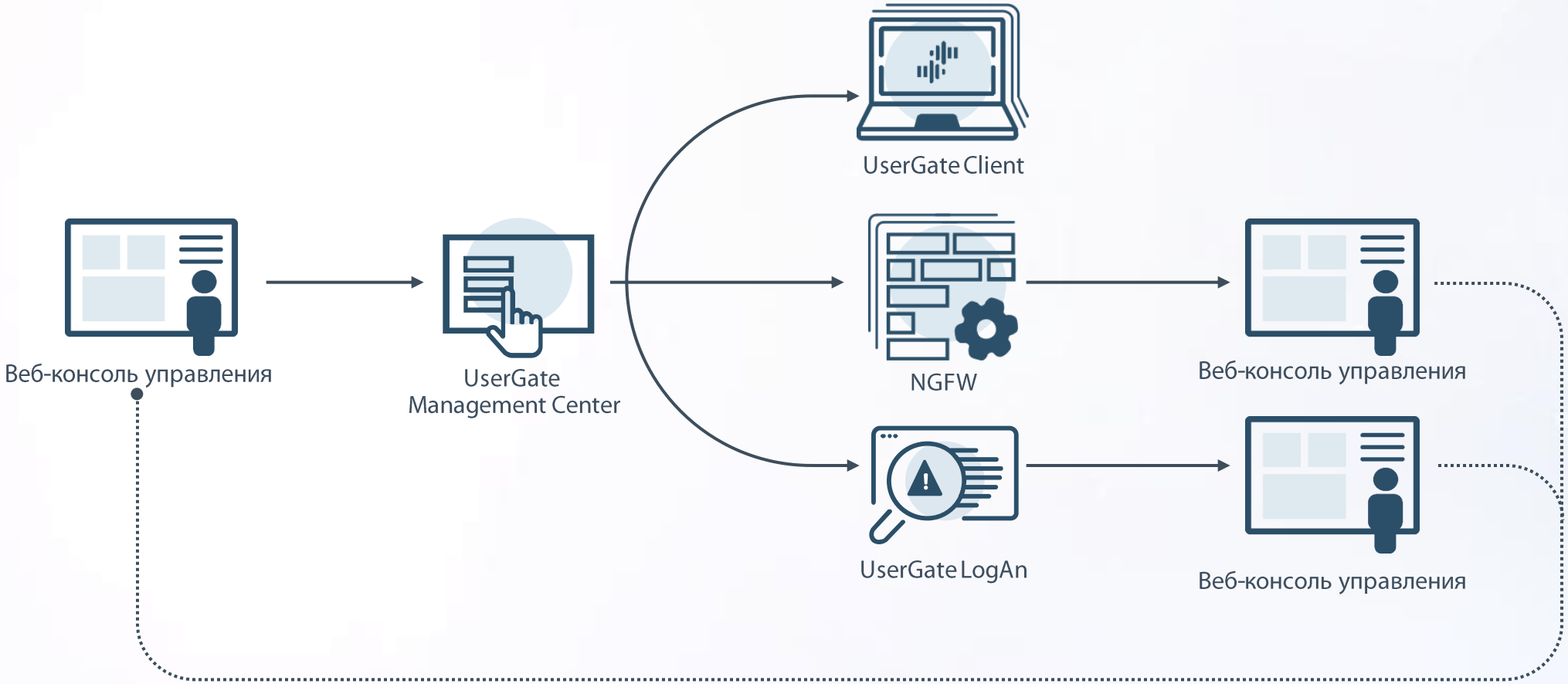


UserGate

TECHDAY

Management Center

Веб-консоль управления



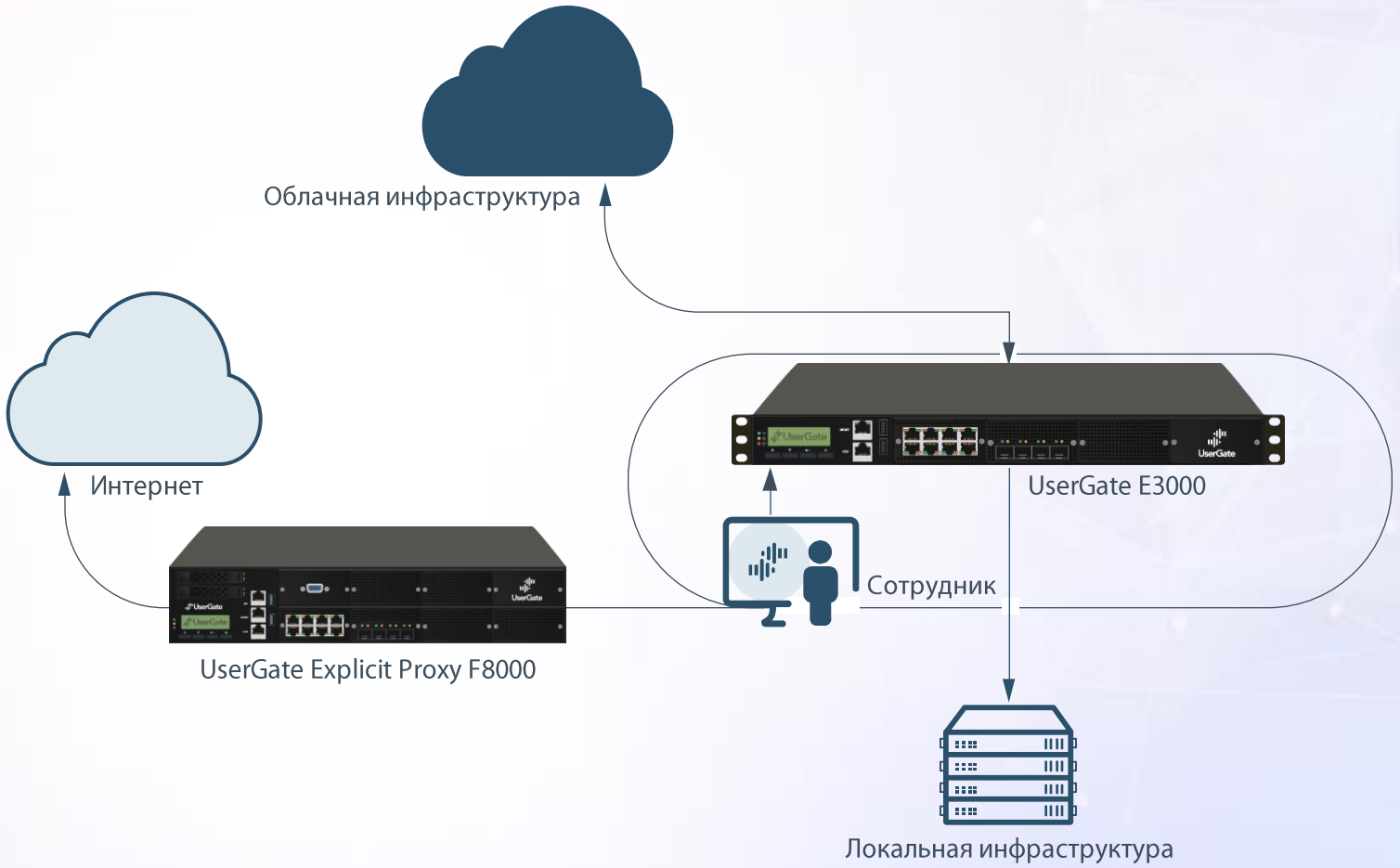
UserGate Management Center – зачем?

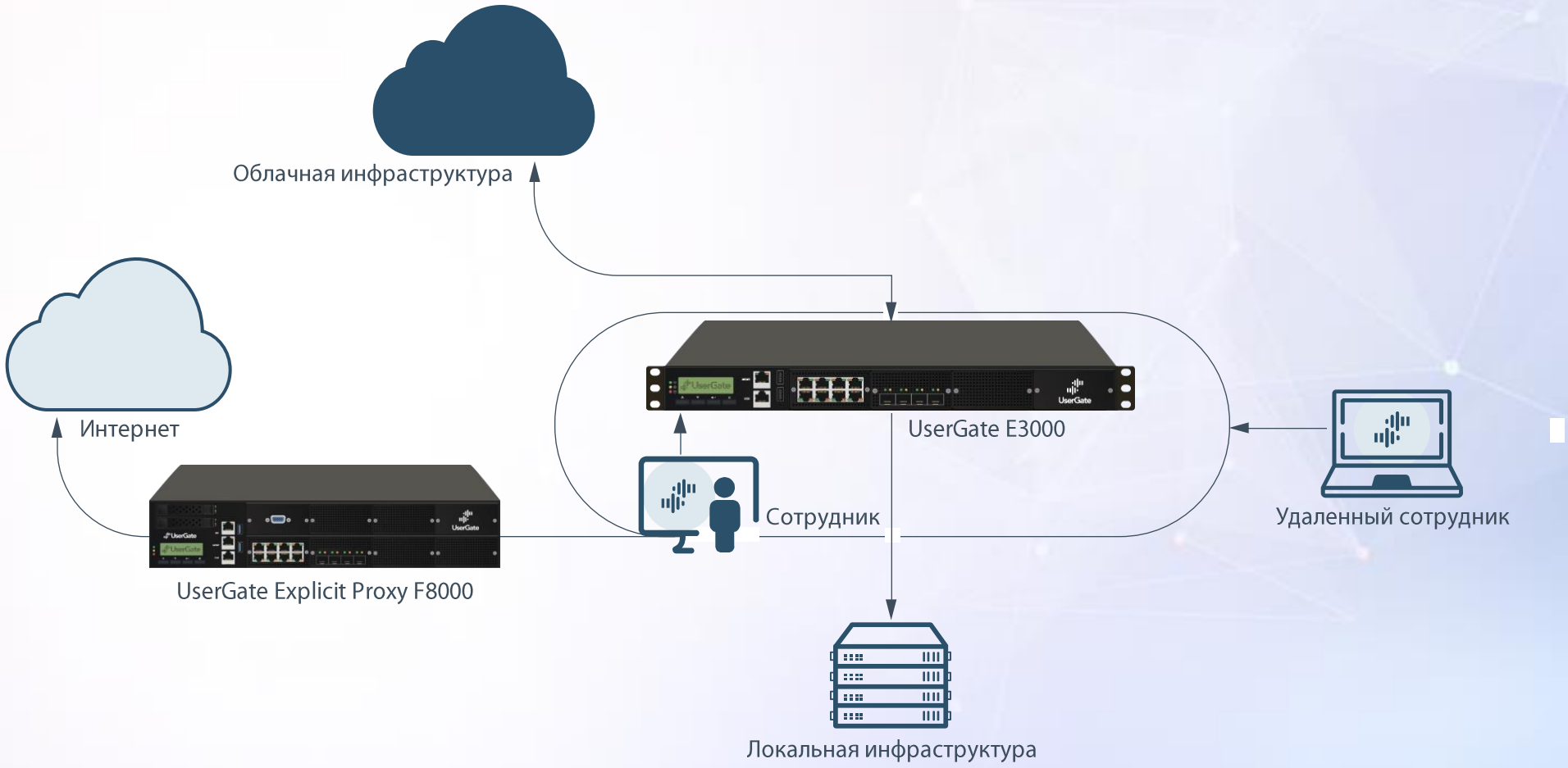
- упрощение администрирования большим парком продуктов UserGate (управление списками объектов: IP-адреса, URL-адреса, морфология, типы контента и т.д.);
- централизованное управление политиками безопасности и шаблонами политик безопасности;
- ролевая модель доступа к управлению;
- создание мультитенантной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

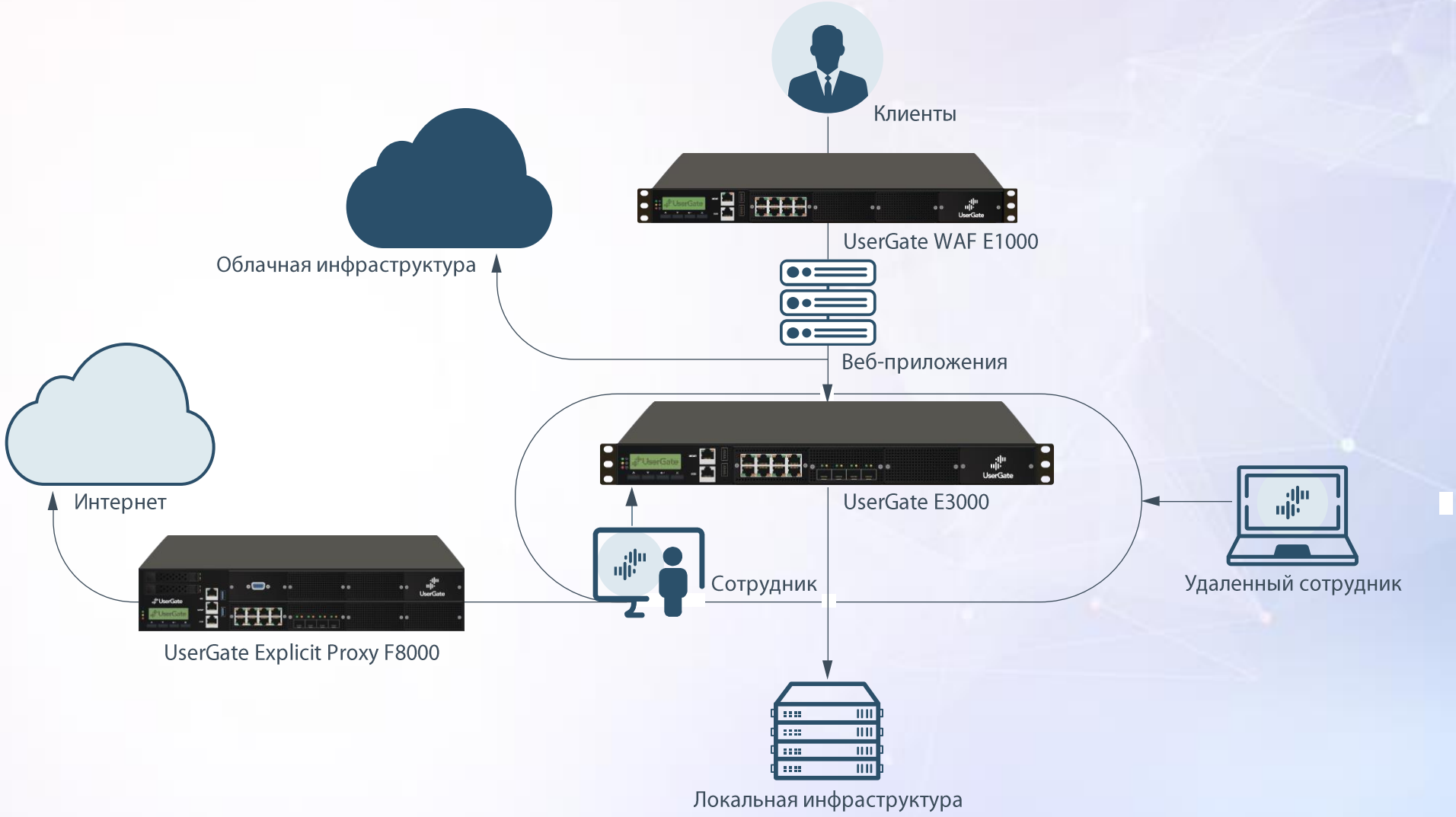
UserGate

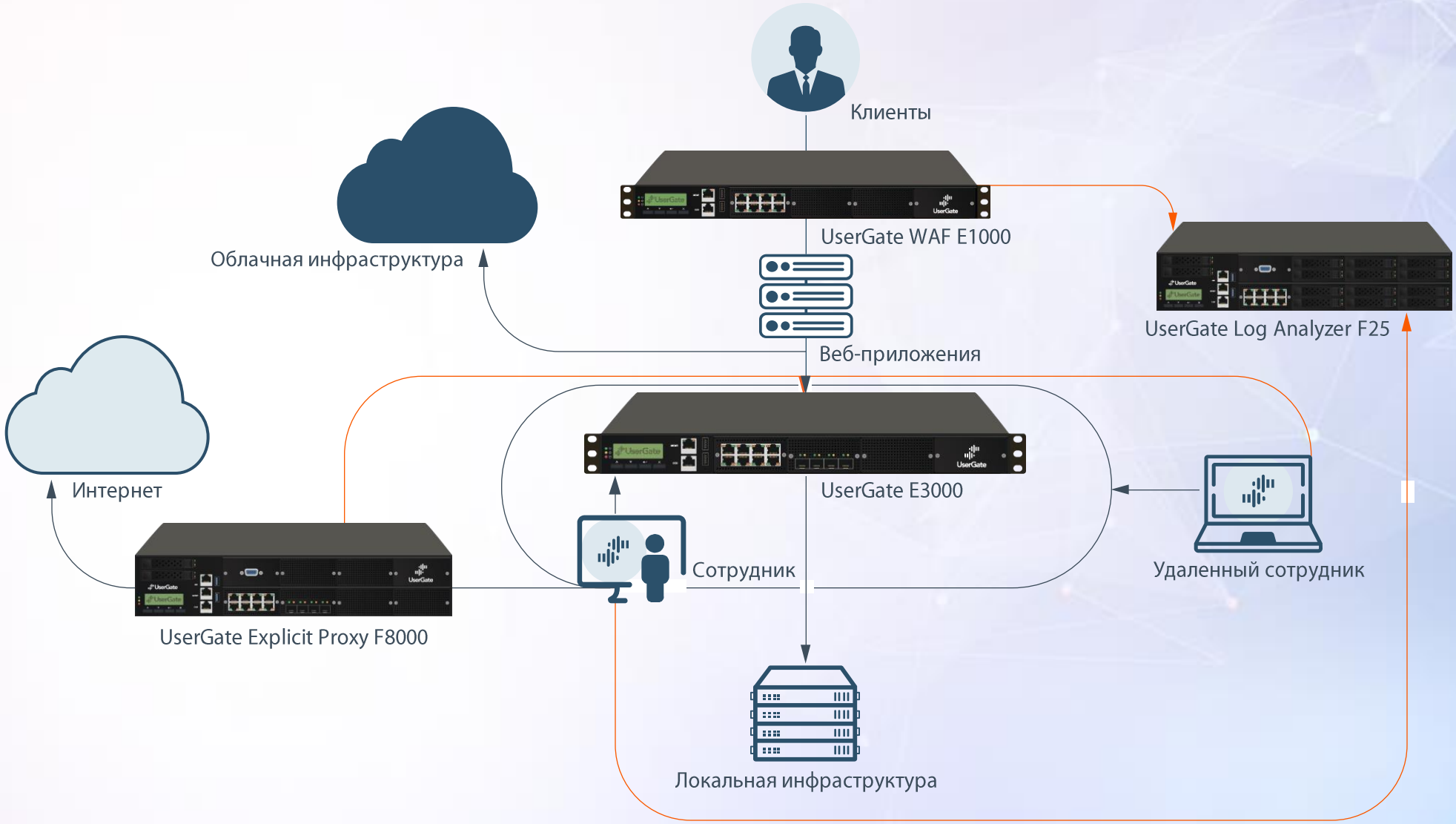
TECHDAY

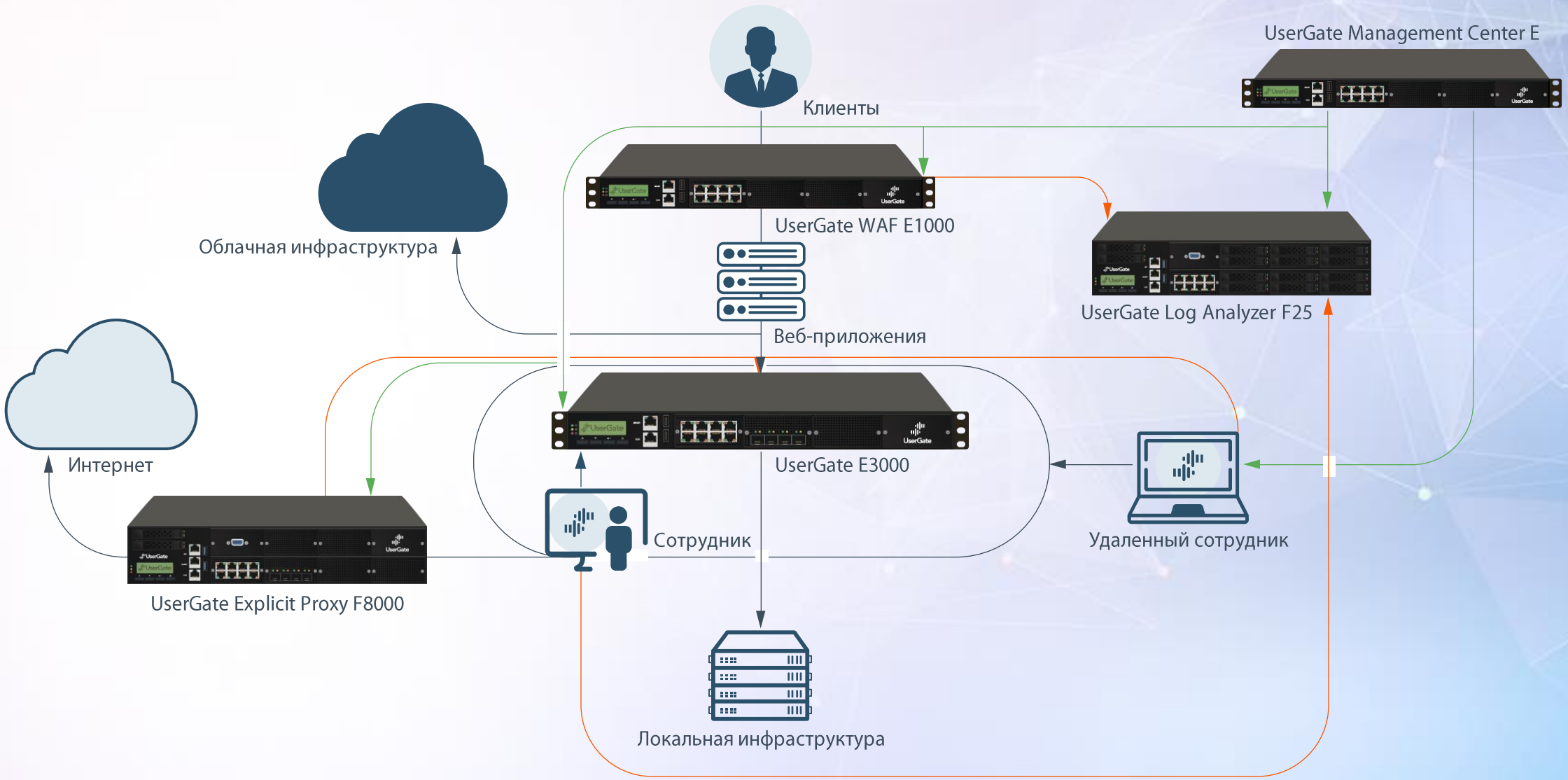
UserGate SUMMA


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

Пилотирование UserGate

DEMO

Отправьте заявку на пилотирование или запросите демонстрацию решений UserGate

sales@usergate.ru

8 (800) 500-40-32

UserGate

Спасибо за внимание!

Дмитрий Аловацкий

Ведущий менеджер по работе с корпоративными заказчиками

dalovatsky@usergate.com

+7 (913) 750 63 90