



техно infotecs  
2021 Фест

ТЕХНИЧЕСКИЙ  
ФЕСТИВАЛЬ

# Практические аспекты эксплуатации NGFW

Алексей Данилов  
Руководитель направления  
Отдела развития продуктов ИнфоТеКС

Мир  
изменился



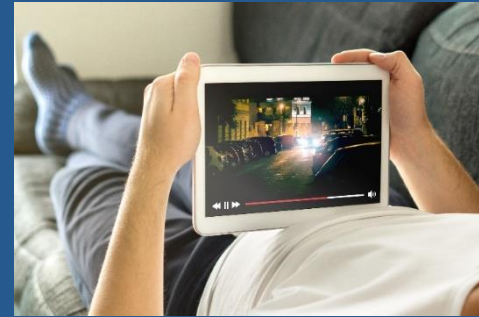
# Мир изменился



Web 2.0



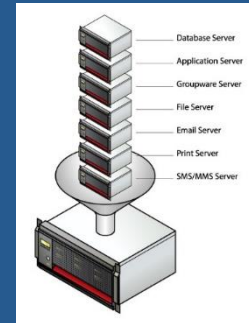
Mobile Devices



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)



# 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

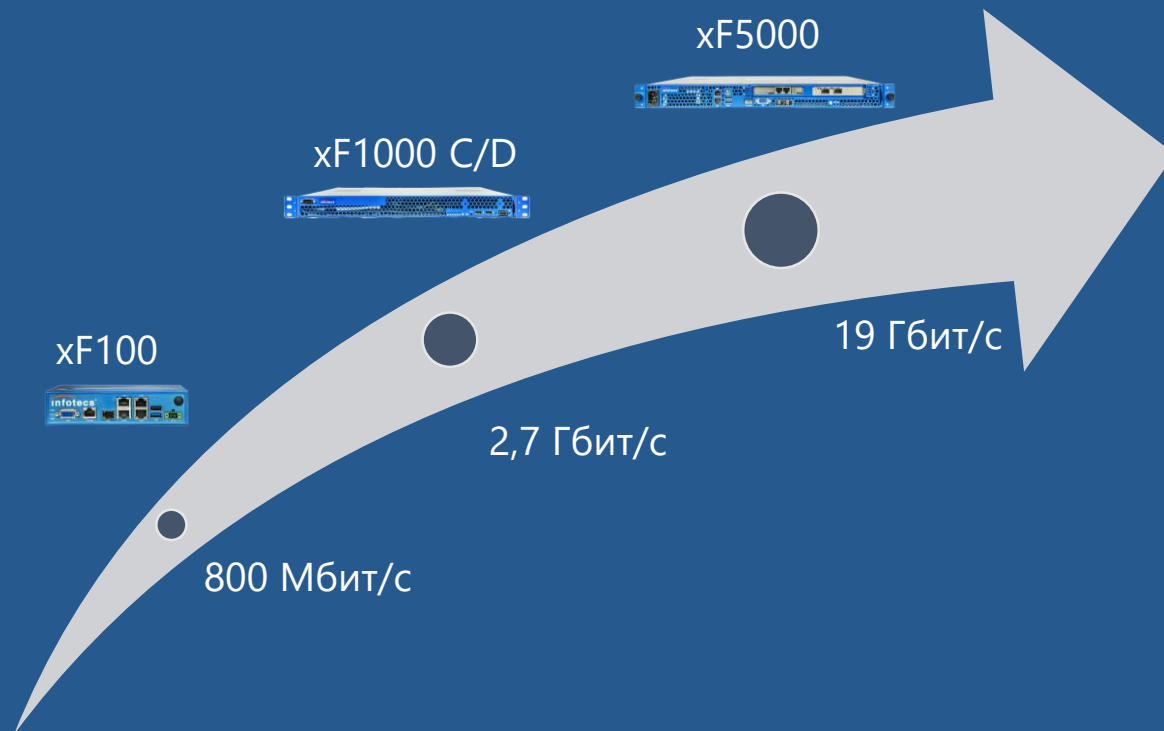
Система  
предотвращения  
вторжений

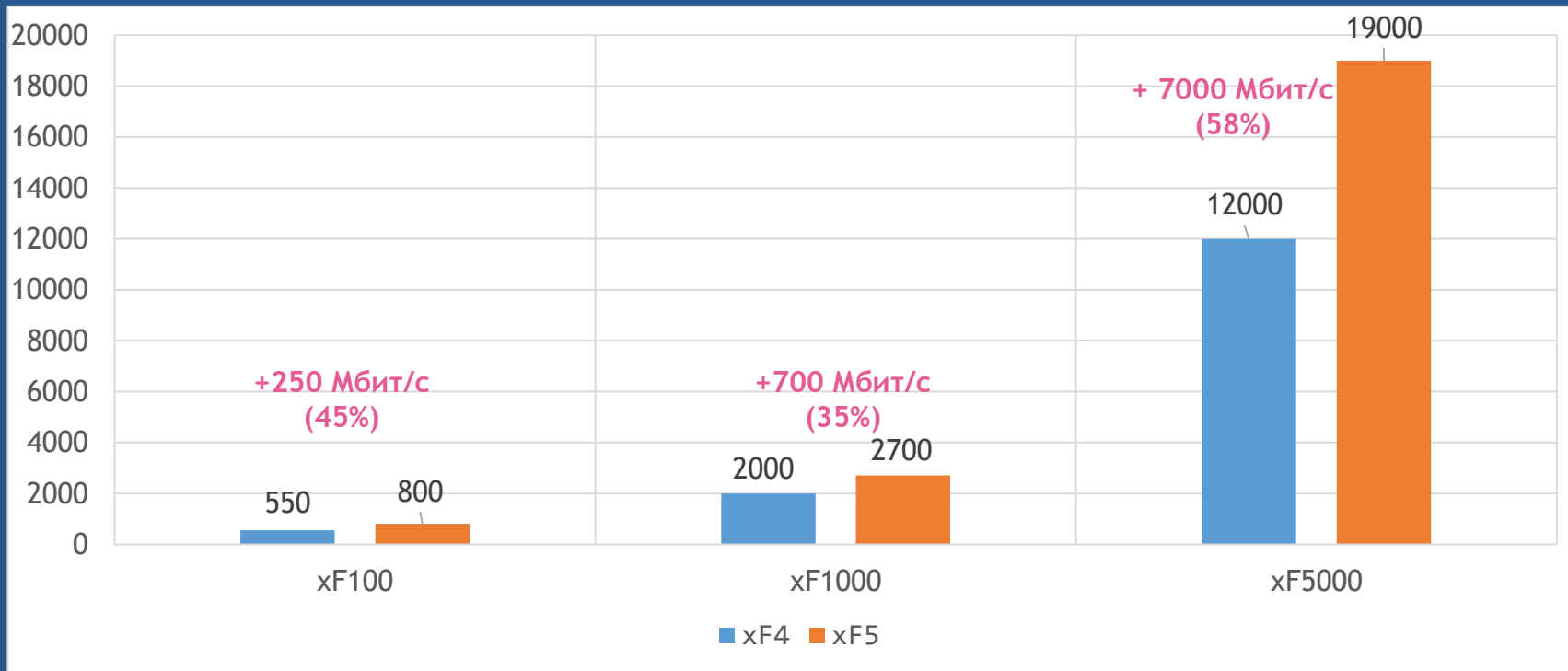
Шлюзовой  
антивирус

Интеграция с  
Active Directory

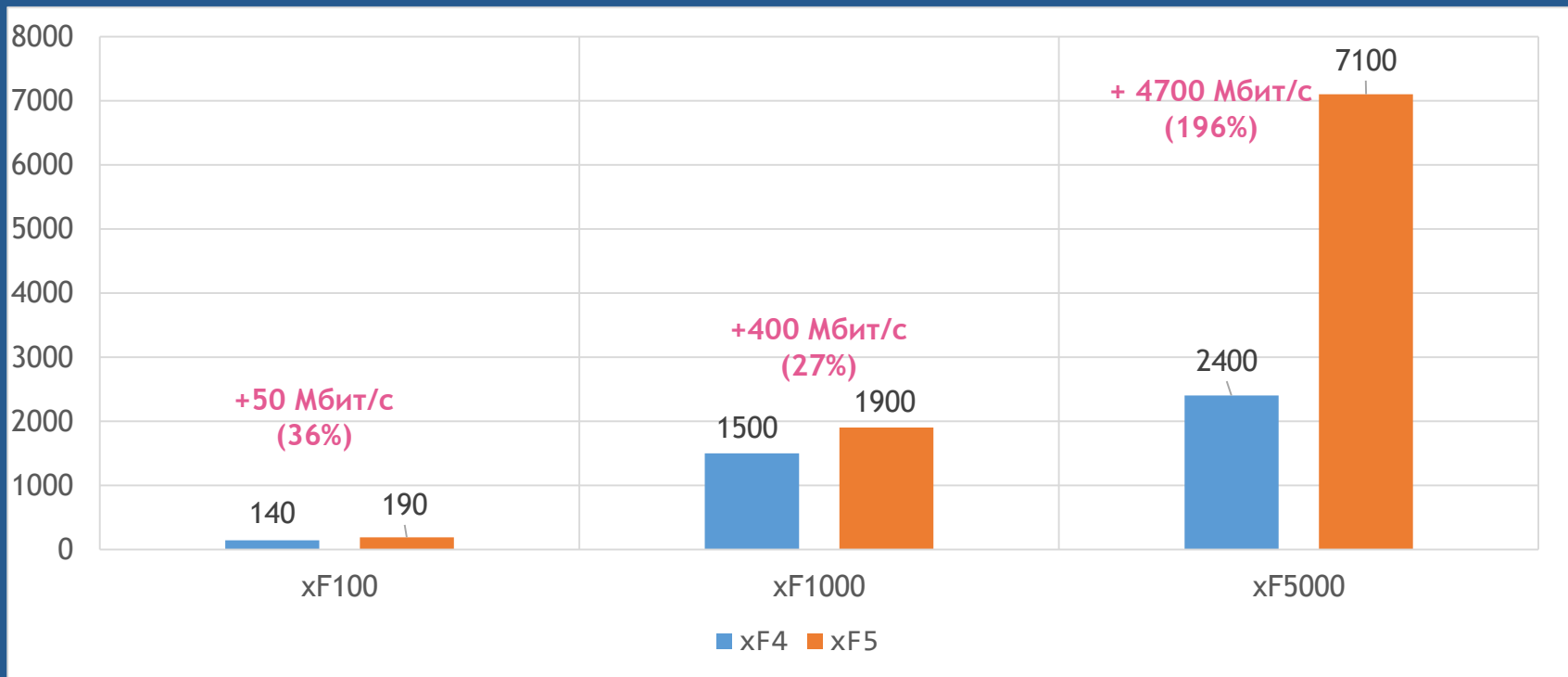


# VIPNet xFirewall. Платформы



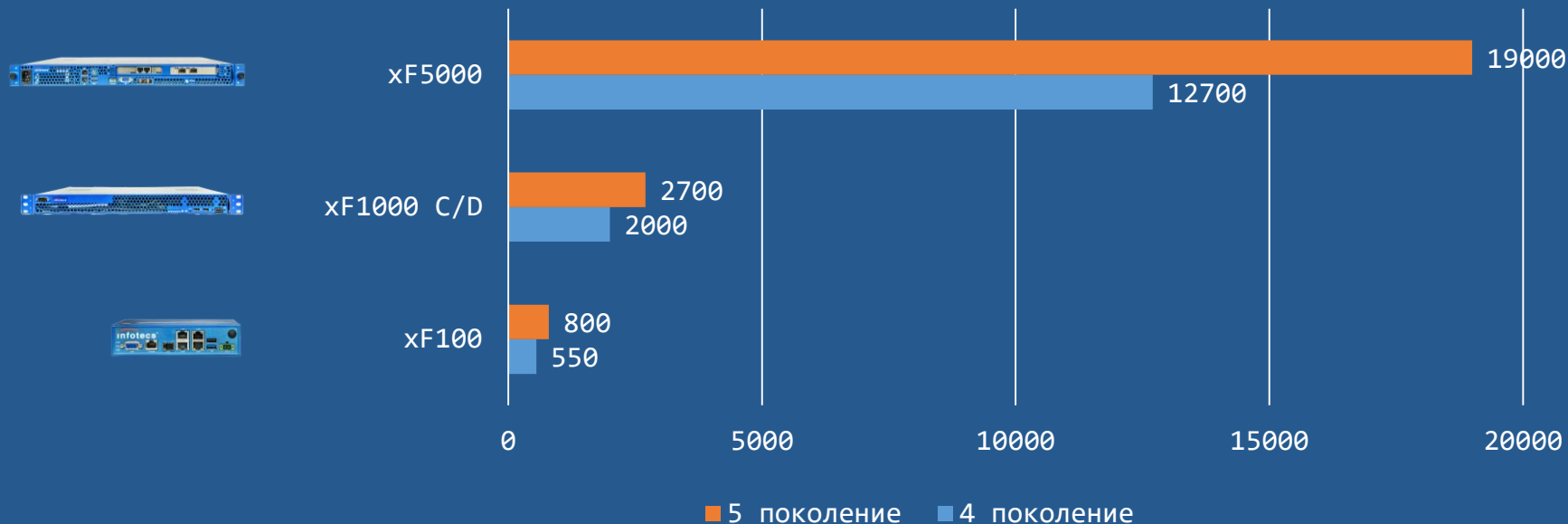


# Производительность Application Control



# 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.

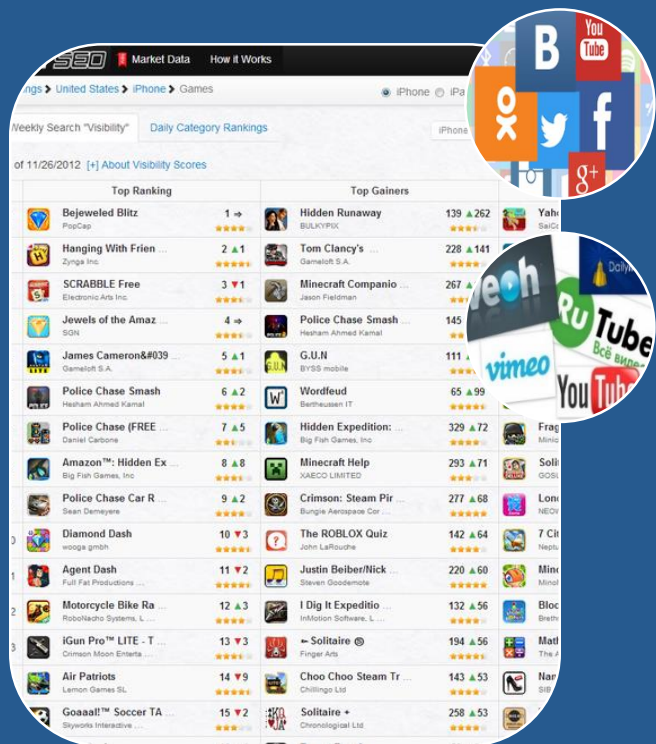
7,1 Gb/ 6000 users  
= 1,18 Mbps/user



## Знать, что охранять

Открыл порты 80/443 == Открыл

# 2065 уникальных приложений/протоколов



95 из  
категории  
«Социальные  
сети»

45 –  
поток  
видео  
тран  
мис

- Palo Alto – 2368 приложений
- Cisco – 2500 приложений

Управлять доступом

# ACCESS CONTROL





## 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

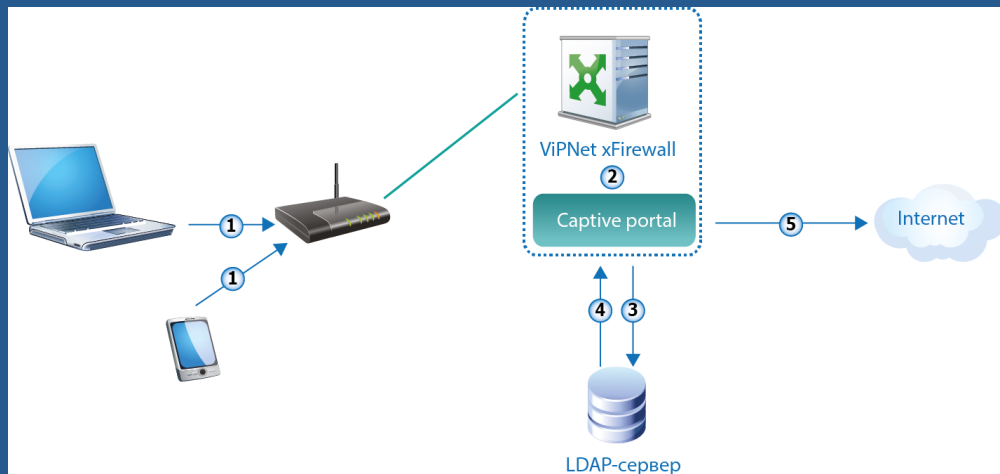


# BYOD – принеси свое устройство и работай



# 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



**Для таких пользователей можно создать политику с ограниченным доступом к ресурсам компании, потому что их устройства могут быть без средств защиты.**

Защита от сетевых атак

# INTRUSION DETECTION AND PREVENTION SYSTEM



# 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

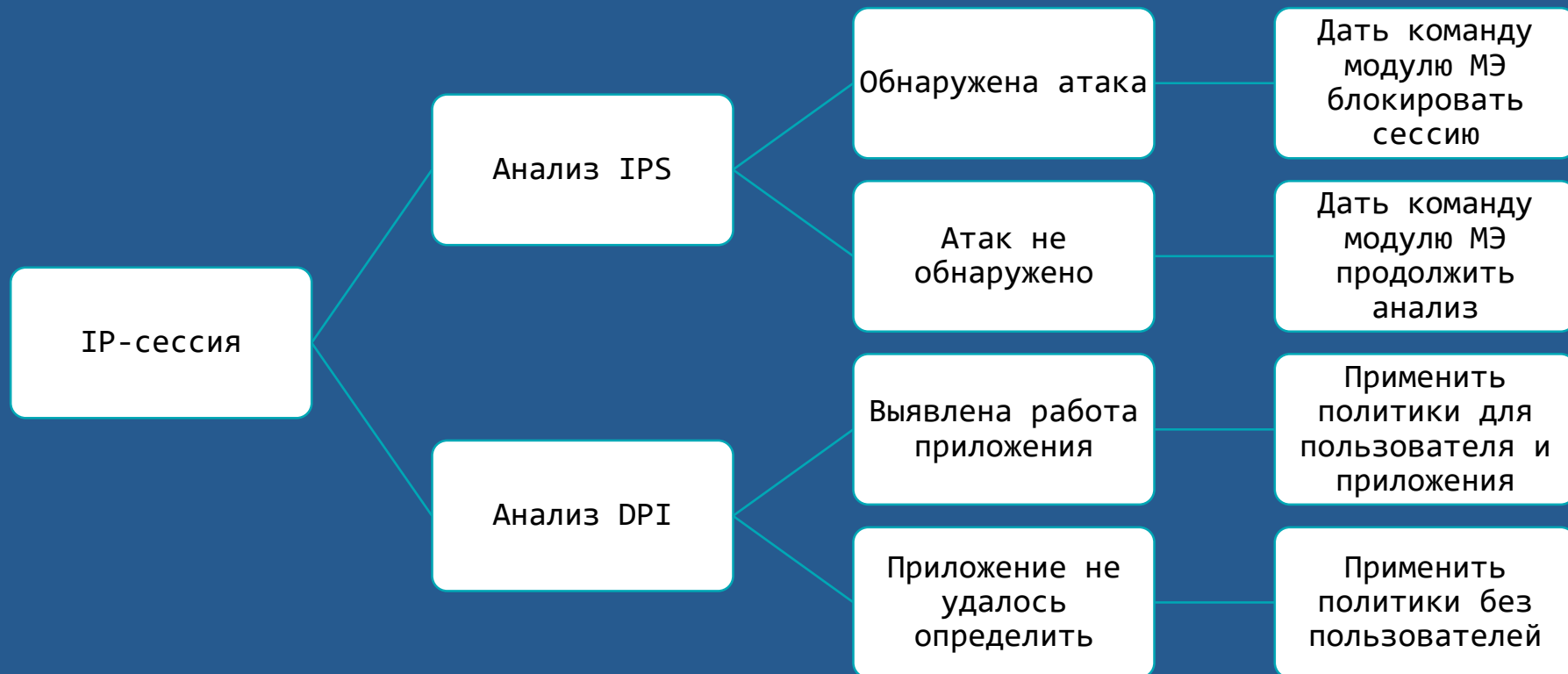
Событие: Блокированные IP-пакеты

Группа правил IPS: Любая

Правило IPS: Любое

Найти Восстановить значения по умолчанию

# Порядок применения правил IPS



# 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.





# Что делать с SSL



# Классификация SSL



- Разрешить тот SSL трафик, который известен:
  - Yandex, Google, Facebook и т.д.
- Блокировать известный SSL запрещенных политикой приложений: социальные сети, мессенджеры и т.д.
- Запретить любой неизвестный SSL трафик.

# 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

ТЕХНО infotecs  
2021 Фест

Спасибо  
за внимание!

Подписывайтесь на наши соцсети



@infotecs.ru



@vpninfotecs



@InfoTeCS\_Moscow