Практические аспекты эксплуатации NGFW

Мир изменился

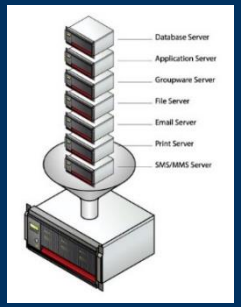
Мир изменился

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

Malware uses Social Networks

Social engineering will remain one of the easiest ways for a cybercriminal to gain access to a computer system to deploy a ransomware attack –

https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

ViPNet xFirewall

7 задач

ТЕХНО 2020 infotecs ФЕСТ

Знать, что охранять

Управлять доступом

Защитить от сетевых атак

Реализовать BYOD

Защитить от вирусов

Что делать с SSL

Защита от неизвестных угроз

ViPNet xFirewall

ТЕХНО 2020 infotecs ФЕСТ

Шлюзы безопасности

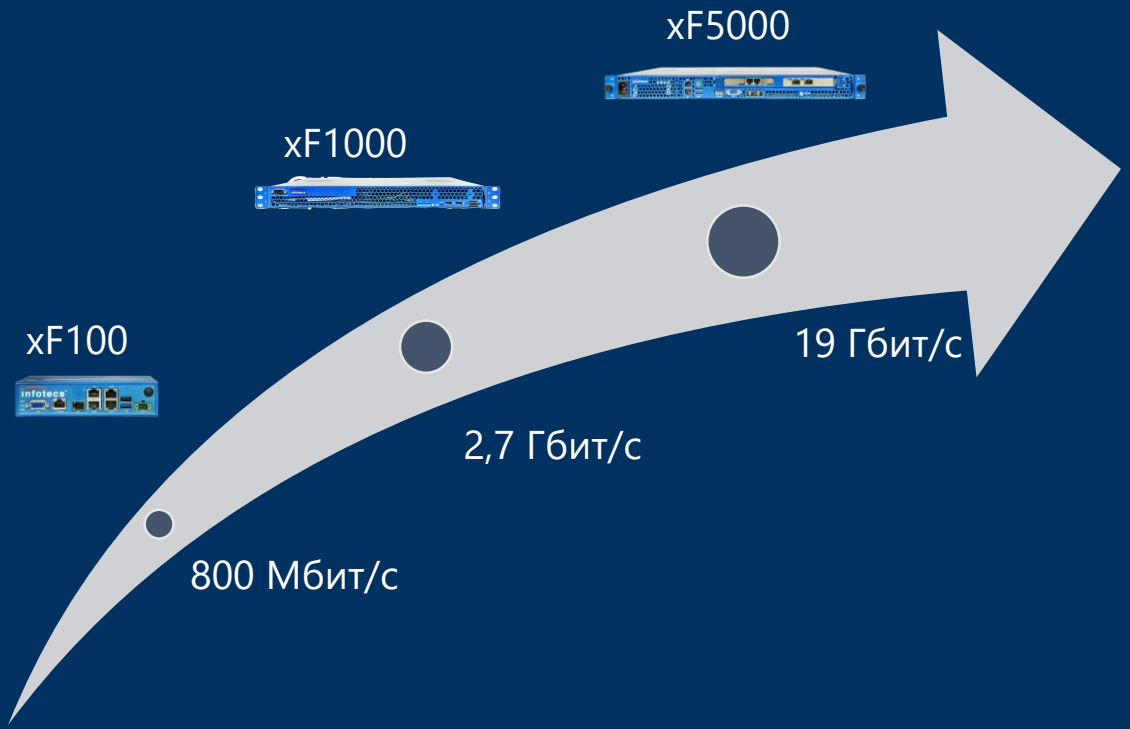
FW/VPN			NGFW	IDS
Coordinator for Win/Linux	Coordinator KB	HW 4 поколения	xFirewall	IDS NS

Что такое ViPNet xFirewall

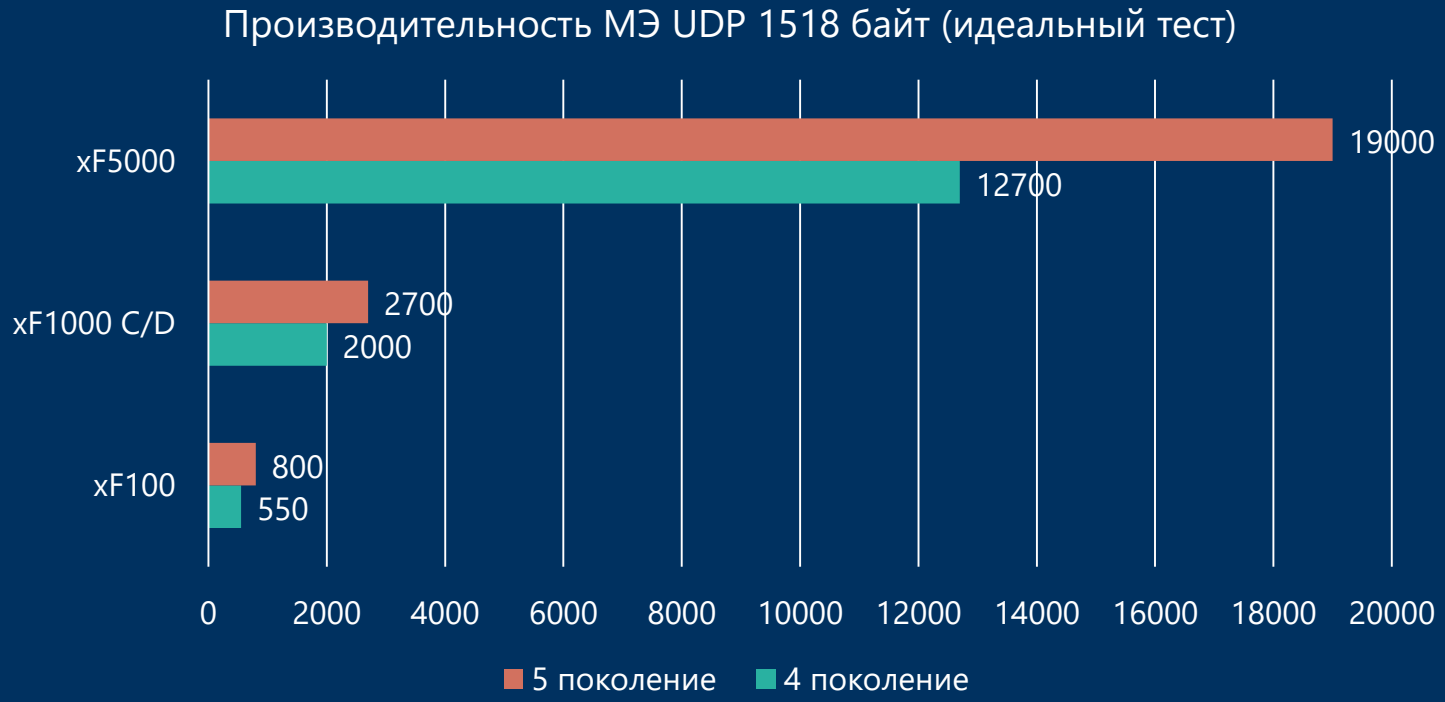
ТЕХНО 2020 infotecs фест

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

ViPNet xFirewall. Платформы



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

Открыл порты 80/443 ==
Открыл всЁ!

Stateful Packet Inspection

Stateful packet inspection looks at the header and footer of a packet.

Deep Packet Inspection

Deep packet inspection examines the data part of a packet.

Stateful Packet Inspection и Deep Packet Inspection

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

Бесклиентская 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

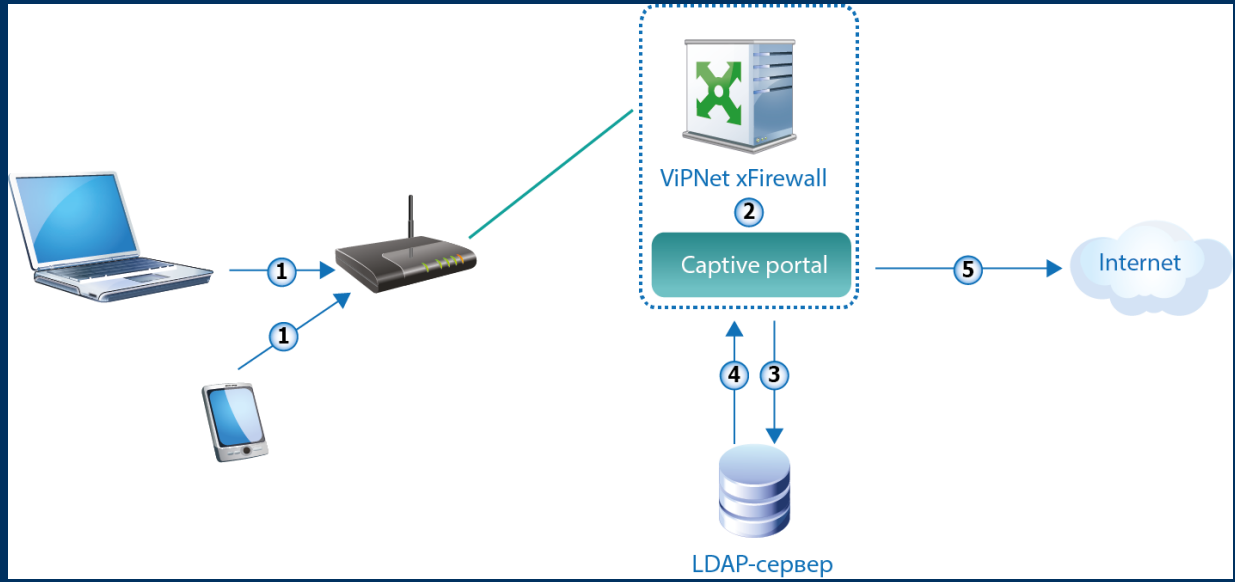
Использование учетных записей пользователей MS AD в правилах фильтрации

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

BYOD – принеси свое устройство и работай

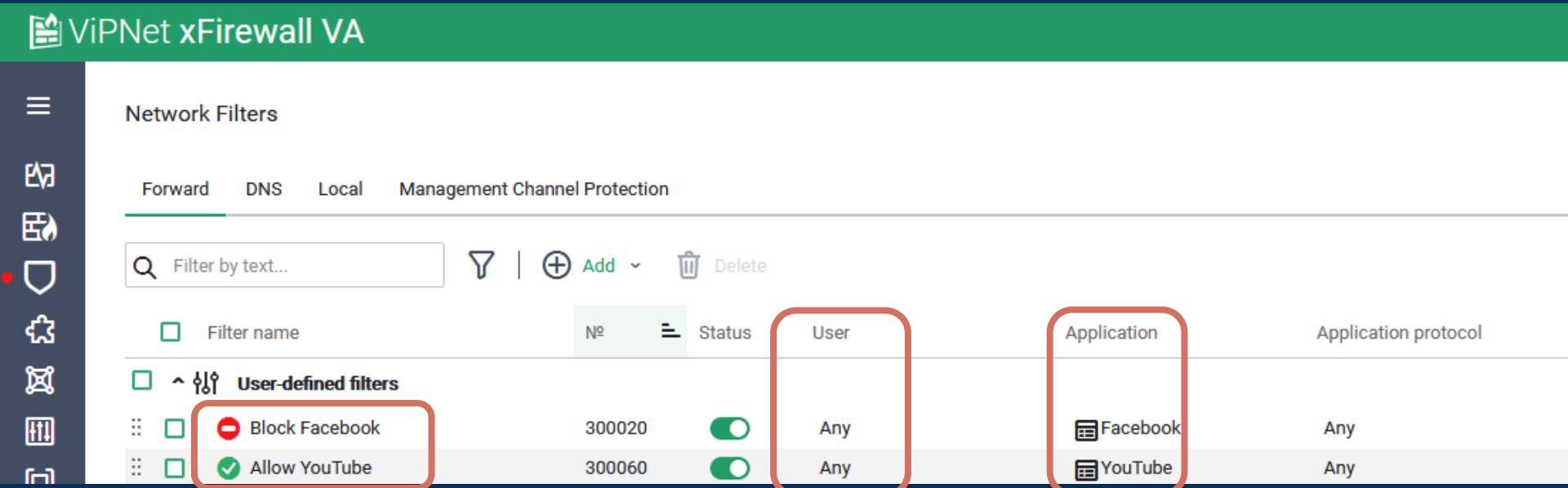
Captive portal – аутентификация с помощью браузера

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



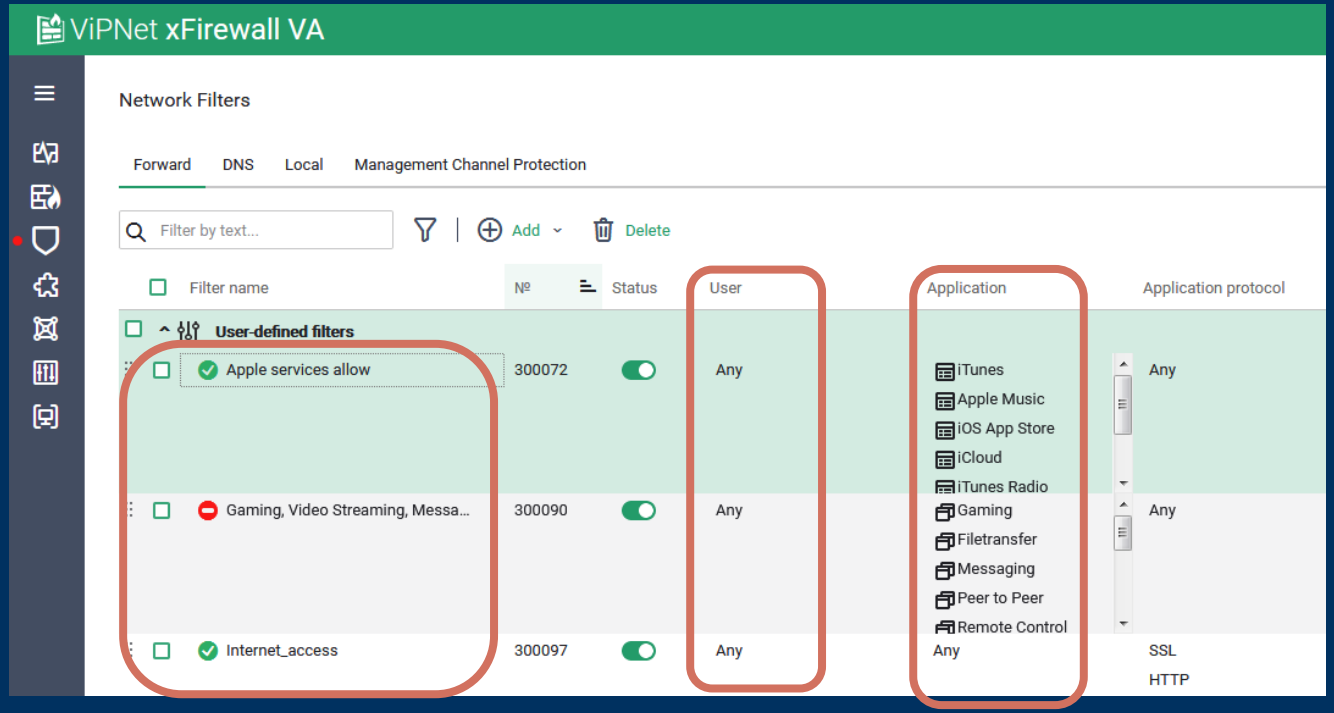
Политики доступа стали просты и понятны

ТЕХНО infotecs ФЕСТ 2020



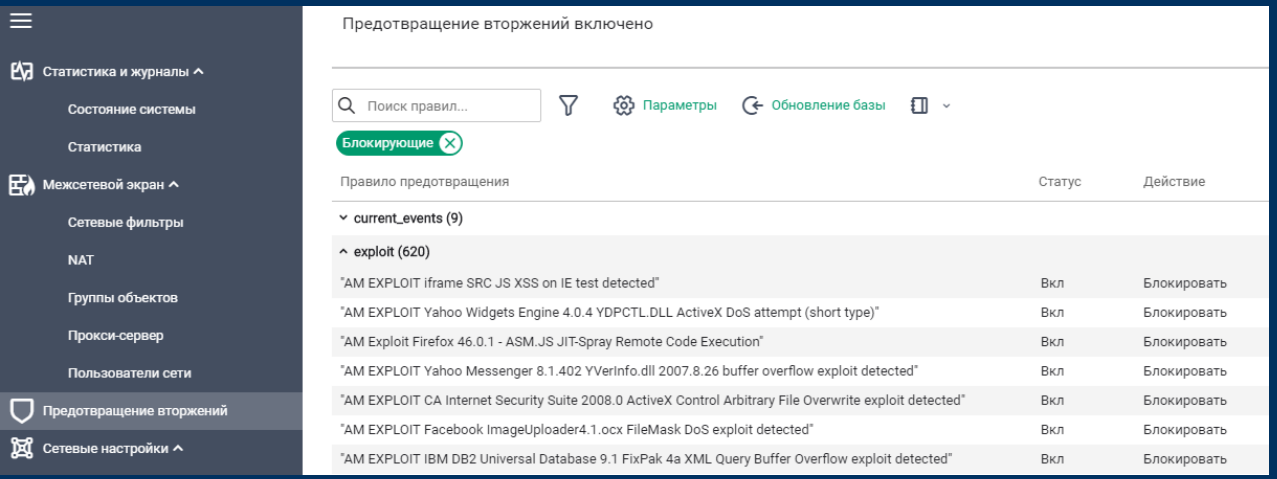
Как быстро и просто контролировать доступ в Интернет

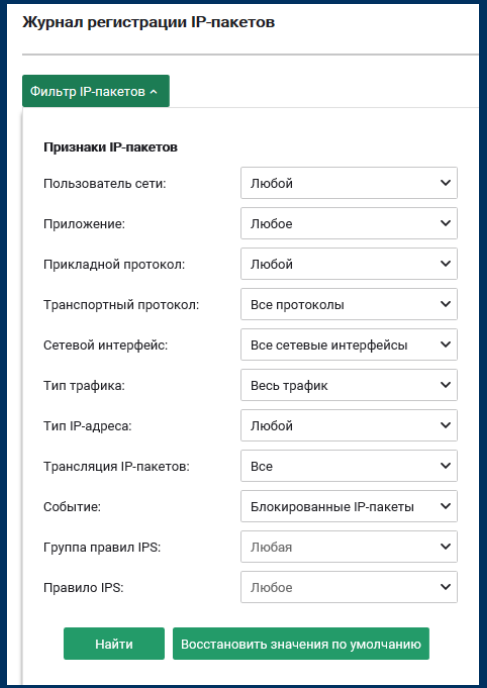
ТЕХНО 2020 infotecs ФЕСТ



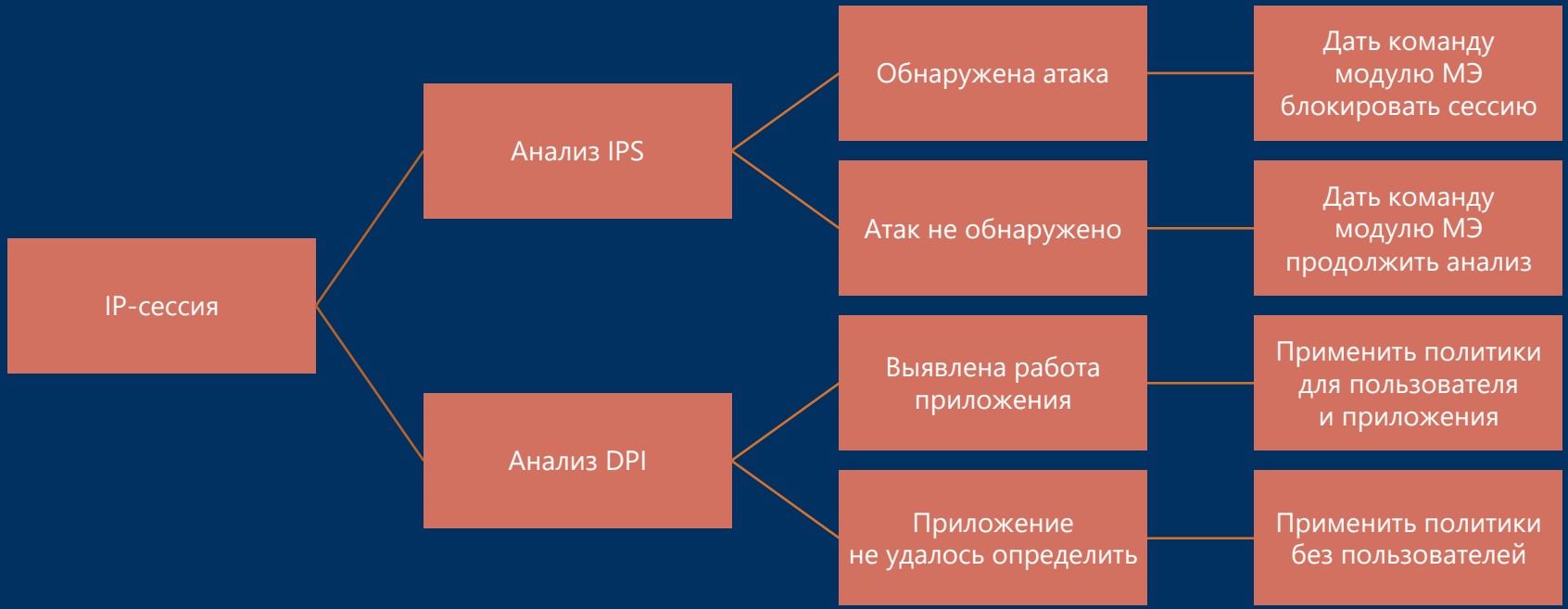
№3 – Защита от сетевых атак

Система предотвращения вторжений





Порядок применения правил IPS



№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

Поддержка песочниц

- ViPNet xFirewall выполняет функции прокси-сервера
- ViPNet xFirewall передает загружаемые файлы из сети Интернет в «песочницу» ATHENA через службу прокси-сервера по протоколу ICAP
- «Песочница» проводит исследования файлов на подозрительное содержимое

№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

ТЕХНО 2020 infotecs ФЕСТ

Максимальная видимость – фильтрация на 7 уровне ISO OSI

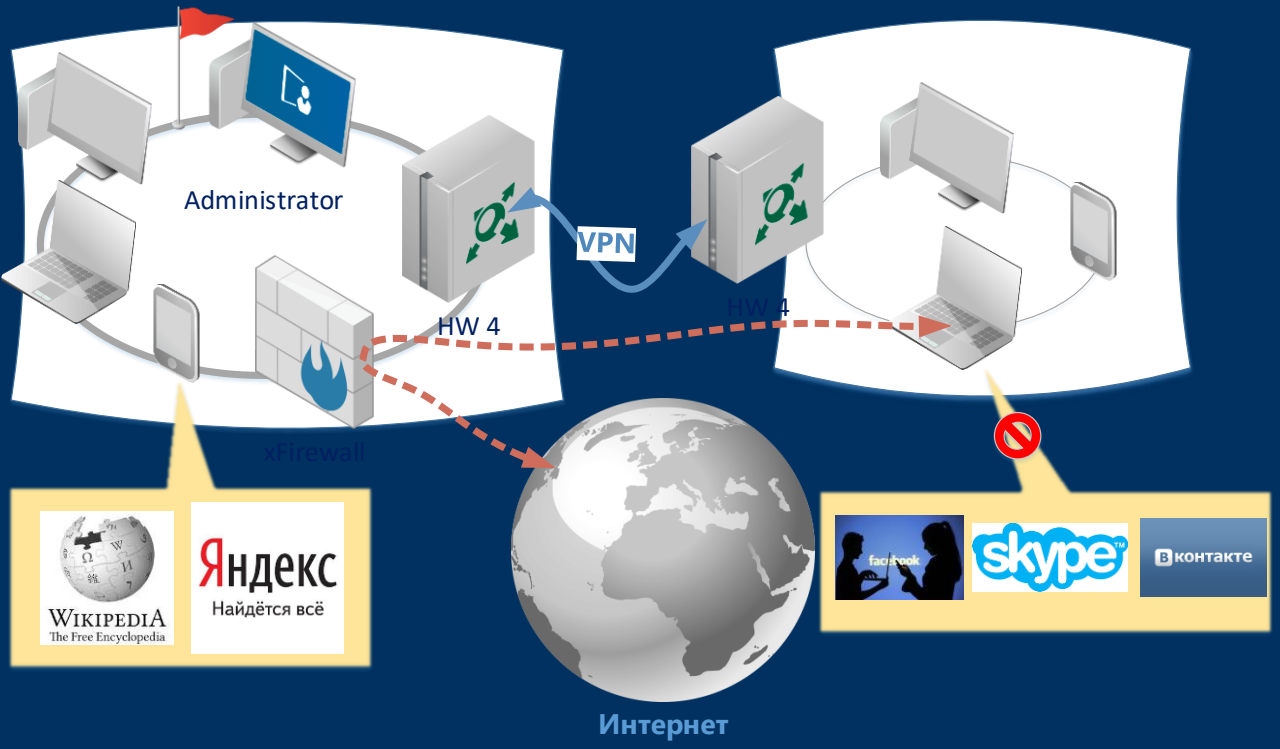
Защита от сетевых атак – блокировка аномалий, запретных команд

Защита от вирусных атак

Уменьшение поверхности атаки

Схема использования

Схема использования



ТЕХНО 2020 infotecs Фест

Спасибо за внимание!