Практика импортозамещения в обеспечении сетевой безопасности критически важных объектов

Евгений Ханов
Ведущий менеджер по работе с корпоративными клиентами
ekhanov@usergate.ru
8 800 500 40 32 | +7 (913) 390-01-88

UserGate

Требования регуляторов

Всем новым ИС (или модернизируемым) необходимо прохождение сертификации по требованиям к УД с 1 января 2021 года

По новым требованиям к УД для УД5 и выше с 1 января 2022 года необходимо присутствие платформы в едином реестре российской радиоэлектронной продукции (Реестр)

Для УД4 и выше с 1 января 2028 года необходимо присутствие платформы в Реестре, а также используемых процессоров, микроконтроллеров и памяти

Приказ ФСТЭК России от 28.05.2020 № 75

«Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования.

В соответствии с Требованиями по обеспечению безопасности ЗОКИИ Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239…, достаточным для обеспечения безопасности значимого объекта при его подключении к сети связи общего пользования является применение следующих средств защиты информации, прошедших оценку на соответствие требованиям по безопасности в форме обязательной сертификации, испытаний или приемки

СЗИ\КЗ	3 КЗ	2 КЗ	1 КЗ
Программно-аппаратный граничный маршрутизатор	✓	✓	✓
Выделенные физические интерфейсы для каждого сервиса		✓	✓
МЭ тип “А” на границе с ССОП (Интернет)	✓	✓	✓
Средство обнаружения (предотвращения) вторжений		✓	✓

UserGate

Реестр сертифицированных СЗИ ФСТЭК России

МЭ типа «А»

применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы.

МЭ типа «Б»

применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы

МЭ типа «В»

применяемый на узле (хосте) информационной системы

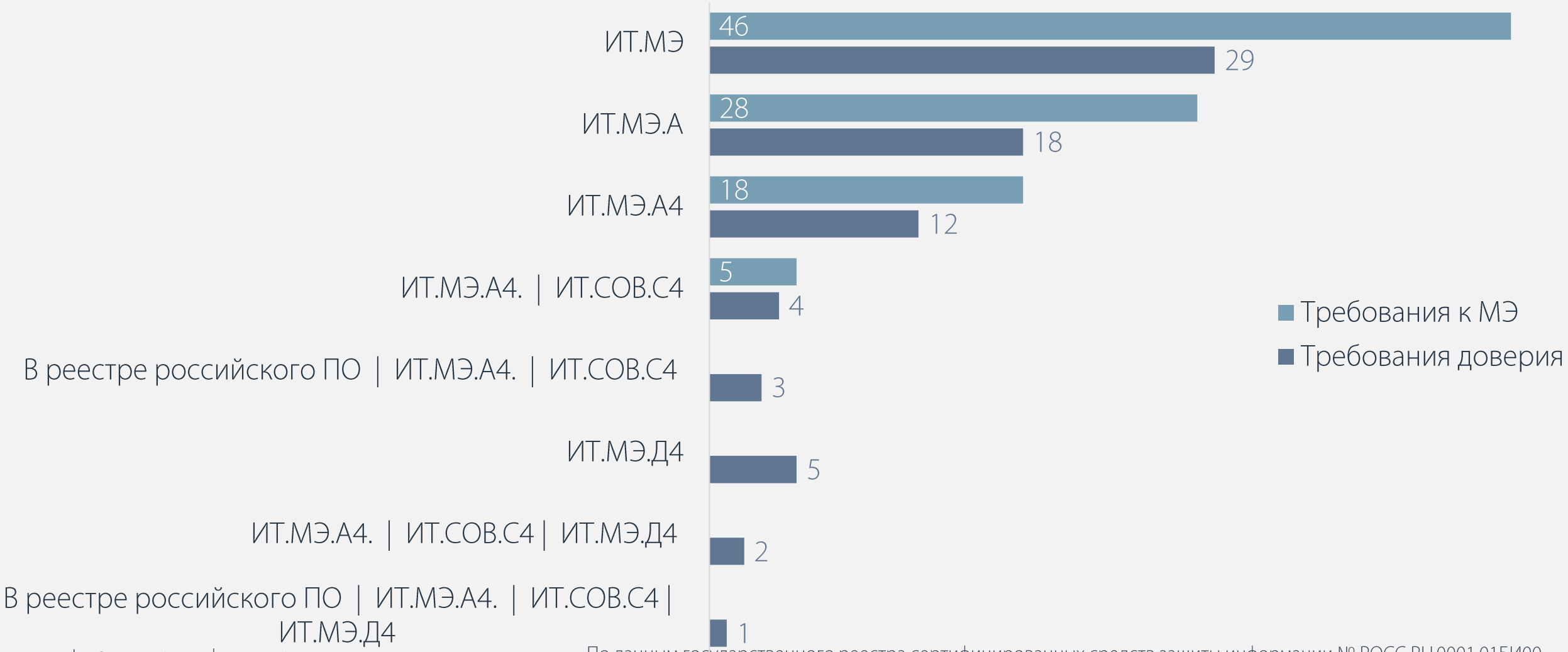
МЭ типа «Г»

применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера

МЭ тип «Д»

применяемый в автоматизированной системе управления технологическими или производственными процессами. МЭ типа «Д» может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы)

Сертификаты, выданные на серию в реестре ФСТЭК России*:

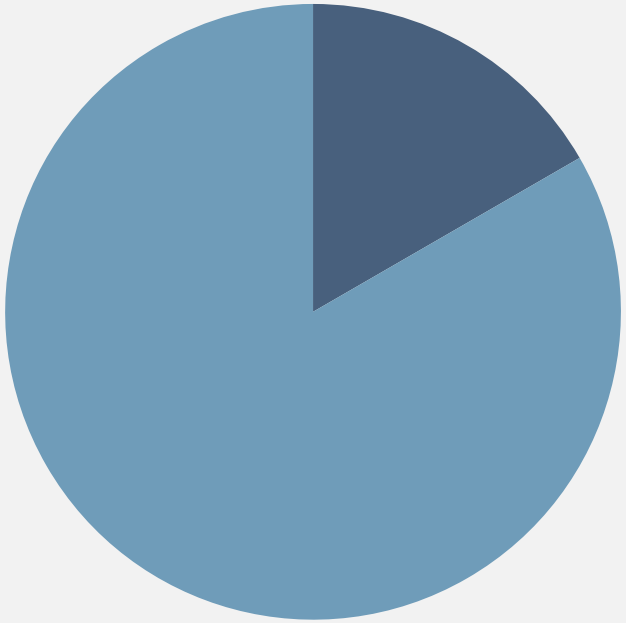


По данным государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 от 03.10.2021 сертификатов, выданных на серию в реестре ФСТЭК России:

Соотношение сертификатов ФСТЭК России выданных на серию, с профилем защиты ИТ.МЭ.А4

Российские вендоры
15 сертификатов

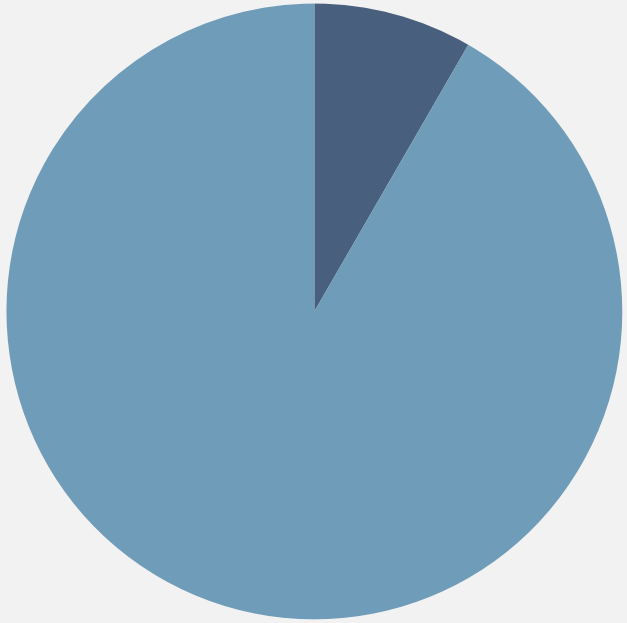
Иностранные вендоры
3 сертификата



Требования к МЭ

Российские вендоры
11 сертификатов

Иностранные вендоры
1 сертификат



Требования доверия

По данным государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 от 03.10.2021 сертификатов, выданных на серию в реестре ФСТЭК России:

ПРИКАЗ МИНЗДРАВА РФ ОТ 24.12.2018 №911-Н

«Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».
В программно-технических средствах информационных систем допускается применение только сертифицированных СЗИ.

Кроме того, эти программно-технические средства должны соответствовать требованиям, предусмотренным постановлением Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

Требования Минздрава ужесточают требования приказов ФСТЭК России № 235 и 239, допуская использование только сертифицированных средств защиты информации.

UserGate

Экосистема решений UserGate SUMMA

Безопасная публикация ресурсов и сервисов

Межсетевой экран NGFW

Система обнаружения и предотвращения вторжений

Безопасность АСУ ТП

Анализ и предотвращение новых угроз (SOAR)

Интернет фильтрация

Защита почты

Антивирус

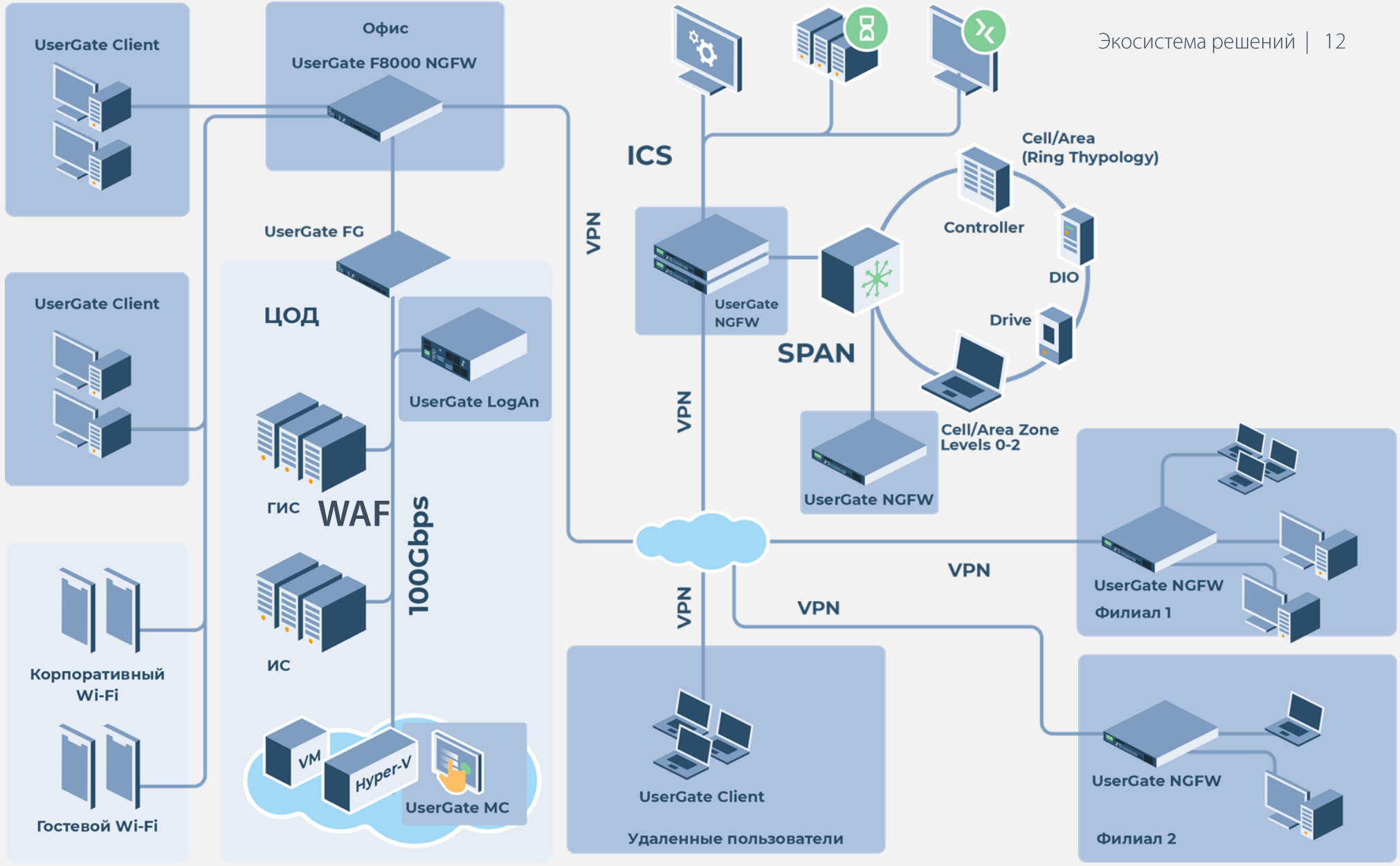
Защита клиентских устройств

Управление устройствами

Анализ инцидентов ИБ

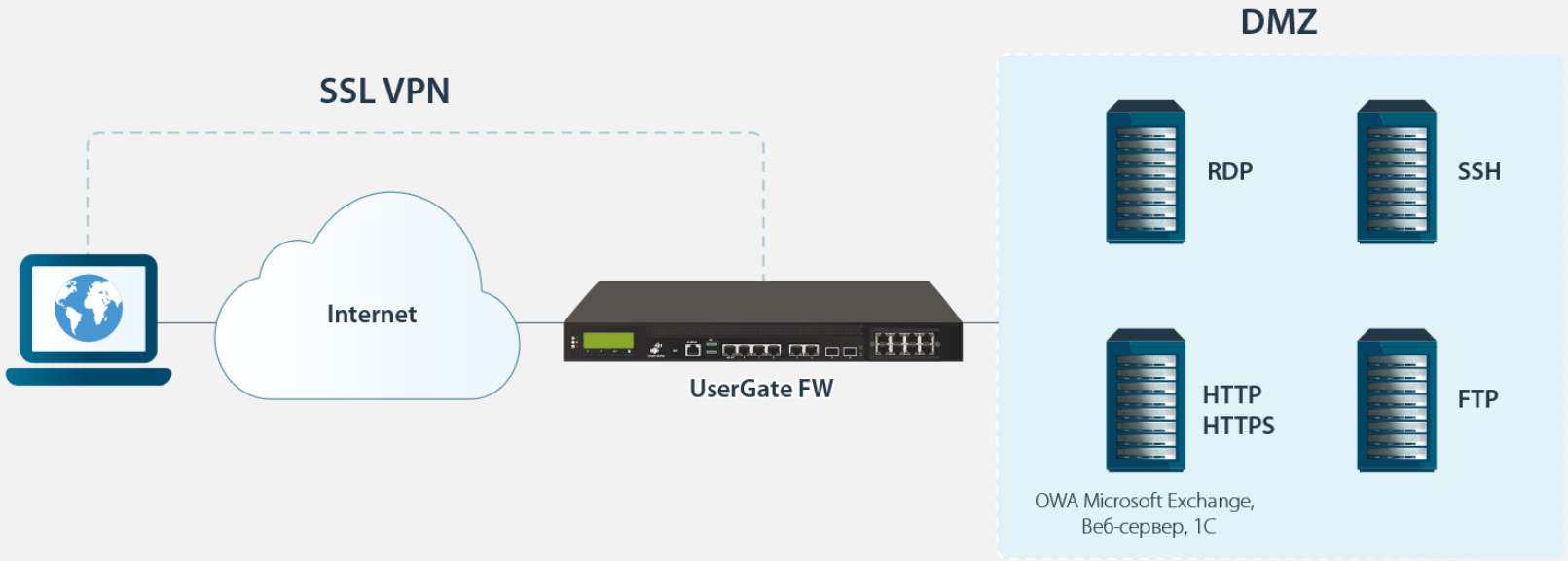
решение уровня “Wire speed”

WAF

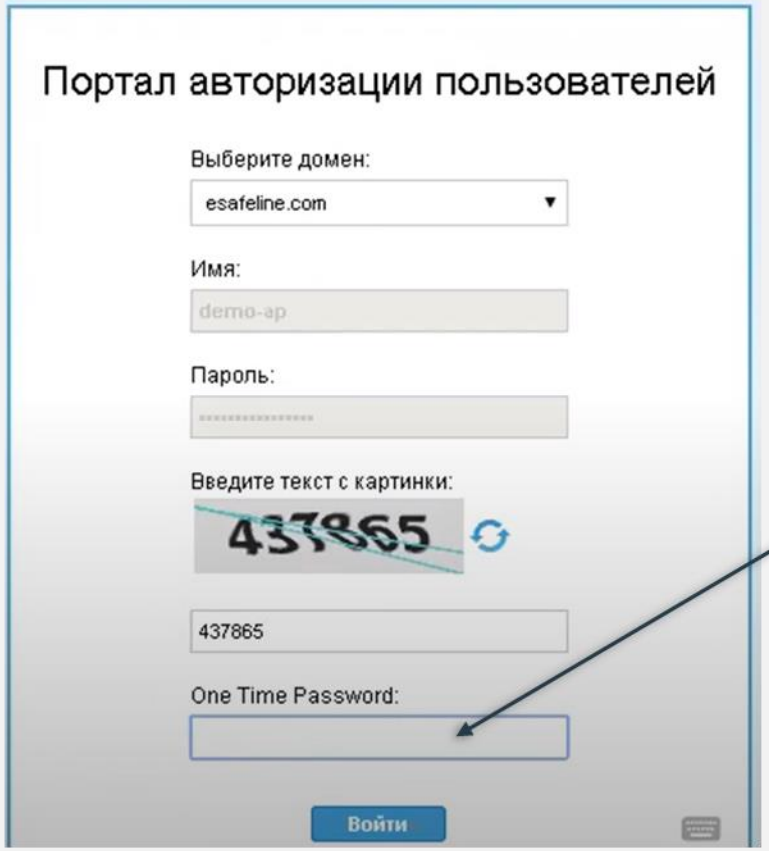

UserGate Client
Офис
UserGate F8000 NGFW
UserGate FG
UserGate Client
ЦОД
UserGate LogAn
ГИС
WAF
ИС
100Gbps
VM
Hyper-V
UserGate MC
Корпоративный Wi-Fi
Гостевой Wi-Fi
ICS
VPN
UserGate NGFW
Cell/Area (Ring Thypology)
Controller
DIO
Drive
SPAN
Cell/Area Zone Levels 0-2
UserGate NGFW
VPN
VPN
VPN
VPN
UserGate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

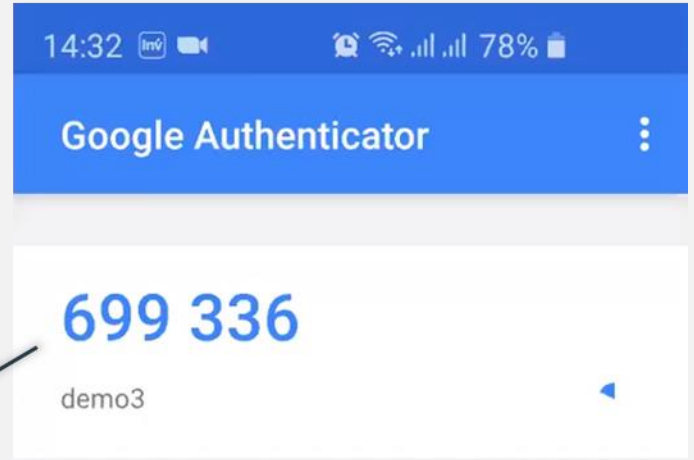
Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

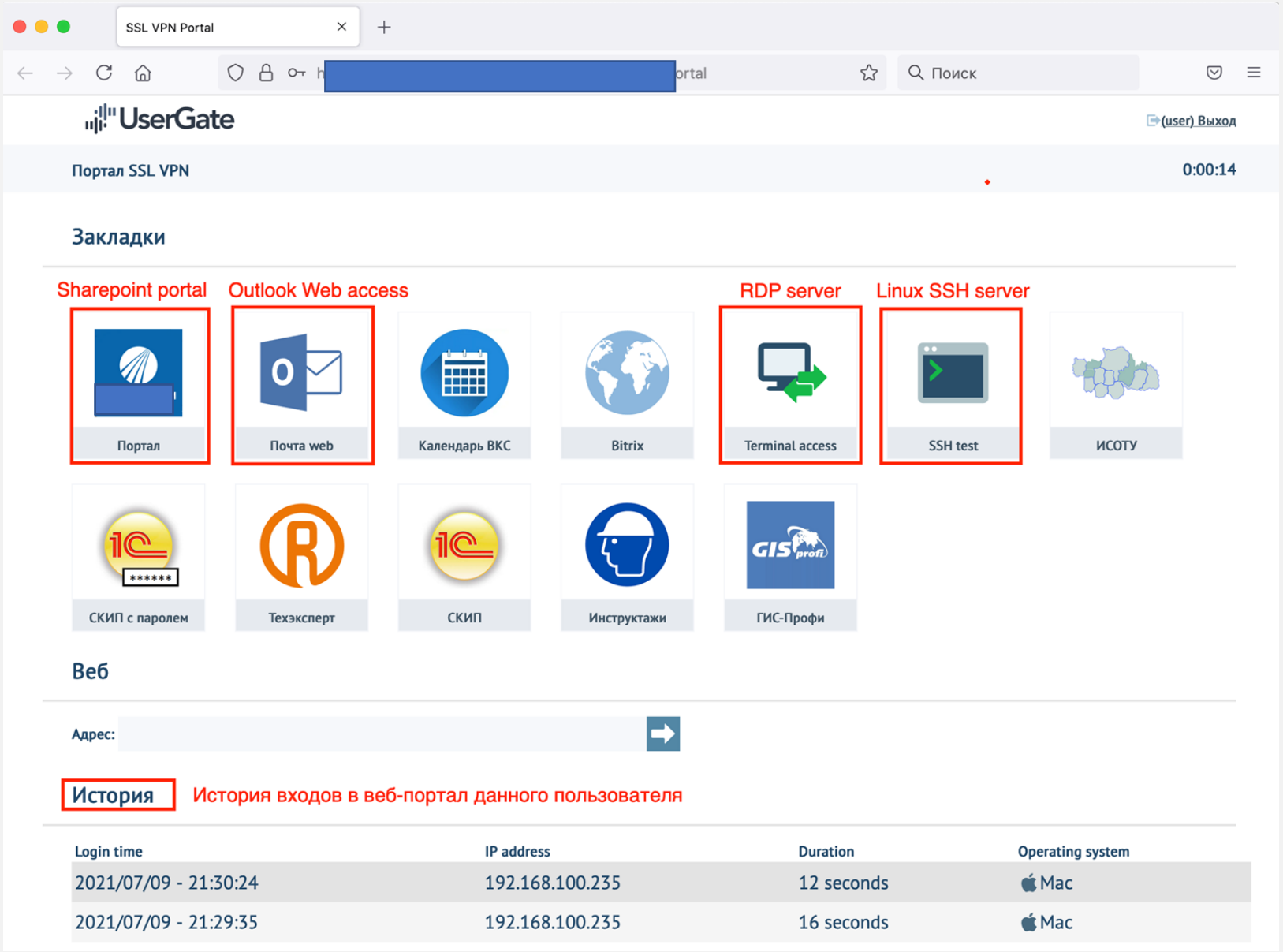
SSL VPN (Веб-портал) – позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML в том числе с поддержкой MFA.



- MFA (TOTP, SMS, Email)
- Настройка политик доступа к отдельным сервисам по пользователям и группам
- Доступ через браузер
- SSO






SSL VPN 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

UserGate

EDR

- Дополнительная видимость
- Инструмент обнаружения сложных угроз: **IoC** и **IoA**
- Углубленная информация
- Автоматизация процессов безопасности
- Межсетевой экран типа «B»
- Дополнительный уровень аутентификации
- VPN-клиент для организации безопасного удаленного доступа

UserGate

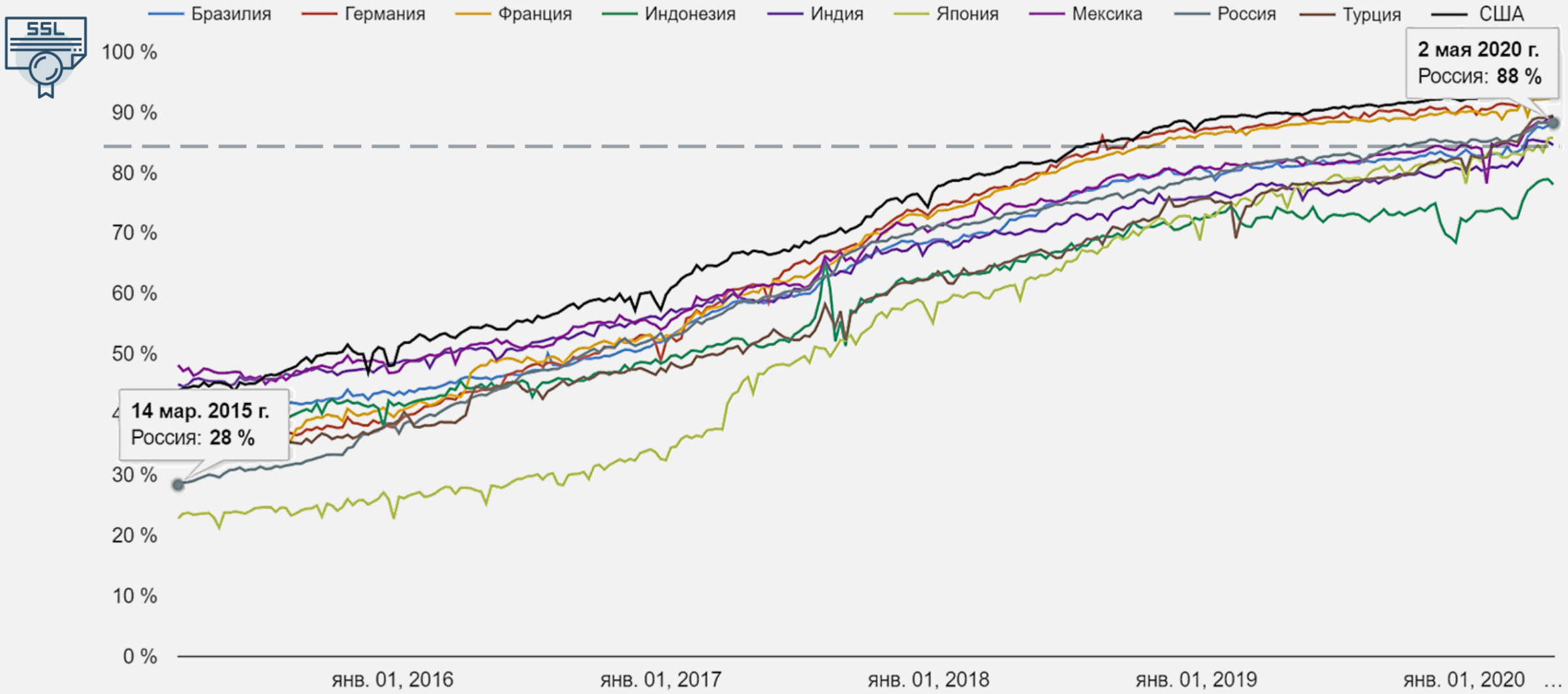
NAC

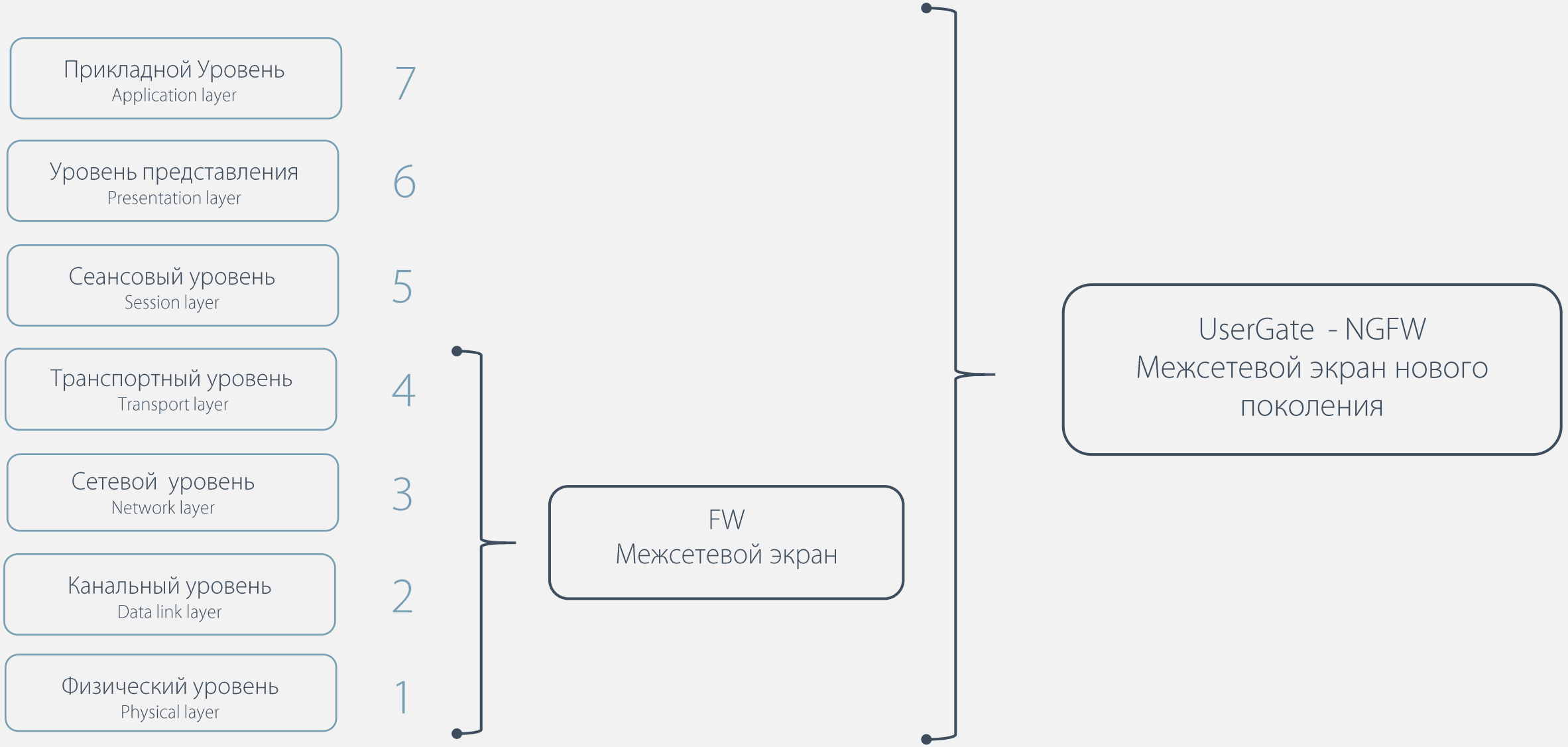
- информации о пользователе, который подключается;
- информации о состоянии хоста (установленное программное обеспечение, наличие обновлений и др.);
- времени подключения;
- точки подключения.
- информацию об устройстве, изменения в железе

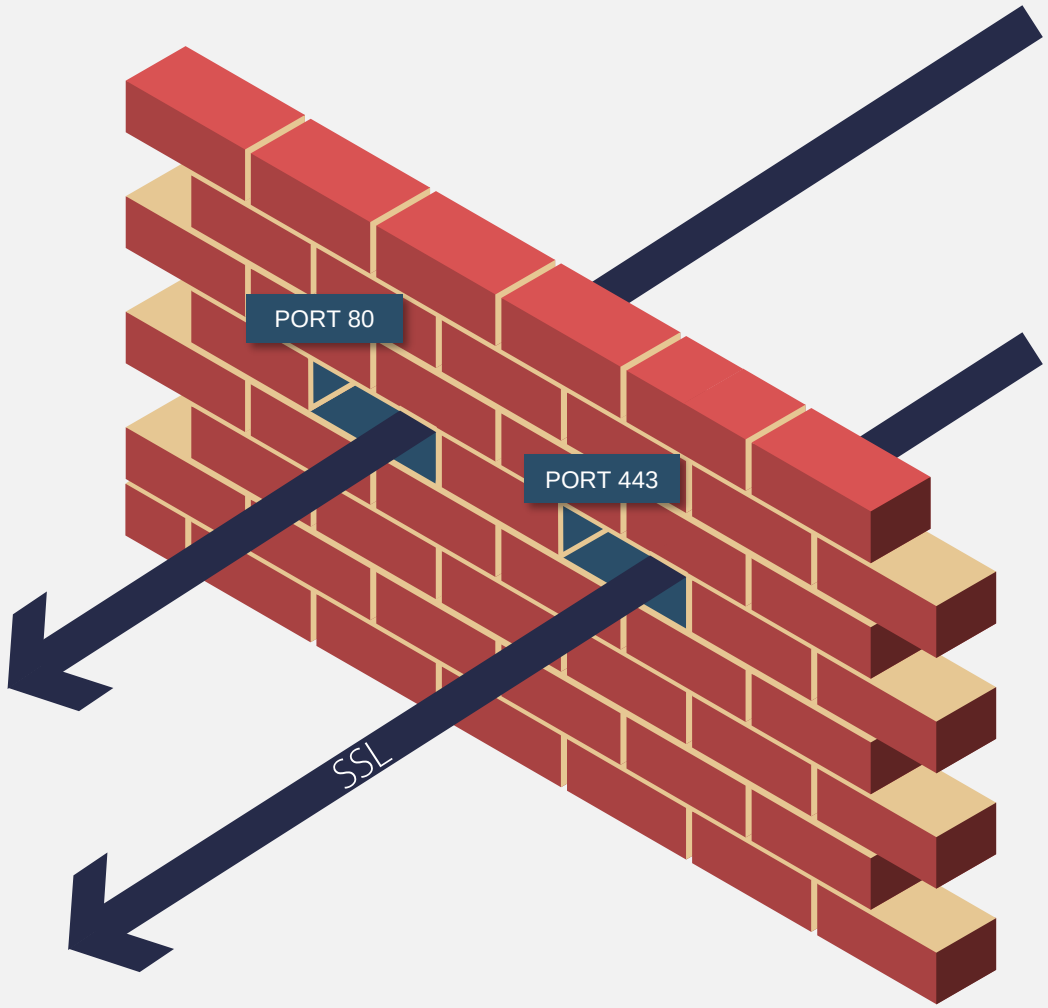
Next Generation Firewall

- 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

Процент страниц, загружаемых по HTTPS в Chrome по странам/регионам

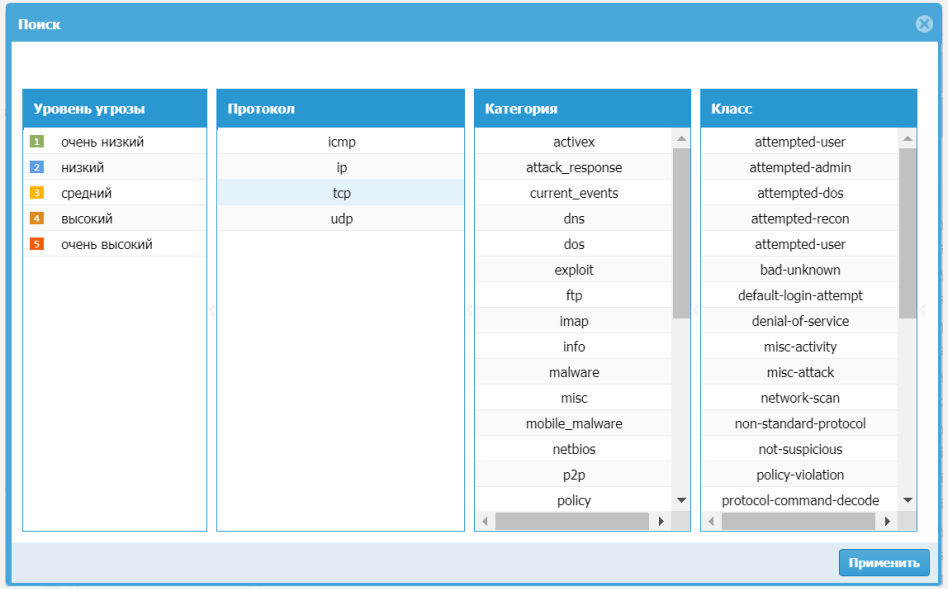


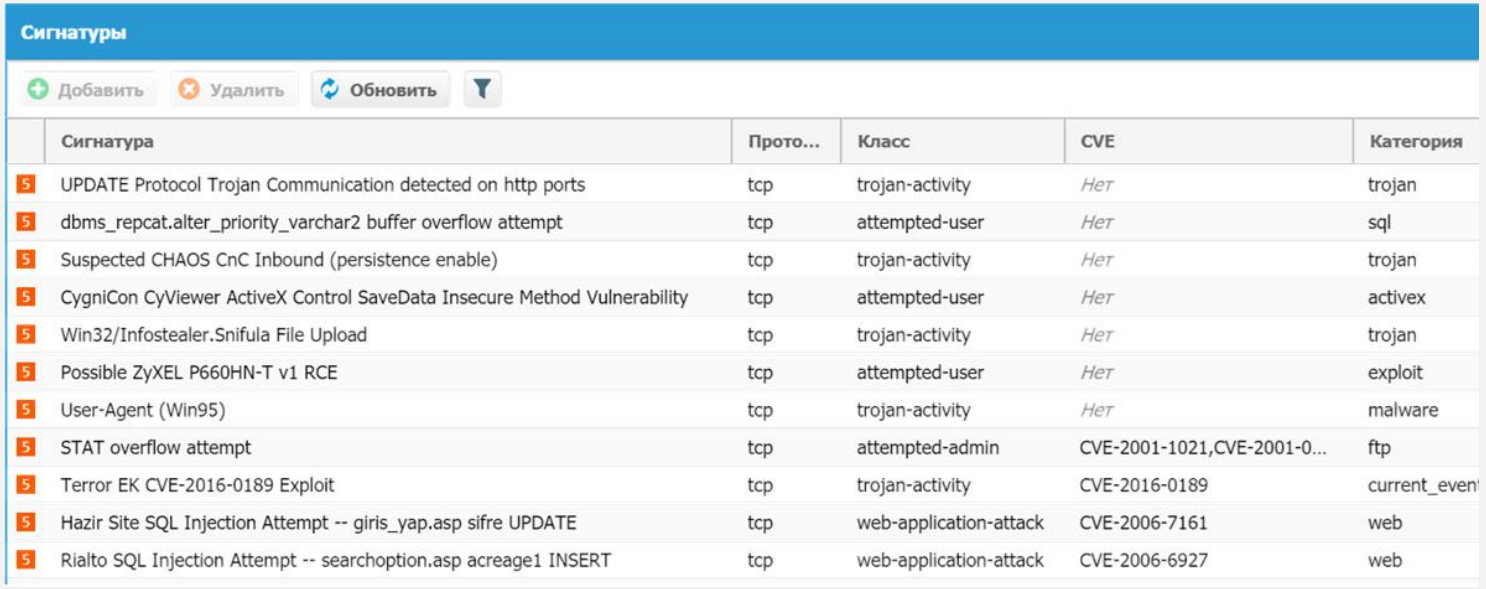

Прикладной Уровень
Application layer
7
Уровень представления
Presentation layer
6
Сеансовый уровень
Session layer
5
Транспортный уровень
Transport layer
4
Сетевой уровень
Network layer
3
Канальный уровень
Data link layer
2
Физический уровень
Physical layer
1
FW
Межсетевой экран
UserGate - NGFW
Межсетевой экран нового поколения


PORT 80
PORT 443
SSL

СОВ - Система обнаружения и предотвращения вторжений (IPS - Intrusion Prevention System)

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

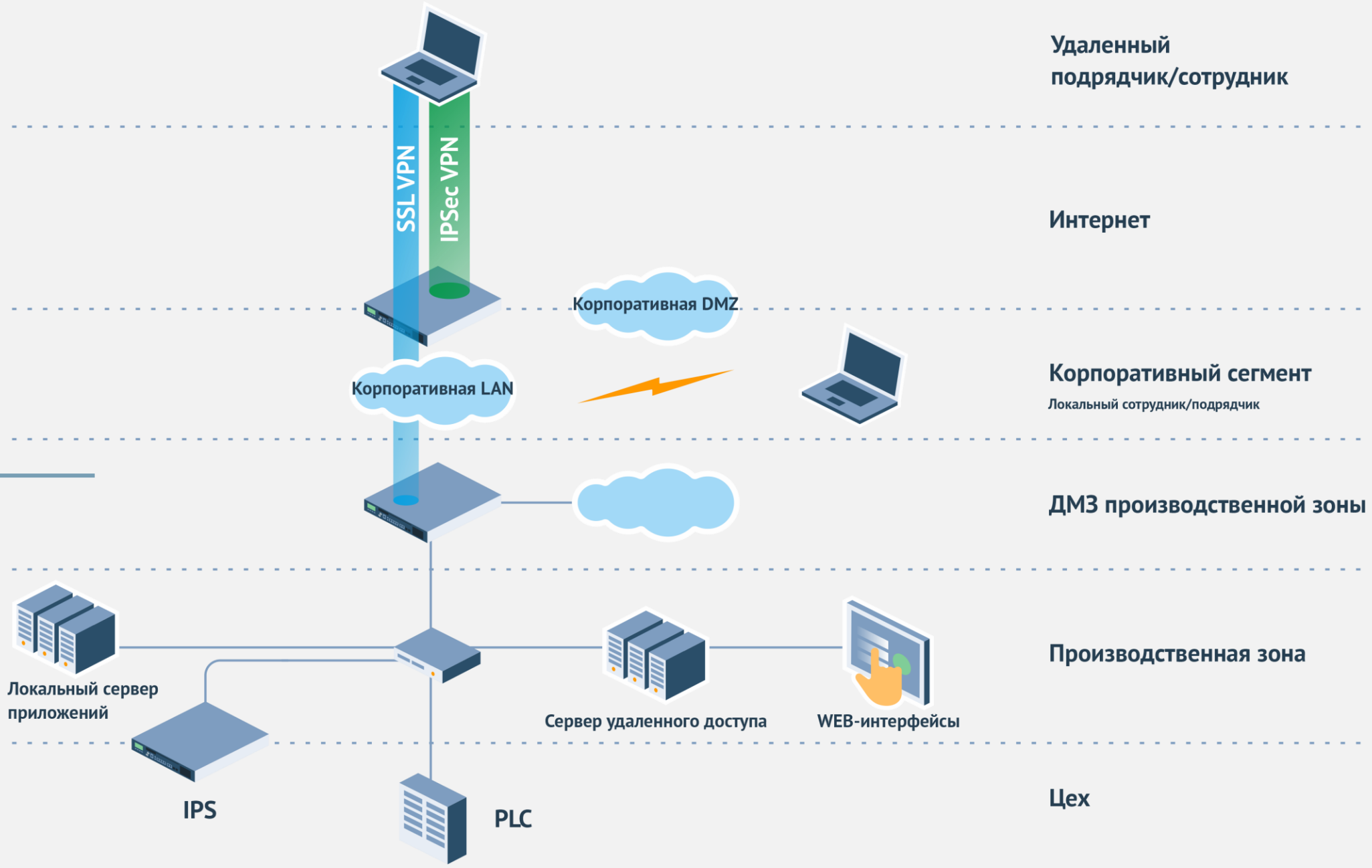




Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon 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_event
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

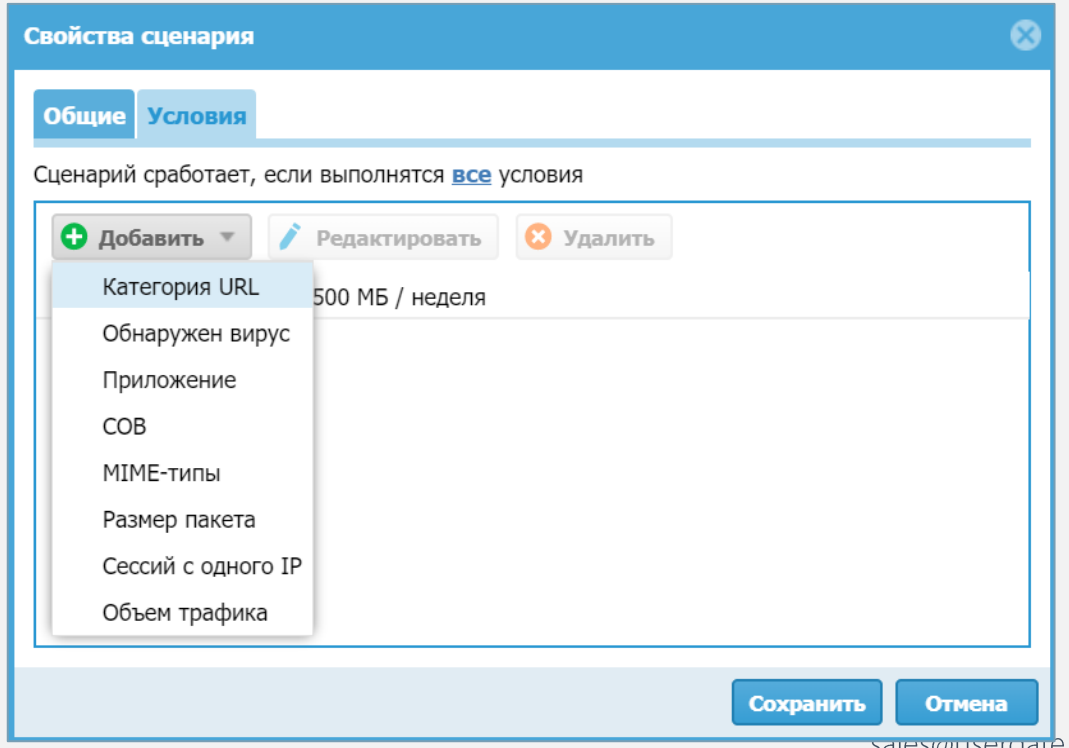
Итоговая Архитектура

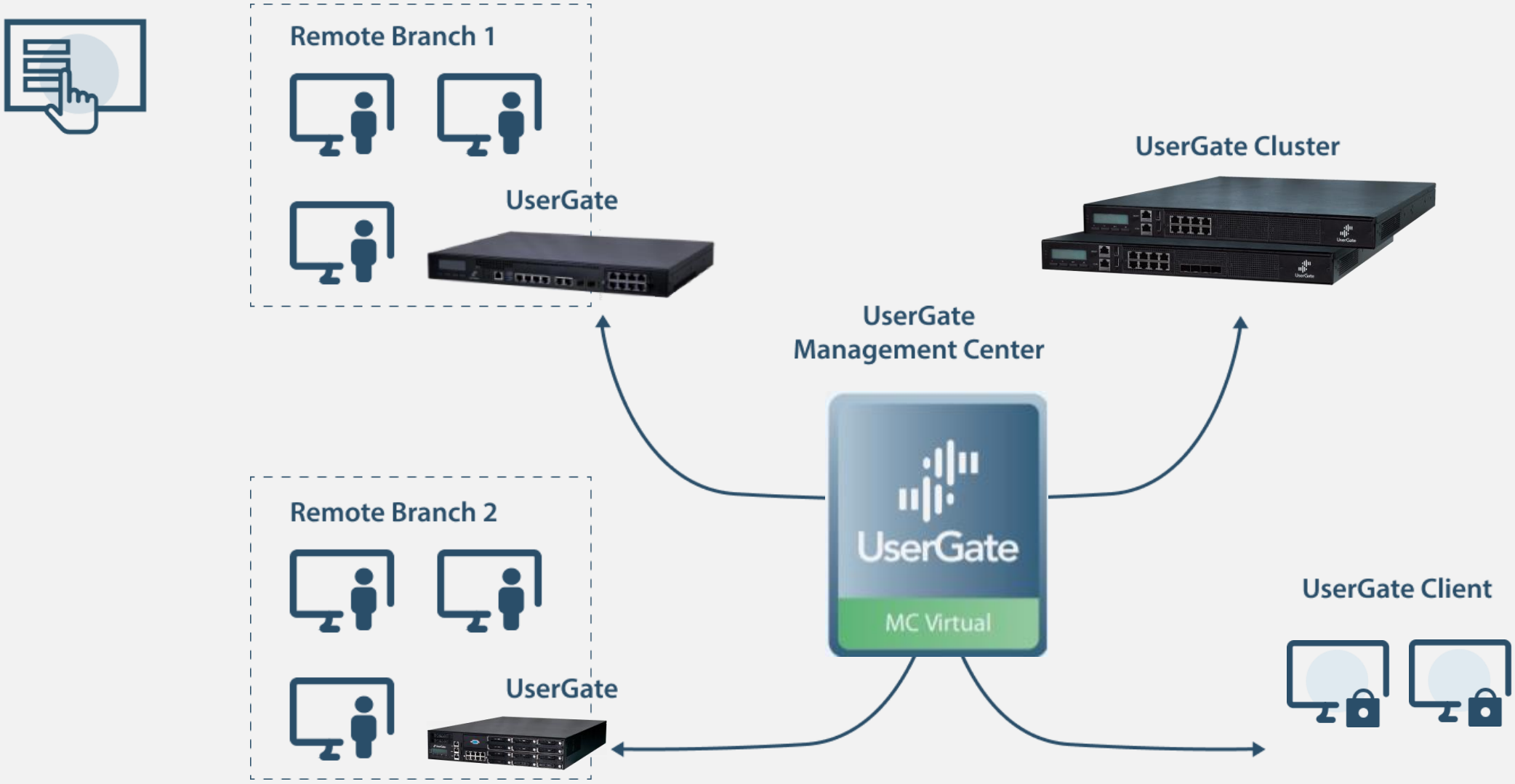


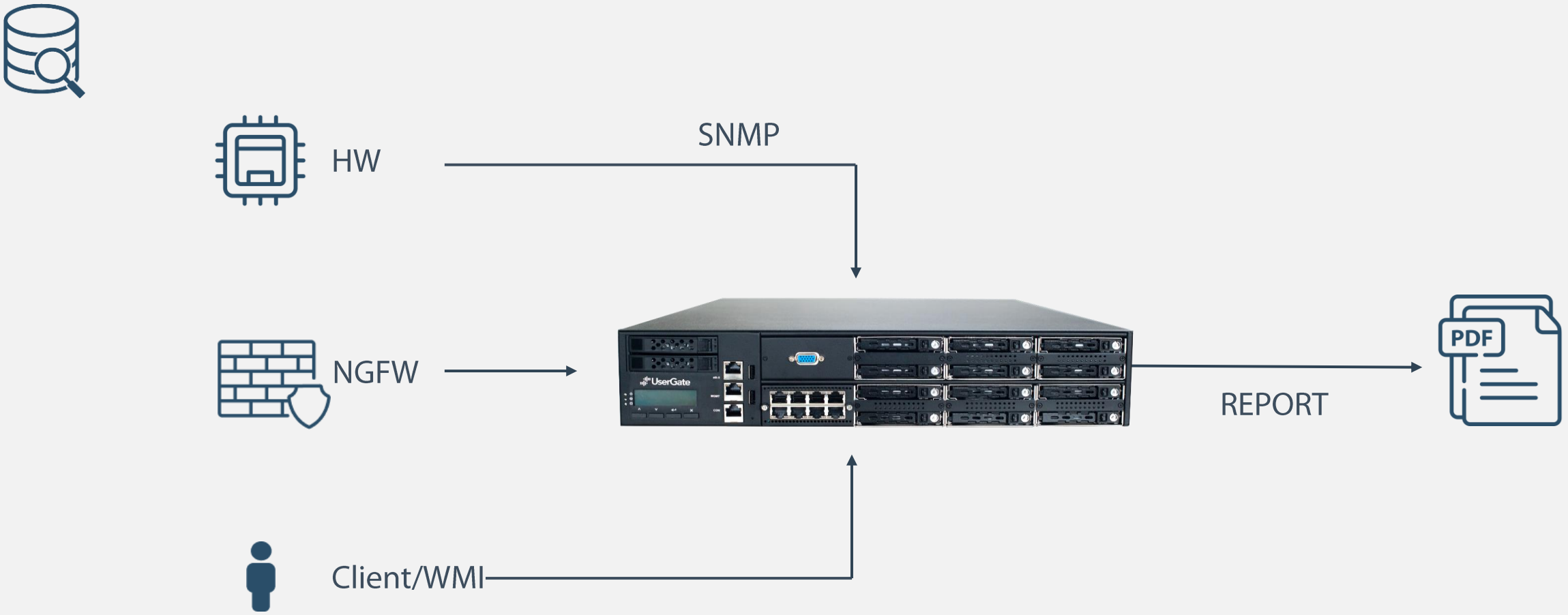
Различные механизмы фильтрации:

- 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 поддержкой TLS ГОСТ

SOAR (Security Automation, Orchestration and Response), позволяют анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, обеспечивая защиту от угрозы или просто от аномального поведения на самой ранней стадии.




Remote Branch 1
UserGate
UserGate Cluster
UserGate
Management Center
UserGate
MC Virtual
Remote Branch 2
UserGate
UserGate Client


HW
SNMP
NGFW
REPORT
PDF
Client/WMI

События
Срабатывание
Тикет
Автоматическое
реагирование
Ручной разбор,
расследование
MC
NGFW
Client

Новые платформы UserGate NGFW для АСУ ТП

UserGate

Ростелеком

ПЕНСИОНЫЙ ФОНД РОССИЙСКОЙ ФЕДЕРАЦИИ

MEGAFON

lady & gentleman CITY

горки город

29TH WINTER UNIVERSIADE KRASNOYARSK 2019

РОССИЙСКАЯ ГОСУДАРСТВЕННАЯ БИБЛИОТЕКА

УрГУПС УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

САХАЛИН ЭНЕРДЖИ SAKHALIN ENERGY

РОССЕТИ

ГОСКОРПОРАЦИЯ по ОРВД

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

ГАЗПРОМ МЕЖРЕГИОНГАЗ

РОСНЕФТЬ

ГалоПолимер

Транснефть

РусГидро

ФОСАГРО

UserGate

Спасибо за внимание!

Евгений Ханов

Ведущий менеджер по работе с
корпоративными клиентами

ekhanov@usergate.ru

8 800 500 40 32 | +7 (913) 390-01-88