Практика в выборе решений в обеспечении сетевой безопасности

Евгений Ханов
ekhanov@usergate.ru

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

Безопасная публикация ресурсов и сервисов

Межсетевой экран NGFW

Система обнаружения и предотвращения вторжений

Безопасность АСУ ТП

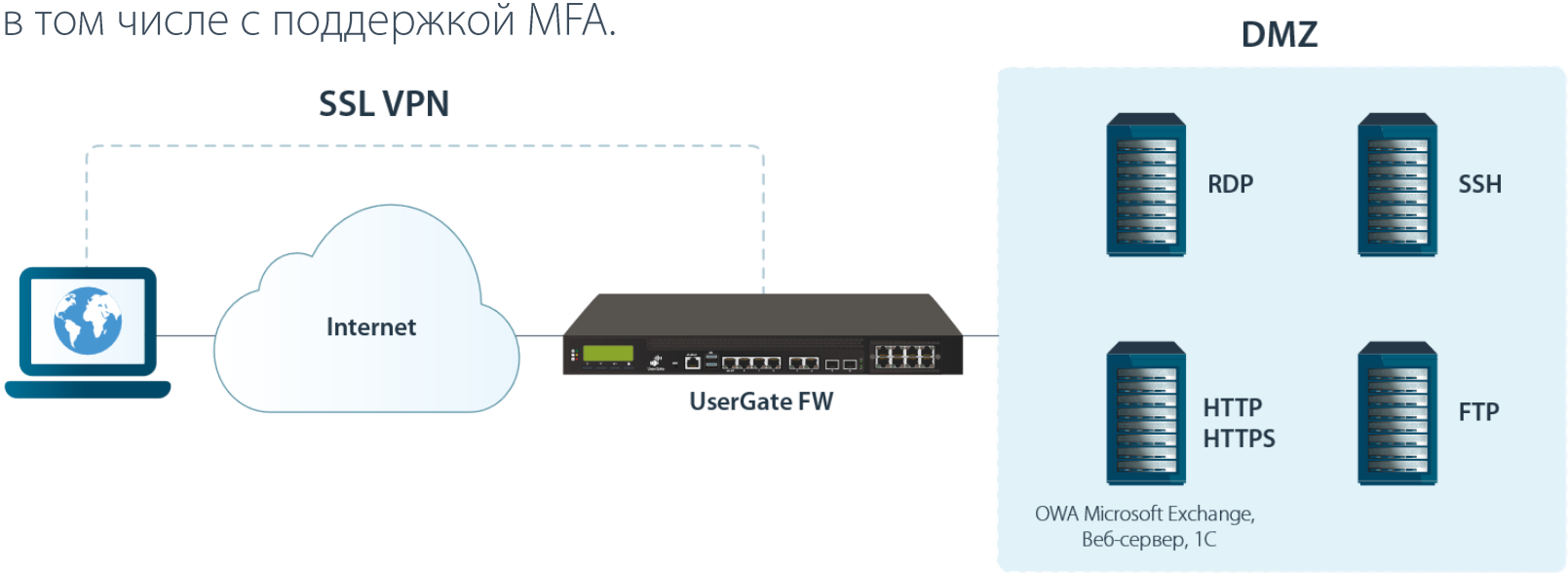
Защита клиентских устройств

Интернет фильтрация

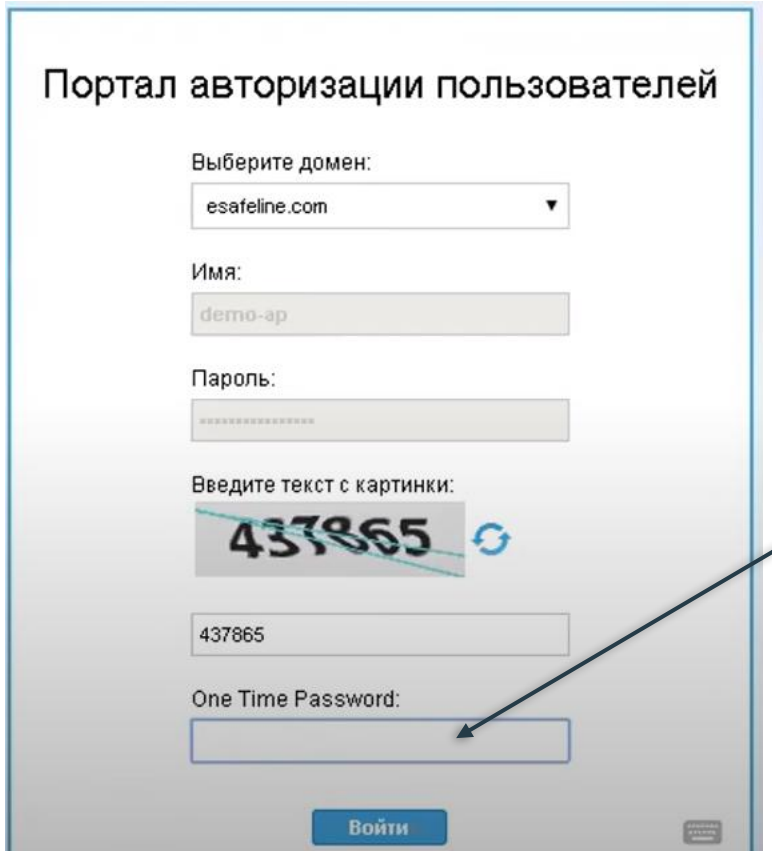
Безопасная публикация ресурсов и сервисов

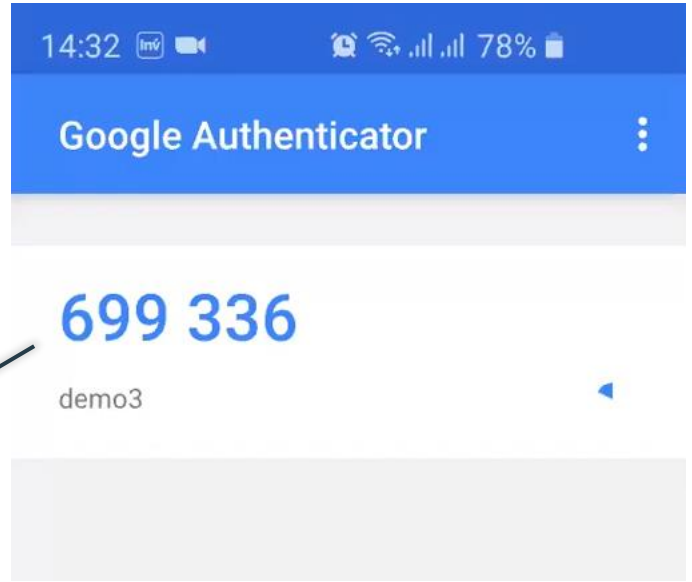
Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

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





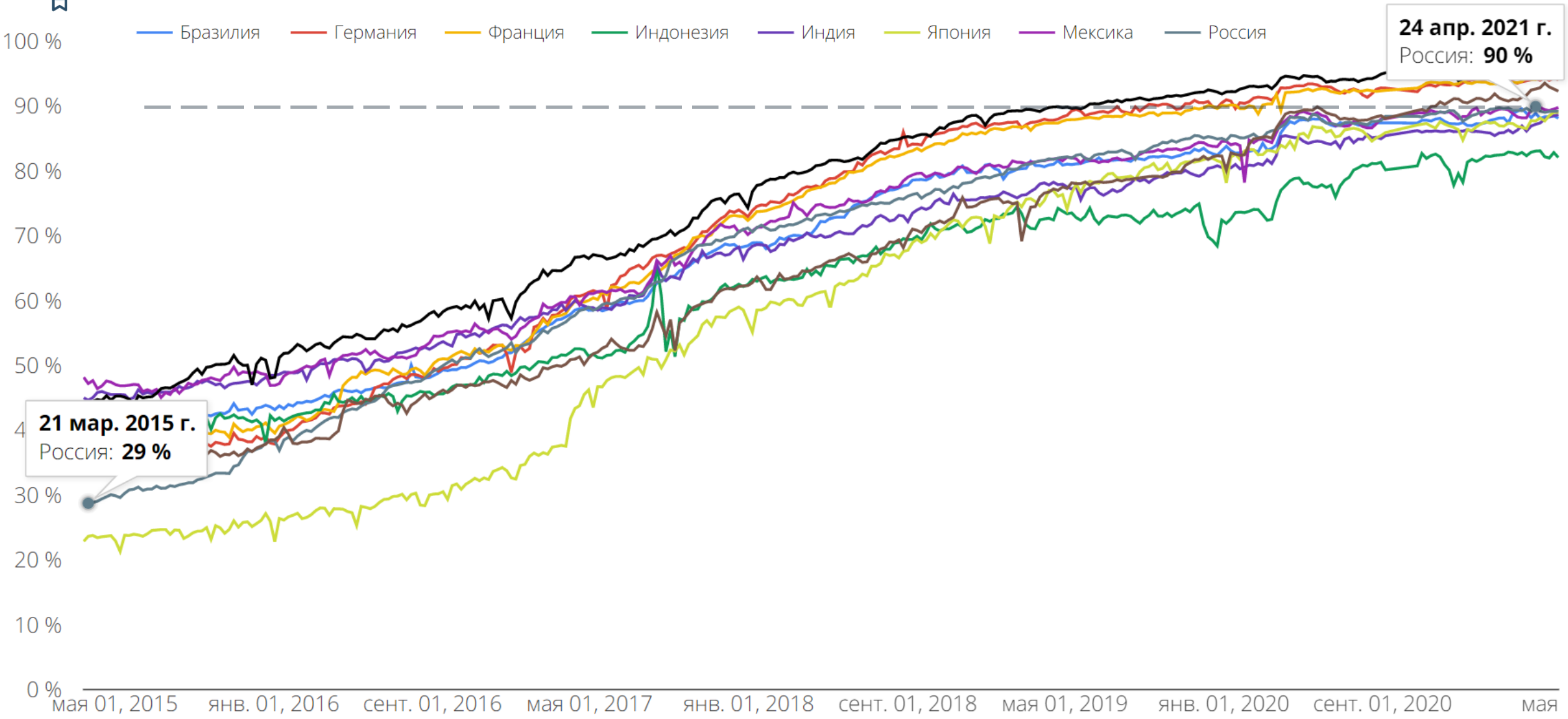
- Публикуется конкретный Сервис/Приложение
- Данные передаются в рамках HTTPS-сессии

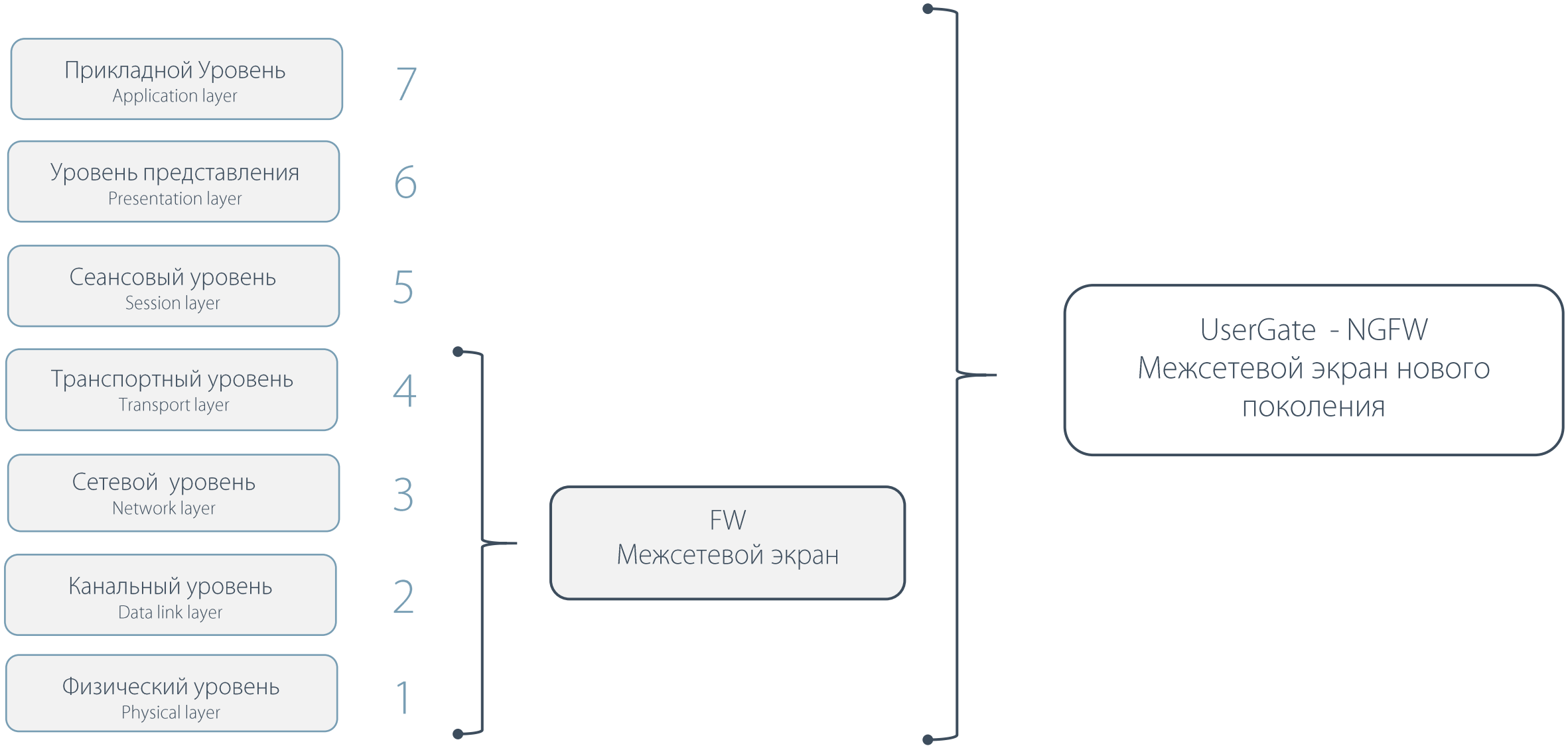
NGFW

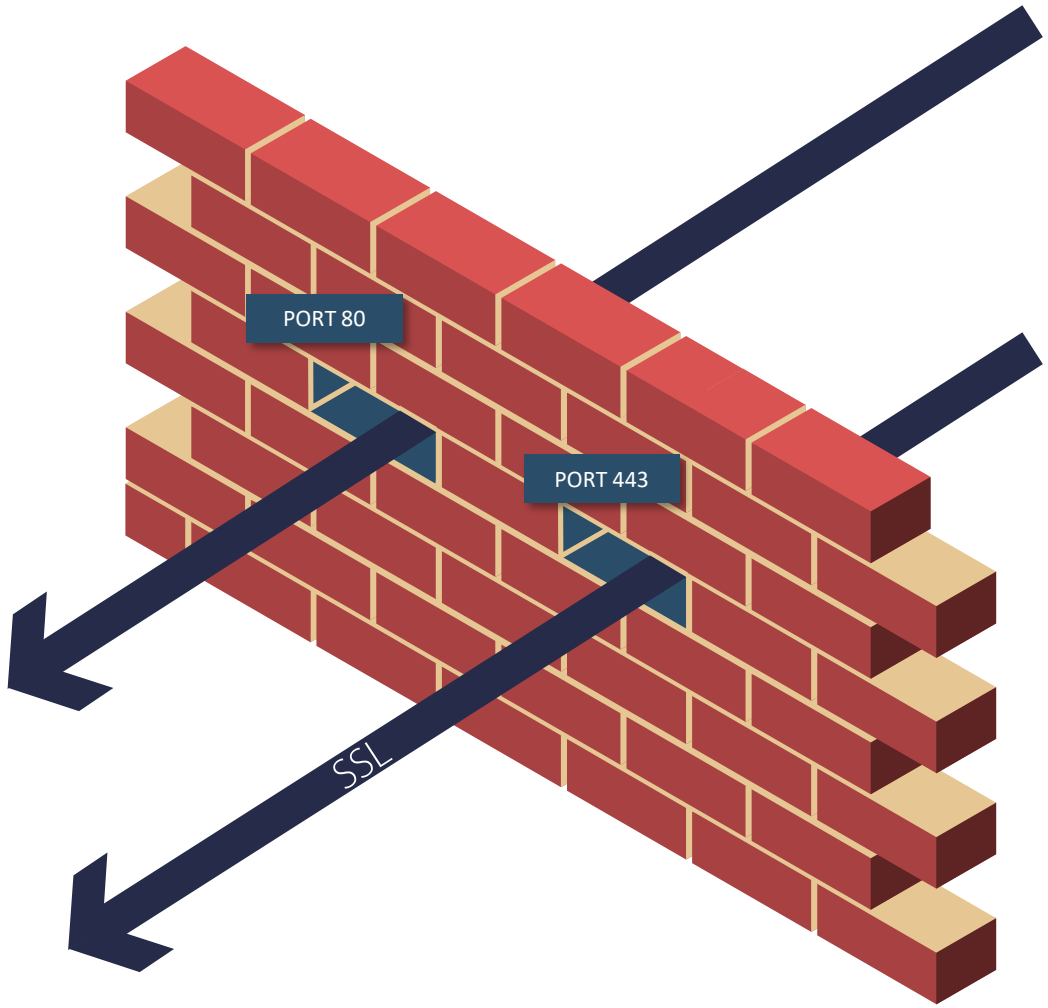
UserGate - Next Generation Firewall

- 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

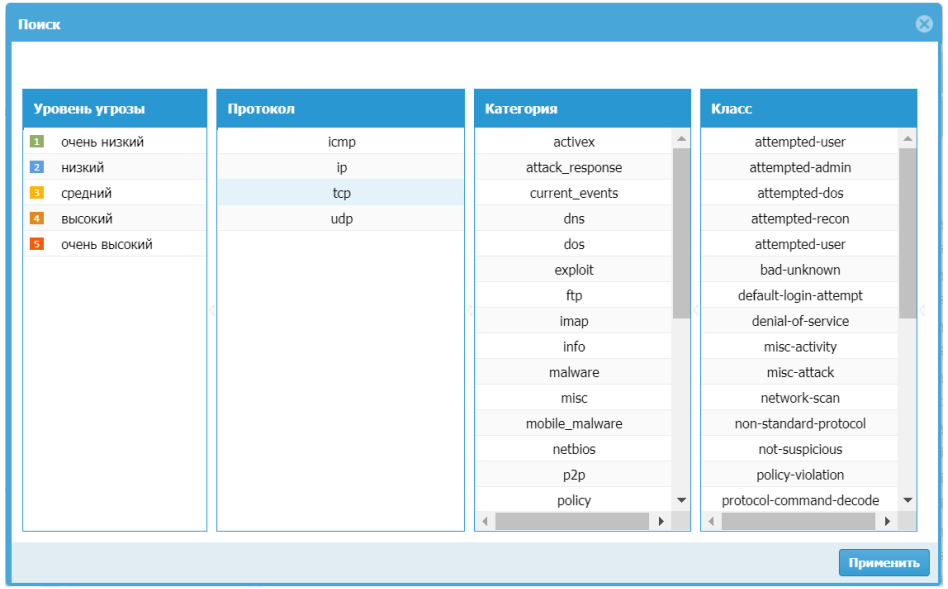

PORT 80
PORT 443
SSL

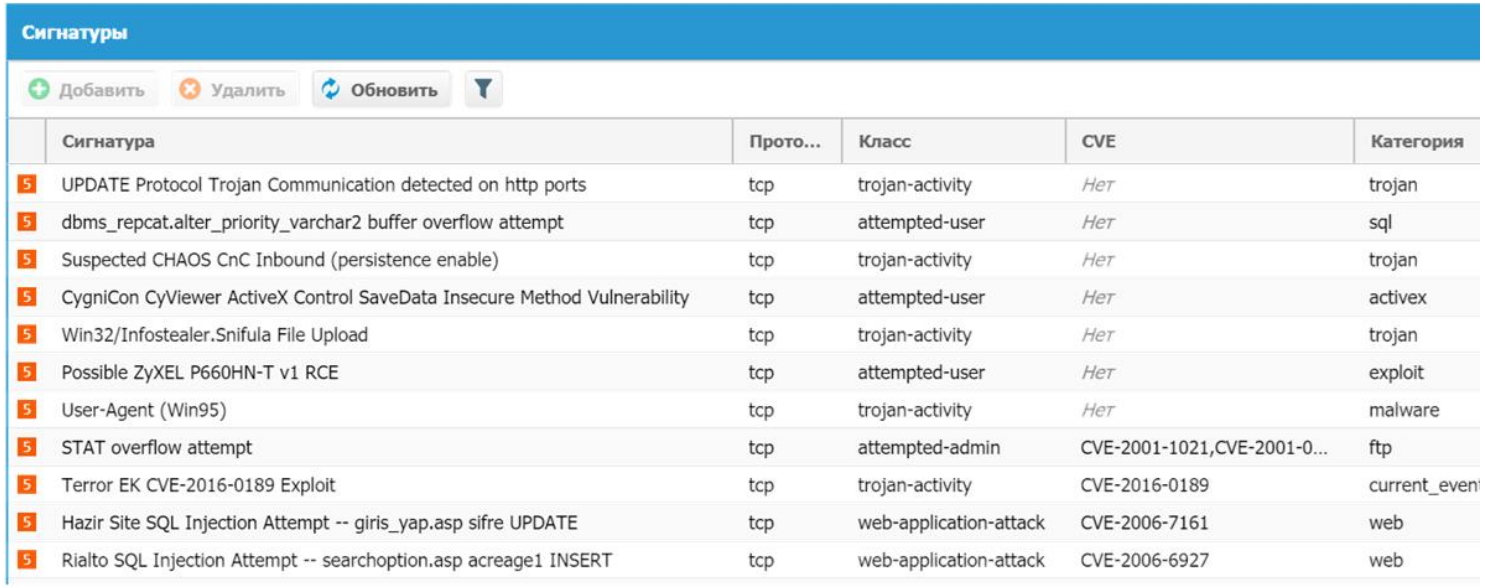

kaspersky
Yandex
Яндекс.Диск
zoom
Viber
Gmail
by Google
eset
@mail.ru
Microsoft
OfficeUpdate
ssh
COMMUNICATIONS SECURITY
AMMYY
JUST DO IT REMOTELY
SSL

Система обнаружения и предотвращения вторжений

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

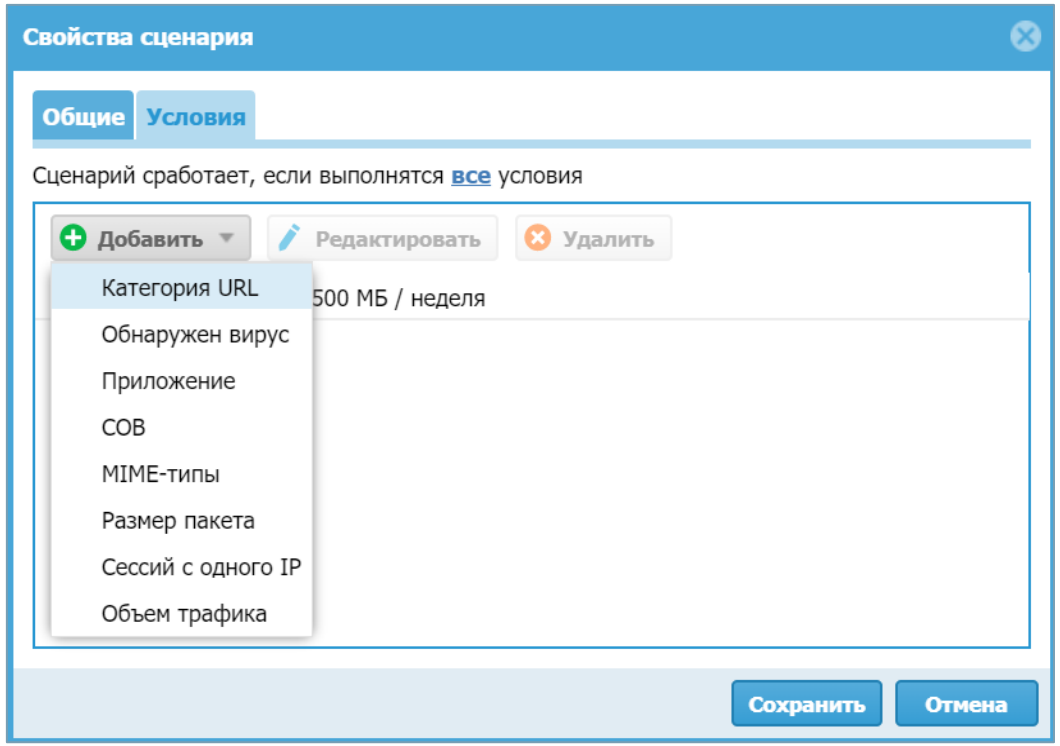
Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.





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_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

Технологии, используемые в UserGate, соответствуют современной концепции 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.



Защита АСУ ТП

Сращивание IT и OT влияют на производство

и на множество других областей

Управление зданиями

Энергетика

Логистика

Добыча ресурсов

Нефть и газ

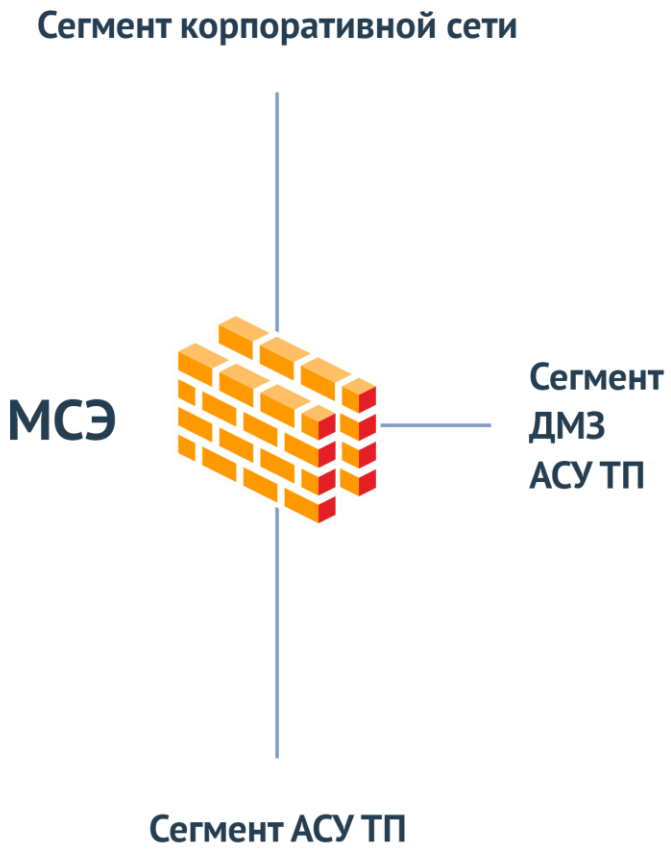
Умный город

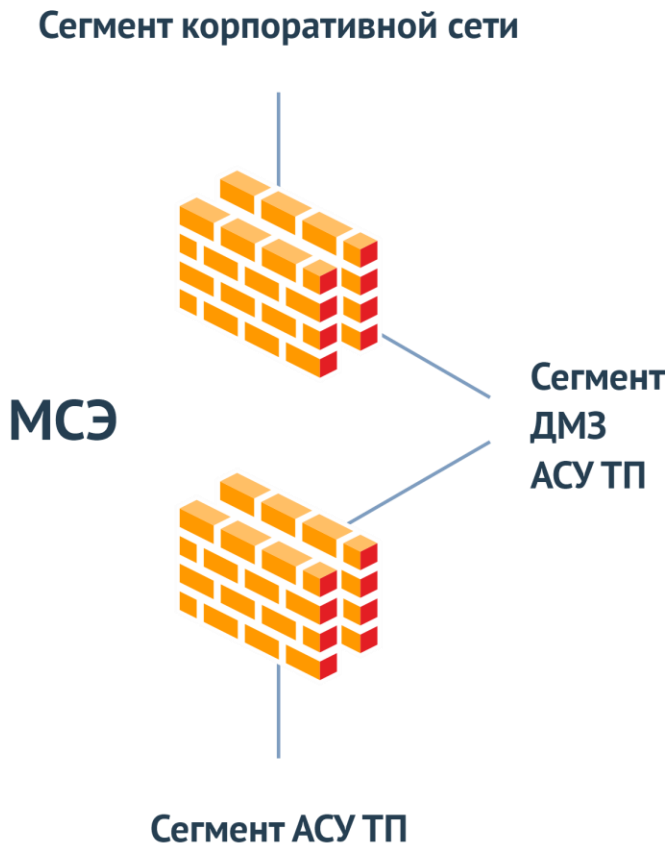
Водоснабжение

Химическая промышленность

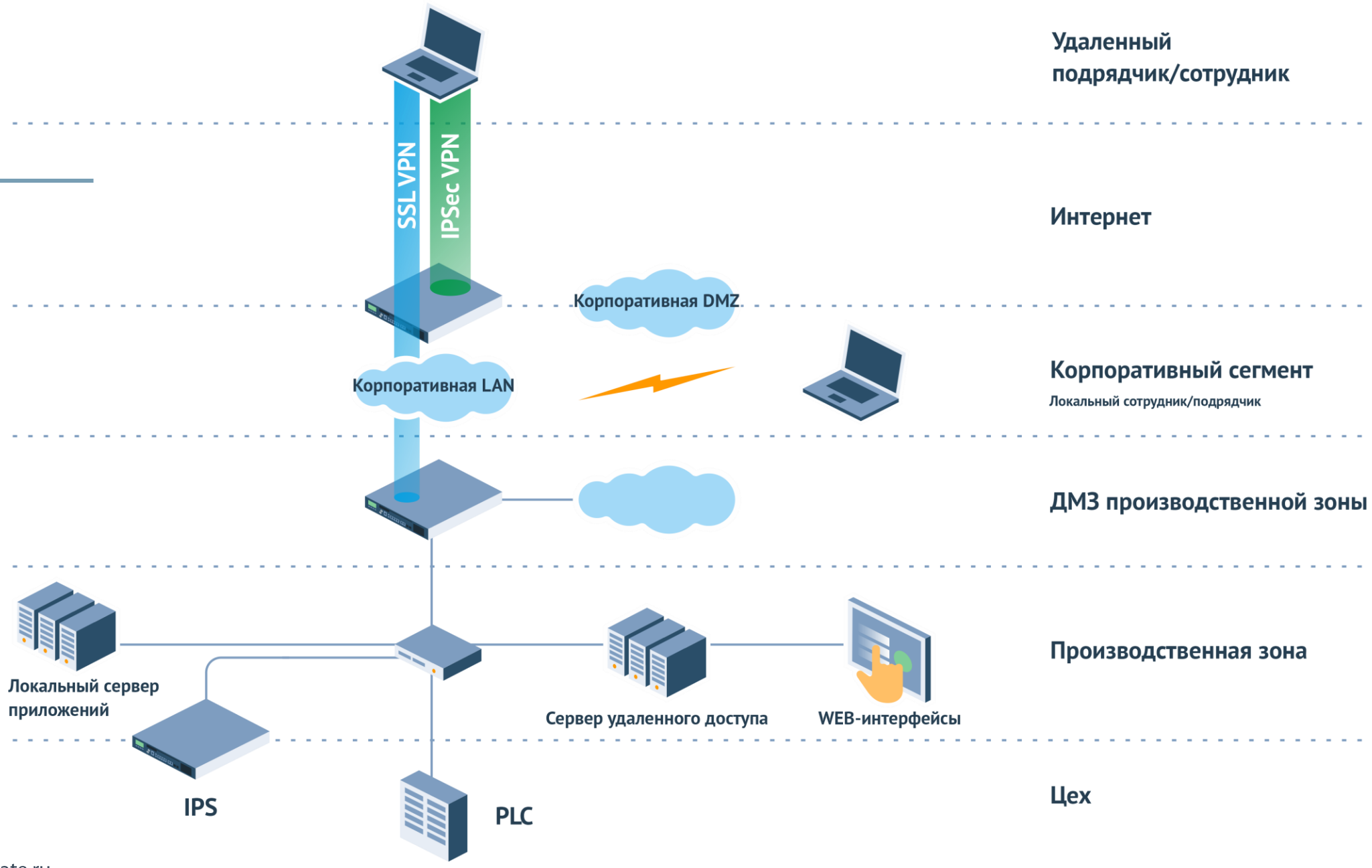
Угрозы IT	Угрозы OT
Конфиденциальность	Человеческие жертвы Техногенные катастрофы
Целостность	Повреждение оборудования Простои производства
Доступность	Конфиденциальность данных

NIST
ISA 99
ГОСТ
МЭК
CpwE





Итоговая Архитектура

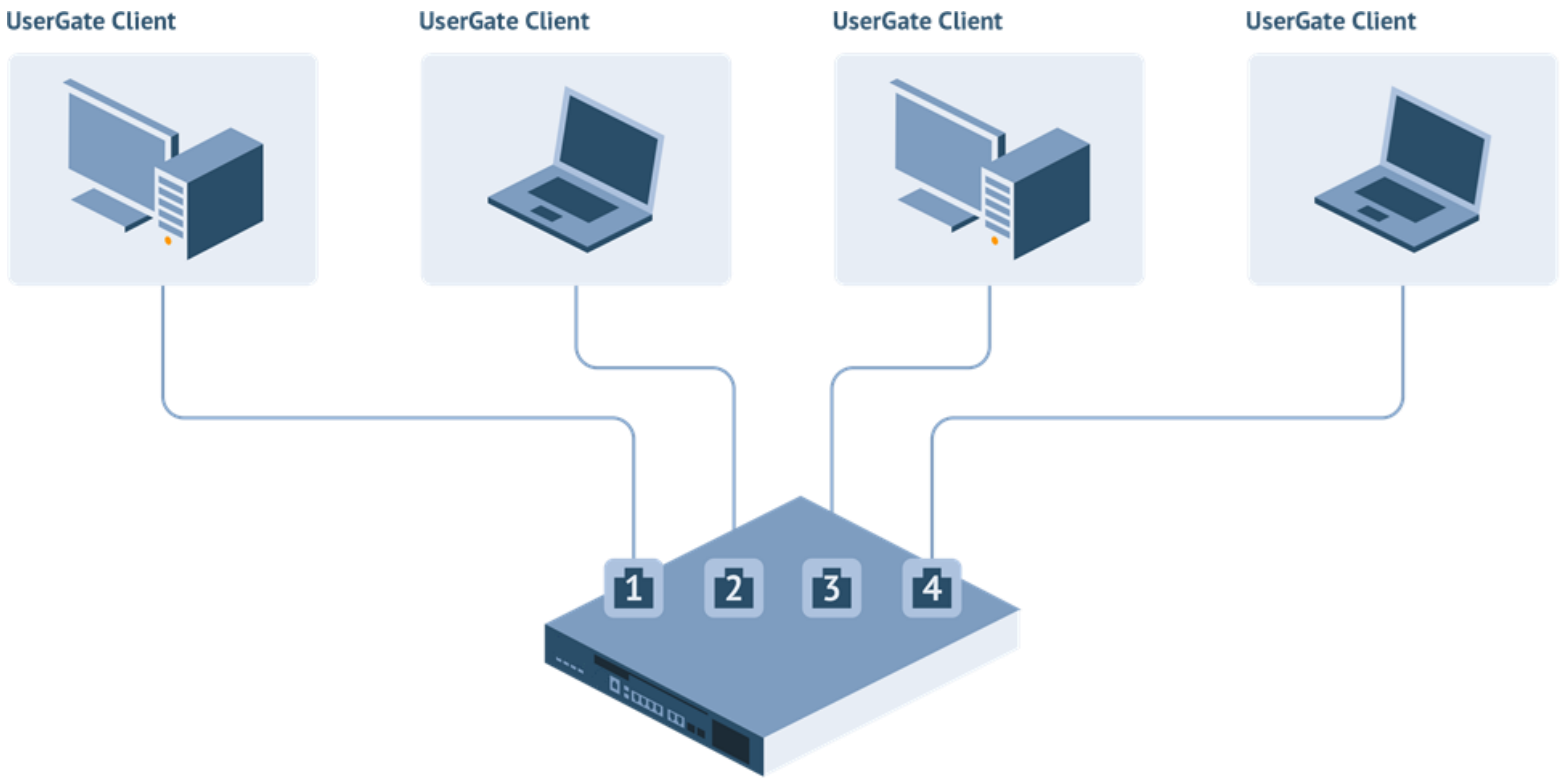


Защита клиентских устройств

- Одноразовые факторы компрометации
- Используются легитимные учетные данные
- Применение штатных средств ОС и легитимного ПО
- Отсутствие «общей» картины

- Дополнительная видимость
- Инструмент для обнаружения сложных угроз: IoC и IoA
- Углубленная информация
- Автоматизация процессов безопасности

- Сети без шлюзов с полной видимостью



- Межсетевой экран типа «В»
- Дополнительный уровень аутентификации
- VPN-клиент для организации безопасного удаленного доступа

Интернет фильтрация

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

- Собственная крупнейшая база электронных ресурсов – более 500 миллионов сайтов
- Более 80 категорий
- Ежедневное обновление списка сайтов
- Повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории

Группы URL категорий

Добавить | Редактировать | Удалить | Обновить

Название
Threats
Parental Control
Productivity
Safe categories
Recommended for morphology checking
Recommended for virus check

Категории

Добавить | Удалить | Экспорт | Обновить | Импорт

	Название
4	Азартные игры
2	Жестокое обращение с детьми
2	Игры
2	Наркотики
2	Насилие
5	Нелегальное ПО
2	Ненависть и нетерпение
2	Нецензурная лексика
2	Нудизм
4	Обмен картинками
2	Оружие
4	Пиринговые сети
1	Поиск работы
2	Покупки

Списки морфологии

Добавить | Редактировать | Удалить | Обновить

	Название списка	Author	Порог
1	Нецензурная лексика	© UserGate	Обычный
2	Наркотики	© UserGate	Обычный
3	Порнография	© UserGate	Обычный
2	Суицид	© UserGate	Обычный
5	Терроризм	© UserGate	Обычный
3	Соответствие списку запрещенных матер...	© UserGate	Обычный
4	Азартные игры	© UserGate	Обычный
3	Соответствие ФЗ-436 (защита детей)	© UserGate	Обычный
1	Юридический (DLP)	© UserGate	Обычный
3	Бухгалтерия (DLP)	© UserGate	Обычный
3	Финансы (DLP)	© UserGate	Обычный
5	Персональные данные (DLP)	© UserGate	Обычный
2	Маркетинг (DLP)	© UserGate	Обычный
1	Соответствие списку запрещенных матер...	© UserGate	Обычный

Списки URL

Добавить | Редактировать | Удалить

	Название
3	Microsoft Windows Internet checker
5	Соответствие реестру запрещенных сайтов Роскомнадзора (URL)
3	Соответствие списку запрещенных URL Министерства Юстиции РФ (URL)
5	Соответствие списку запрещенных URL Республики Казахстан
1	Список образовательных учреждений
4	Список поисковых систем без безопасного поиска
5	Список фишинговых сайтов

СЕРТИФИКАТ ФСТЭК России № 3905

Решение UserGate имеет действующий сертификат ФСТЭК России по 4 уровню доверия до 26.03.2026 г.

- Требования к МЭ

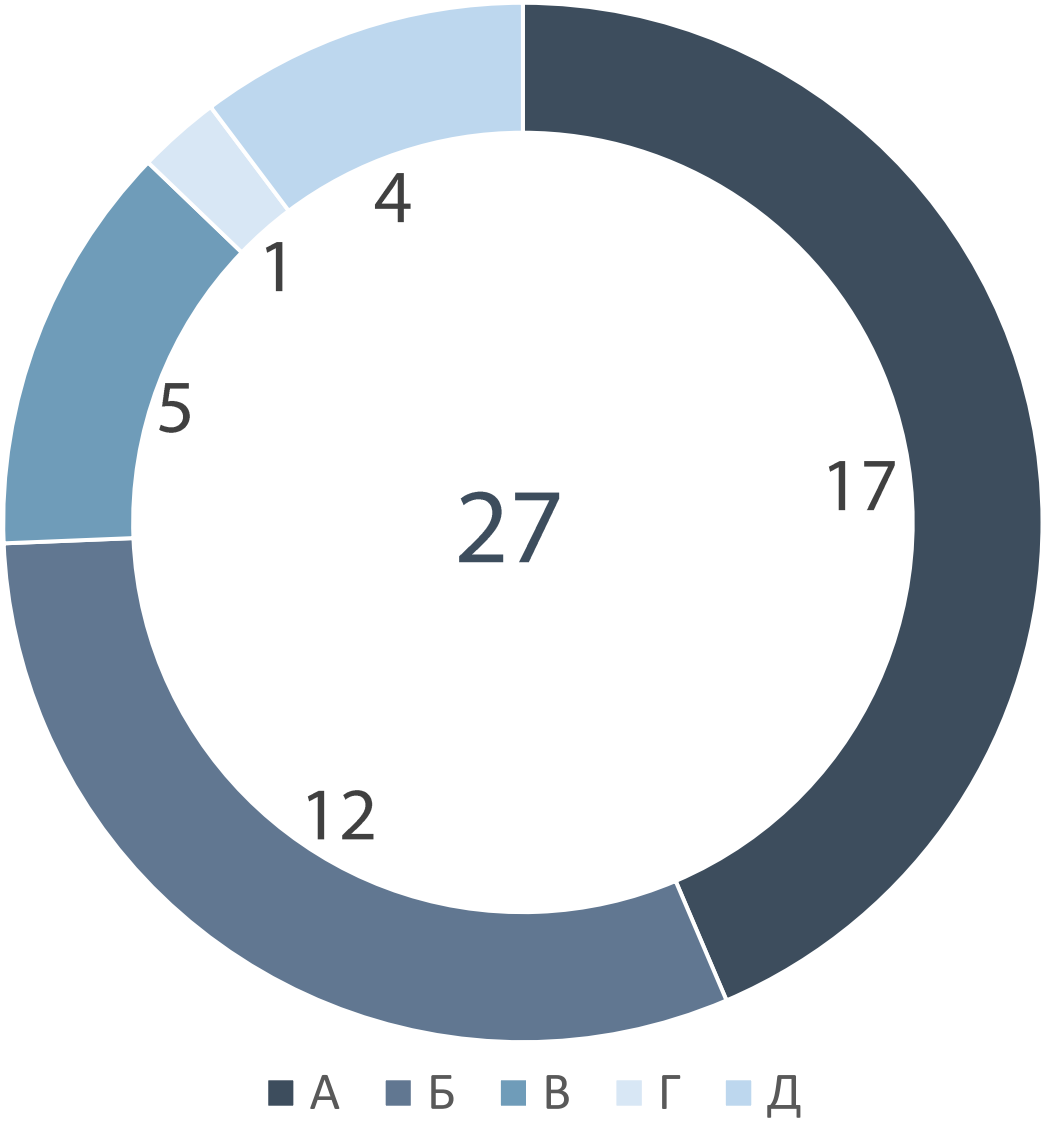
  «Профиль защиты МЭ типа А 4-го класса защиты»
  «Профиль защиты МЭ типа Б 4-го класса защиты»
  «Профиль защиты МЭ типа Д 4-го класса защиты».

- Требования к СОВ

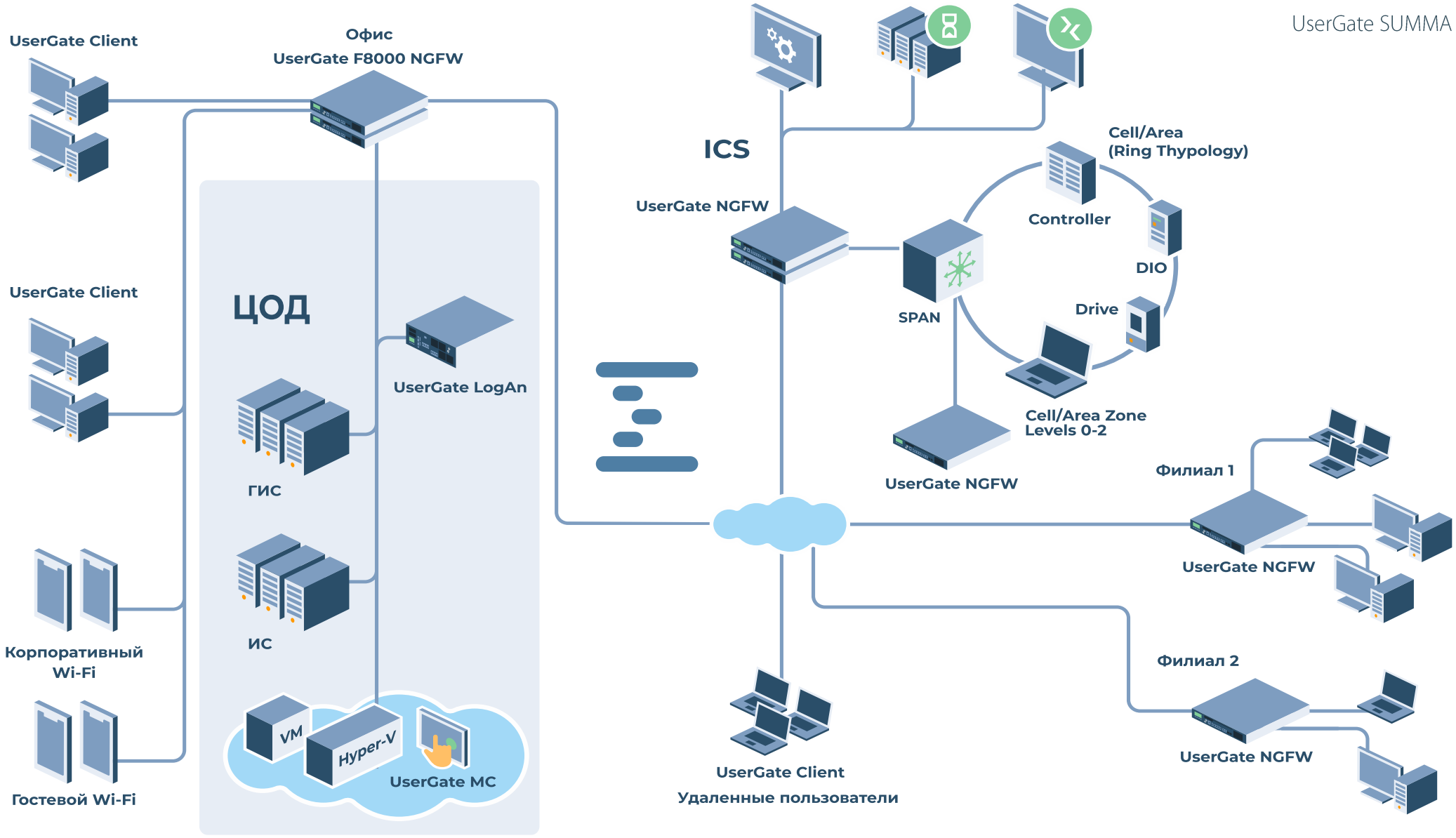
«Профиль защиты СОВ уровня сети 4- го класса защиты»

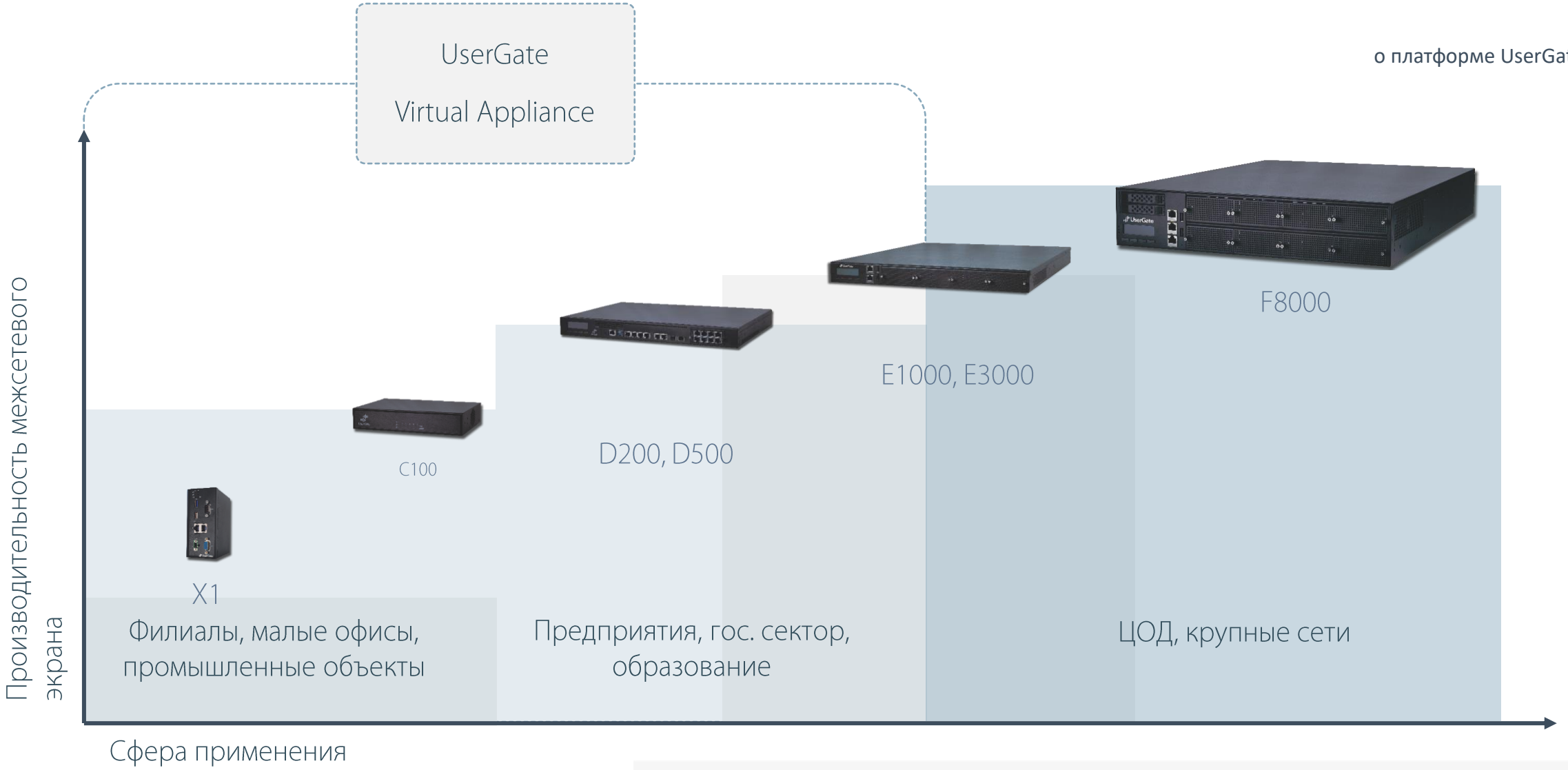
Уровень доверия 4:

- Классы защиты СЗИ 4;
- ЗО КИИ 1 категории;
- ГИС 1 класса;
- АСУТП 1 класса;
- ИСПДн 1 уровня;
- ИСОП II класса



Экосистема UserGate SUMMA

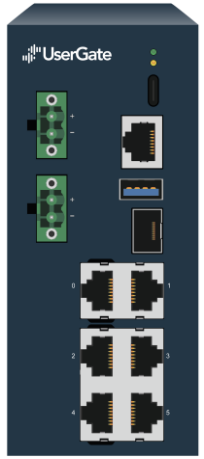

UserGate Client
Офис
UserGate F8000 NGFW
ICS
Cell/Area
(Ring Thypology)
UserGate NGFW
Controller
DIO
SPAN
Drive
UserGate Client
ЦОД
UserGate LogAn
ГИС
Cell/Area Zone
Levels 0-2
UserGate NGFW
Филиал 1
UserGate NGFW
ИС
Корпоративный
Wi-Fi
Филиал 2
VM
Hyper-V
UserGate MC
UserGate NGFW
Гостевой Wi-Fi
UserGate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



vmware | Microsoft Azure amazon web services | Xen | KVM | Hyper-V | openstack | VirtualBox

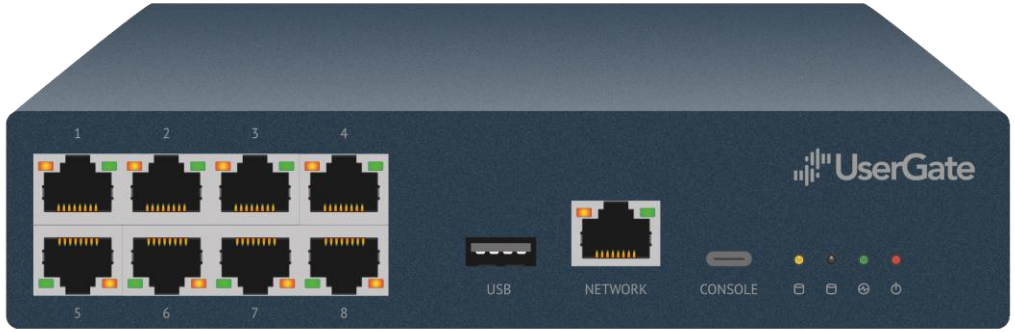
Собственные аппаратные платформы

Модель X1



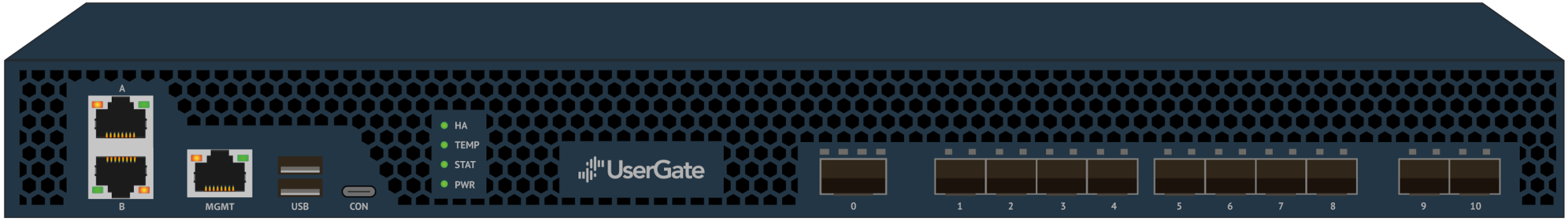
- МЭ до 2,5 Гб/с
- ARM 4 cores
- 6 портов 1GbE с поддержкой bypass
- 1 порт SFP
- Два блока питания
- От -40 до + 70 °C
- Крепление на DIN рейку

Модель C100



- МЭ до 2,5 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- Два блока питания
- От 0 до +70 °C

UserGate FG



- Аппаратная обработка трафика на ПЛИС
- Производительность МЭ более 80+ Gbps пакеты 64 байта, трафик реальных приложений
- Производительность PPS ~ 120 Mpps
- Wire speed – производительность МЭ = скорости сетевого интерфейса
- Собственная разработка
- Доверие к ПАК из Минпромторга

Сетевые порты:

- 10 x 10 Gbps SFP+
- 1 x 100 Gbps QSFP28
- 2 x 1 Gbps BASE-T
- IPMI
- SSD: от 128 Гб
- RAM: от 64 Гб
- БП: 2 с горячей заменой

UserGate

FORCEPOINT POWERED BY Raytheon

FORTINET

STONESOFT

Barracuda

KerioControl

BlueCoat

McAfee SECURE™

Microsoft Forefront

Check Point SOFTWARE TECHNOLOGIES LTD.

Ростелеком

ПЕНСИОННЫЙ ФОНД РОССИЙСКОЙ ФЕДЕРАЦИИ

MEGAFON

lady & gentleman CITY

горки город

29TH WINTER UNIVERSIADE KRASNOYARSK 2019

РЕСПУБЛИКА САХА (ЯКУТИЯ) • САХА ӨРӨСПҮҮБҮЛҮЭ

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

СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЦЕНТРАЛЬНАЯ ИЗБИРАТЕЛЬНАЯ КОМИССИЯ РОССИЙСКАЯ ФЕДЕРАЦИЯ

Спасибо за внимание!

Евгений Ханов
ekhanov@usergate.ru
8 800 500 40 32 | +7 (913) 390-01-88