



Техно infotecs  
2021 Фест

ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

Практические  
аспекты эксплуатации  
NGFW



Мир изменился

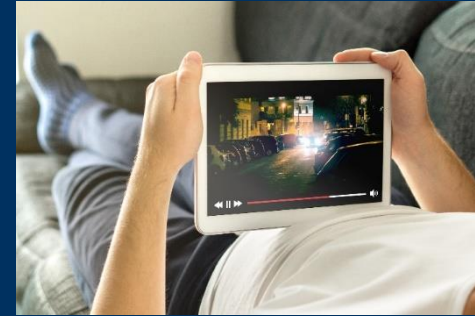
# Мир изменился



Web 2.0



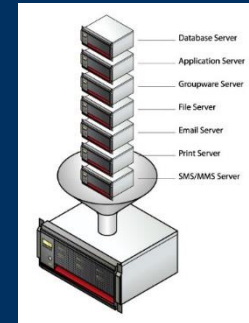
Mobile Devices



Streaming video



Cloud/SaaS



Virtualization



# Рабочий день сотрудника

- Чтение блогов
- Facebook, VK, Одноклассники
- Twitter
- IM/WhatsApp
- Загрузка файлов (Dropbox, Яндекс.Диск)
- Потокное видео (Youtube, Ivi)
- Потокное аудио (Яндекс.Музыка)
- Качаем торренты
- Удаленный рабочий стол (TeamViewer, RDP)



25% of office traffic is non-business related



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

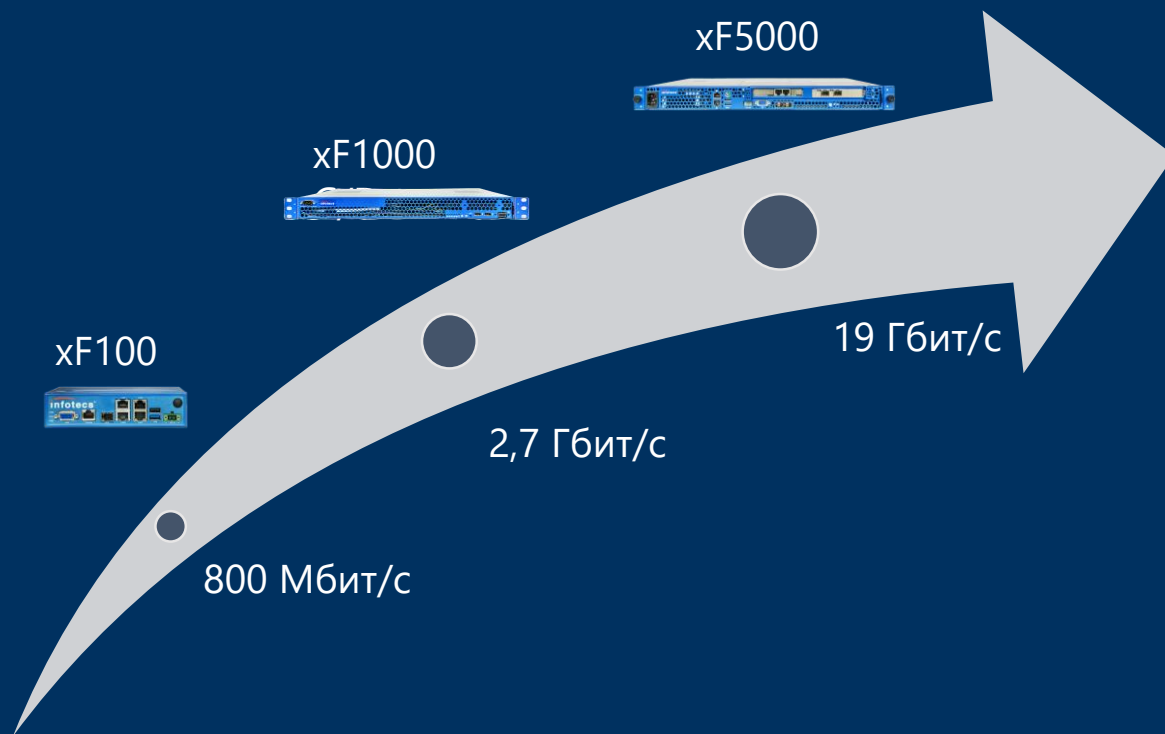
Система  
предотвращени  
я вторжений

Шлюзовой  
антивирус

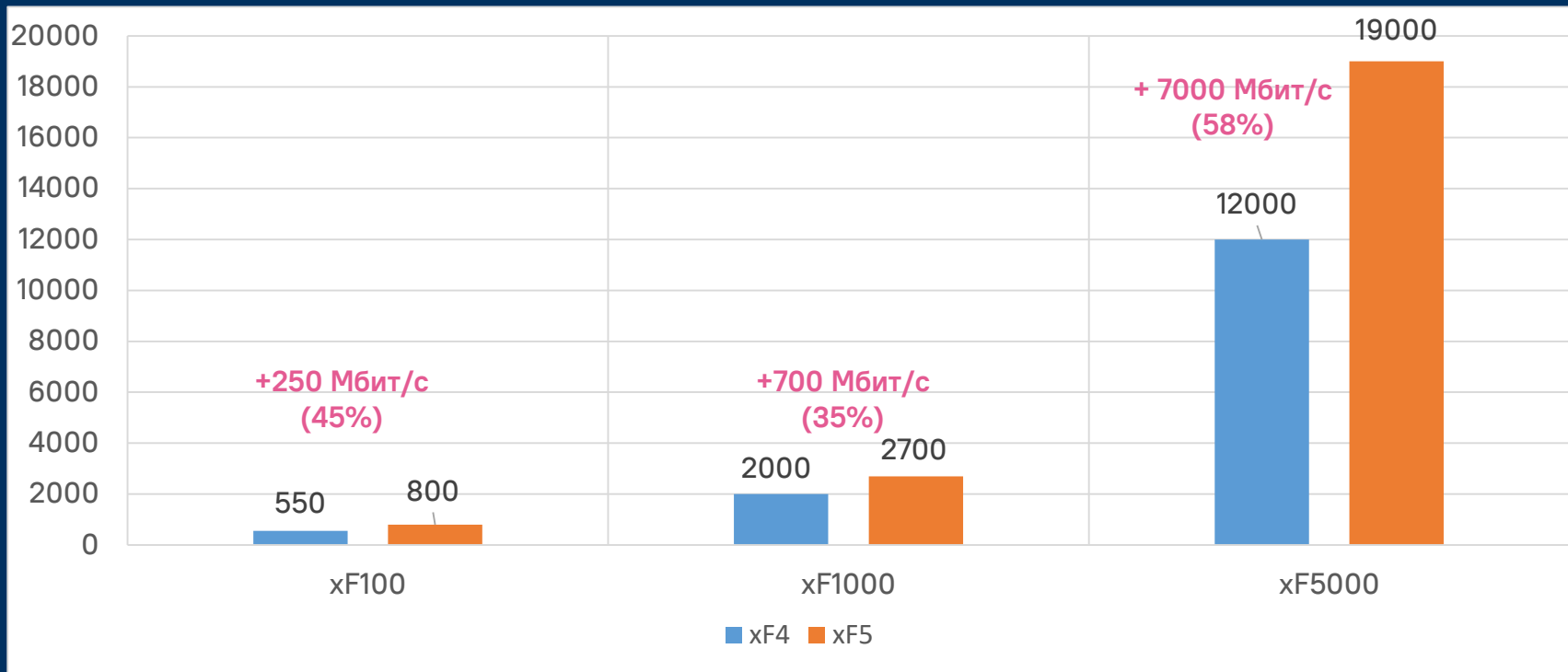
Интеграция с  
Active Directory



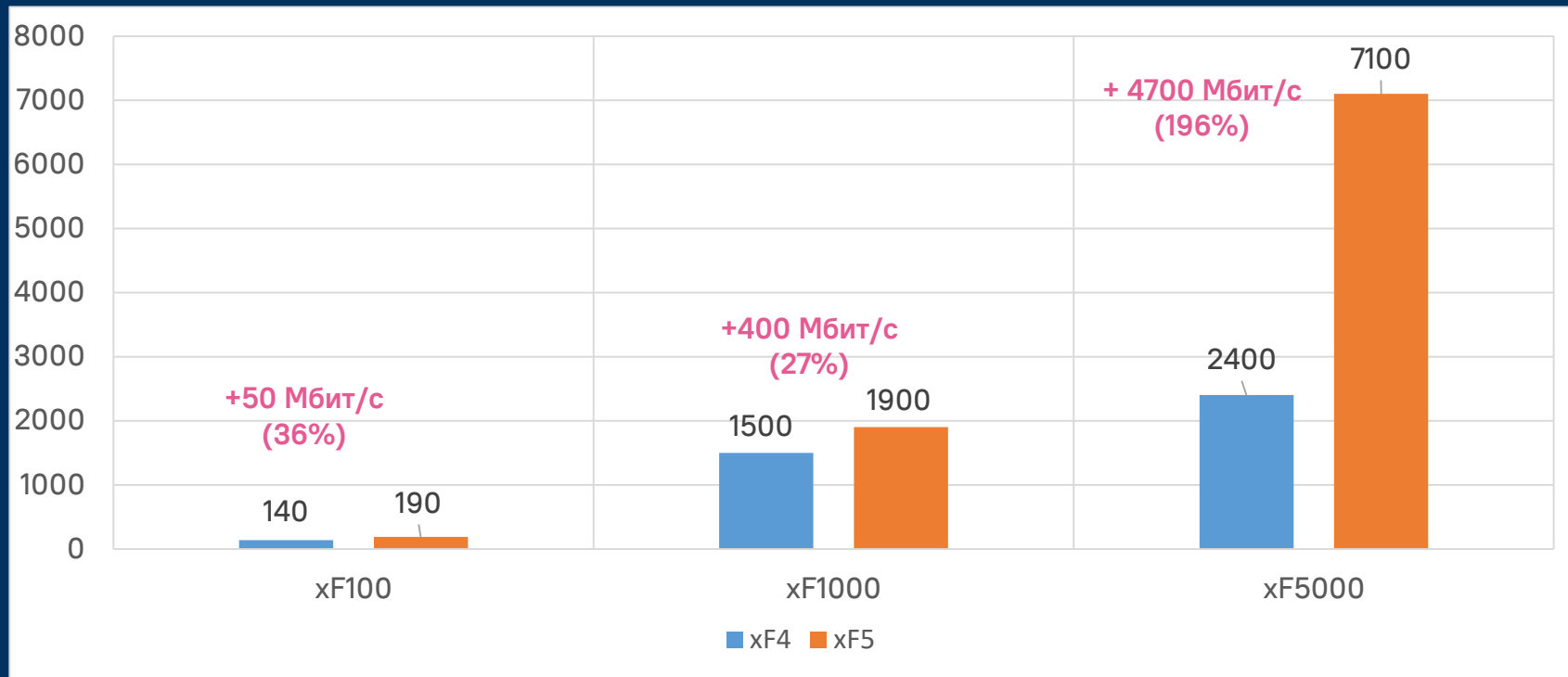
# ViPNet xFirewall. Платформы



# Производительность МЭ (UDP)

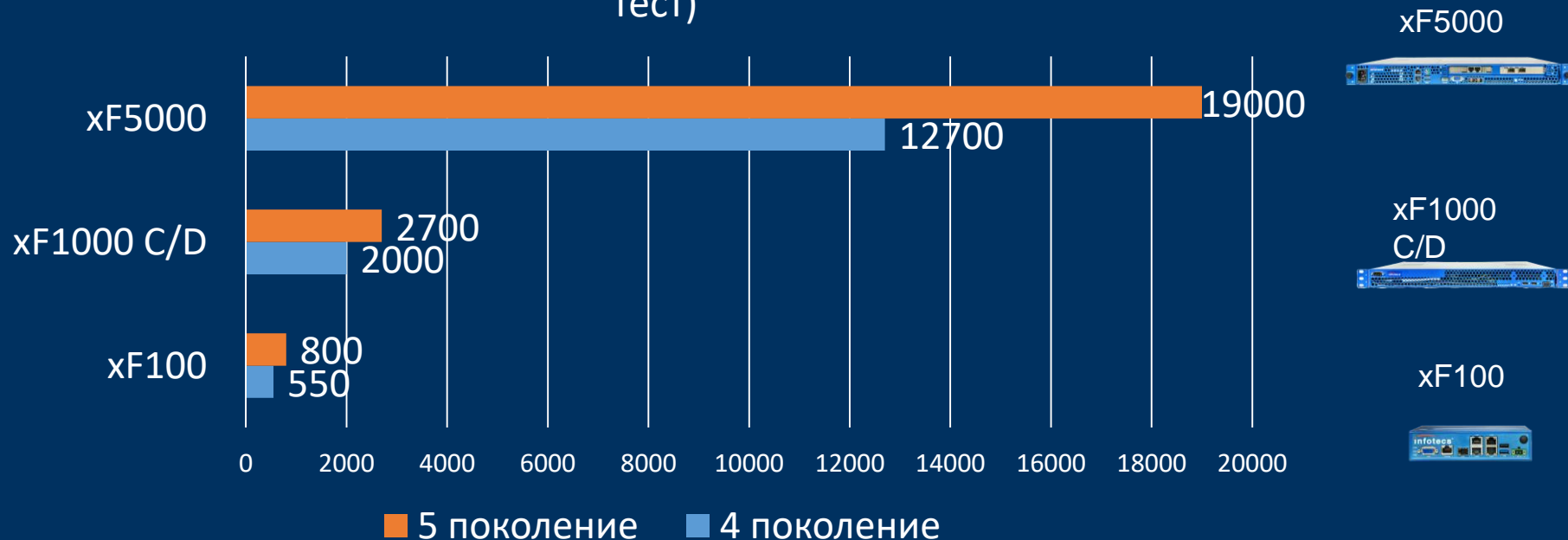


# Производительность Application Control



# ViPNet xFirewall 5. Платформы

Производительность МЭ UDP 1518 байт (идеальный тест)



# Производительность

| Исполнение  | xF100   | xF1000 C/D | xF5000    |
|---|---------|------------|-----------|
| Firewall, 1518 byte UDP (Mbps)                    | 800     | 2 700      | 19 000    |
| Firewall, TCP Multistream (Mbps)                  | 720     | 2 700      | 9 300     |
| AppControl (Firewall+DPI) (Mbps)                  | 190     | 1 900      | 7 100     |
| Firewall Throughput (64 bytes packets Per Second) | 90 000  | 1 300 000  | 4 000 000 |
| Connections per Second                            | 2 500   | 20 000     | 50 000    |
| Concurrent Connections                            | 148 500 | 990 000    | 9 900 000 |
| Users   | ~ 100   | ~ 1000     | ~ 6000    |

Max UDP > Max TCP > NGFW

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

$7,1 \text{ Gb} / 6000 \text{ users} = 1,18 \text{ Mbps/user}$



# Знать что охранять



# 2065 уникальных приложений/протоколов

| Top Ranking                 |        | Top Gainers                |           |
|-----------------------------|--------|----------------------------|-----------|
| Bejeweled Blitz             | 1 →    | Hidden Runaway             | 139 ▲ 262 |
| Hanging With Friends        | 2 ▲ 1  | Tom Clancy's Splinter Cell | 228 ▲ 141 |
| SCRABBLE Free               | 3 ▼ 1  | Minecraft Companion        | 267 ▲     |
| Jewels of the Amazon        | 4 →    | Police Chase Smash         | 145       |
| James Cameron's Avatar      | 5 ▲ 1  | G.U.N.                     | 111       |
| Police Chase Smash          | 6 ▲ 2  | Wordfeud                   | 65 ▲ 99   |
| Police Chase (FREE)         | 7 ▲ 5  | Hidden Expedition          | 329 ▲ 72  |
| Amazon™: Hidden Expeditions | 8 ▲ 8  | Minecraft Help             | 293 ▲ 71  |
| Police Chase Car Rally      | 9 ▲ 2  | Crimson: Steam Pirates     | 277 ▲ 68  |
| Diamond Dash                | 10 ▼ 3 | The ROBLOX Quiz            | 142 ▲ 64  |
| Agent Dash                  | 11 ▼ 2 | Justin Bieber/Nicki Minaj  | 220 ▲ 60  |
| Motorcycle Bike Rally       | 12 ▲ 3 | I Dig It Expedition        | 132 ▲ 56  |
| iGun Pro™ LITE - The Game   | 13 ▼ 3 | Solitaire                  | 194 ▲ 56  |
| Air Patriots                | 14 ▼ 9 | Choo Choo Steam Train      | 143 ▲ 53  |
| Goaaal!™ Soccer Tactics     | 15 ▼ 2 | Solitaire                  | 258 ▲ 53  |

95 из категории «Социальные сети»

45 – потоковое видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

Управлять доступом

# ACCESS CONTROL



# Интеграция с Microsoft AD

## Без клиентская идентификация

- xFirewall использует технологическую учетную запись MS AD с ее помощью производится чтение EventLog
- Синхронизация с MS AD каждые 5 секунд
- Допустимое время отсутствия связи 1800 секунд

## Использование учетных записей пользователей MS AD в правилах фильтрации

- Отсутствует потребность в «привязке» пользователей к ip-адресам
- Отсутствует потребность в «привязке» пользователей к устройствам

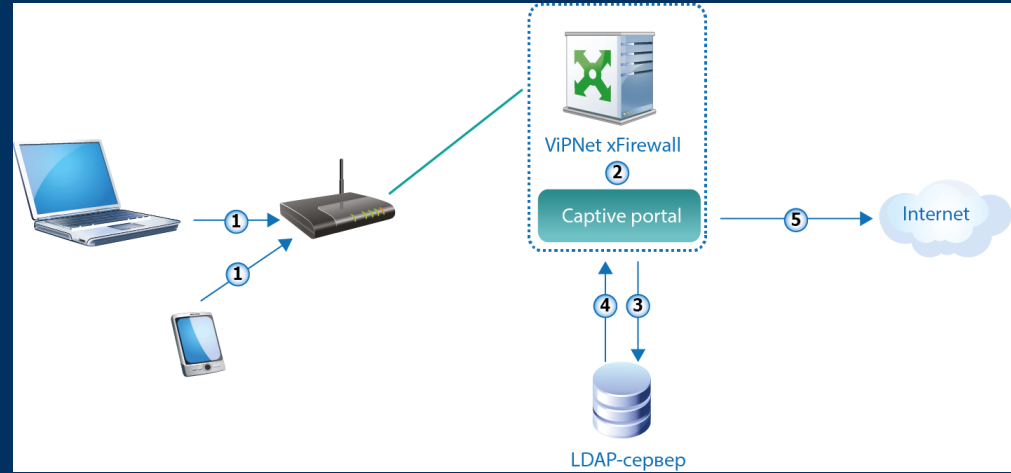


# BYOD – принеси свое устройство и работай



# Captive portal – аутентификация с помощью браузера

- Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства
- Предоставление контролируемого доступа подрядчикам, партнерам
- Автоматическое перенаправление на Портал аутентификации – Captive Portal



# INTRUSION DETECTION AND PREVENTION SYSTEM

A person in a dark suit is pointing their right index finger towards the center of the frame. The background is a blurred blue-toned image of a person in a suit. Overlaid on this background is a grid of hexagonal icons. Some icons are padlocks (some locked, some unlocked), and others are magnifying glasses. The text 'INTRUSION DETECTION AND PREVENTION SYSTEM' is written in large, white, bold, sans-serif capital letters across the middle of the image.

# Система предотвращения вторжений

- 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 X

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

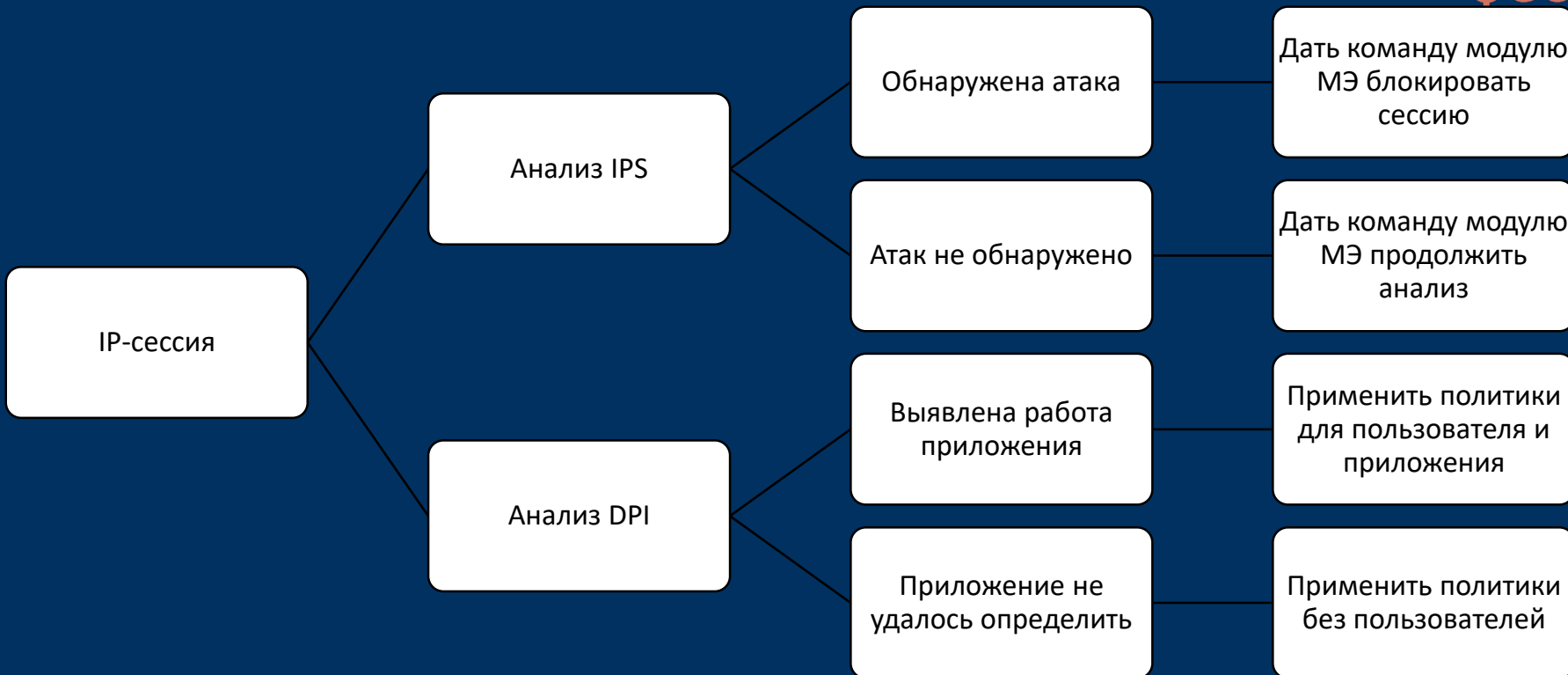
Группа правил IPS: Любая

Правило IPS: Любое

Найти

Восстановить значения по умолчанию

# Порядок применения правил IPS



# №5 – Защита от вирусов



# Поддержка песочниц

- Тестировался сценарий проверки на содержание вредоносного контента файлов, загружаемых из сети Интернет в «песочницу» ATHENA через службу прокси-сервера xFirewall по протоколу ICAP.
- Межсетевой экран ViPNet xFirewall служит шлюзом между приложениями, функционирующими на узлах локальной сети, и внешними сетевыми ресурсами, к которым эти приложения обращаются (выполняет функции прокси-сервера).
- Система AVSOFT ATHENA работает на основе комбинации технологий мультисканера и «песочницы» для исследования файлов на подозрительное содержимое и поведение существенно повышает точность результата проверки.





# Если нельзя запретить – нужно возглавить



- Разрешить тот SSL трафик, который известен:
  - Yandex, Google, Facebook и тд
- Блокировать известный SSL запрещенных политикой приложений: Социальные сети, мессенджеры и тд
- 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

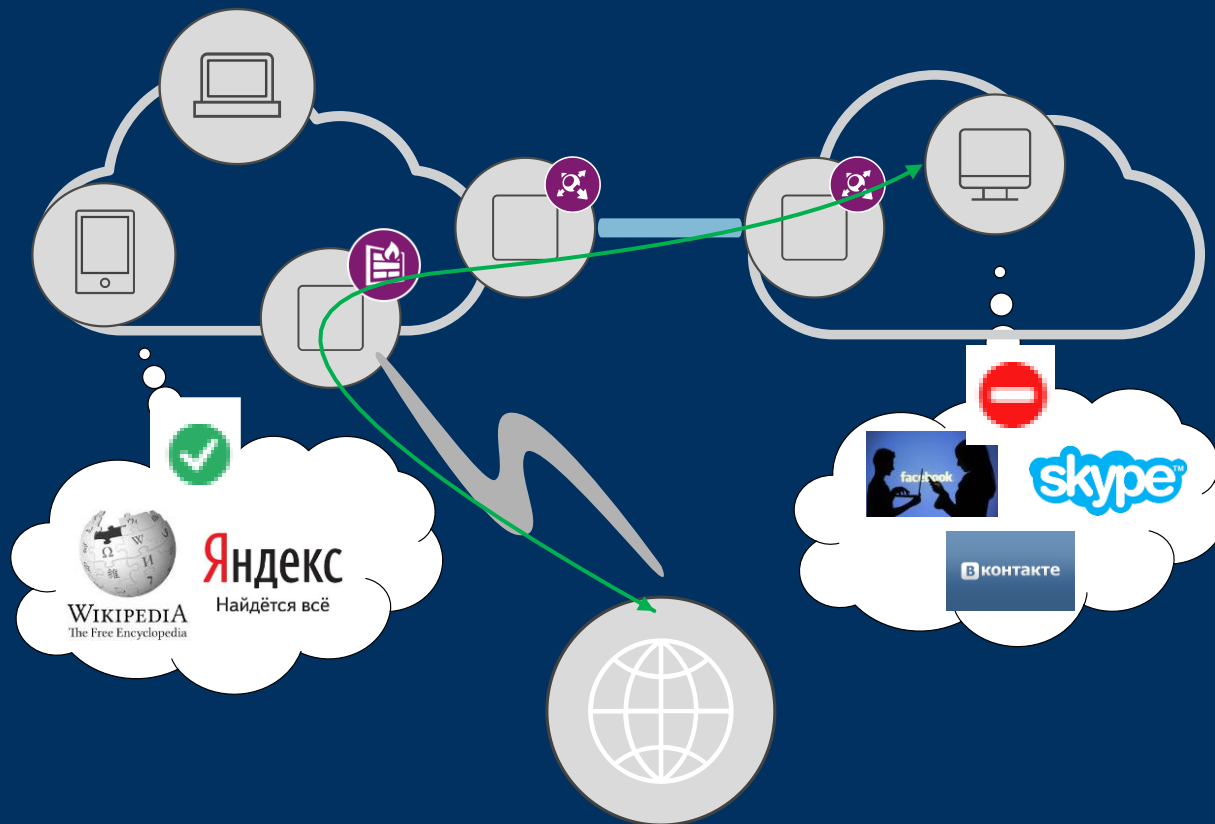
Уменьшение  
поверхности атаки





Схема использования

# Схема использования





ТЕХНО infotecs  
2021 Фест

Спасибо  
за внимание!



# ZeroTrust Network Access (ZTNA)

# Всех переводят на удалёнку

- 73% организации перевели 50 – 100% персонала на удаленный режим работы
- 45% при этом не использовали удаленный режим работы ранее
- А 18% справились с переводом за 1 день
- А 52% потратили на переход от 2 до 5 дней

**ВСЕХ ПЕРЕВОДЯТ НА УДАЛЕНКУ:**

**СПАСАТЕЛИ:**



# Личное или корпоративное устройство



17% используют только  
личные устройства

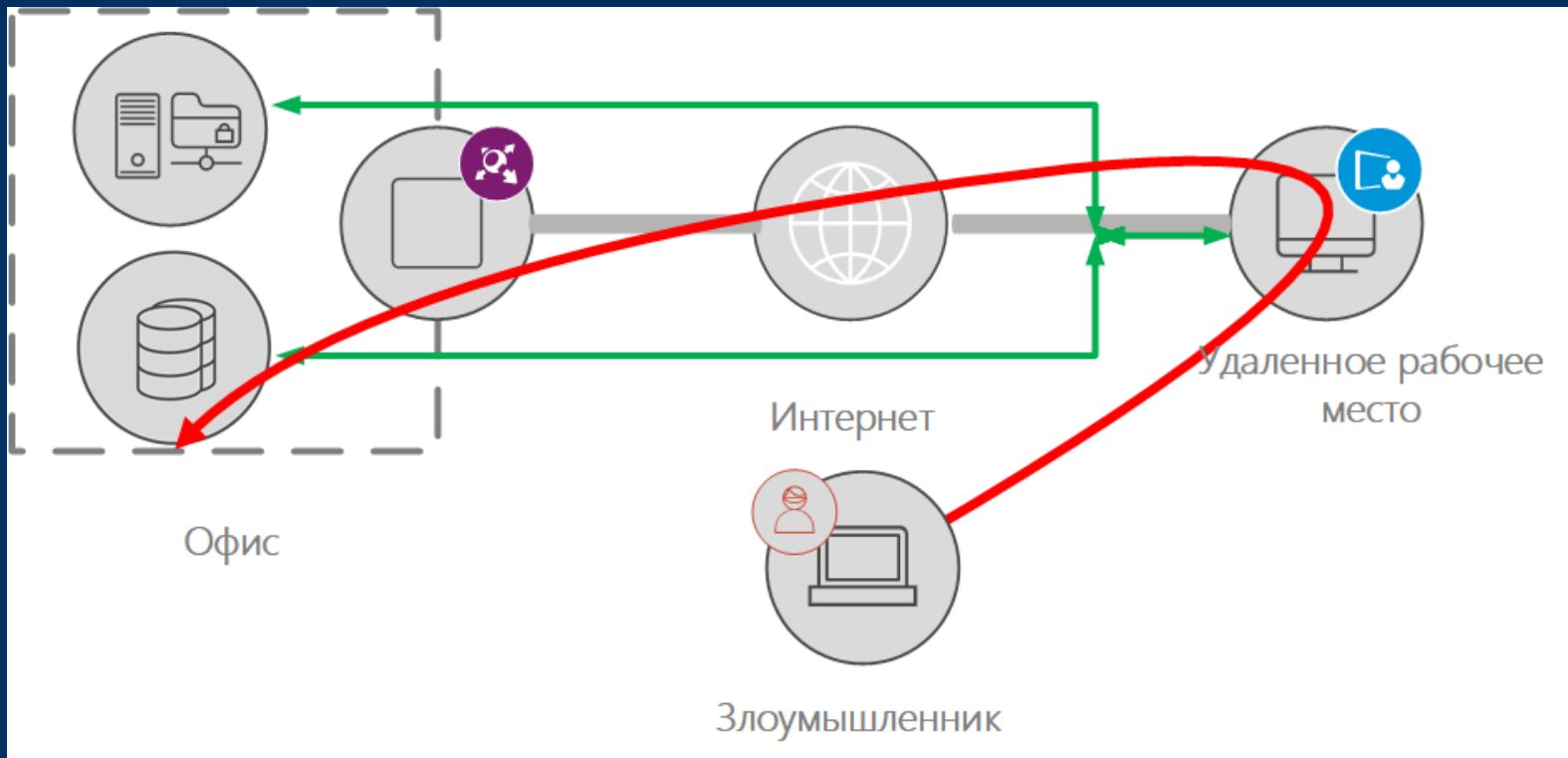


17% используют только  
корпоративные устройства

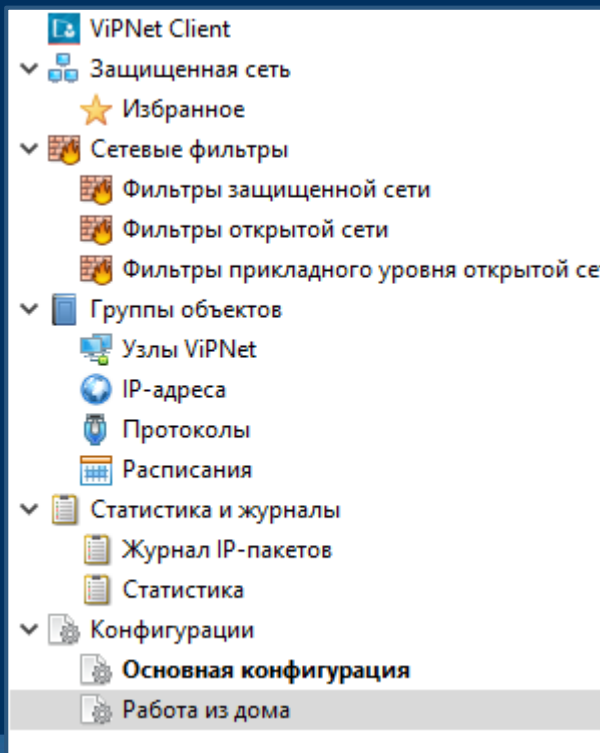




# Где риски



# ViPNet Client: Software Defined Perimeter (SDP)



**ViPNet Client** позволяет настраивать уникальные шаблоны настроек и фильтров открытой и защищенной сети, называемых конфигурациями

Это позволяет одновременно использовать продукт как для работы с защищаемыми ресурсами через закрытый канал, так и для работы с ресурсами сети интернет

# ZTNA = SDP + ViPNet xFirewall



# Что дает решение

## ○ ViPNet Client

- Маршрутизирует весь трафик через VPN туннель в корпоративную сеть
- Ограничивает взаимодействие с домашней сетью – блокирует на время работы

## ○ ViPNet xFirewall

- Разграничивает доступ к ресурсам по логинам
- Разграничивает доступ к ресурсам по приложениям
- Анализирует входящий/исходящий трафик на наличие сетевых атак
- Регламентирует доступ к ресурсам Интернет





ТЕХНО infotecs  
2021 ФЕСТ

Спасибо  
за внимание!