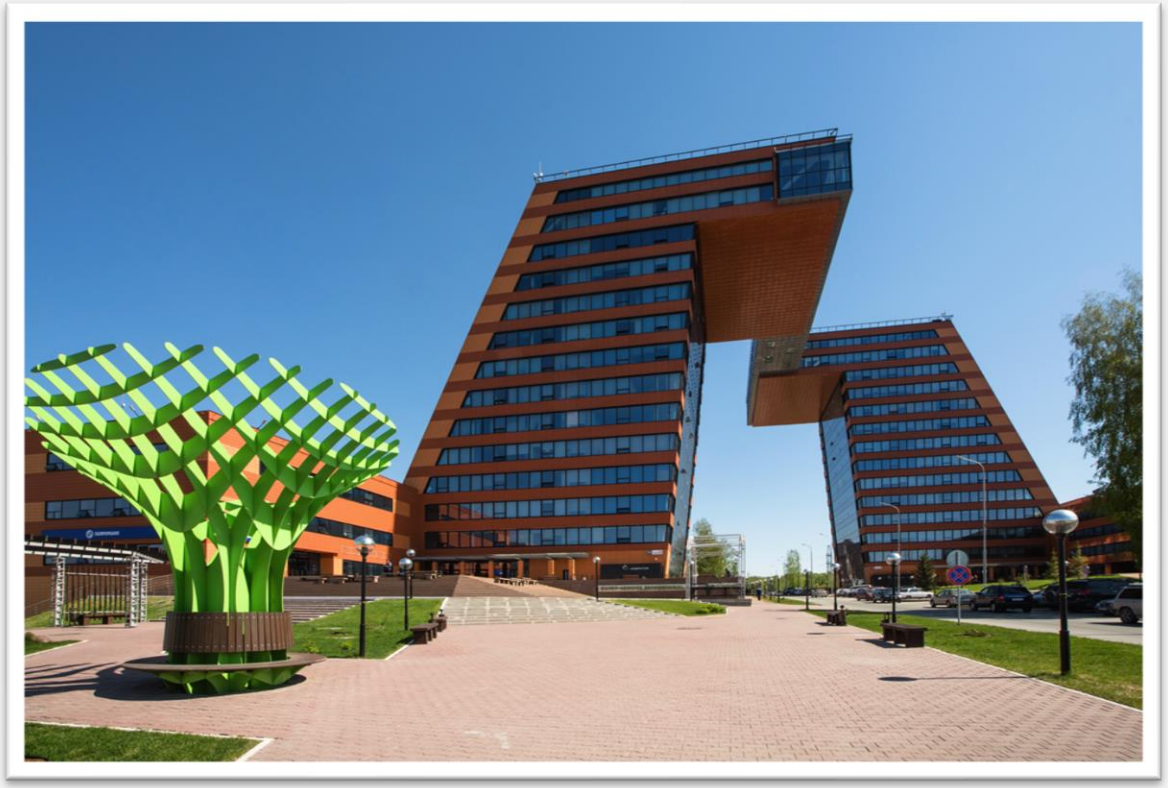
Практика импортозамещения в обеспечении информационной безопасности

Андрей Полянский
Региональный представитель в ЮФО, СКФО
apolyanskiy@usergate.ru
8 800 500 40 32 | +7 (915) 340 04 21



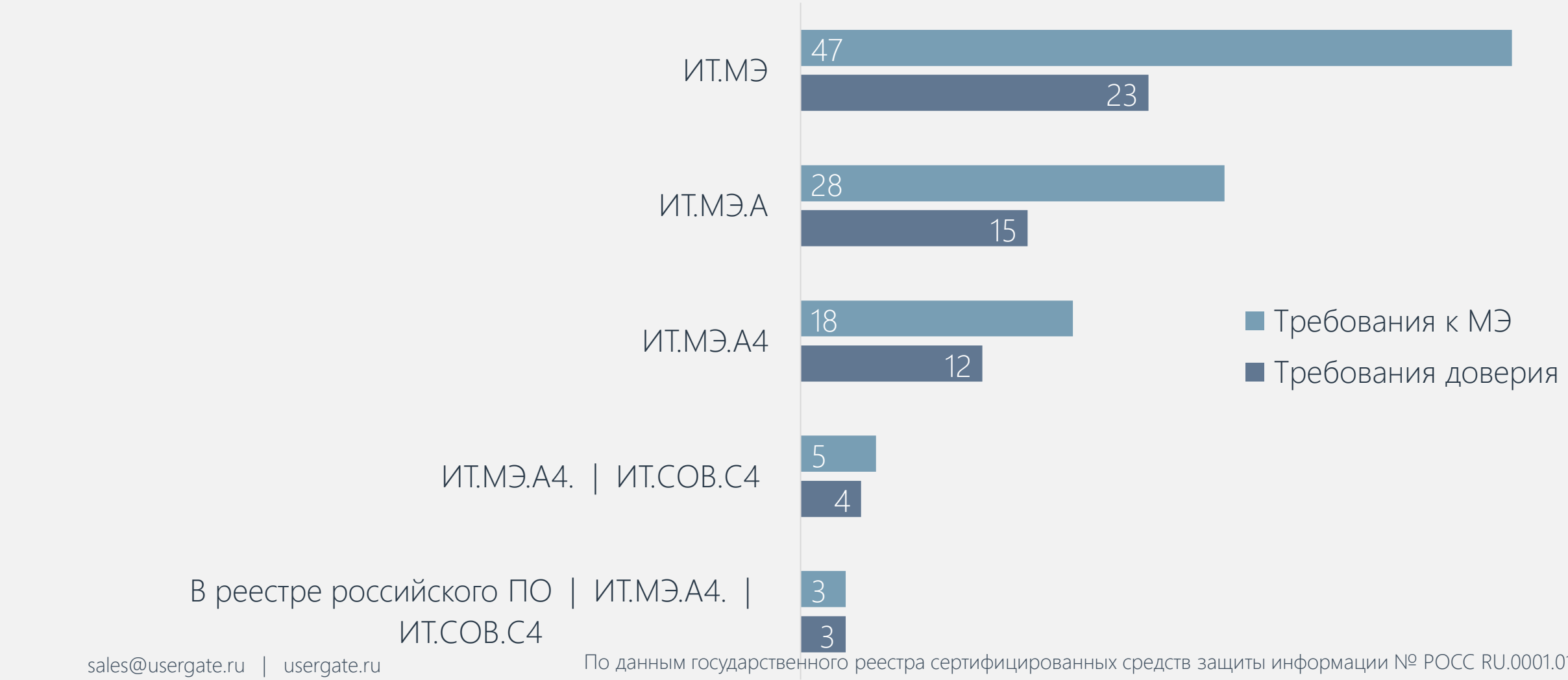
Наш офис разработки находится в Технопарке Новосибирского Академгородка, в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

Дополнительные офисы:
г. Москва, ИЦ «Сколково»
г. Хабаровск

UserGate

Реестр сертифицированных средств защиты информации ФСТЭК России

Сертификатов, выданных на серию в реестре ФСТЭК России*:



По данным государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 от 17.05.2021 сертификатов, выданных на серию в реестре ФСТЭК России:

Изначально дедлайном по импортозамещению установили 2021 год

2023 год – импортозамещение в ПО

2024 год – импортозамещение в железе

Приобретение новых зарубежных СЗИ/ПО – нецелевое расходование средств

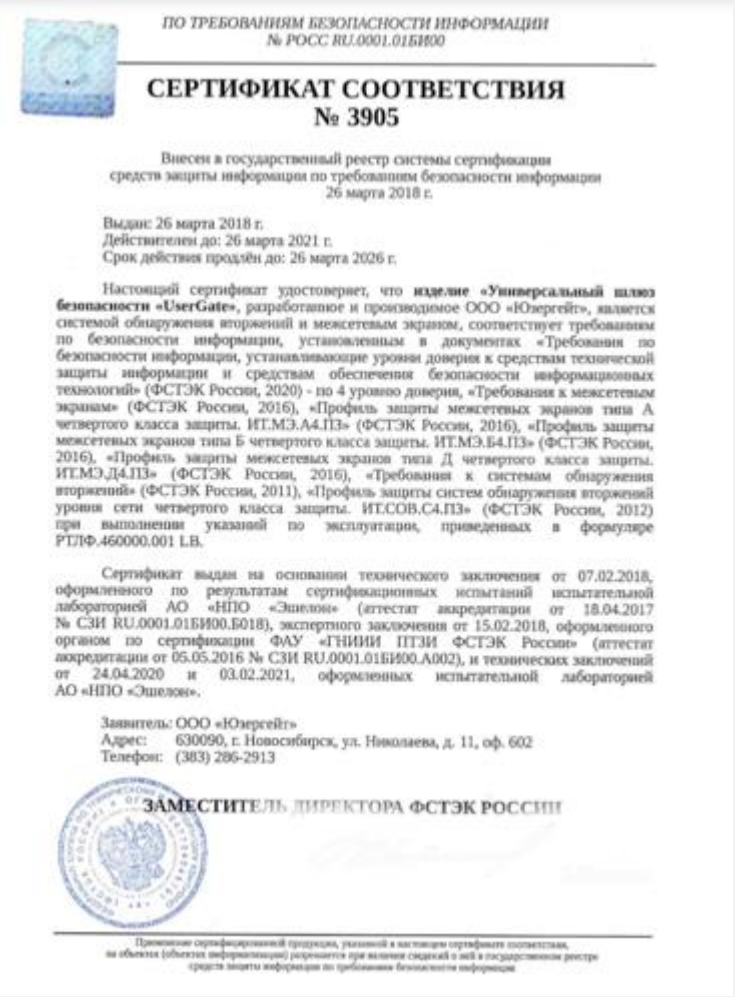
СЕРТИФИКАТ ФСТЭК России № 3905

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



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 26 марта 2018 г.

Выдан: 26 марта 2018 г.
Действителен до: 26 марта 2021 г.
Срок действия продлён до: 26 марта 2026 г.

Настоящий сертификат удостоверяет, что **изделие «Универсальный шлюз безопасности «UserGate»**, разработанное и производимое ООО «Юзергейт», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре РТЛФ.460000.001 ЛФ.

Сертификат выдан на основании технического заключения от 07.02.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), экспертного заключения от 15.02.2018, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технических заключений от 24.04.2020 и 03.02.2021, оформленных испытательной лабораторией АО «НПО «Эшелон».

Заявитель: ООО «Юзергейт»
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602
Телефон: (383) 286-2913

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

UserGate

Что нужно для обеспечения информационной безопасности?

Безопасная публикация ресурсов и сервисов

Межсетевой экран NGFW

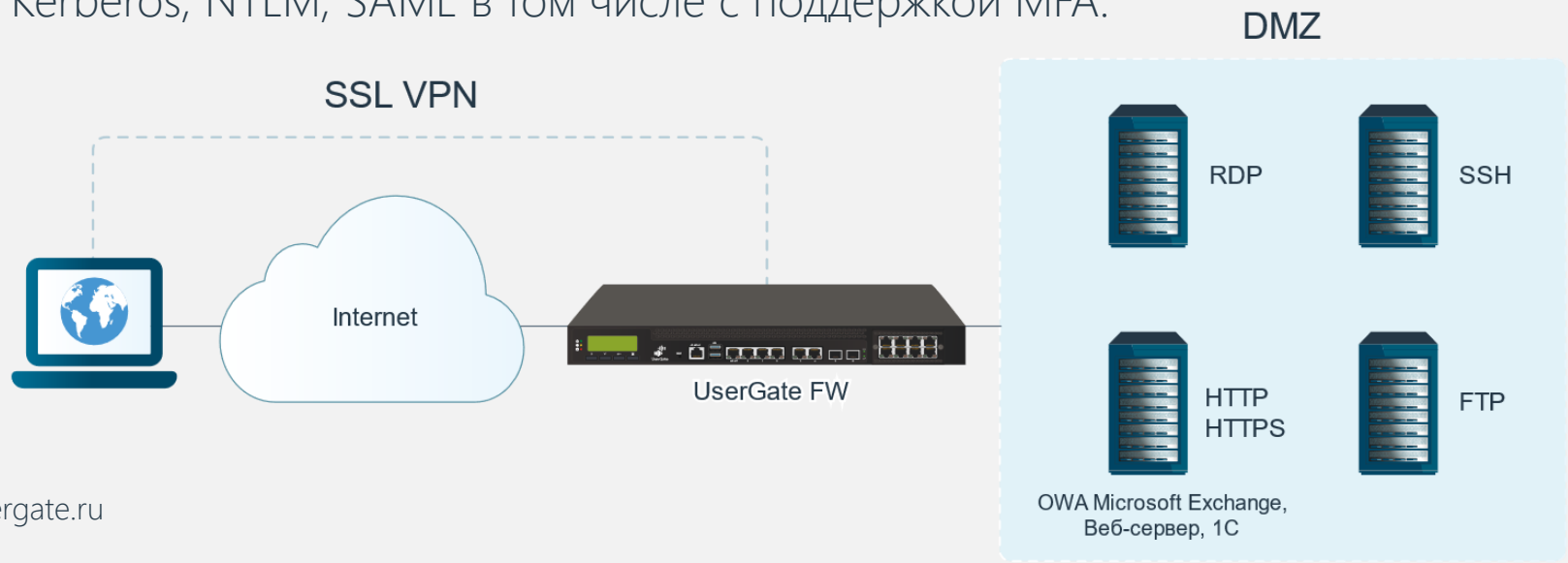
Система обнаружения и предотвращения вторжений

Анализ и предотвращение новых угроз (SOAR)

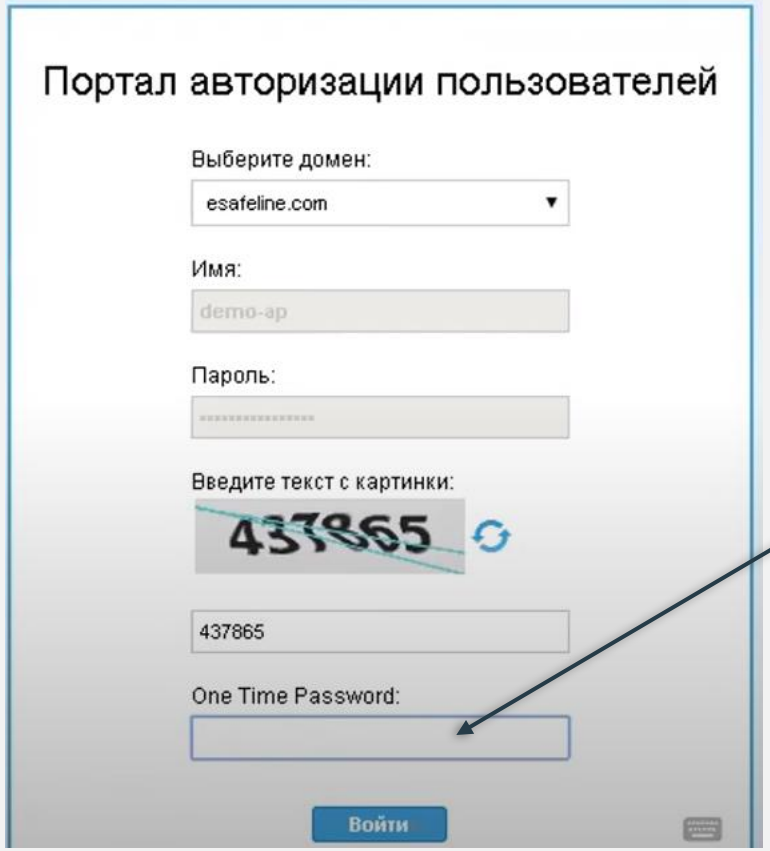
Интернет фильтрация

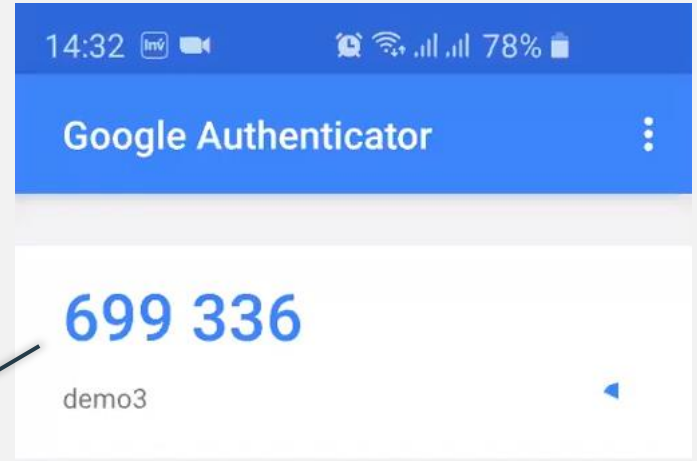
Reverse Proxy - обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

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.

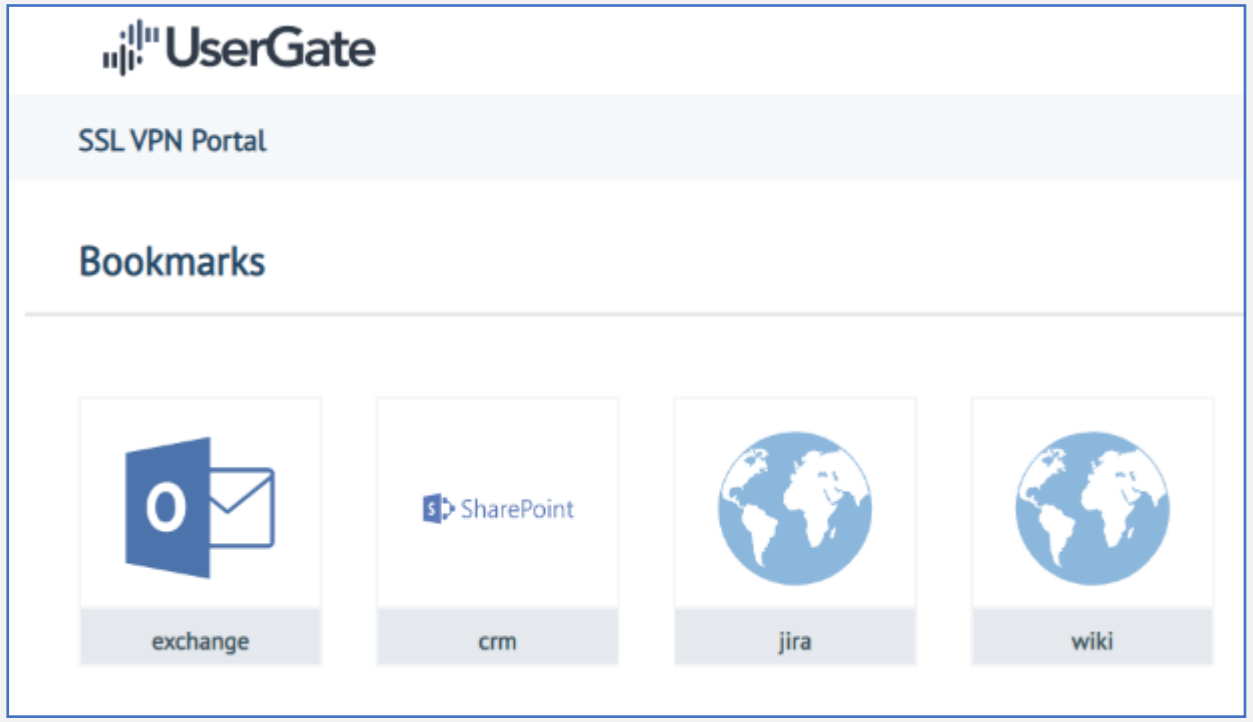


- MFA (TOTP, SMS, Email)
- Настройка политик доступа к отдельным сервисам по пользователям и группам
- Доступ через браузер
- SSO





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



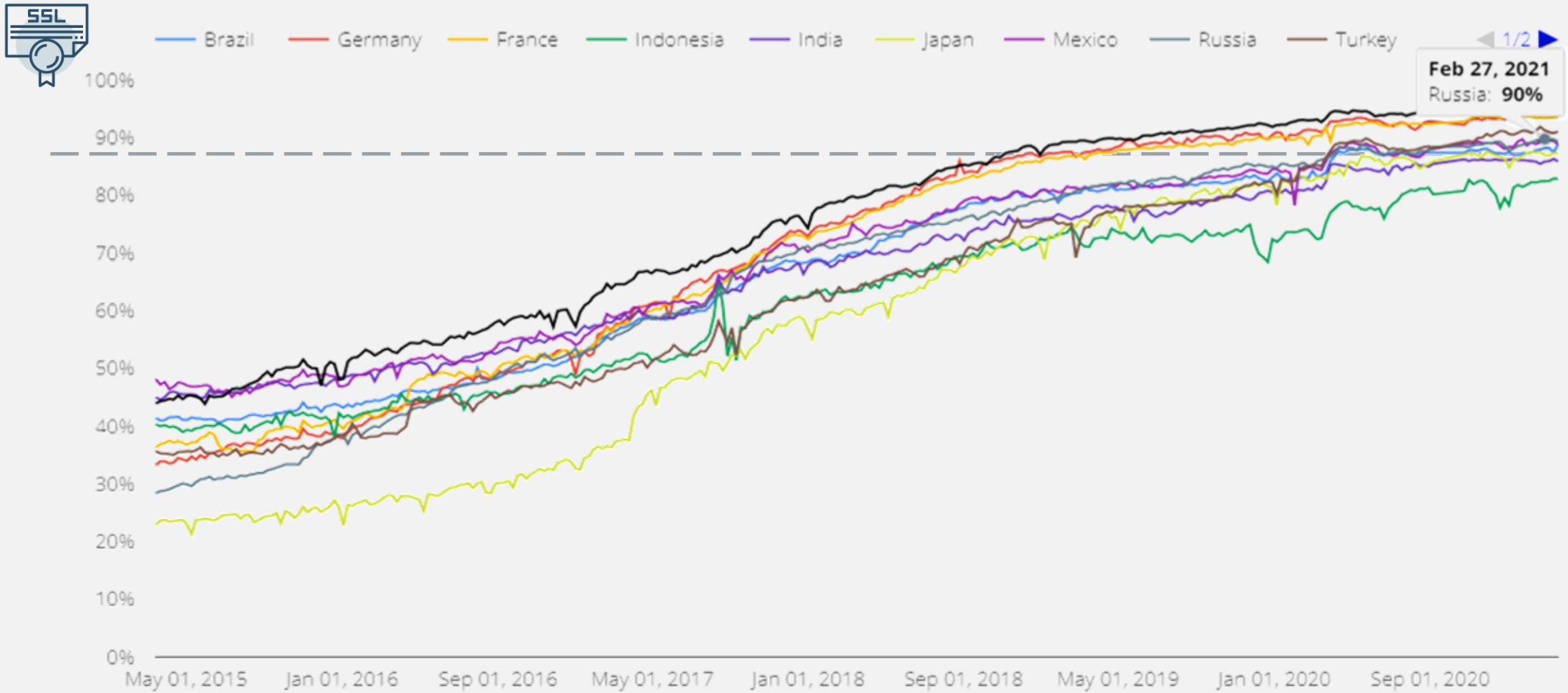
Аутентификация пользователей и применение к пользователям правил межсетевого экранирования, контентной фильтрации, контроля приложений с поддержкой таких средств и протоколов аутентификации, как Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, MFA.

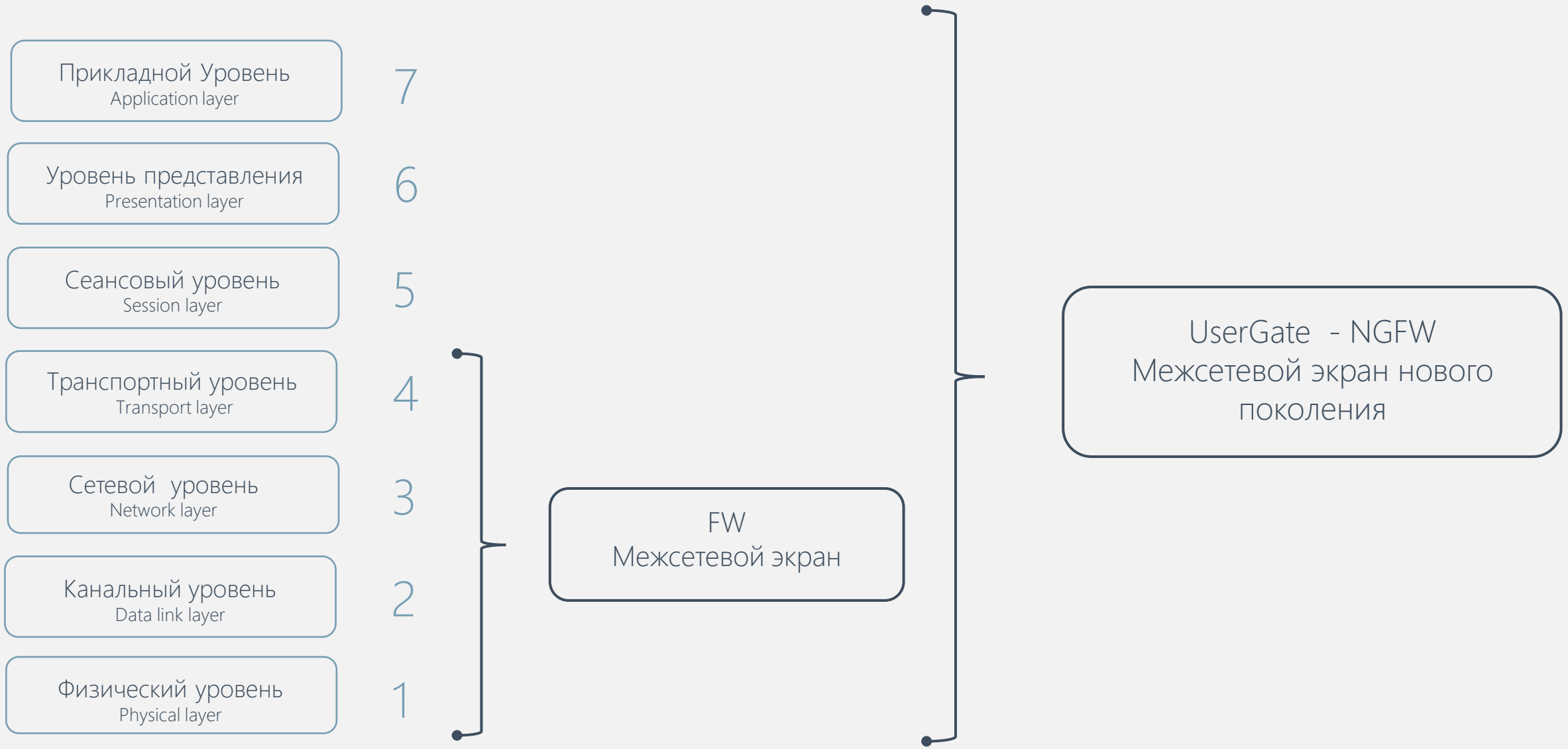
Администраторы могут применить определенные политики безопасности к любому пользователю, группе пользователей или, например, ко всем неизвестным пользователям.

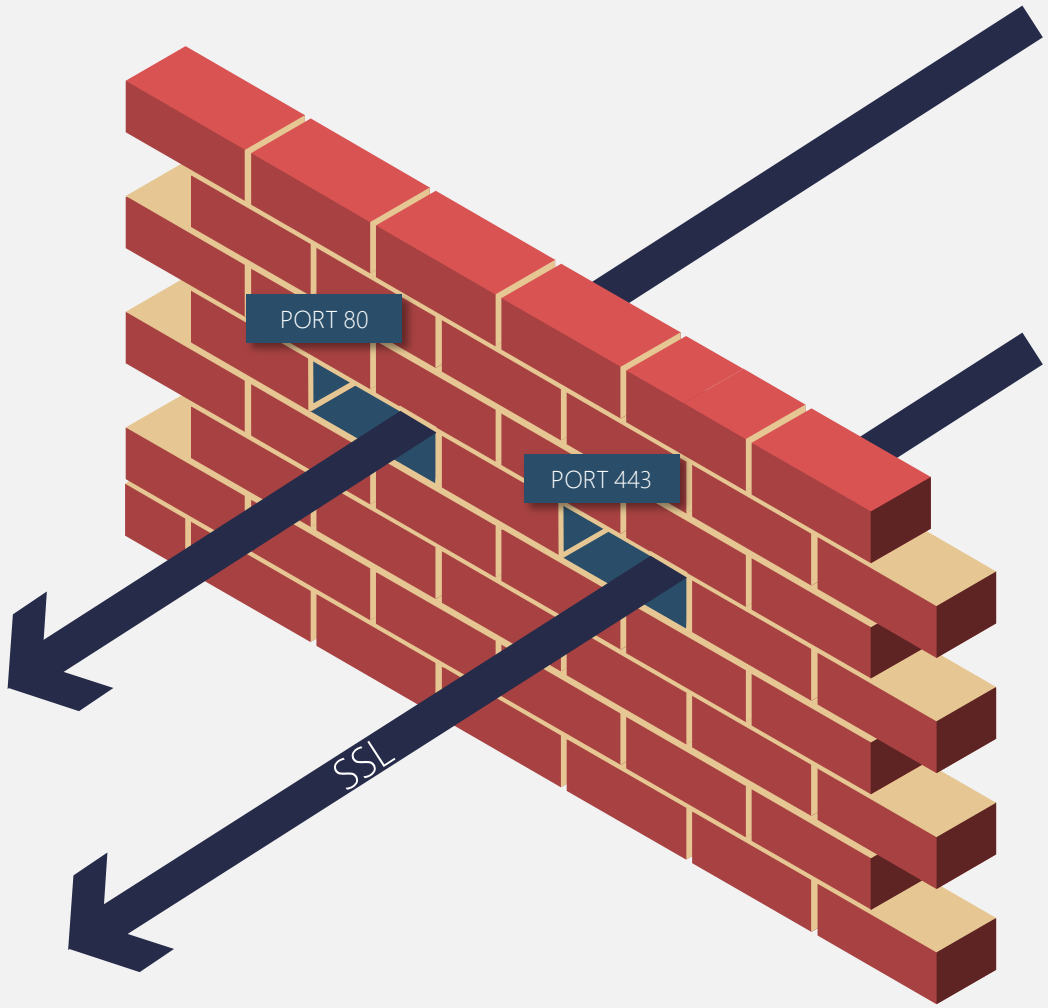
UserGate - Next Generation Firewall

- Высокая скорость обработки трафика
- Идентификация пользователей
- Применение гибких политик к пользователям
- Контроль приложений на L7 уровне по всем портам
- Интернет-фильтрация, инспекция SSL-трафика
- Защита от DoS-атак

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

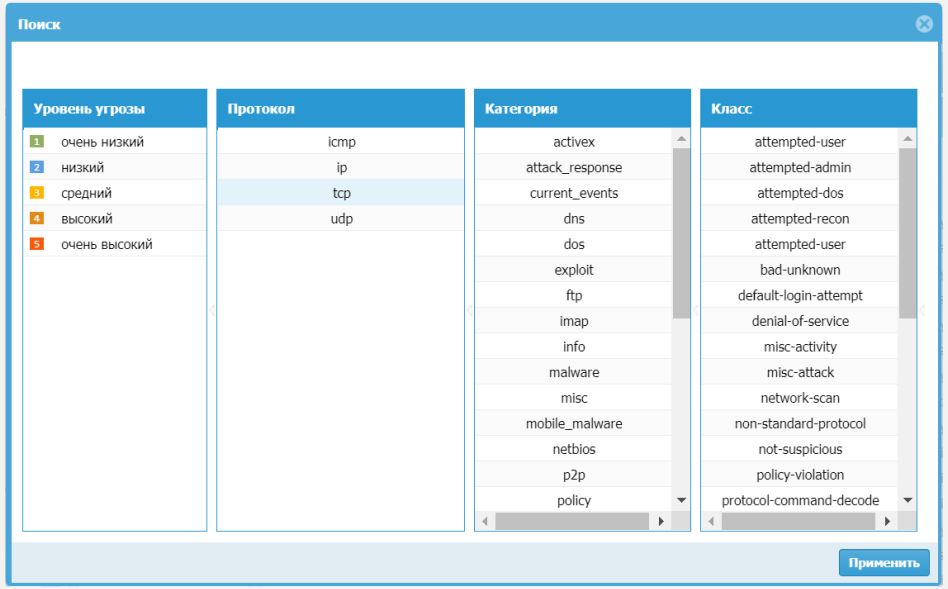


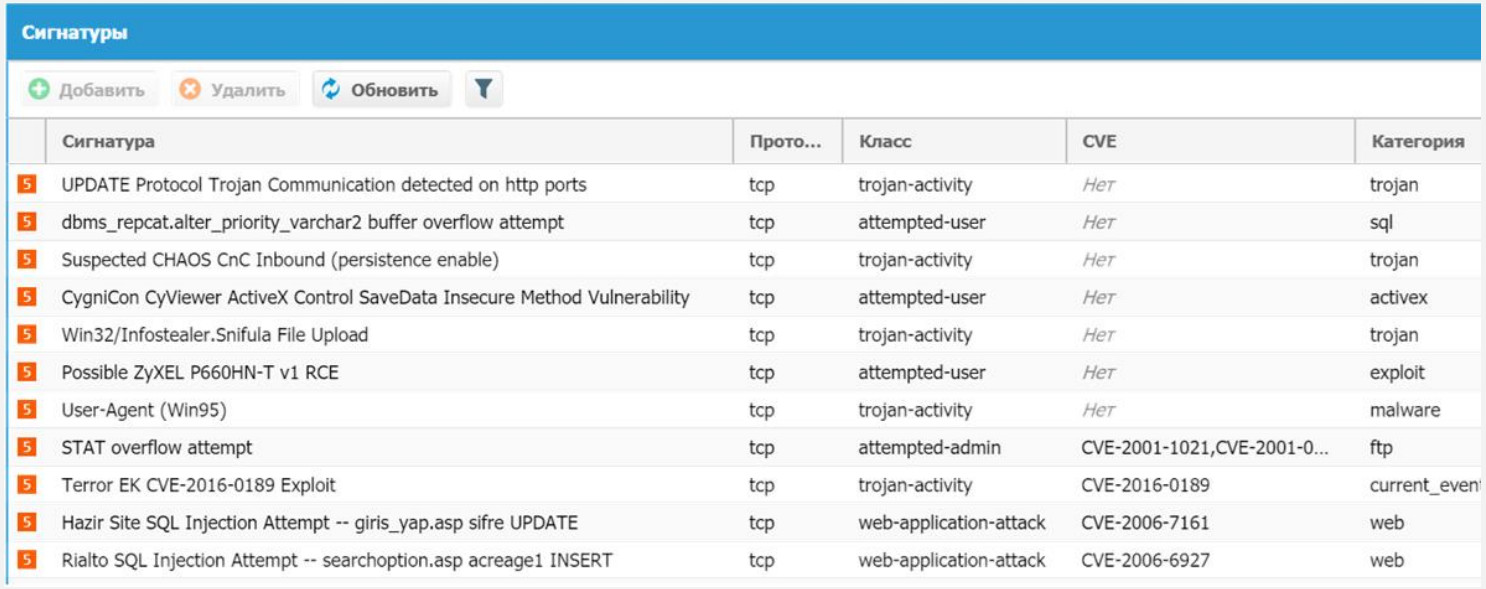

Прикладной Уровень
Application layer
7
Уровень представления
Presentation layer
6
Сеансовый уровень
Session layer
5
Транспортный уровень
Transport layer
4
Сетевой уровень
Network layer
3
Канальный уровень
Data link layer
2
Физический уровень
Physical layer
1
FW
Межсетевой экран
UserGate - NGFW
Межсетевой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

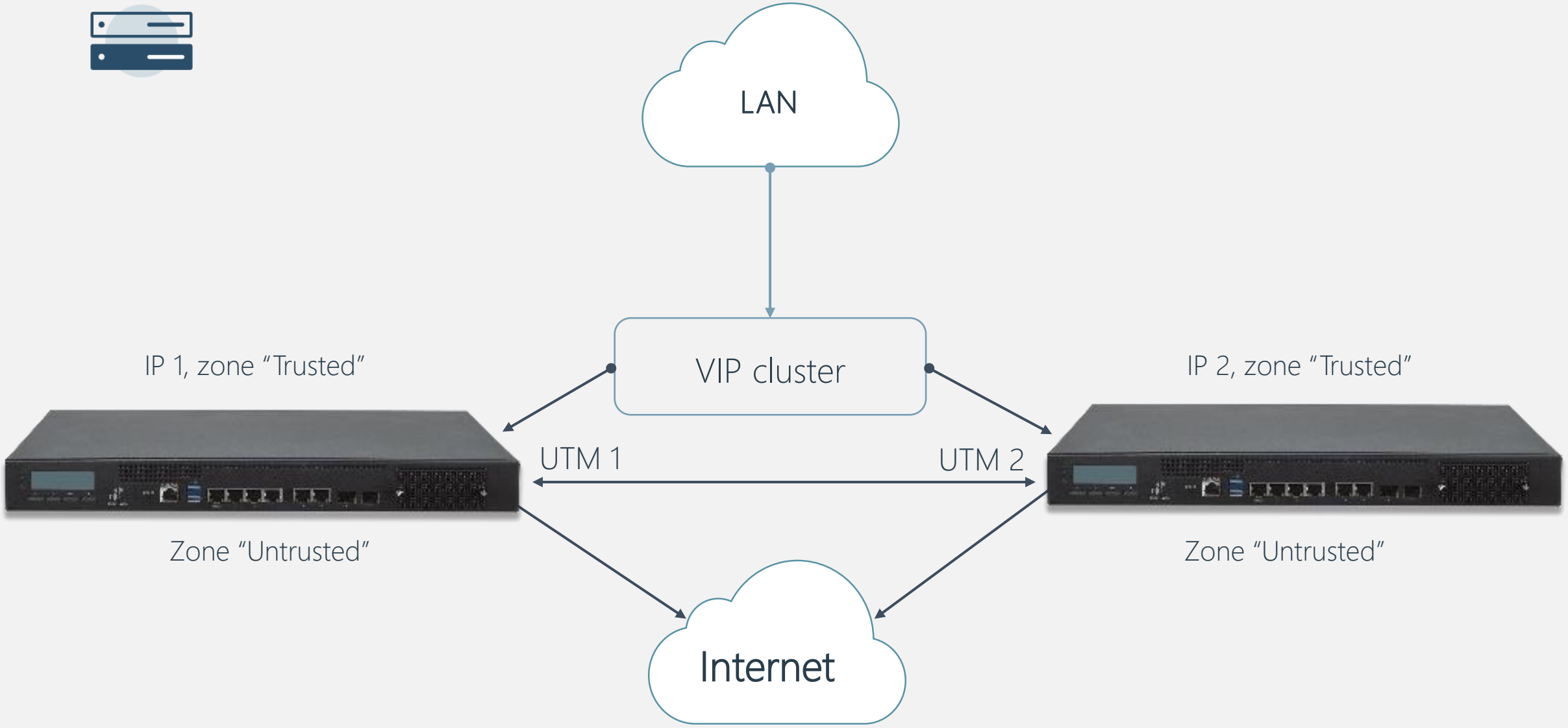




Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repcat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon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

Различные механизмы фильтрации:

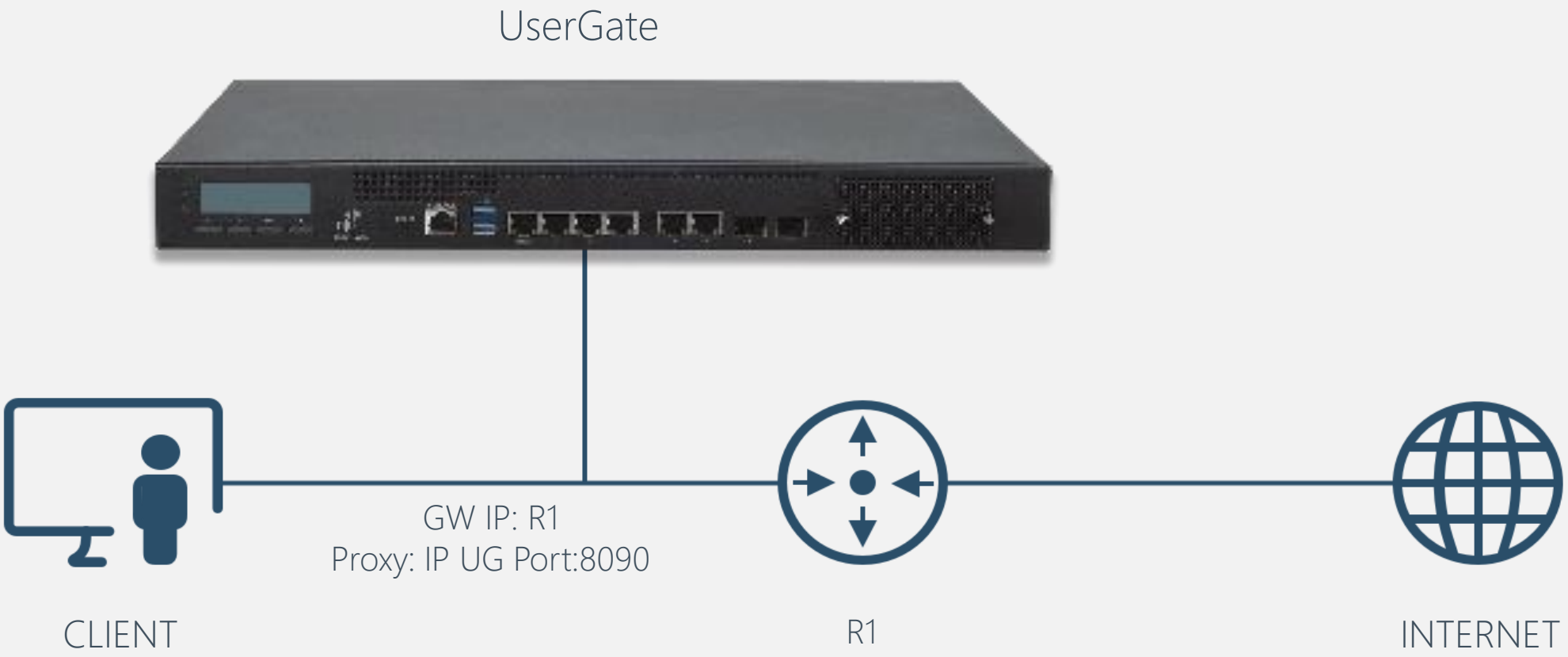
- фильтрация по категориям (UserGate URL filtering 4.0)
- морфологический анализ
- безопасный поиск
- белые и черные списки
- блокировка контекстной рекламы
- запрет загрузки определенных видов файлов
- антивирусная проверка трафика на базе технологии dci


LAN
VIP cluster
IP 1, zone “Trusted”
IP 2, zone “Trusted”
UTM 1
UTM 2
Zone “Untrusted”
Zone “Untrusted”
Internet

UserGate

Сценарии применения


GW IP: UG
UserGate
CLIENT
Rule: NAT
INTERNET


UserGate
GW IP: R1
Proxy: IP UG Port:8090
CLIENT
R1
INTERNET


UserGate
PDF
STATISTICS
SPAN
PORT
CLIENT
R1

Популярные IP-адреса источников атак по сигнатурам

Популярные IP-адреса источников атак за указанный промежуток времени сгруппированные по сигнатурам

№	Сигнатура	Угроза	Категория	IP-адрес	Событий	Процент
1	**Suspicious inbound to MSSQL port 1433**	**4**	**Potentially Bad Traffic**		**10,459**	**72.66%**
				61.188.18.251	37	0.35%
				221.194.44.156	32	0.31%
				116.252.35.206	31	0.3%
				221.194.44.208	31	0.3%
				103.238.69.88	30	0.29%
				Другие: 6395	10,298	98.46%
2	**Suspicious User Agent (BlackSun)**	**5**	**A Network Trojan was detected**		**2,451**	**17.03%**
				138.68.85.159	2,451	100%
3	**Potential MySQL bot scanning for SQL server**	**5**	**A Network Trojan was detected**		**445**	**3.09%**
				211.141.207.5	24	5.39%
				139.162.110.42	21	4.72%
				219.129.237.188	15	3.37%
				51.91.212.81	15	3.37%
				83.97.20.33	13	2.92%
				Другие: 234	357	80.22%

Топ категорий СОВ

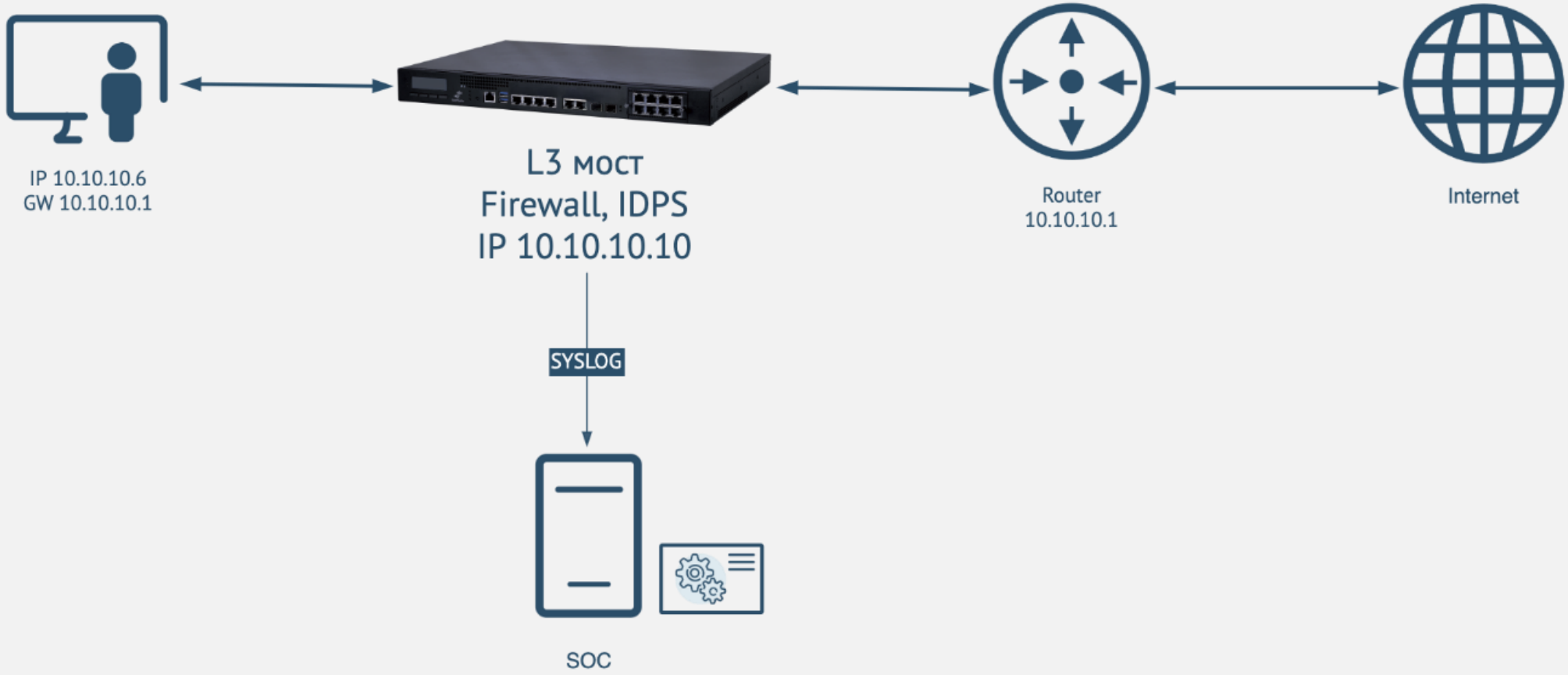
Топ категорий атак по количеству атак за указанный промежуток времени

№	Угроза	Категория	Событий	Процент
1	4	Potentially Bad Traffic	11,324	78.67%
2	5	A Network Trojan was detected	2,896	20.12%
3	5	Attempted Administrator Privilege Gain	120	0.83%
4	5	Attempted User Privilege Gain	33	0.23%
5	2	Attempted Information Leak	11	0.08%
6	4	Potential Corporate Privacy Violation	11	0.08%
Всего: 6			**14,395**	**100%**

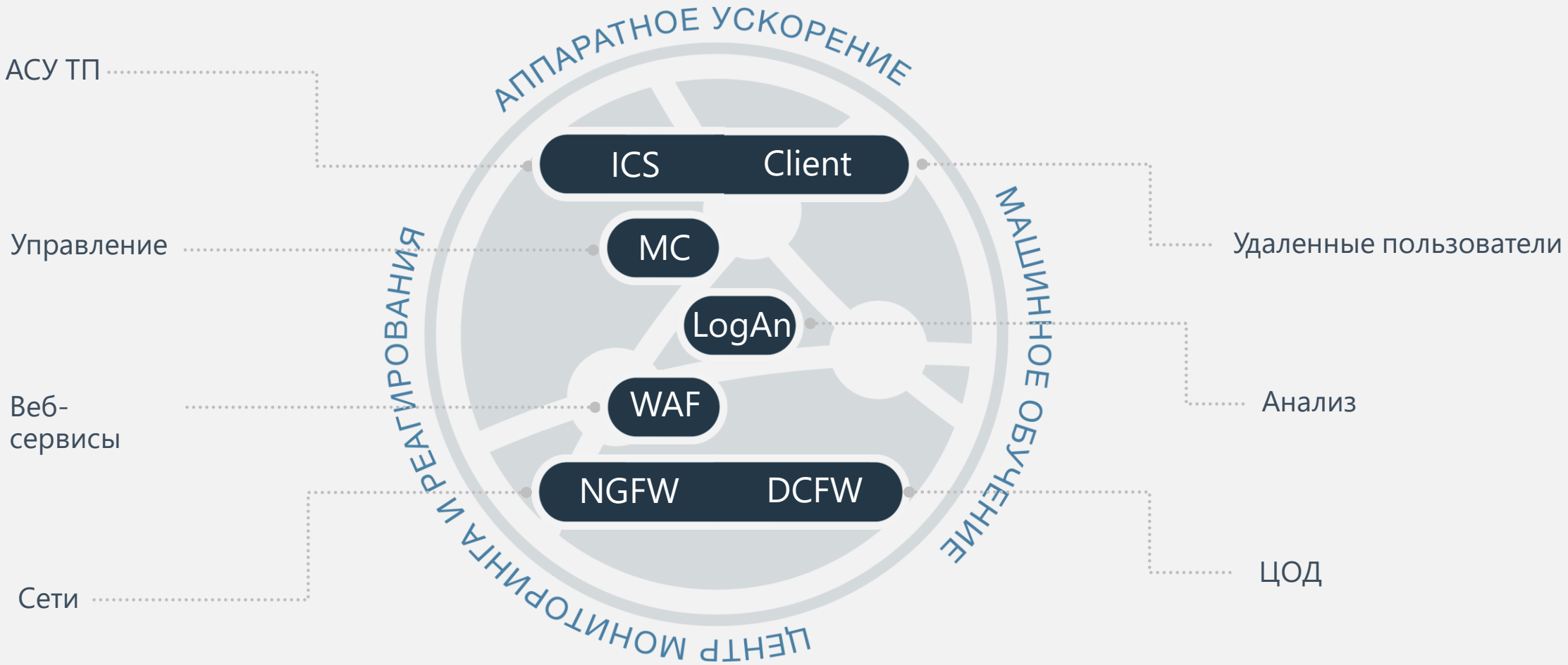
IP-адреса источников атак по адресам назначения

IP-адреса источников атак за указанный промежуток времени сгруппированные по IP-адресам назначения

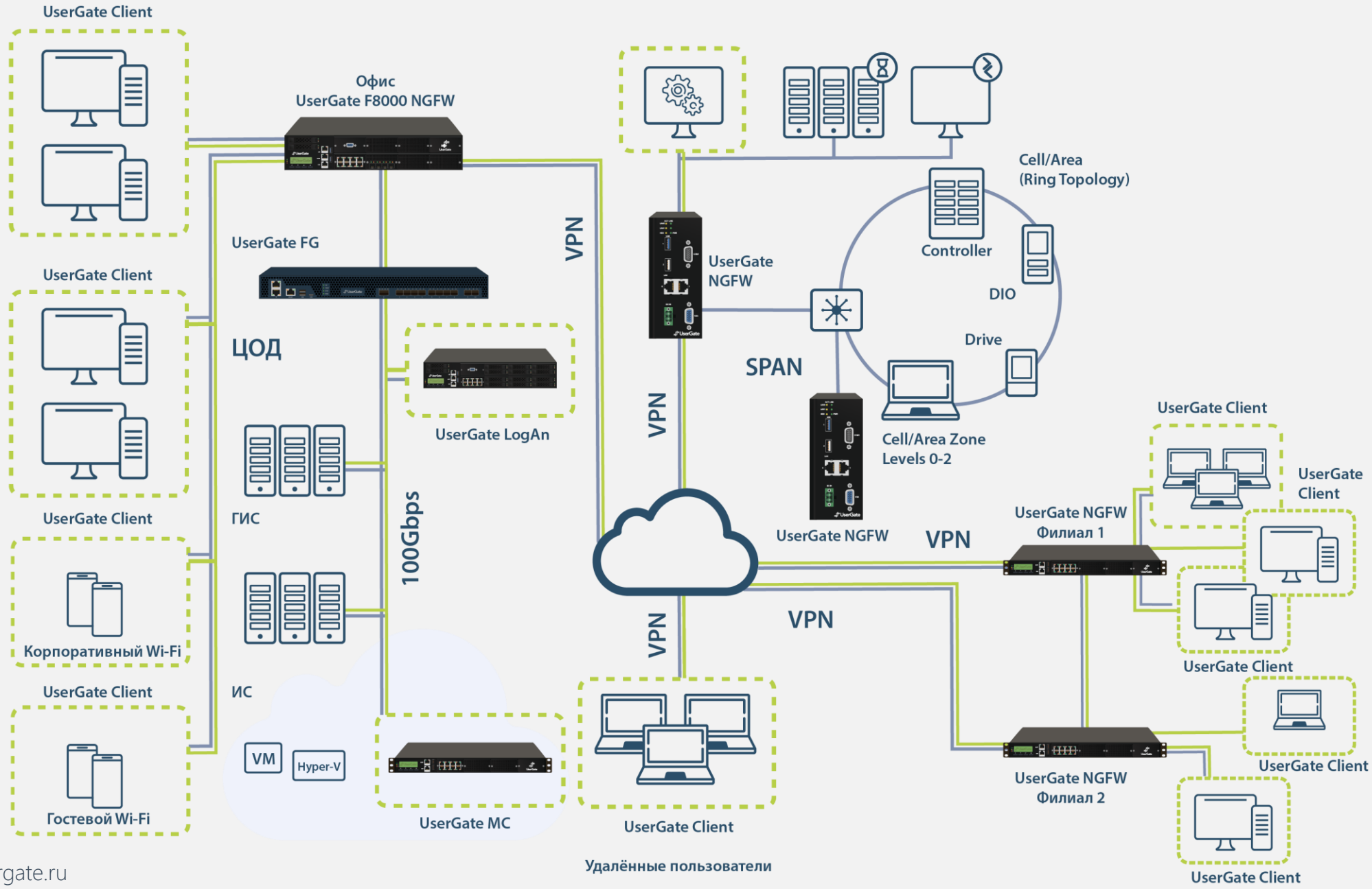
№	IP назначения	IP источника	Событий	Процент
1	**138.68.85.159**		**11,944**	**82.97%**
		83.97.20.33	65	0.54%
		211.141.207.5	48	0.4%
		51.91.212.81	44	0.37%
		139.162.110.42	42	0.35%
		61.188.18.251	37	0.31%
		Другие: 6835	11,708	98.02%
2	**178.248.232.27**		**1,226**	**8.52%**
		138.68.85.159	1,226	100%


IP 10.10.10.6
GW 10.10.10.1
L3 мост
Firewall, IDPS
IP 10.10.10.10
Router
10.10.10.1
Internet
SYSLOG
SOC

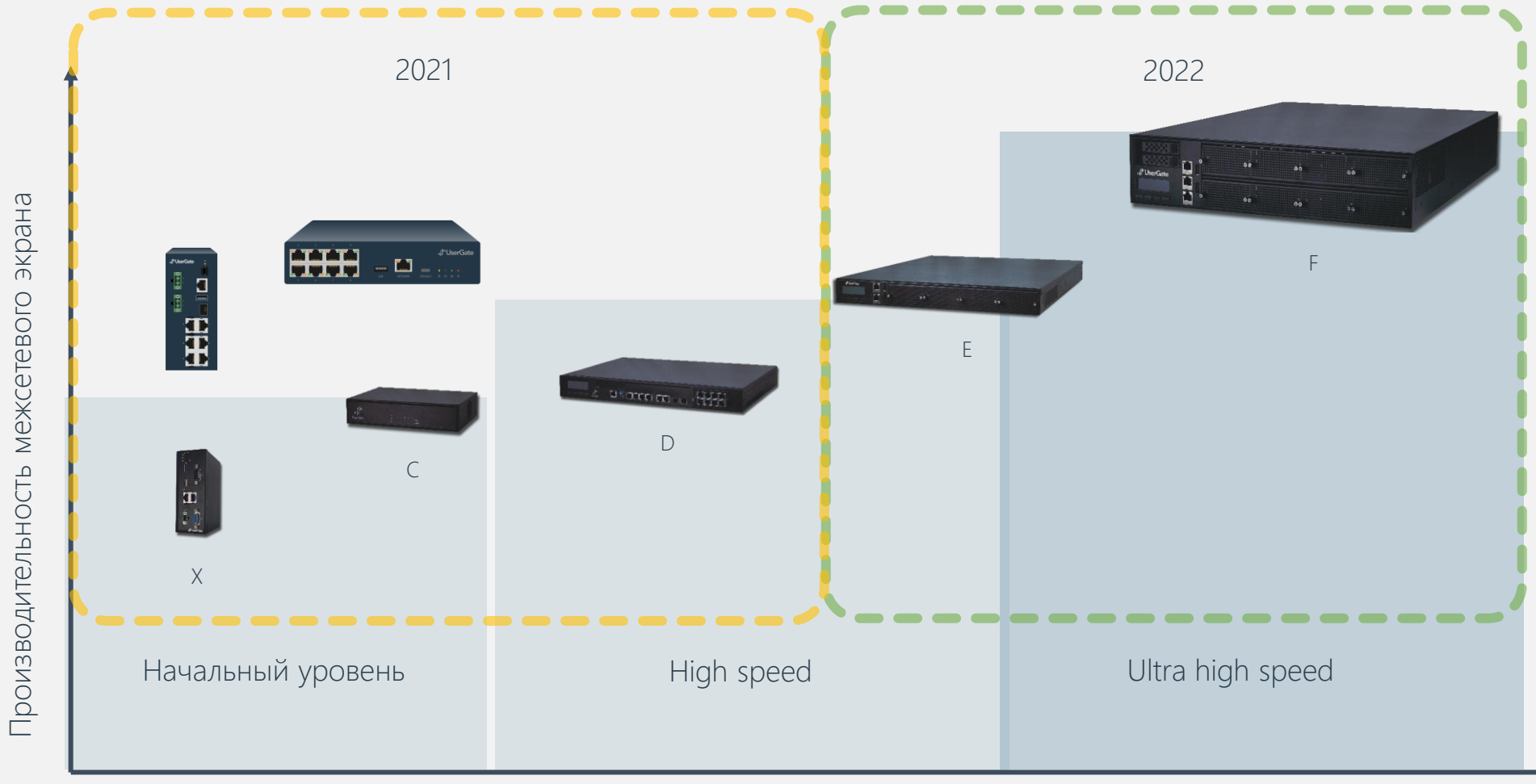

UserGate
GW IP: R1
Bridge L2
CLIENT
R1


АППАРАТНОЕ УСКОРЕНИЕ
МАШИННОЕ ОБУЧЕНИЕ
ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ
ICS
Client
MC
LogAn
WAF
NGFW
DCFW
АСУ ТП
Управление
Веб-сервисы
Сети
Удаленные пользователи
Анализ
ЦОД

UserGate


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

Обновленная линейка



UserGate Log Analyzer

UserGate Management Center

Сетевые функции

Межсетевой экран L7
VLAN, PPPoE, LACP, Bridge
GRE, VXLAN, IP-IP
VRF, Multicast маршрутизация
Routing Static, BGP, OSPF, RIP
NAT, DNAT, PBR
Traffic shaping

Система обнаружения вторжений

L7
СОВ Новый собственный движок
Инспектирование SSL Гранулированная настройка SSL
ГОСТ TLS
ICAP
Инспектирование SSH

Идентификация пользователей

Captive-портал
AD
Kerberos, NTLM, SSO
Radius, TACACS+
MFA

Операционная система UGOS

Безопасность АСУ ТП

L7, IEC 104, Modbus, DNP3, MMS
Новые протоколы
Обработка зеркального трафика

Интернет-фильтрация

Контентная фильтрация
Морфология
Антивирус
Инспектирование SSL

Безопасность почты

Антиспам
Антивирус

Анализ угроз

Поддержка концепции SOAR

Организация удаленной работы

L2TP IPSec VPN
Совместимость с Cisco VPN
Web-портал (SSL VPN) ГОСТ TLS
Reverse-прокси ГОСТ TLS
Гранулированная настройка SSL

Отказоустойчивость

Кластер конфигурации
Кластер А-А
Кластер А-П

Новые платформы UserGate NGFW для АСУ ТП

sales@usergate.ru | usergate.ru

FORCEPOINT POWERED BY Raytheon
FORTINET
STONESOFT
Barracuda
KerioControl
BlueCoat
McAfee SECURE
Microsoft Forefront
Check Point SOFTWARE TECHNOLOGIES LTD.

МИНФИН
РОССИИ

Спасибо за внимание

Андрей Полянский
Региональный представитель в ЮФО, СКФО
apolyanskiy@usergate.ru
8 800 500 40 32 | +7 (915) 340 04 21