Практические аспекты эксплуатации NGFW

Мир изменился

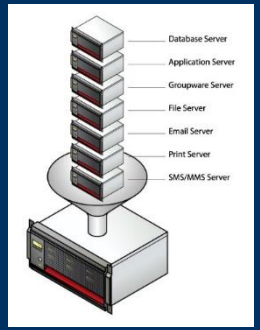
Мир изменился

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)
- Потоковое видео (Youtube, Ivi)
- Потоковое аудио (Яндекс.Музыка)
- Качаем торренты
- Удаленный рабочий стол (TeamViewer, RDP)

25% of office traffic is non-business related

ViPNet xFirewall

7 задач

ТЕХНО 2021 infotecs ФЕСТ

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

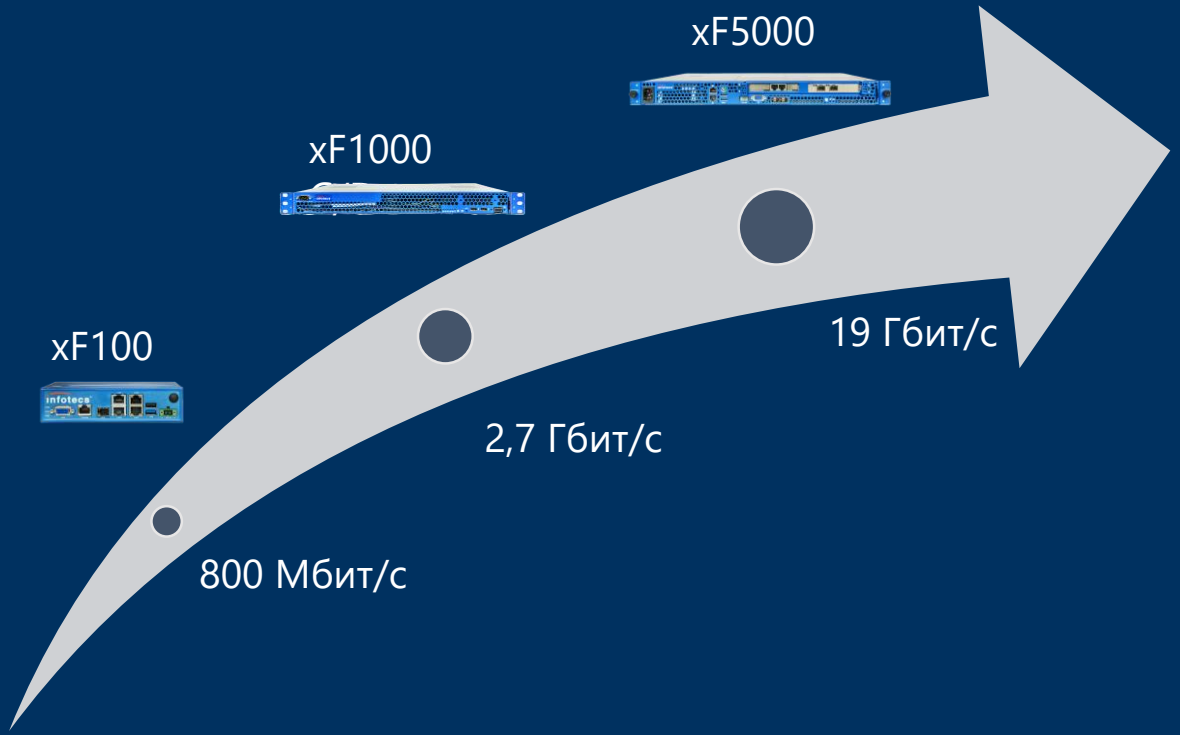
Coordinator for Win/Linux	Coordinator KB	HW 4 поколения	xFirewall	IDS NS

Что такое ViPNet xFirewall

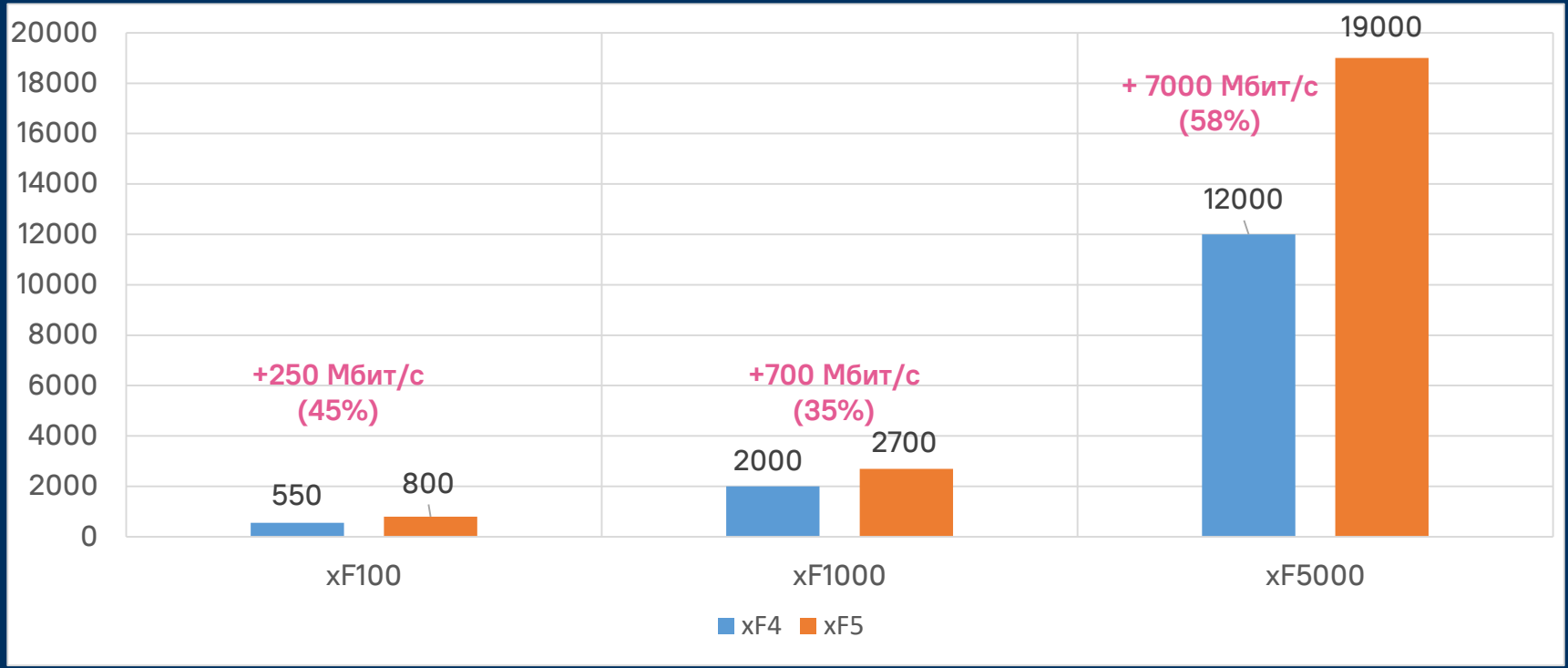
ТЕХНО infotecs ФЕСТ 2021

Сетевая платформа в составе:	Межсетевой экран	Сетевой экран приложений - DPI
Система предотвращения вторжений	Шлюзовой антивирус	Интеграция с Active Directory

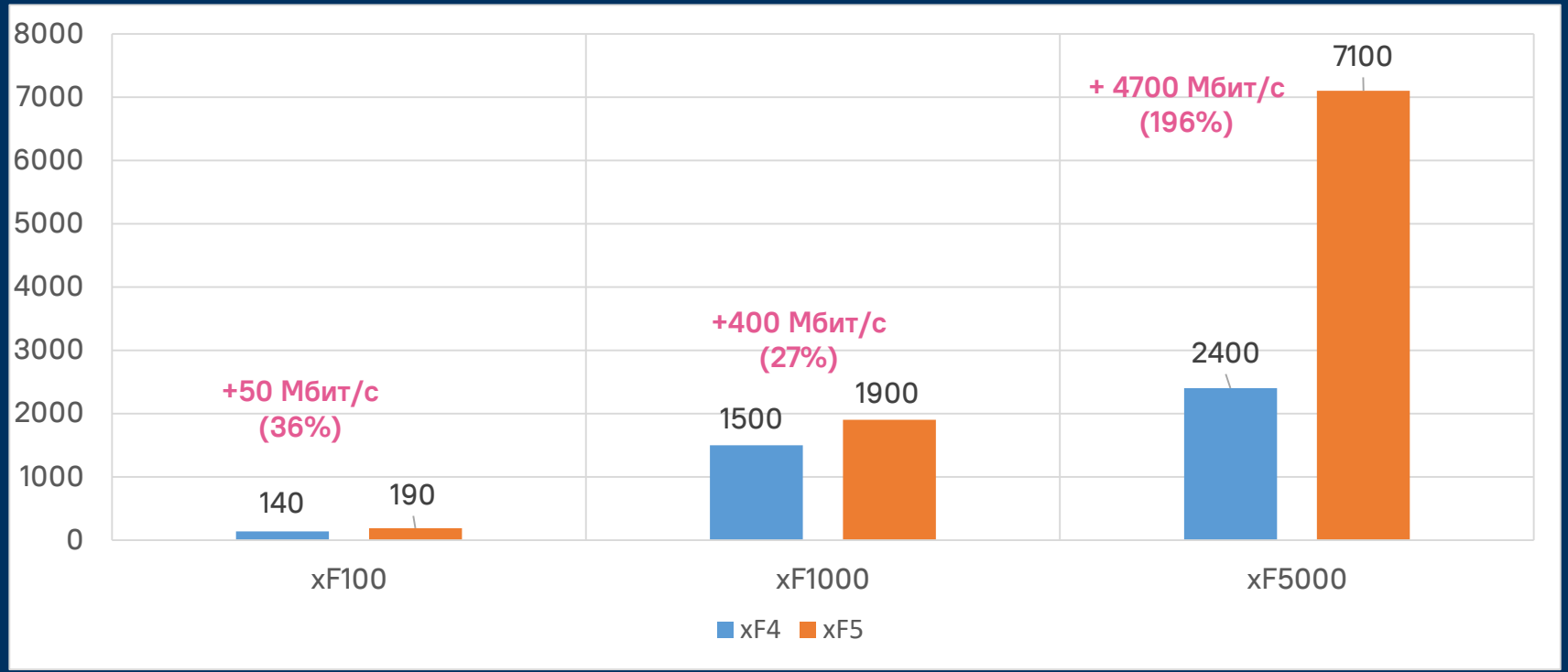
ViPNet xFirewall. Платформы



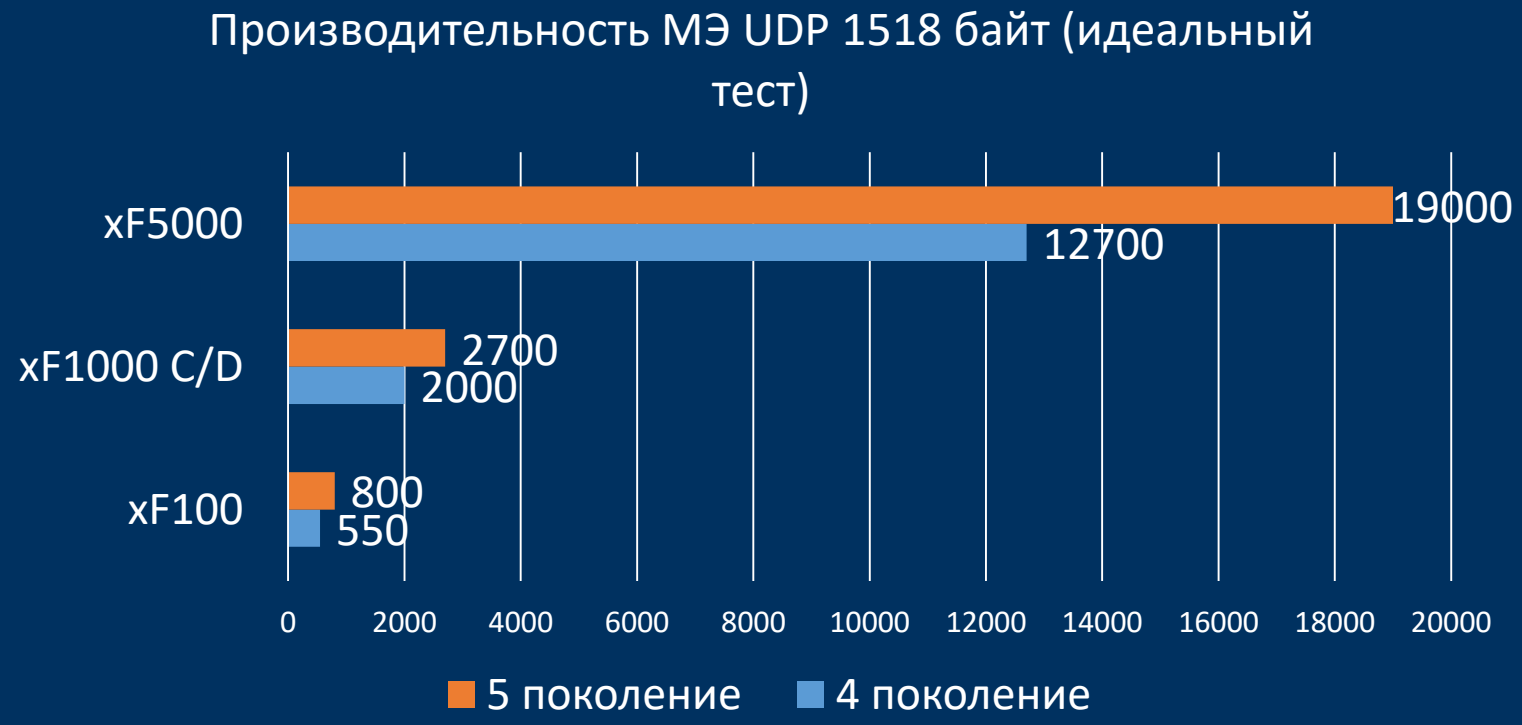
Производительность МЭ (UDP)



Производительность Application Control



ViPNet xFirewall 5. Платформы



xF5000

xF1000 C/D

xF100

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 Gb/ 6000 users = 1,18 Mbps/user

Знать что охранять

2065 уникальных приложений/протоколов

95 из категории «Социальные сети»

45 – потоковое видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

Управлять доступом

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

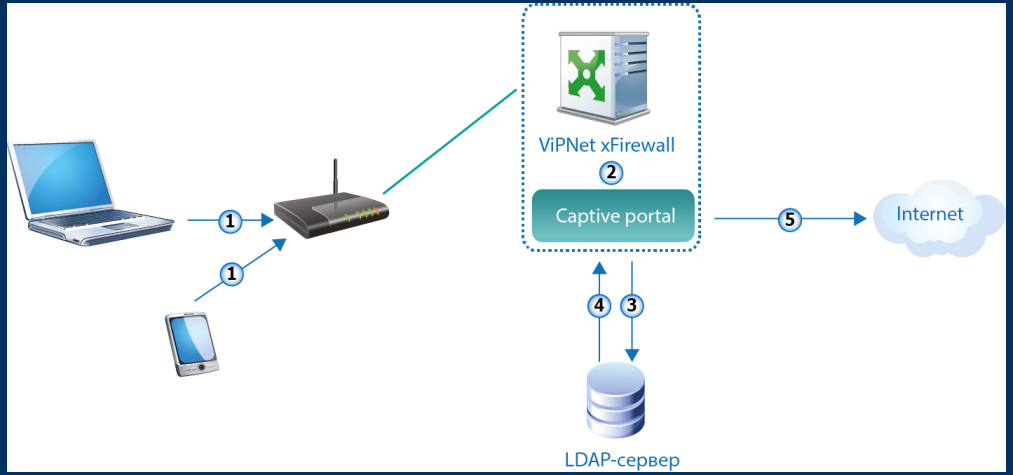
Использование учетных записей пользователей MS AD в правилах фильтрации

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

BYOD – принеси свое устройство и работай

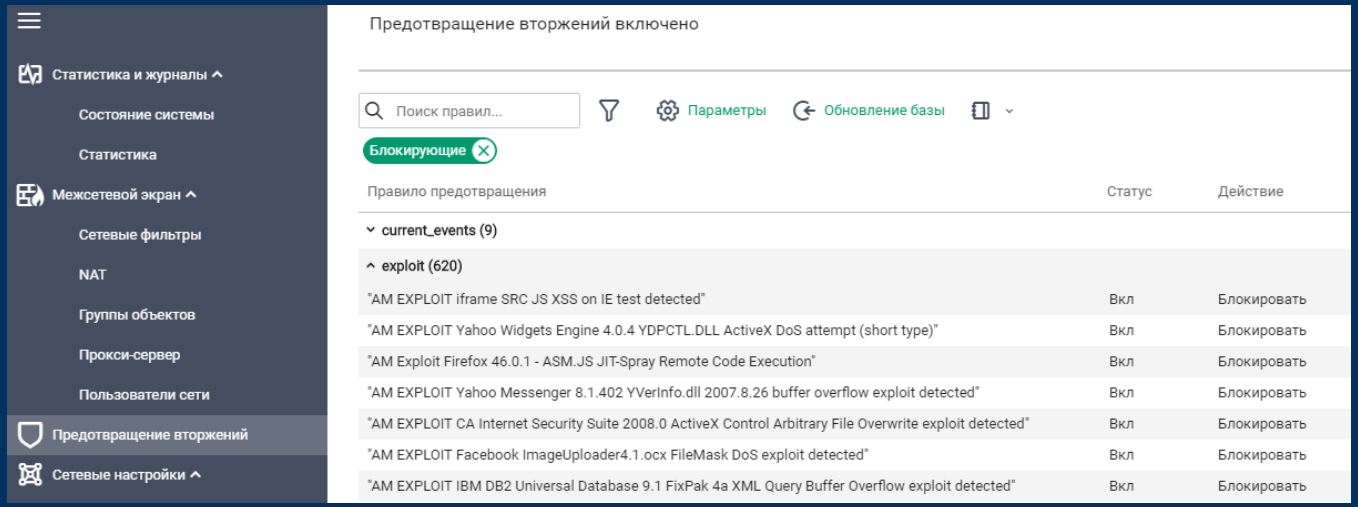
Captive portal – аутентификация с помощью браузера

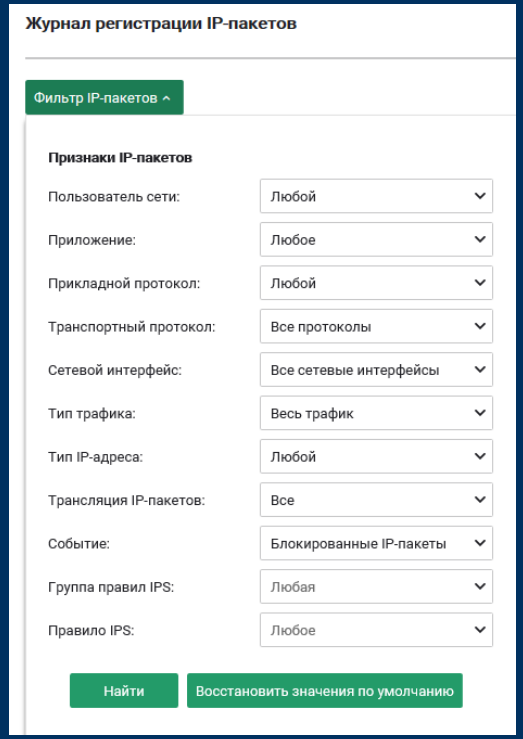
- Идентификация пользователей, использующих Linux компьютеры, iPhone, iPad и Android-устройства
- Предоставление контролируемого доступа подрядчикам, партнерам
- Автоматическое перенаправление на Портал аутентификации – Captive Portal



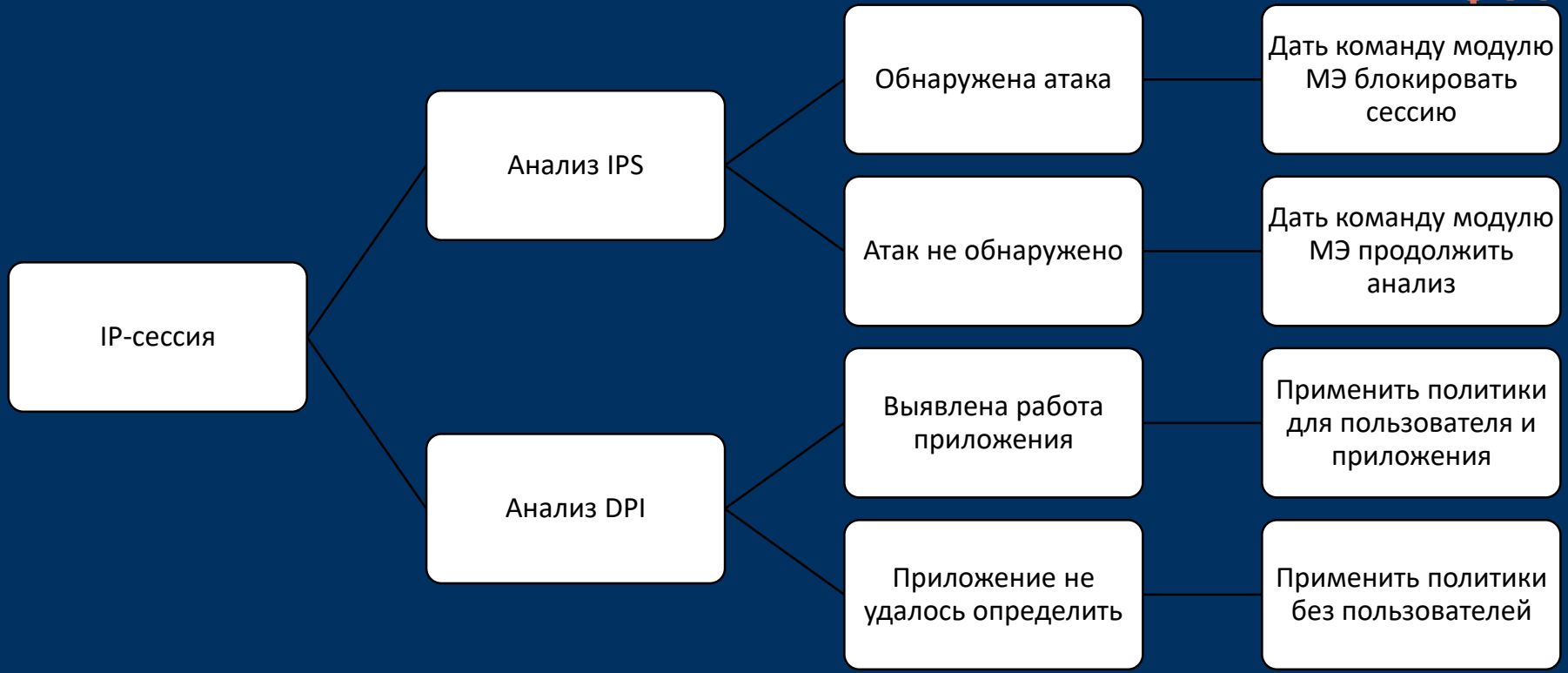
№3 – Защита от сетевых атак

Система предотвращения вторжений





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.

№6 – Что делать с SSL

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

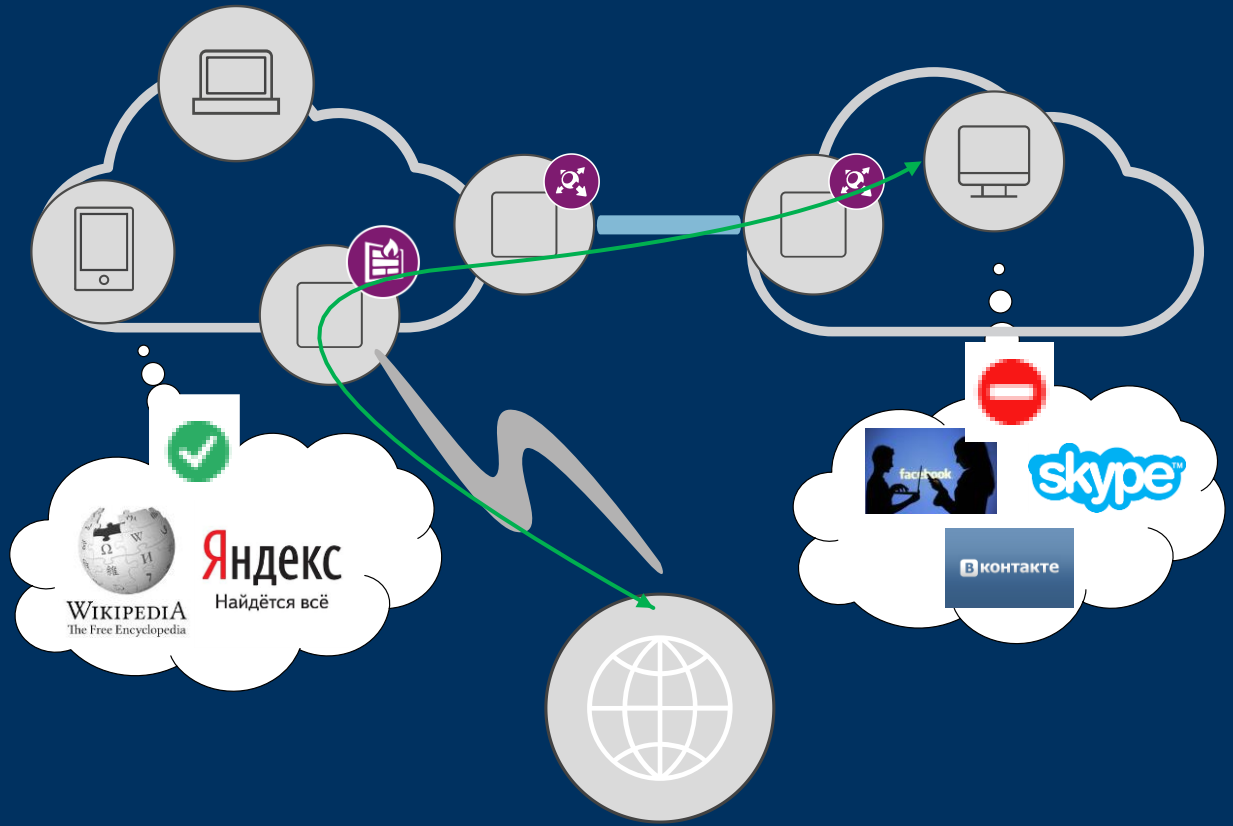
Защита от сетевых атак – блокировка аномалий, запретных команд

Защита от вирусных атак

Уменьшение поверхности атаки

Схема использования

Схема использования



ТЕХНО 2021 infotecs Фест

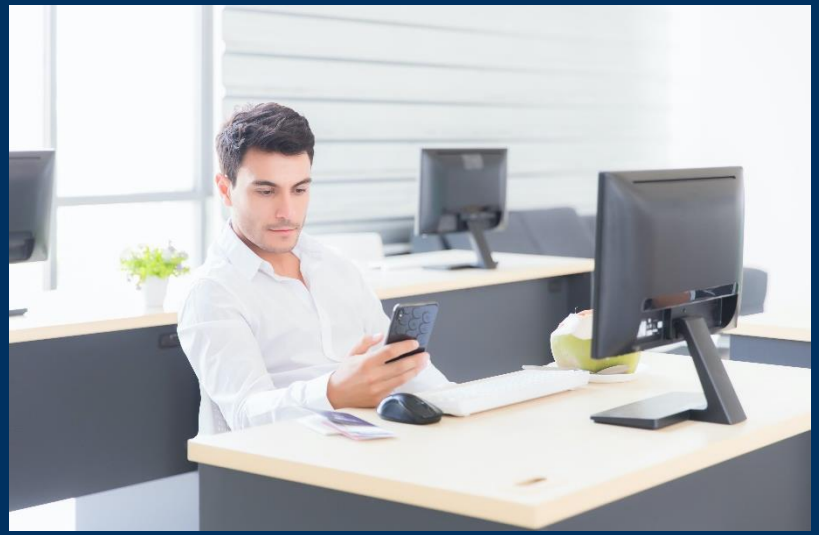
Спасибо за внимание!

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

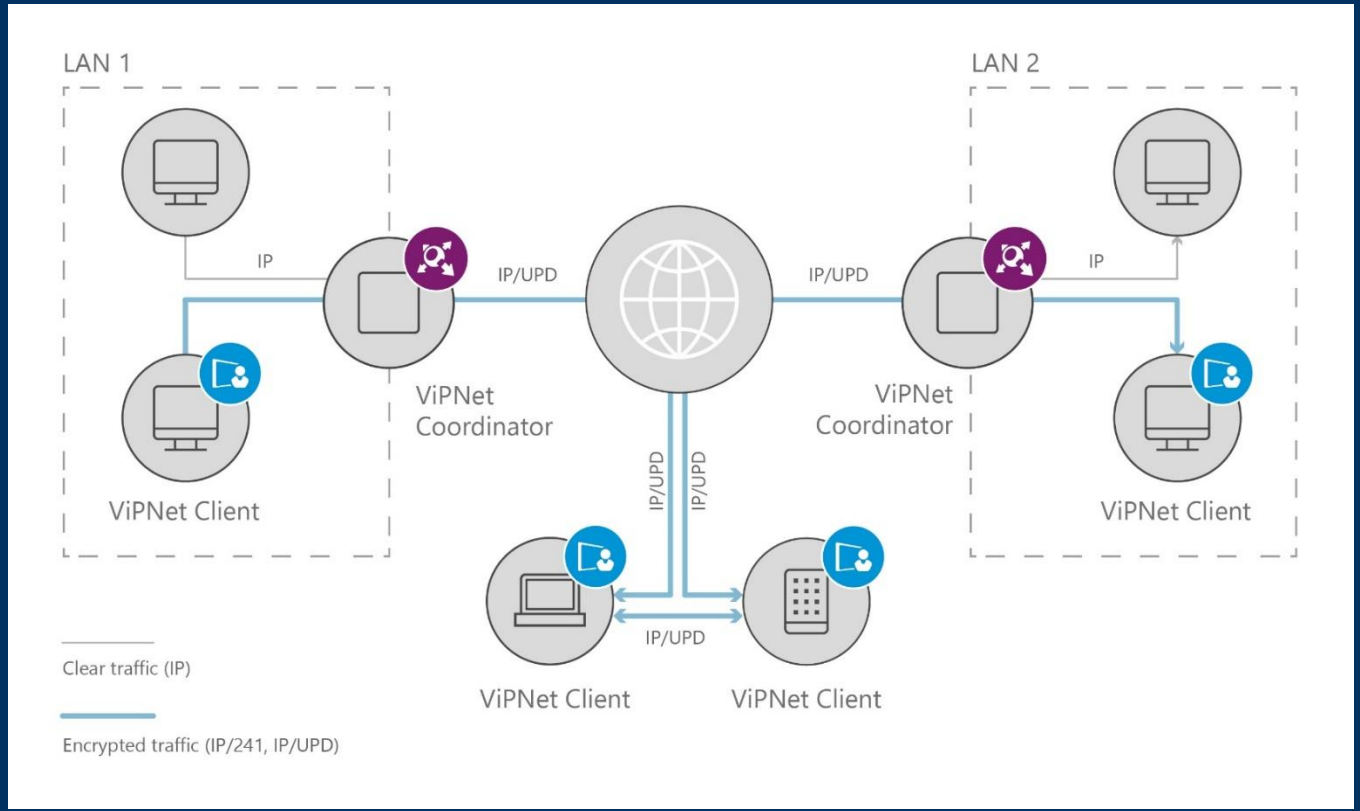
Личное или корпоративное устройство



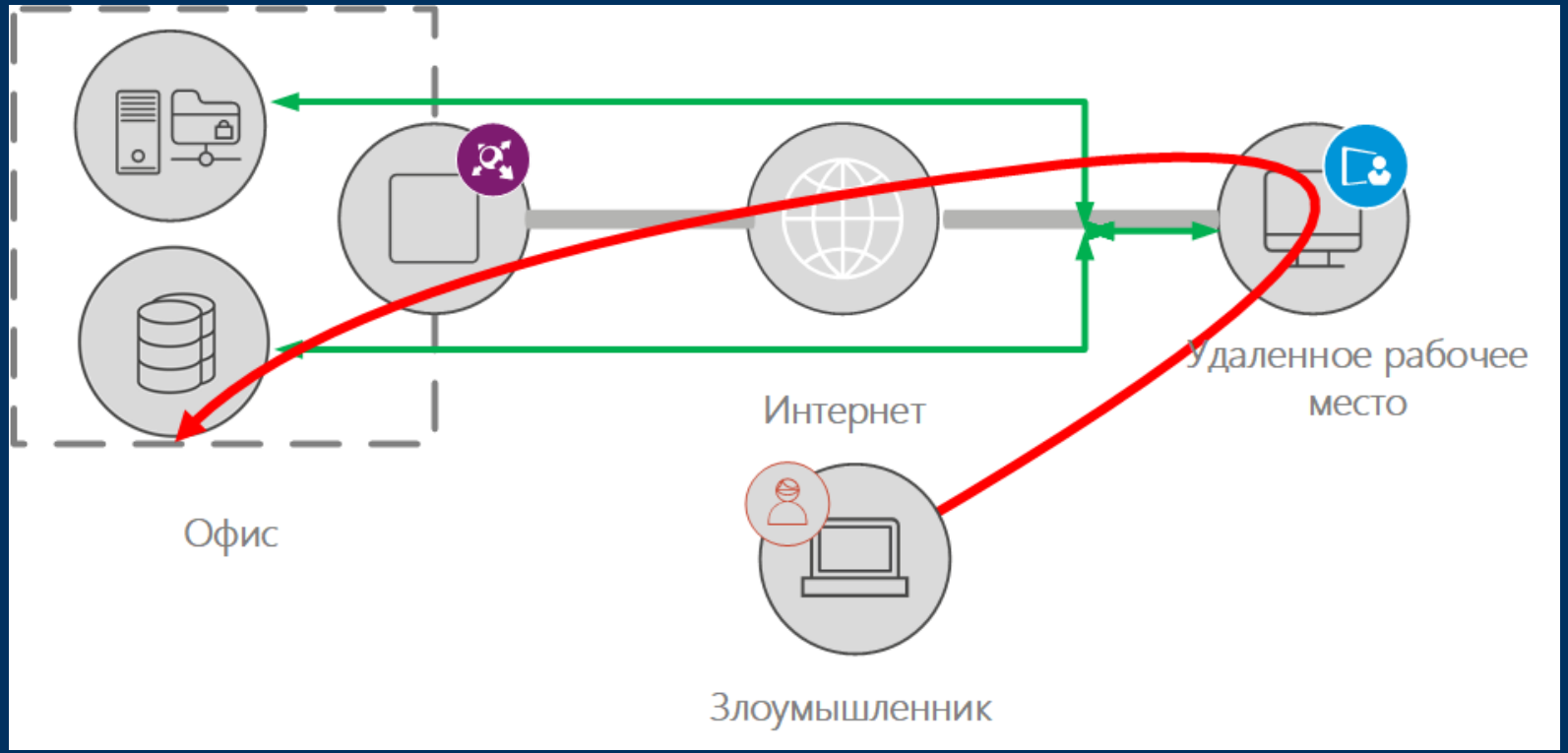
17% используют только личные устройства

17% используют только корпоративные устройства

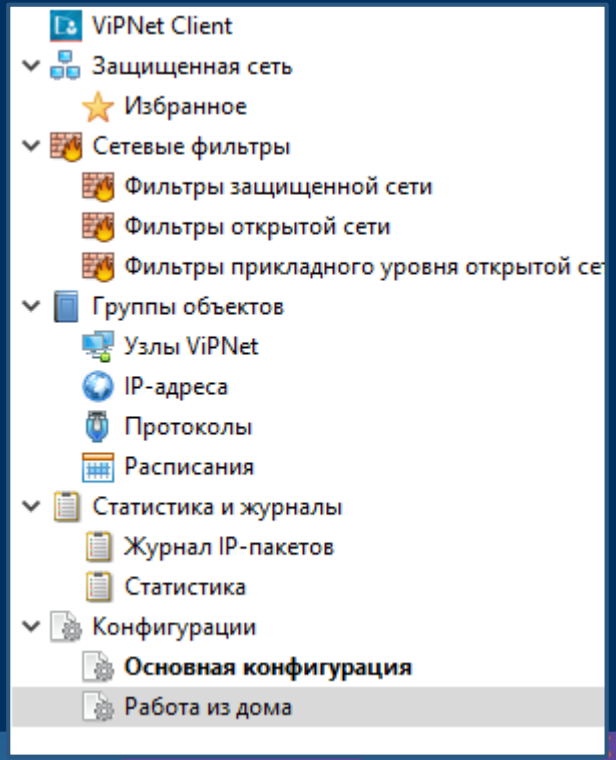
Удаленный доступ



Где риски



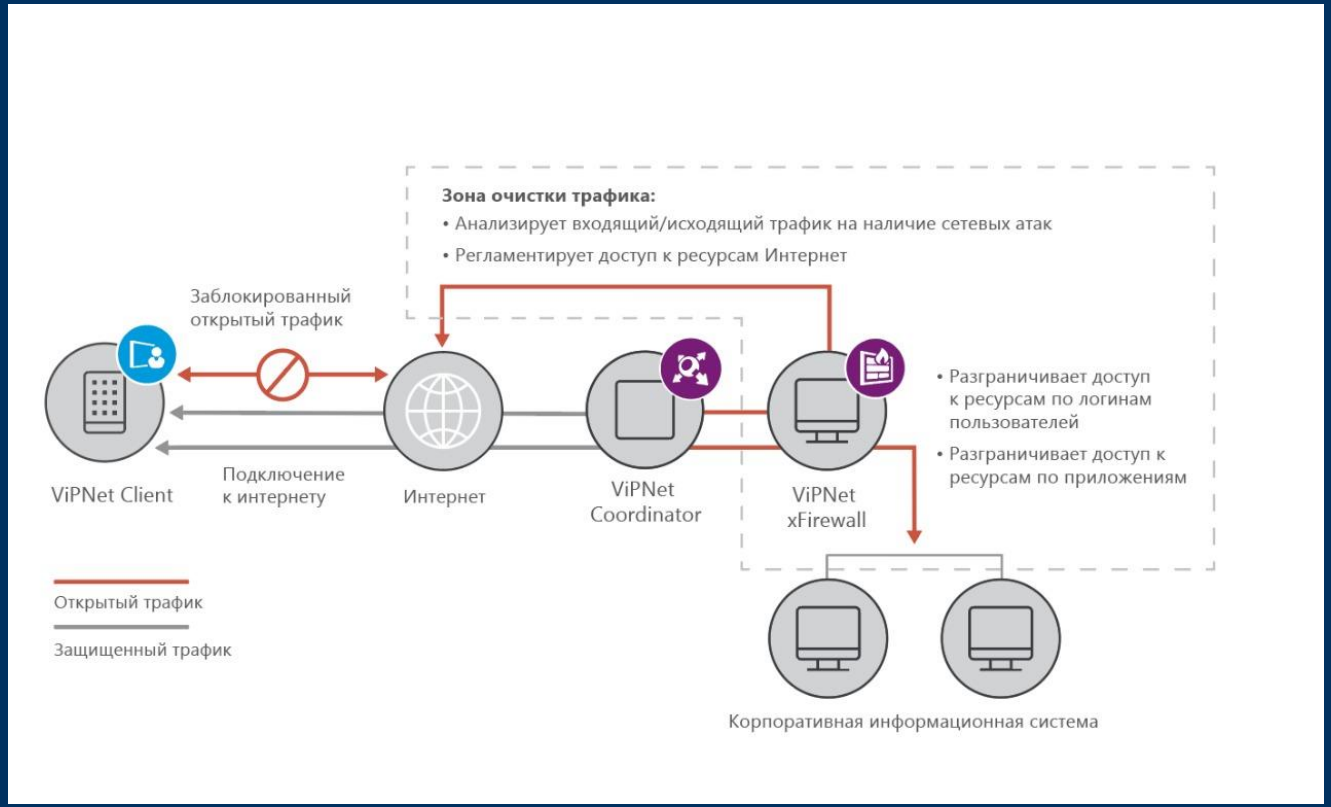
ViPNet Client: Software Defined Perimeter (SDP)



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 2021 infotecs Фест

Спасибо за внимание!