

техно infotecs
2019 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

12
09 2019

Next Generation Firewall
- универсальное
средство ИБ
современного мира IT



Мир изменился

Мир изменился



Web 2.0



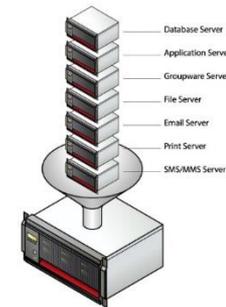
Mobile Devices



Streaming video



Cloud/SaaS

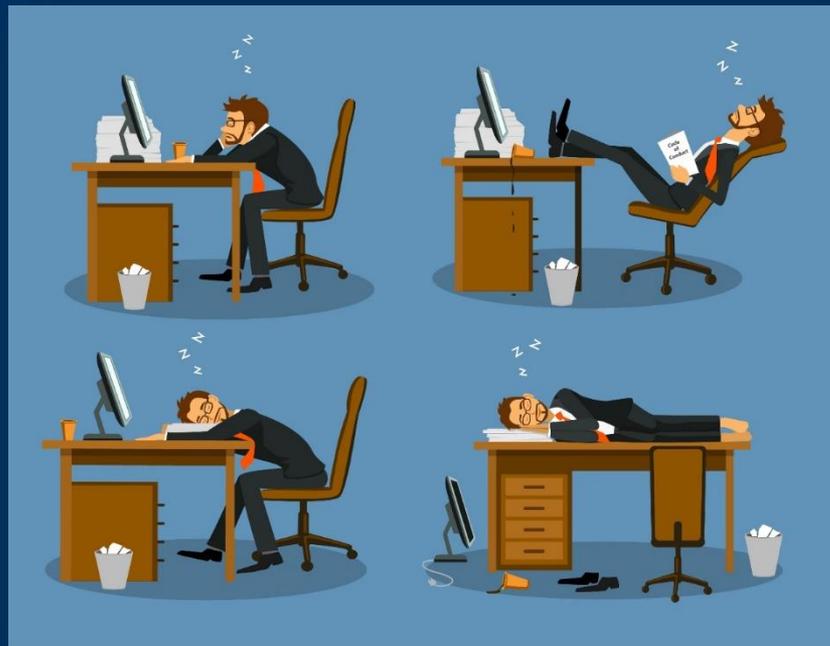


Virtualization



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

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

Знать что
охранять

Управлять
доступом

Защитить от
сетевых атак

Реализовать
BYOD

Защитить от
вирусов

Что делать с
SSL

Защита от
неизвестных
угроз



Что такое ViPNet xFirewall

Сетевая
платформа в
составе:

Межсетевой
экран

Сетевой экран
приложений -
DPI

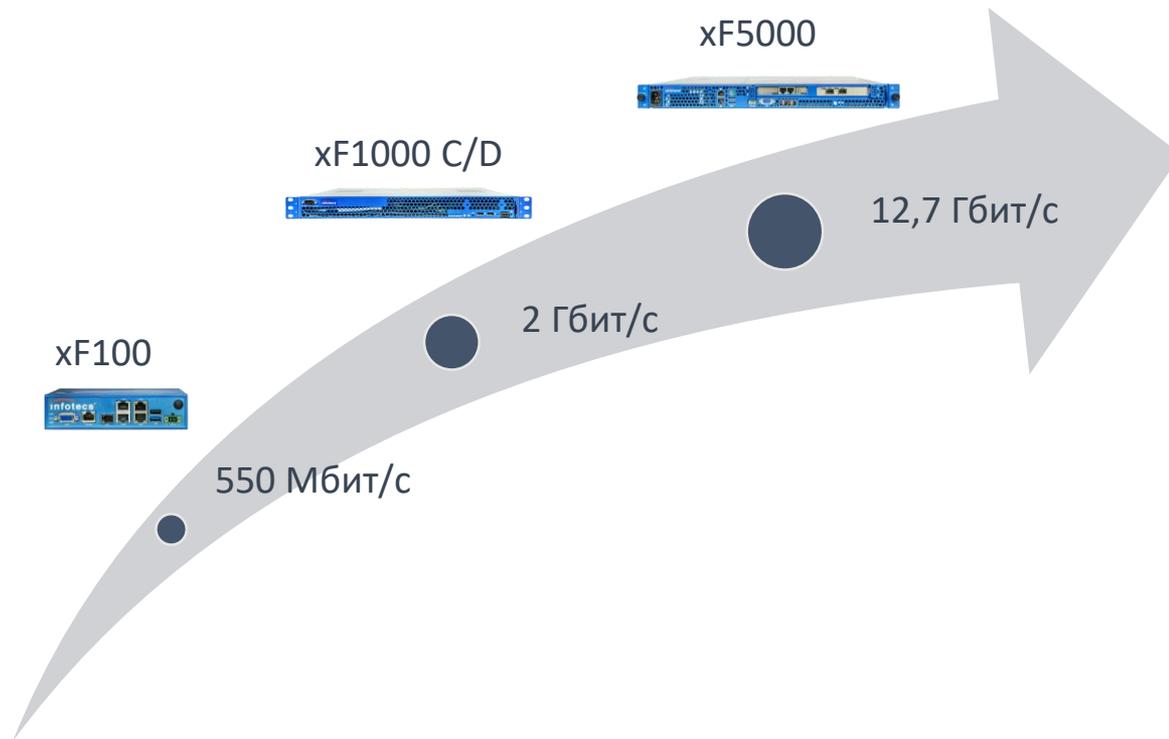
Система
предотвращения
вторжений

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.

$2,4 \text{ Gb} / 6000 \text{ users} = 400 \text{ Kbps/user}$

Знать что охранять



2065 уникальных приложений/протоколов

Top Ranking		Top Gainers	
1	Bejeweled Blitz PopCap	Hidden Runaway BULKYPIX	139 ▲ 262
2 ▲ 1	Hanging With Friends Zynga Inc.	Tom Clancy's Splinter Cell GameLoft S.A.	228 ▲ 141
3 ▼ 1	SCRABBLE Free Electronic Arts Inc.	Minecraft Companion Jason Fieldman	267 ▲
4	Jewels of the Amazon SCW	Police Chase Smash Hasham Ahmed Kamal	145
5 ▲ 1	James Cameron's Avatar GameLoft S.A.	G.U.N. BYSS mobile	111 ▲
6 ▲ 2	Police Chase Smash Hasham Ahmed Kamal	Wordfeud Bertheussen IT	65 ▲ 99
7 ▲ 5	Police Chase (FREE) Daniel Carbone	Hidden Expedition Big Fish Games, Inc.	329 ▲ 72
8 ▲ 8	Amazon™: Hidden Expeditions Big Fish Games, Inc.	Minecraft Help XAECC LIMITED	293 ▲ 71
9 ▲ 2	Police Chase Car Racer Sean Demeyere	Crimson: Steam Pirates Bungie Aerospace Corporation	277 ▲ 68
10 ▼ 3	Diamond Dash wozje GmbH	The ROBLOX Quiz John LaRouche	142 ▲ 64
11 ▼ 2	Agent Dash Full Fat Productions LLC	Justin Beiber/Nick Steven Goodemote	220 ▲ 60
12 ▲ 3	Motorcycle Bike Race RoboTech Systems, LLC	I Dig It Expedition IMotion Software, LLC	132 ▲ 56
13 ▼ 3	iGun Pro™ LITE - The Game Orion Moon Eiretta	Solitaire Finger Arts	194 ▲ 56
14 ▼ 9	Air Patriots Lemon Games SL	Choo Choo Steam Train Chillingo Ltd	143 ▲ 53
15 ▼ 2	Goaaal!™ Soccer Tactics Skyworks Interactive	Solitaire + Chepnological Ltd	258 ▲ 53

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

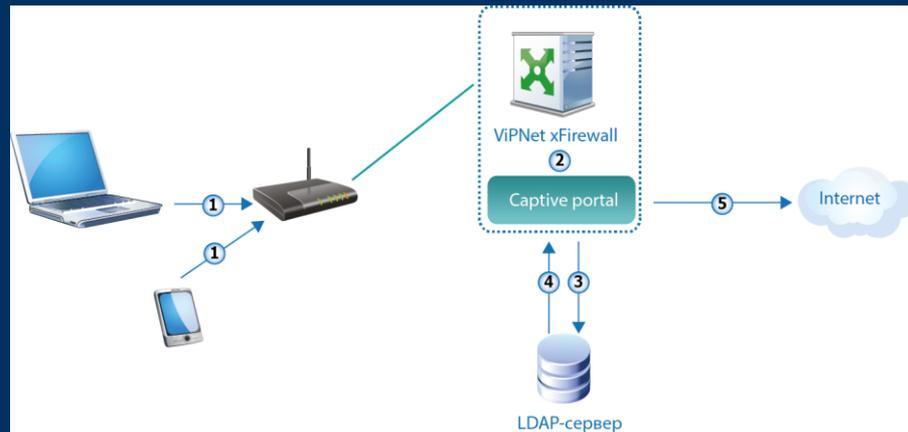


BYOD – принеси свое устройство и работай



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



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 dark blue, semi-transparent grid of hexagons. Inside some hexagons are icons: a padlock (some are closed, some are open) and a magnifying glass. The overall aesthetic is high-tech and cybersecurity-oriented.

ViPNet xFirewall 5 -IPS

☰

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 ^

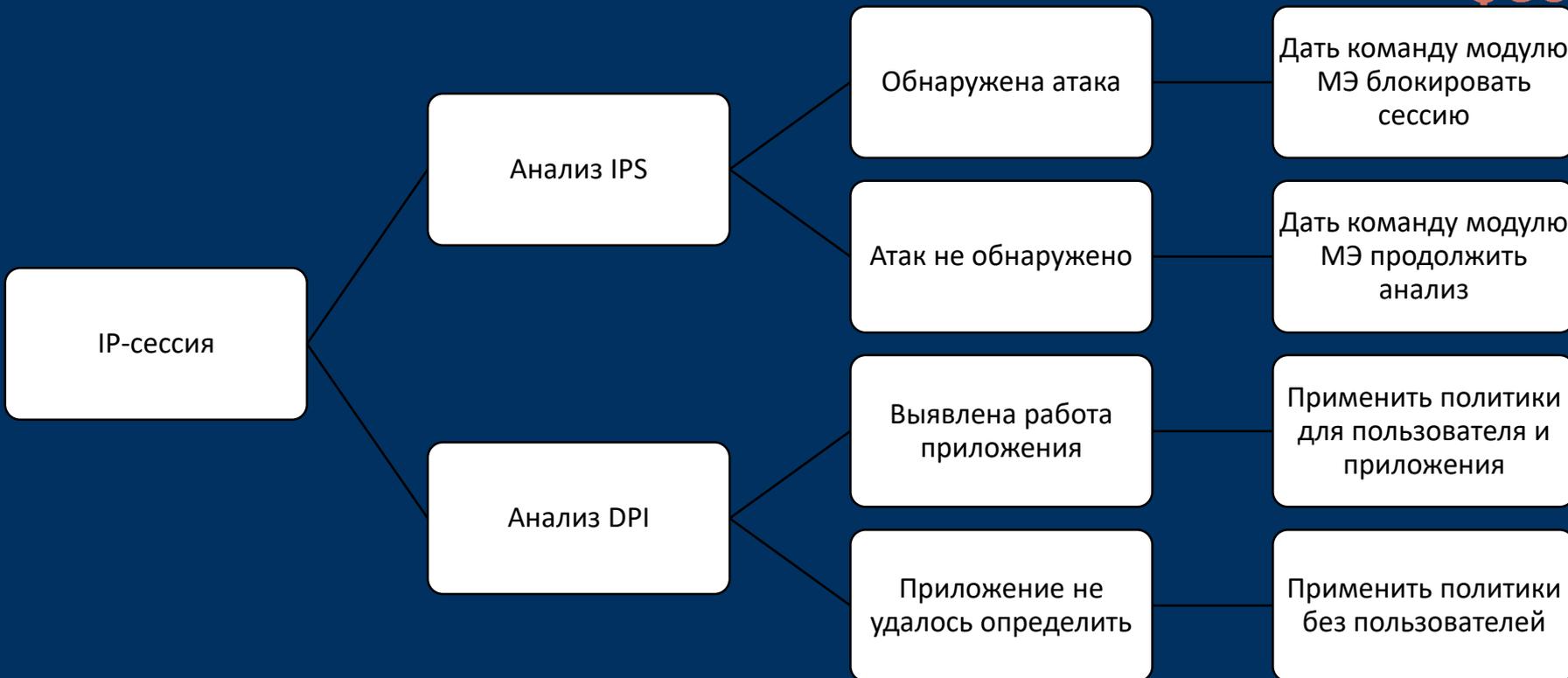
Признаки IP-пакетов

- 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

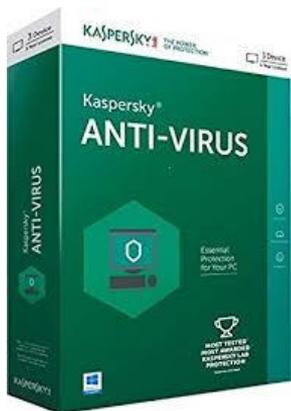
Порядок применения правил IPS



№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.

№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

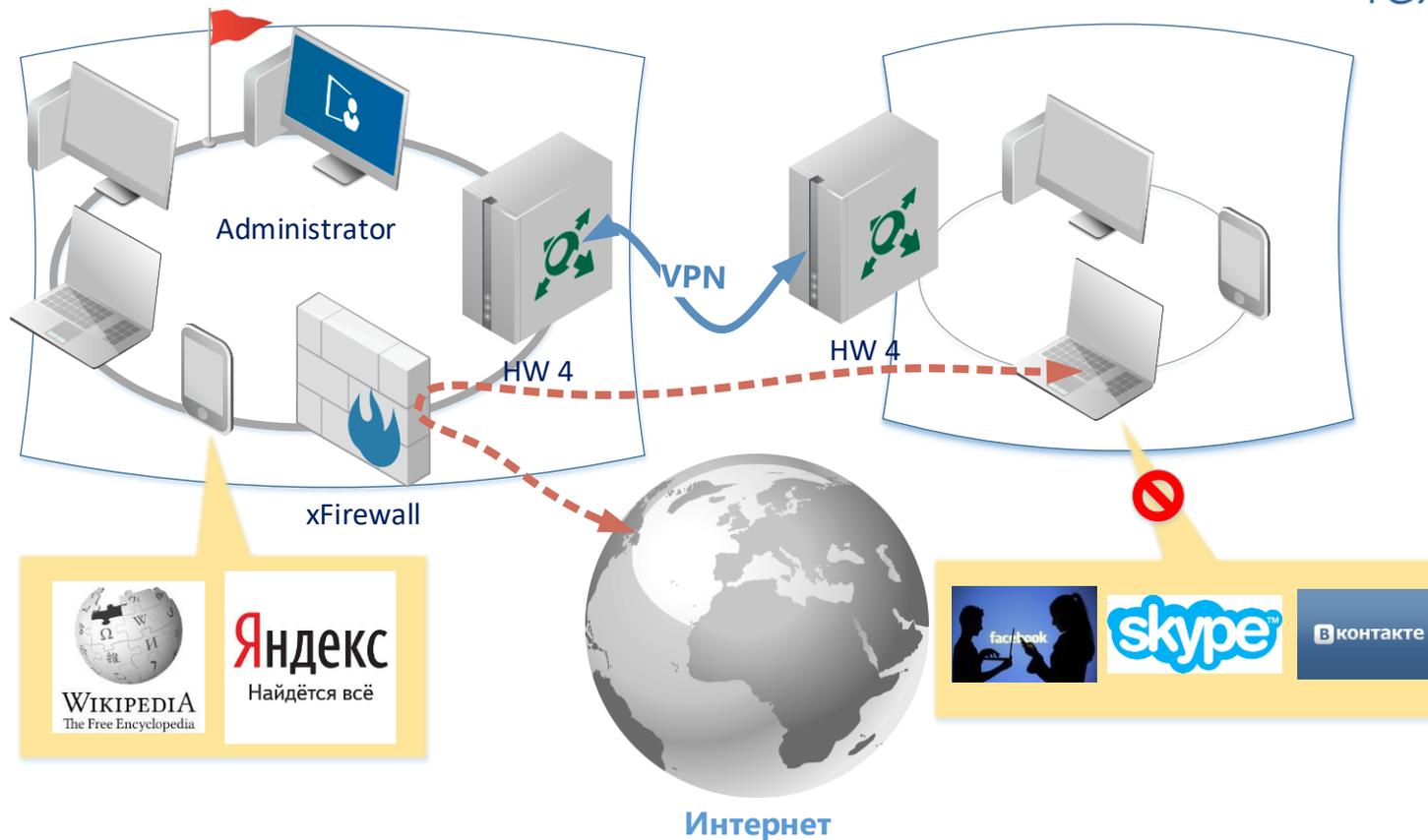
Уменьшение
поверхности атаки





Схема использования

Схема использования





ТЕХНО infotecs
2019 Фест

Спасибо
за внимание!