

The background of the slide is a photograph of a businessman in a dark suit and blue tie, holding a large, metallic, 3D-rendered gear. The gear is complex, with many smaller gears and mechanical parts attached to its outer edge. The scene is lit with a cool, blueish light, and the background is slightly blurred, showing what appears to be a modern office or server room environment.

# 7 бед один ответ – ViPNet xFirewall

# 7 задач

Знать что  
охранять

Управлять  
доступом

Защитить от  
сетевых атак

Реализовать  
BYOD

Защитить  
от вирусов

Что делать с  
SSL

Защита от  
неизвестных  
угроз

## Шлюзы безопасности

FW/VPN

NGFW

IDS

Coordinator  
for Win/Linux

Coordinator KB

HW 4 поколения

xFirewall

IDS NS

# Что такое ViPNet xFirewall

Сетевая  
платформа  
в составе:

Межсетевой  
экран

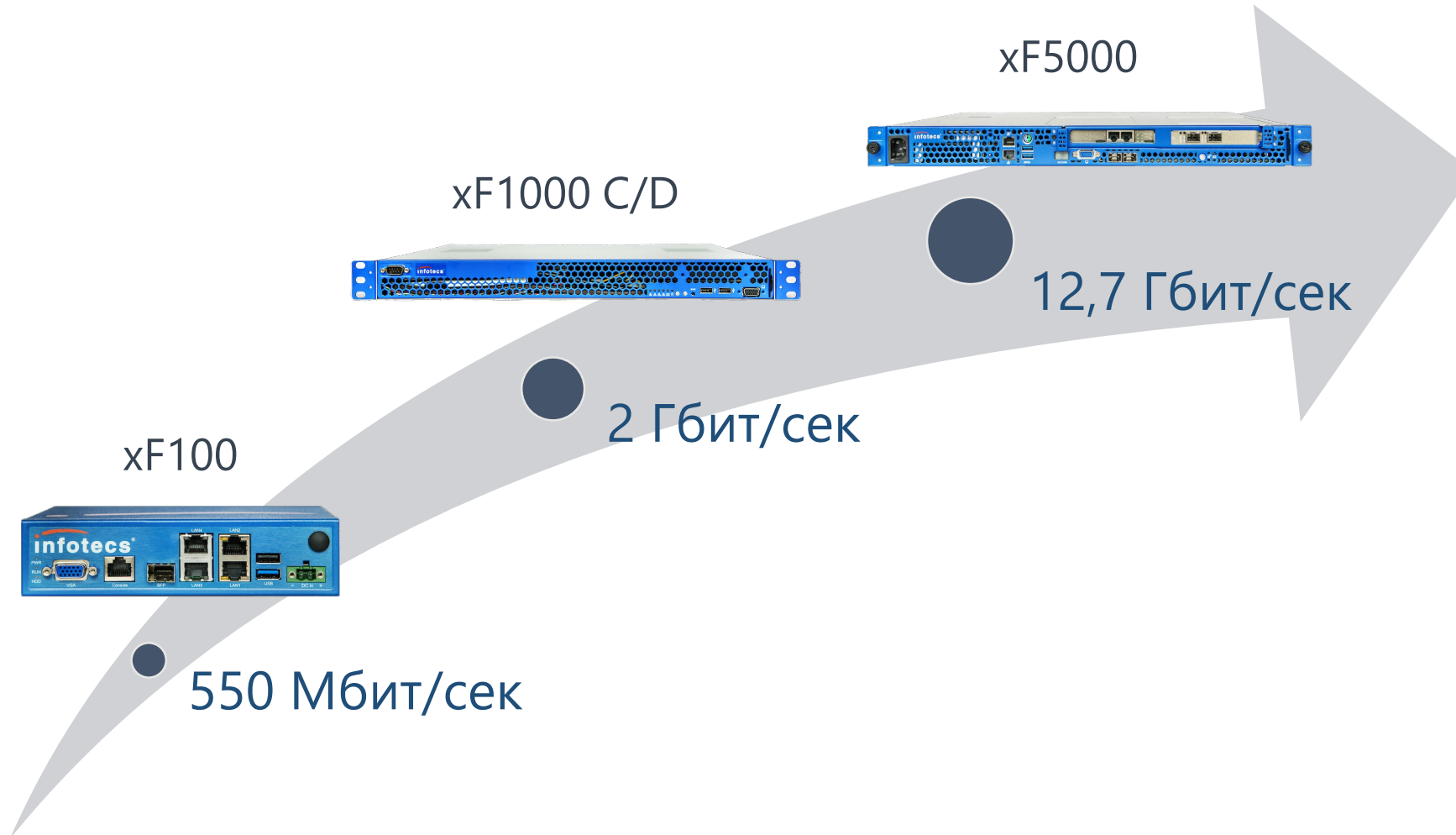
Сетевой экран  
приложений -  
DPI

Система  
предотвращения  
вторжений

Шлюзовой  
антивирус

Интеграция  
с Active Directory

# ViPNet xFirewall. Платформы



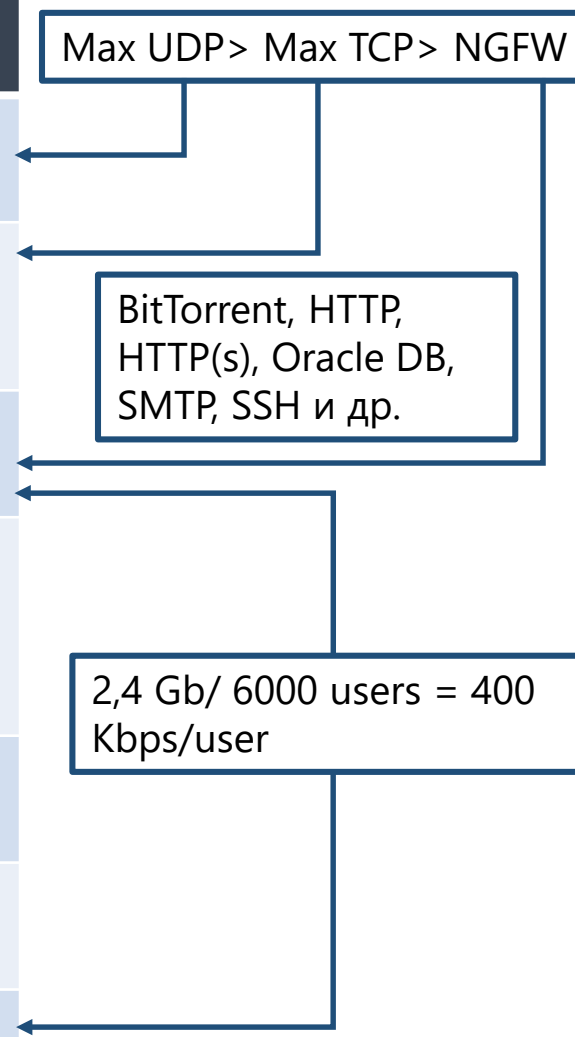
# Производительность

Исполнение	xF100	xF1000 C/D	xF5000
Firewall, 1518 byte UDP (Mbps)	550	2 000	12 700
Firewall, TCP Multistream (Mbps)	550	2 000	9 300
NGFW Througput (Mbps)	140	1 500	2 400
Firewall Throughput (64 bytes packets Per Second)	71 000	960 000	1 000 000
Connections per Second	2 500	19 500	17 500
Concurrent Connections	149 900	990 000	9 900 000
Users	~ 100	~ 1000	~ 6000

Max UDP > Max TCP > NGFW

BitTorrent, HTTP, HTTP(s), Oracle DB, SMTP, SSH и др.

2,4 Gb/ 6000 users = 400 Kbps/user

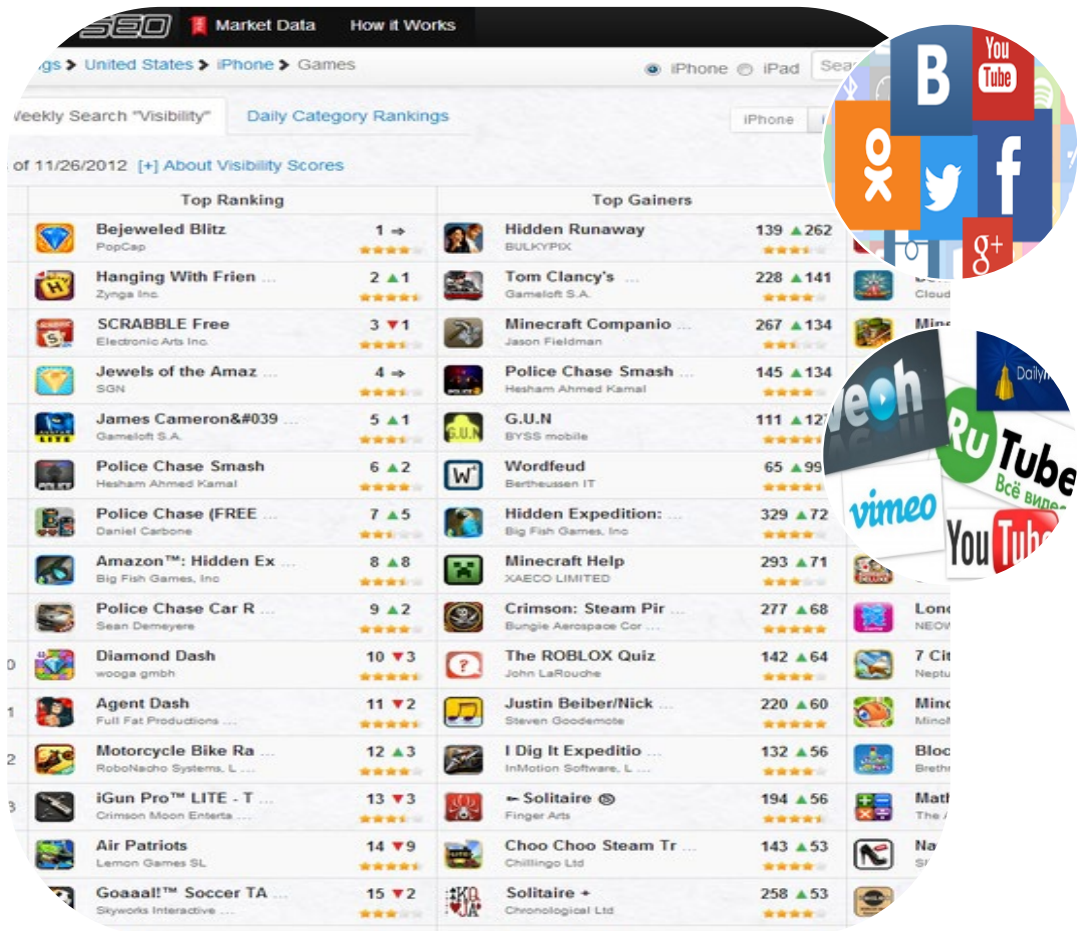


# №1 – знать что охранять



Открыл порты 80/443 == Открыл всё!

# 2065 уникальных приложений/протоколов



The image shows a screenshot of an app store ranking page for the 'Games' category on the iPhone platform. The page is titled 'Market Data' and 'How it Works'. It displays 'Daily Category Rankings' for the date 11/26/2012. The table is divided into two columns: 'Top Ranking' and 'Top Gainers'. The 'Top Ranking' column lists apps like 'Bejeweled Blitz', 'Hanging With Friends', and 'SCRABBLE Free'. The 'Top Gainers' column lists apps like 'Hidden Runaway', 'Tom Clancy's Splinter Cell', and 'Minecraft Companion'. The table includes columns for app name, developer, rank, change in rank, and a star rating. Overlaid on the screenshot are several social media and video platform icons, including YouTube, Facebook, Twitter, and Vimeo.

Top Ranking			Top Gainers		
	Bejeweled Blitz PopCap	1 →		Hidden Runaway BULKYPDX	139 ▲ 262
	Hanging With Friends Zynga Inc.	2 ▲ 1		Tom Clancy's Splinter Cell Gameloft S.A.	228 ▲ 141
	SCRABBLE Free Electronic Arts Inc.	3 ▼ 1		Minecraft Companion Jason Fieldman	267 ▲ 134
	Jewels of the Amazon SGN	4 →		Police Chase Smash Hesham Ahmed Kamal	145 ▲ 134
	James Cameron & 039 Gameloft S.A.	5 ▲ 1		G.U.N BYSS mobile	111 ▲ 127
	Police Chase Smash Hesham Ahmed Kamal	6 ▲ 2		Wordfeud Bertheussen IT	65 ▲ 99
	Police Chase (FREE) Daniel Carbone	7 ▲ 5		Hidden Expedition Big Fish Games, Inc.	329 ▲ 72
	Amazon™: Hidden Expedition Big Fish Games, Inc.	8 ▲ 8		Minecraft Help XAECO LIMITED	293 ▲ 71
	Police Chase Car Race Sean Demeyere	9 ▲ 2		Crimson: Steam Pirates Bungie Aerospace Cor...	277 ▲ 68
	Diamond Dash wooga gmbh	10 ▼ 3		The ROBLOX Quiz John LaRouche	142 ▲ 64
	Agent Dash Full Fat Productions...	11 ▼ 2		Justin Bieber/Nick Steven Goodemote	220 ▲ 60
	Motorcycle Bike Race RoboNacho Systems, L...	12 ▲ 3		I Dig It Expedition InMotion Software, L...	132 ▲ 56
	iGun Pro™ LITE - T Crimson Moon Enterta...	13 ▼ 3		Solitaire Finger Arts	194 ▲ 56
	Air Patriots Lemon Games SL	14 ▼ 9		Choo Choo Steam Train Chillingo Ltd	143 ▲ 53
	Goaaal!™ Soccer TA Skyworks Interactive...	15 ▼ 2		Solitaire + Chronological Ltd	258 ▲ 53

95 из категории «Социальные сети»

45 – потоковое видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений



# №2 - Управлять доступом



# Интеграция с MS AD



## INTRUSION DETECTION AND PREVENTION SYSTEM

The image features a central graphic with the text 'INTRUSION DETECTION AND PREVENTION SYSTEM' in large, white, outlined letters. The background is a dark blue gradient. On the right, a hand in a dark suit jacket points towards the text. The background is overlaid with a grid of hexagons. Some hexagons contain a white padlock icon, while others contain a white magnifying glass icon. The overall theme is cybersecurity and network protection.

# ViPNet xFirewall 5.0

## Релиз весной 2019 года

- Статистика и журналы ^
  - Состояние системы
  - Статистика
- Межсетевой экран ^
  - Сетевые фильтры
  - NAT
  - Группы объектов
  - Прокси-сервер
  - Пользователи сети
- Предотвращение вторжений
- Сетевые настройки ^

Предотвращение вторжений включено

Поиск правил...   Параметры  Обновление базы 

Блокирующие 

Правило предотвращения	Статус	Действие
▼ current_events (9)		
^ exploit (620)		
"AM EXPLOIT iframe SRC JS XSS on IE test detected"	Вкл	Блокировать
"AM EXPLOIT Yahoo Widgets Engine 4.0.4 YDPCTL.DLL ActiveX DoS attempt (short type)"	Вкл	Блокировать
"AM Exploit Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution"	Вкл	Блокировать
"AM EXPLOIT Yahoo Messenger 8.1.402 YVerInfo.dll 2007.8.26 buffer overflow exploit detected"	Вкл	Блокировать
"AM EXPLOIT CA Internet Security Suite 2008.0 ActiveX Control Arbitrary File Overwrite exploit detected"	Вкл	Блокировать
"AM EXPLOIT Facebook ImageUploader4.1.ocx FileMask DoS exploit detected"	Вкл	Блокировать
"AM EXPLOIT IBM DB2 Universal Database 9.1 FixPak 4a XML Query Buffer Overflow exploit detected"	Вкл	Блокировать

### Журнал регистрации IP-пакетов

Фильтр IP-пакетов ^

#### Признаки IP-пакетов

- Пользователь сети: Любой
- Приложение: Любое
- Прикладной протокол: Любой
- Транспортный протокол: Все протоколы
- Сетевой интерфейс: Все сетевые интерфейсы
- Тип трафика: Весь трафик
- Тип IP-адреса: Любой
- Трансляция IP-пакетов: Все
- Событие: Блокированные IP-пакеты
- Группа правил IPS: Любая
- Правило IPS: Любое

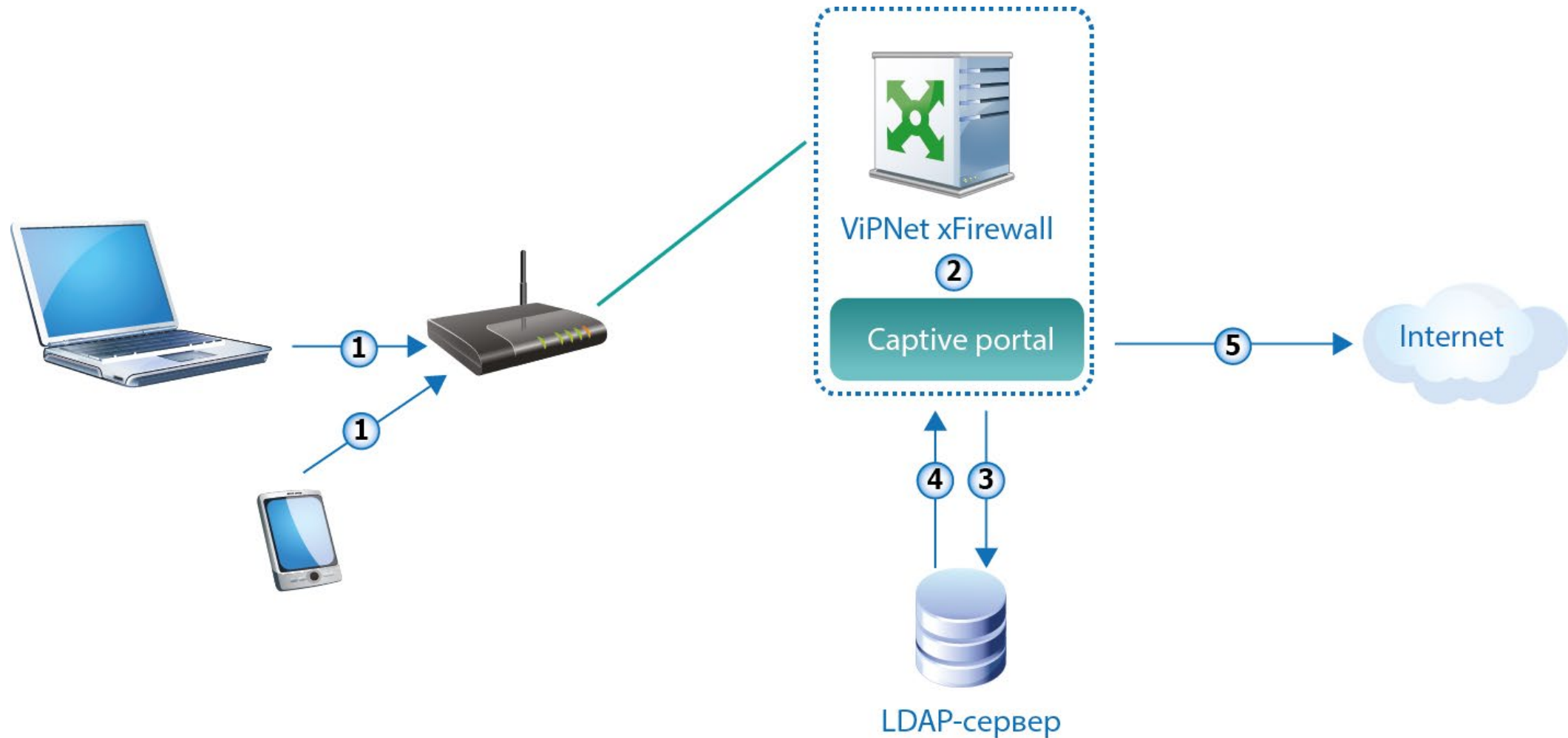
Найти

Восстановить значения по умолчанию

# №4 - BYOD



# Captive portal

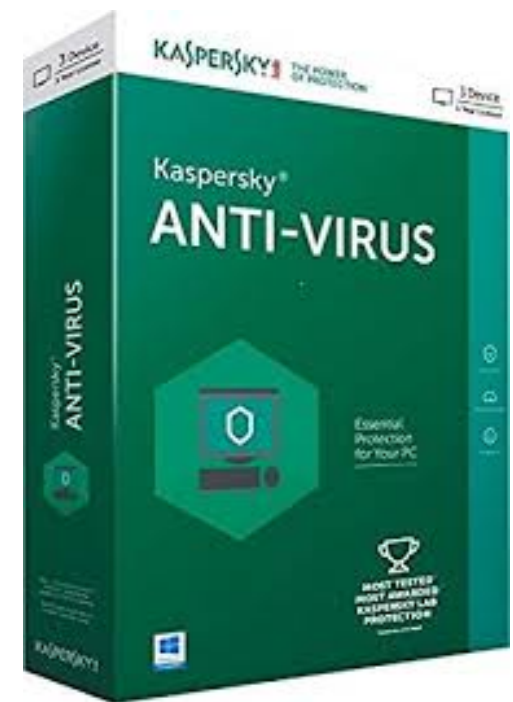


# №5 – Защита от вирусов



# Антивирус Касперского для Proxy Server

- Антивирус Касперского для Proxy Server – это решение для защиты HTTP- и FTP-трафика, проходящего через прокси-сервер
- Приложение обеспечивает защиту пользователей при работе с интернет-ресурсами, удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP и FTP





# №6 – Что делать с SSL



# Если нельзя запретить – нужно возглавить

- **Разрешить тот SSL трафик, который известен:**  
Yandex, Google, Facebook и т.д.
- **Блокировать известный SSL запрещенных политикой приложений:**  
социальные сети, мессенджеры и т.д.
- **Запретить любой неизвестный SSL трафик**

# №7 – Защита от неизвестных угроз



# ViPNet xFirewall – повышает осведомленность

Максимальная видимость –  
фильтрация на 7 уровне ISO  
OSI

Защита от сетевых атак –  
блокировка аномалий,  
запретных команд

Защита от вирусных атак

Уменьшение поверхности  
атаки

ФСТЭК на  
соответствие  
требованиям к МЭ  
типа А 4 класса –  
ожидаем 1 кв. 2019

# В чем польза от ViPNet xFirewall

Комплексная защита от 7  
бед сетевой безопасности

Снижение объема Интернет  
трафика за счет  
блокирования ресурсов  
развлекательного характера

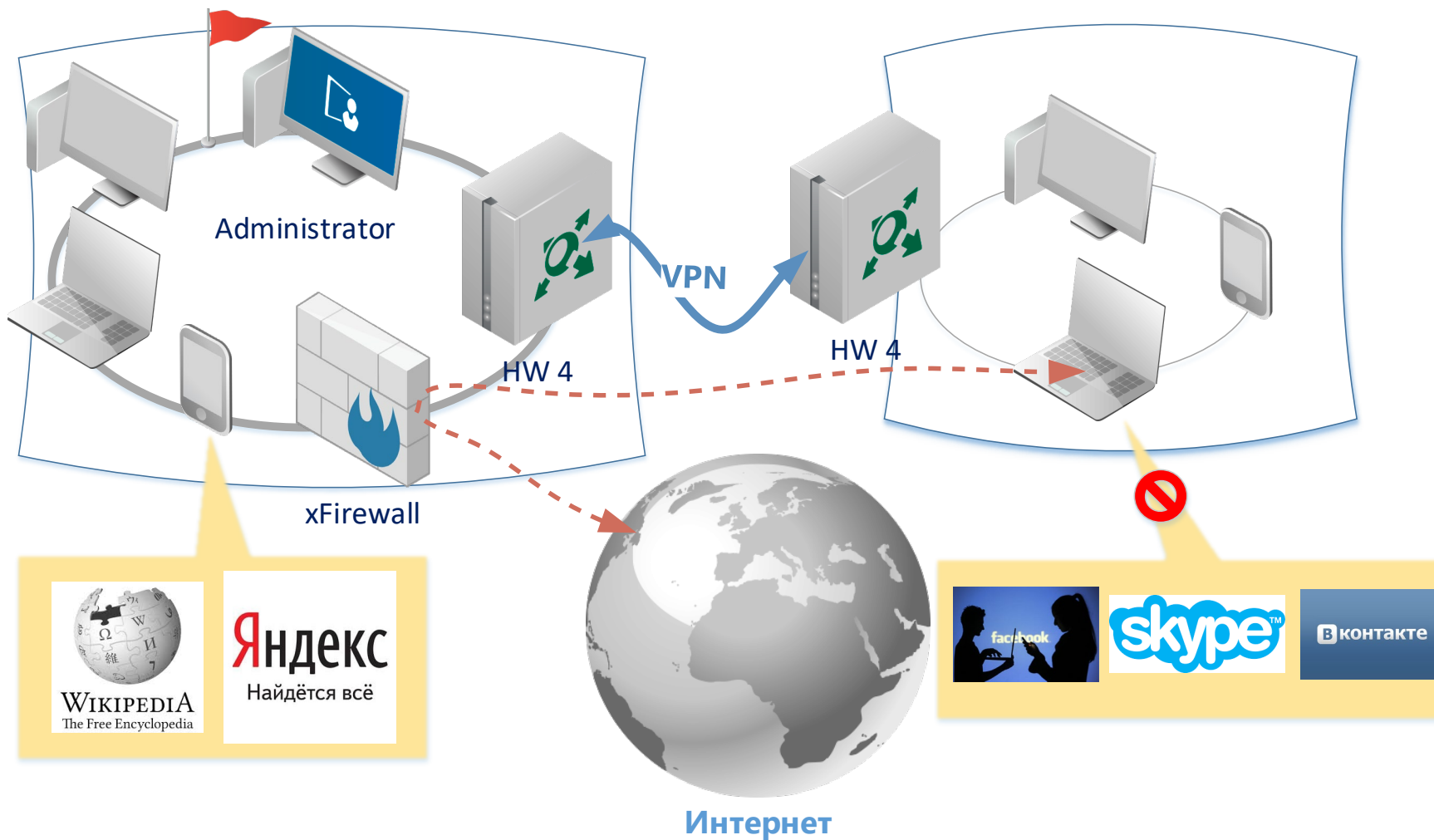
МЭ типа А 4 класса  
по новым требованиям  
ФСТЭК

Сравним по возможностям  
с западными аналогами

The background of the slide is a dark, blurred image of a hand holding a silver padlock. Overlaid on this is a network diagram consisting of several white circular icons, each containing a stylized person in a suit and tie. These icons are connected by thin white lines, forming a web-like structure. A large, semi-transparent dark blue rectangle is positioned in the lower-left quadrant, containing the text 'Схема использования' in white.

# Схема использования

# Схема использования





An overhead view of a business meeting around a large wooden table. Several people are seated around the table, each engaged with a different piece of technology: a smartphone, a laptop, a tablet, or a tablet with a 'Statistical Analysis' chart. The scene is brightly lit, and the wood grain of the table is clearly visible.

Релиз 4.1.0

# 4.1.0

Поддержка групп приложений в транзитных правилах межсетевого экрана

Поддержка нескольких приложений, прикладных протоколов, групп приложений и пользователей в одном транзитном правиле межсетевого экрана

Антивирусная защита с помощью Антивируса Касперского 5.5 для Proxy Server

Изменение размера MTU сетевого интерфейса

Экспорт журнала регистрации IP-пакетов по сети в формате CEF

# Поддерживаемые группы приложений

Business	Conference	Database	E-commerce	Filetransfer	Gaming
Generic	Industrial	Mail	Messaging	Mobile	Network management
Peer to peer	Remote control	Sharehosting	Social	Streaming	Tunnel
		Voice over ip	Web		

## ← Добавление транзитного фильтра открытой сети

Имя фильтра:

Состояние:  Включено

Действие:   Блокировать трафик  
  Пропускать трафик

### Признаки трафика

Значение признаков по группам

#### ^ Приложения (4)

-  windows azure
-  microsoft services
-  skype
-  skype for business

### Добавить:

Пользователей ▾

Приложения ▾

Протоколы ▾

Источники ▾

Назначения ▾

Расписания ▾

Сетевой фильтр применяется всегда для любого пользователя, протокола, источника и назначения.

Сохранить

Сохранить и применить

Отмена

The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, there are several high-voltage power line towers. The sun is low on the horizon, creating a strong glow and casting long shadows.

**СПАСИБО!**