



техно infotecs
2020 ФЕСТ

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Практические
аспекты эксплуатации
NGFW



Мир изменился

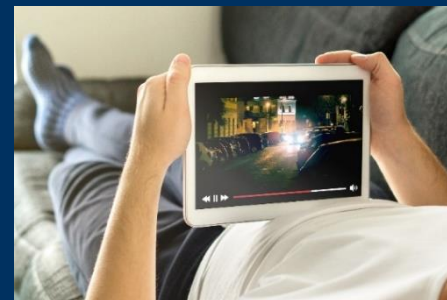
Мир изменился



Web 2.0



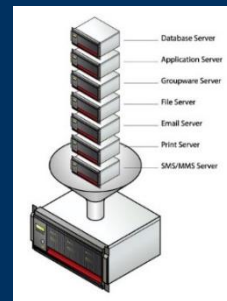
Mobile Devices



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

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



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

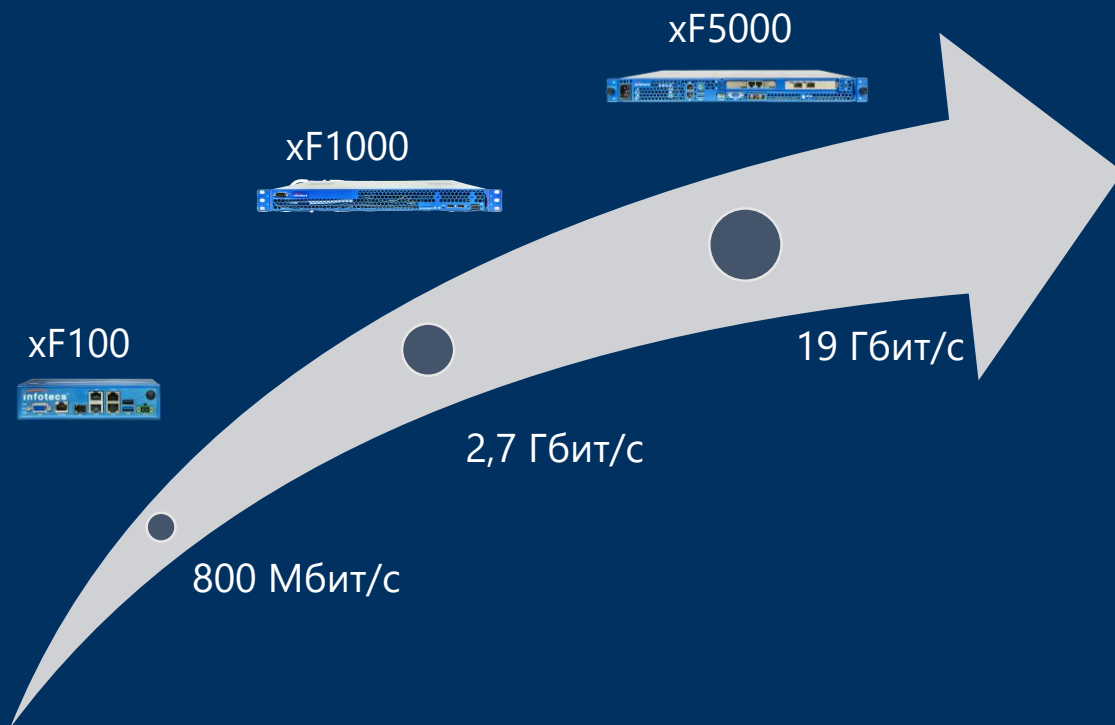
Система
предотвращения
вторжений

Шлюзовой
антивирус

Интеграция
с Active Directory

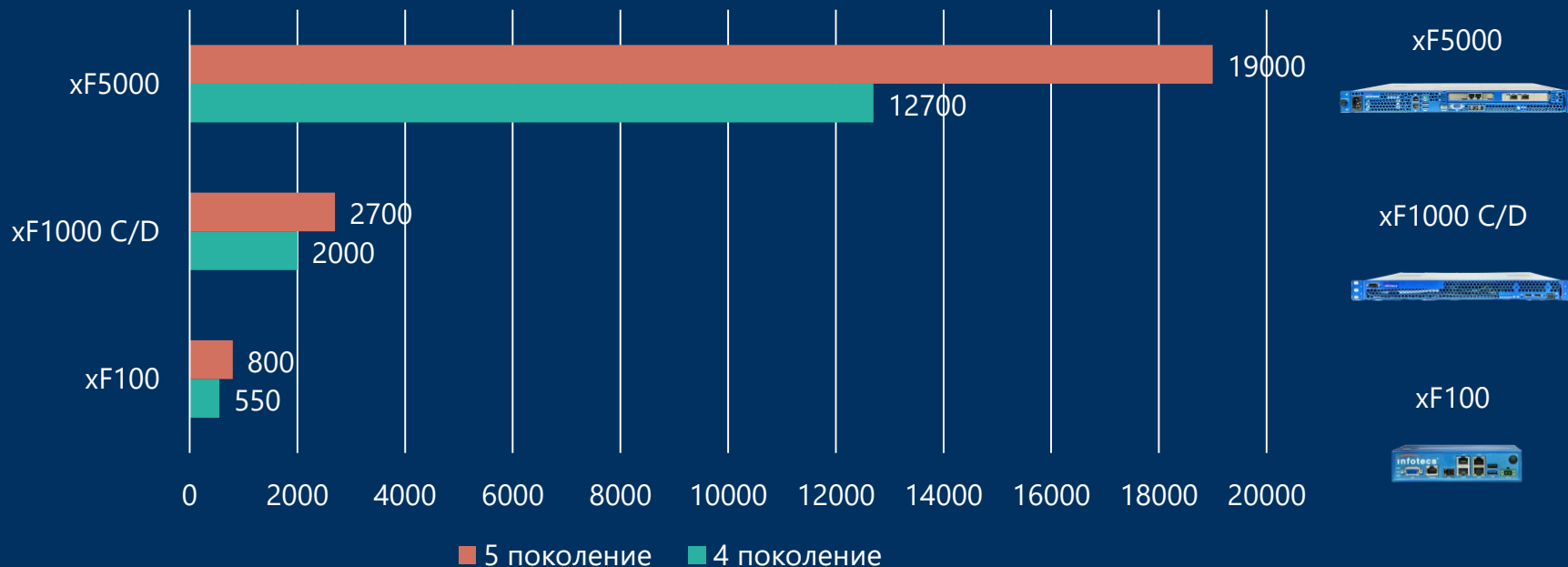


ViPNet xFirewall. Платформы



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 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



Top Ranking		Top Gainers	
Bejeweled Blitz PopCap	1 →	Hidden Runaway SULKVRB	139 ▲ 262
Hanging With Friends Zynga Inc.	2 ▲ 1	Tom Clancy's Splinter Cell Gamebox S.A.	228 ▲ 141
SCRABBLE Free Electronic Arts Inc.	3 ▼ 1	Minecraft Companion Jason Feldman	267 ▲ 134
Jewels of the Amazon SON	4 →	Police Chase Smash Heptam Ahmed Kamal	145 ▲ 134
James Cameron's Avatar: The Game GameLott S.A.	5 ▲ 1	G.U.N. BYSS mobile	111 ▲ 127
Police Chase Smash Heptam Ahmed Kamal	6 ▲ 2	Wordfeud Bertheussen IT	65 ▲ 99
Police Chase FREE Daniel Carbone	7 ▲ 5	Hidden Expedition: Big Fish Games Big Fish Games, Inc.	329 ▲ 72
Amazon™: Hidden Expedition Big Fish Games, Inc.	8 ▲ 8	Minecraft Help XABCO LIMITED	293 ▲ 71
Police Chase Car Race Sean Demeyere	9 ▲ 2	Crimson: Steam Pirates Bungle 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/Nicki Minaj Steven Goodenote	220 ▲ 60
Motorcycle Bike Race RoboNeko Systems, L	12 ▲ 3	I Dig It Expedition iMolition Software, L	132 ▲ 56
iGun Pro™ LITE - T Common Motion Emarte	13 ▼ 3	Solitaire Finger Arts	194 ▲ 56
Air Patriots Lemon Games SL	14 ▼ 9	Choo Choo Steam Train Chimango Ltd	143 ▲ 53
Goaaal!™ Soccer Tournament Skyworks Interactive	15 ▼ 2	Solitaire + Chronological Ltd	258 ▲ 53



95 из категории
«Социальные сети»



45 – потоковое
видеовещание

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений



Управлять доступом



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

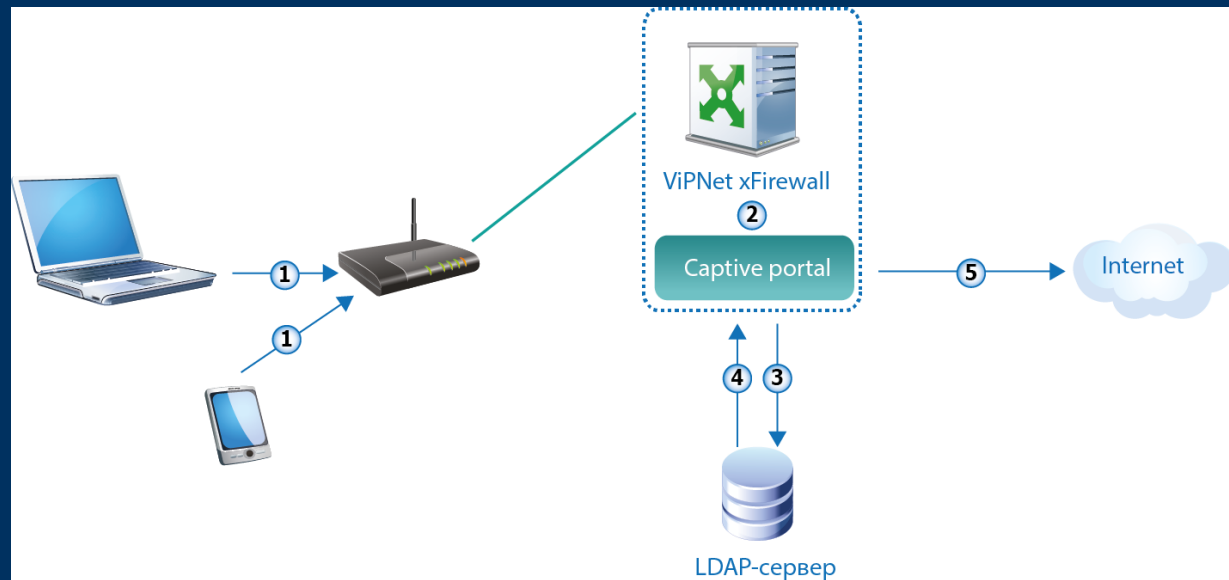


BYOD – принеси свое устройство и работай



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

ViPNet xFirewall VA

Network Filters

Forward DNS Local Management Channel Protection

Filter by text...  |  Add  Delete

<input type="checkbox"/>	Filter name	№	Status	User	Application	Application protocol
<input type="checkbox"/>	User-defined filters					
<input type="checkbox"/>	 Block Facebook	300020	<input checked="" type="checkbox"/>	Any	 Facebook	Any
<input type="checkbox"/>	 Allow YouTube	300060	<input checked="" type="checkbox"/>	Any	 YouTube	Any

Как быстро и просто контролировать доступ в Интернет

The screenshot displays the ViPNet xFirewall VA interface for configuring Network Filters. The 'Forward' tab is selected. A search bar and 'Add'/'Delete' buttons are visible. The main table lists filters, with 'Apple services allow' selected. A pop-up window shows the details for this filter, including its name, ID (300072), status (enabled), user (Any), and application list (iTunes, Apple Music, iOS App Store, iCloud, iTunes Radio, Gaming, Filetransfer, Messaging, Peer to Peer, Remote Control, Any).

Filter name	№	Status	User	Application	Application protocol
<input checked="" type="checkbox"/> Apple services allow	300072	<input checked="" type="checkbox"/>	Any	iTunes Apple Music iOS App Store iCloud iTunes Radio Gaming Filetransfer Messaging Peer to Peer Remote Control Any	Any
<input type="checkbox"/> Gaming, Video Streaming, Messa...	300090	<input checked="" type="checkbox"/>	Any		Any
<input checked="" type="checkbox"/> Internet_access	300097	<input checked="" type="checkbox"/>	Any		SSL HTTP



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

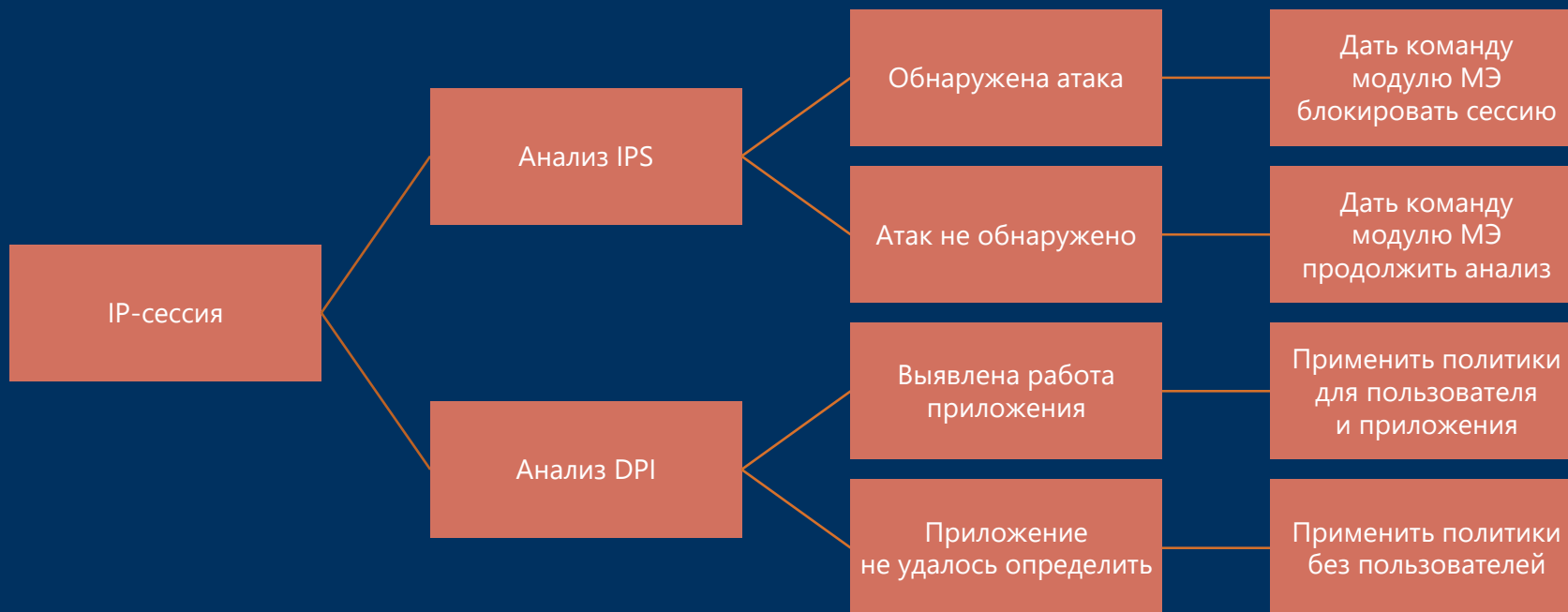
Группа правил IPS: Любая

Правило IPS: Любое

Найти

Восстановить значения по умолчанию

Порядок применения правил IPS



№5 – Защита от вирусов



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

Максимальная видимость –
фильтрация
на 7 уровне ISO OSI

Защита от сетевых атак –
блокировка аномалий,
запретных команд

Защита от вирусных атак

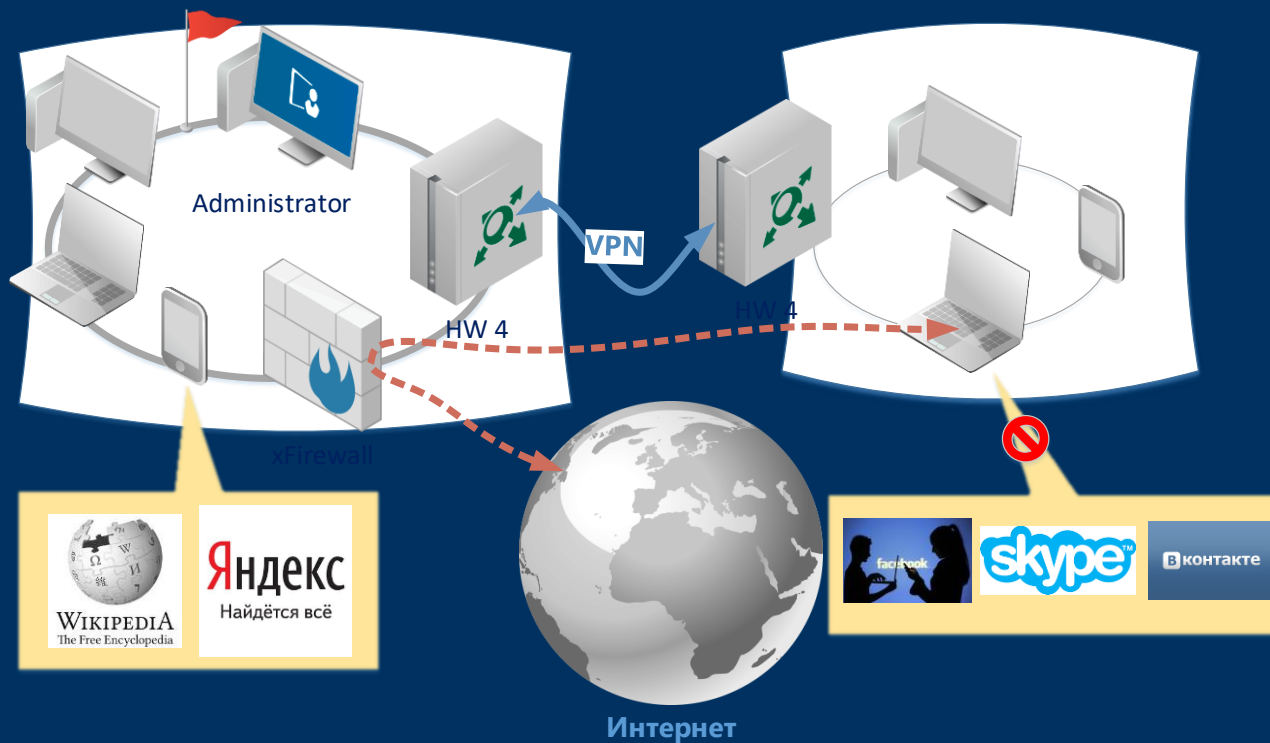
Уменьшение поверхности
атаки



Схема использования



Схема использования





ТЕХНО infotecs
2020 Фест

Спасибо
за внимание!

