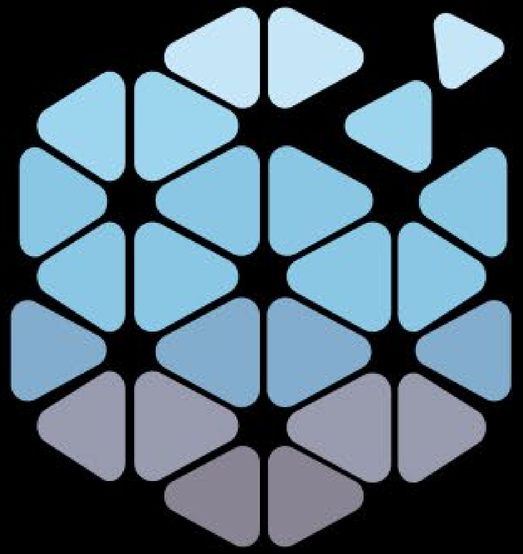


Сетевая Безопасность

[NGFW, WAF, NDR, VPN, ZTNA, Anti-DDOS, NAC, MFA]

09.12.2024

г. Москва, отель «Холидей Инн Сокольники»

Сетевая Безопасность

Архитектура защищенных сетей. NGFW в ядре, NetFlow, NAC, NSPM, PAM, NTA, Honeypot - как собрать конструктор и есть ли в этом смысл?

Ольков Евгений

TS Solution, Технический директор

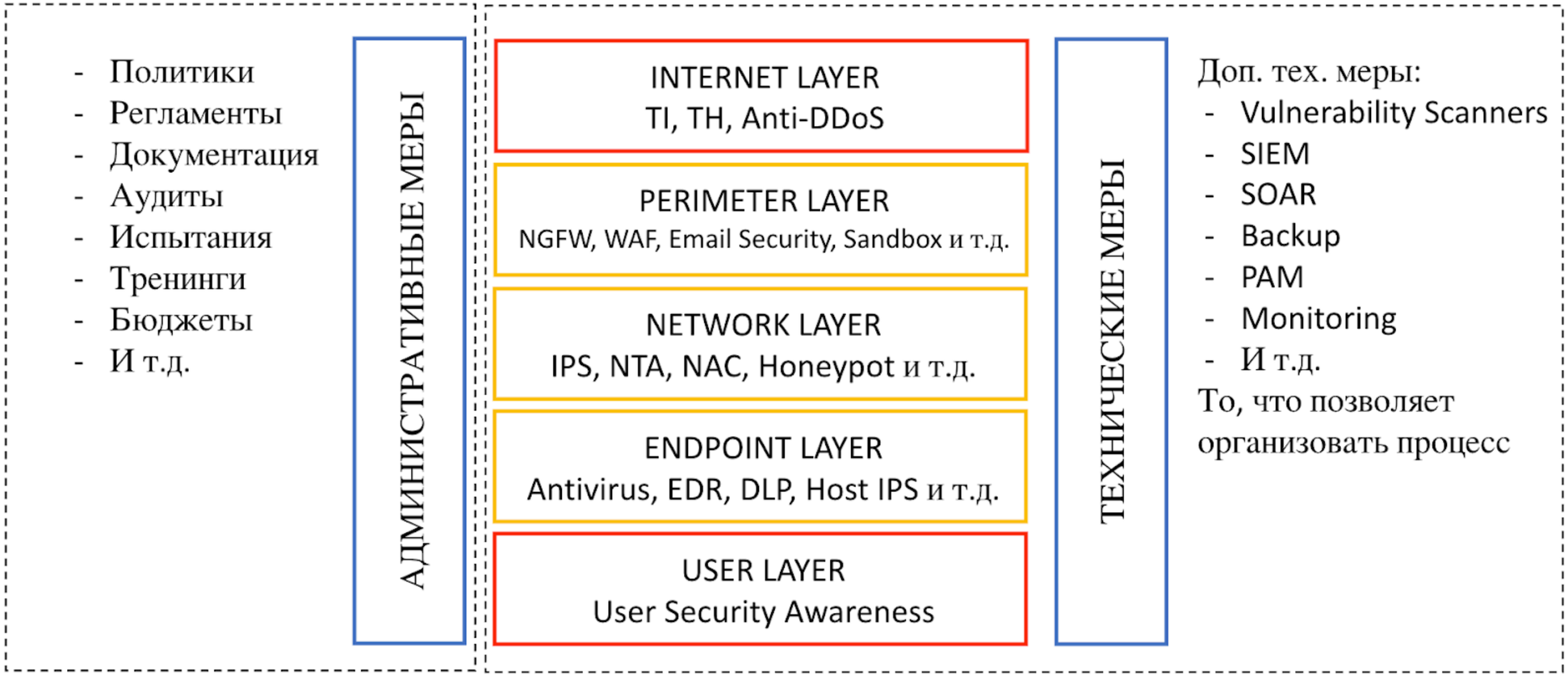
Сетевая Безопасность

Решений очень много

Их становится все больше, но защищенность повышается далеко не у всех

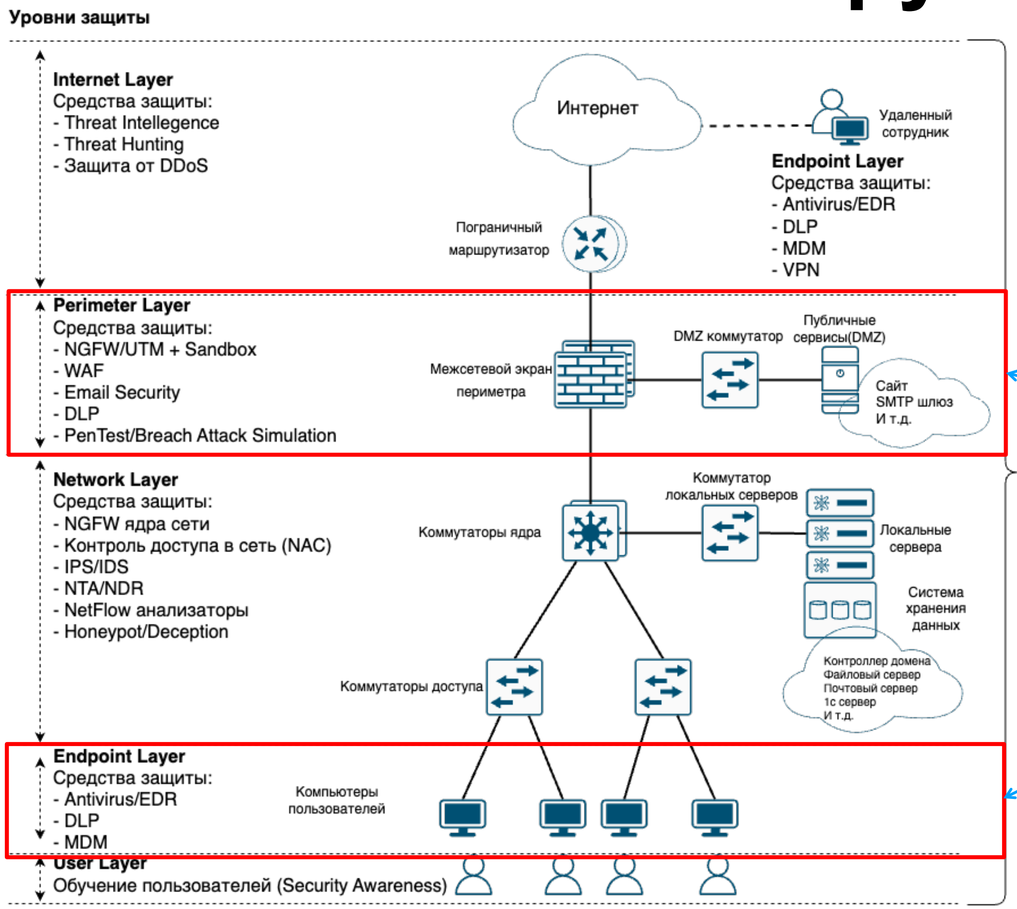
Сетевая Безопасность

Наш ИБ «фреймворк»



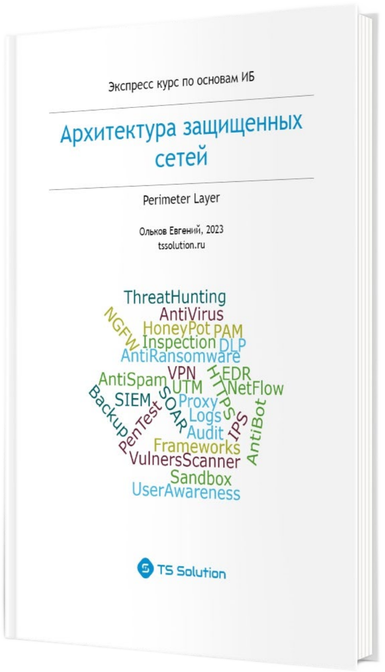
Сетевая Безопасность

Типовая «структурка» по уровням



Дополнительные технические меры:
- Сканер уязвимостей
- Система резервного копирования
- PAM
- SIEM/SOAR
- Мониторинг сети

Есть практически у всех



Сетевая Безопасность

ИБ инциденты все равно продолжаются

Основные причины:

1) Плохая настройка существующих средств защиты

По статистике, в 95% случаев можно было избежать инцидента при грамотной настройке)

2) Отсутствие сегментации

«DMZ» через проброс портов, пользователи в одном сегменте с серверами, открытый доступ к mgmt интерфейсам и т.д.

3) Несоблюдение парольной политики

Отсутствует политика на сложность и частоту смены пароля, нет двухфакторной аутентификации, доменные учетки для «админских» прав

4) Повышенные привилегии пользователей

«Админские учетки» у обычных пользователей, свободное подключение собственных устройств в корпоративную сеть

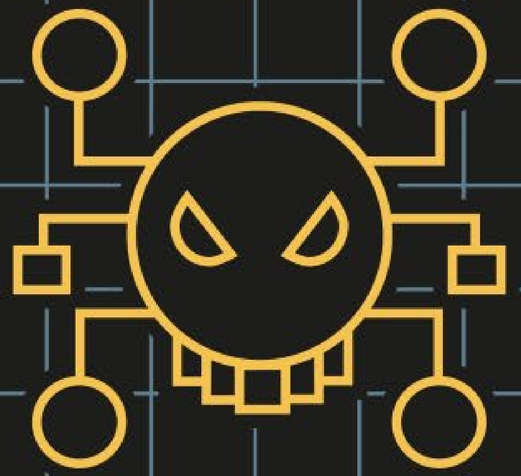
Типовой сценарий отработки инцидента

Сетевая Безопасность

«Куда бежать и что делать»?

1) Непонятно, кто инфицирован и как остановить распространение

2) Восстановление из бэкапов (если они есть) помогает ровно на 1 день



Почему так происходит и что с этим делать?

Сетевая Безопасность

Две главные идеи:

1) Без налаженного процесса закупленные ИБ средства – деньги на ветер

Банально, это всем давно понятно. Есть тех. средства, которые могут помочь с процессом

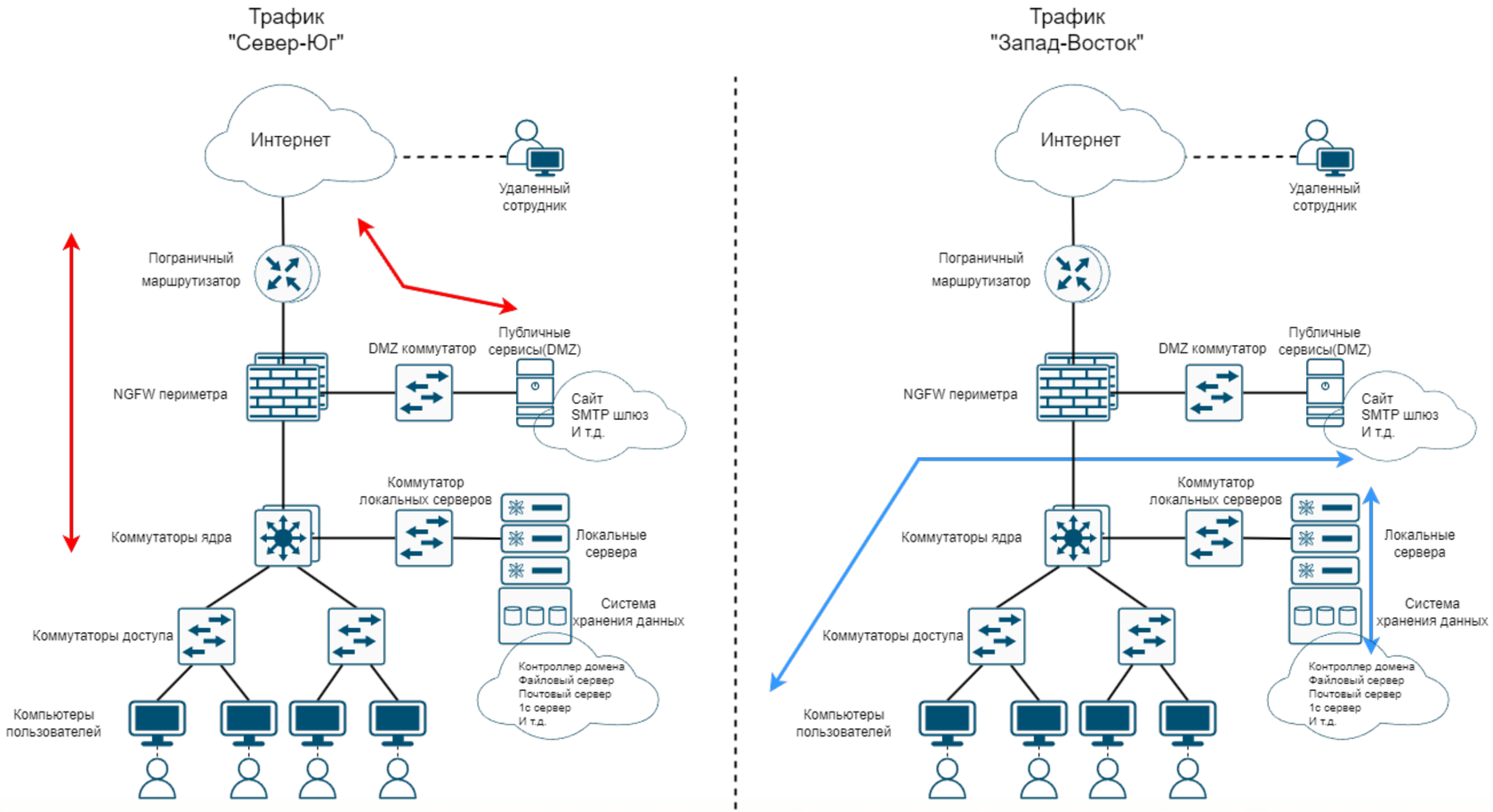
2) Вы 100% «накосячите» в настройке ИБ средств. Просто примите этот факт, что ваш периметр «пройдут»

Нужны дополнительные средства защиты, которые помогут разобраться в том, что же случилось и, самое главное, как теперь обезопасить свою сеть.

Сетевая Безопасность

Принципы защиты на уровне сети

Два типа трафика:



Принципы защиты на уровне сети

Сетевая Безопасность

Чем отличается защита «горизонтального» трафика от «вертикального»?

Да особо ничем:

1)Ограничить доступ (Access Control). Максимально уменьшить площадь возможной атаки. Главный принцип - разрешать только действительно НЕОБХОДИМЫЙ трафик. Для этого могут использоваться как встроенные средства защиты сетевого оборудования, так и специализированные решения. Это позволит нивелировать такие угрозы как сканирование портов, использование уязвимых протоколов, горизонтальное перемещение и т.д.

2)Проверять трафик внутри (Threat Detection). Согласно принципу нулевого доверия (zero trust) - разрешенный трафик не значит, что он безопасен. Мы должны непрерывно его анализировать. Здесь уже не обойтись без специализированных средств защиты. DPI, NetFlow, IDS, NTA, поведенческий анализ, статистика и прочие вещи. Все то, что позволит нам определить зловредную активность уже в разрешенном трафике внутри корпоративной сети.

Усилиние защиты через контроль доступа - главный тренд на 3-5 лет!

Сетевая Безопасность

Харденинг (hardening)

Host Based

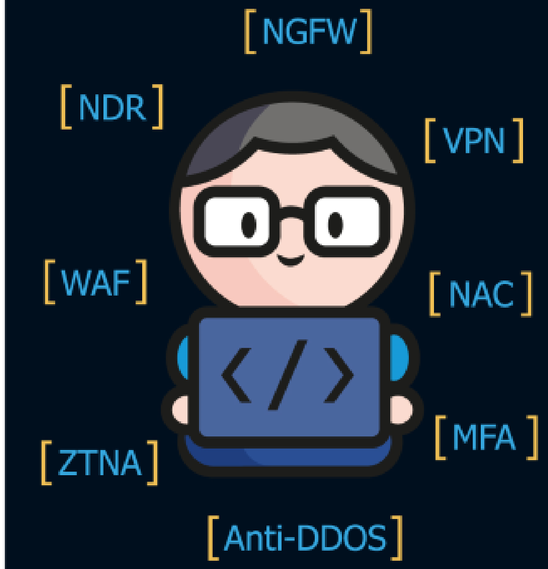
- Разные типы операционных систем: Windows, Linux, MacOS, FreeBSD. Более того, каждый вид ОС может насчитывать несколько версий (Win 7, 10, 11).
- Корпоративные приложения могут быть установлены на физический сервер (bare metal вариант). При этом серверы могут иметь разные BIOS прошивки или технологии удаленного управления (iLO, LOM, DRAC, CIMC и т.д.).
- Часть приложений может работать в виде виртуальных машин на разных гипервизорах и, опять же, разных версий (ESXi, Hyper-V, KVM, XEN и т.д.).
- Некоторые компании уже активно используют микросервисную архитектуру (docker, kubernetes).
- Набор компонентов на основе которых строятся приложения тоже может быть огромным: nginx, apache, IIS, mysql, postgres и т.д.
- Типовые коммерческие продукты: Bitrix24, 1c, ERP системы и т.д.
- Офисную технику тоже надо брать в счет: видеокамеры, принтеры, телефоны, телевизоры.

VS

Network Based

- Грамотная сегментация (DMZ, IoT, Servers, WiFi, Users).
- Грамотные правила доступа (запрещено все, что не разрешено).
- Out of band Management.
- и т.д.

Одним правилом можем закрыть сотни уязвимых устройств!



На чем сегментировать ядро?

Сетевая Безопасность

Два главных варианта:

L3 коммутатор

+ Дешевле
+ Быстрее

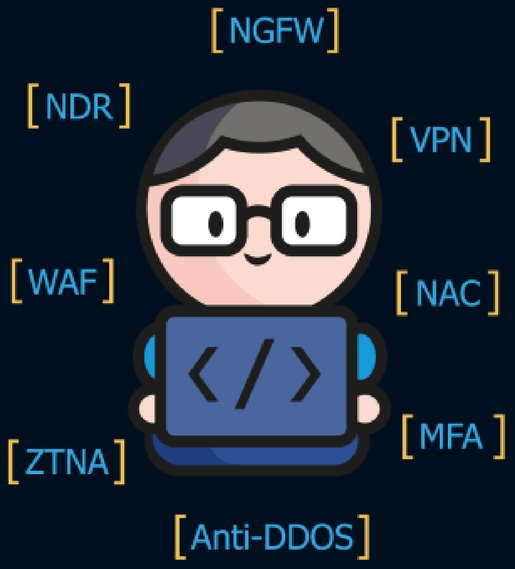
- Правила только на уровне L4
- Нет DPI

VS

NGFW

+ DPI
+ Аналитика по трафику
+ L7 контроль
+ IPS

- Дороже
- Медленнее*



Допустим сегментируем на L3 «свиче»

Сетевая Безопасность

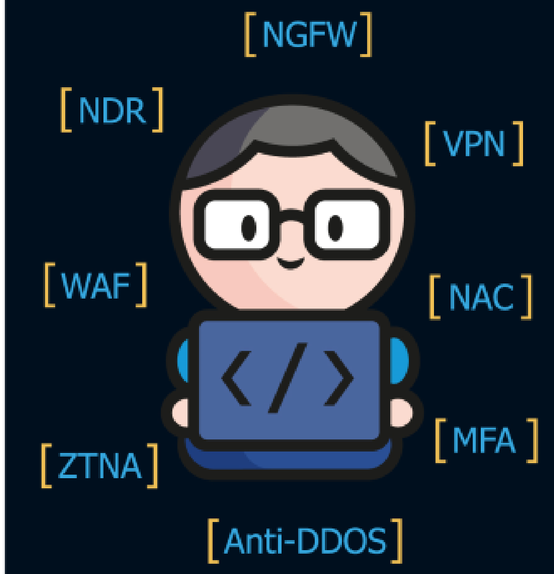
1) Грамотно организовали физическую архитектуру (выделенное ядро, DMZ/SRV коммутаторы)

2) Позаботились об отказоустойчивости (stack, mlag)

3) Грамотно сегментировали сеть (External, DMZ, Servers, Users, WiFi, IoT, и т.д.)

Сегменты без Access Lists - бесполезны!

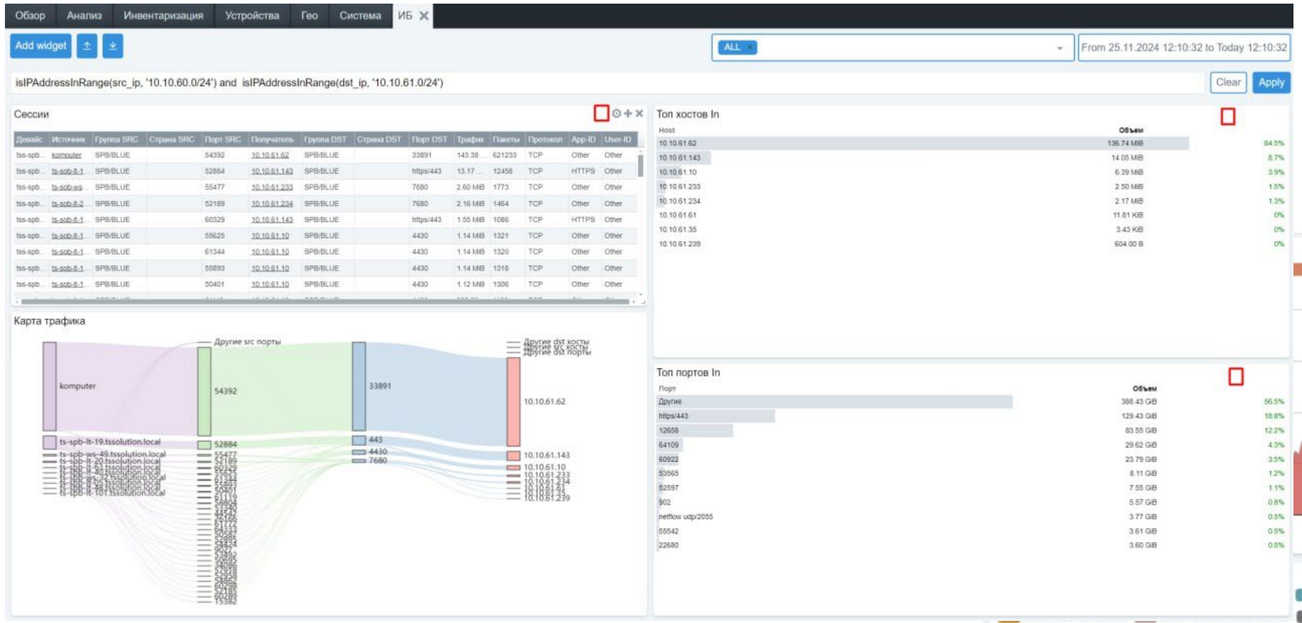
Как создать политику доступа?

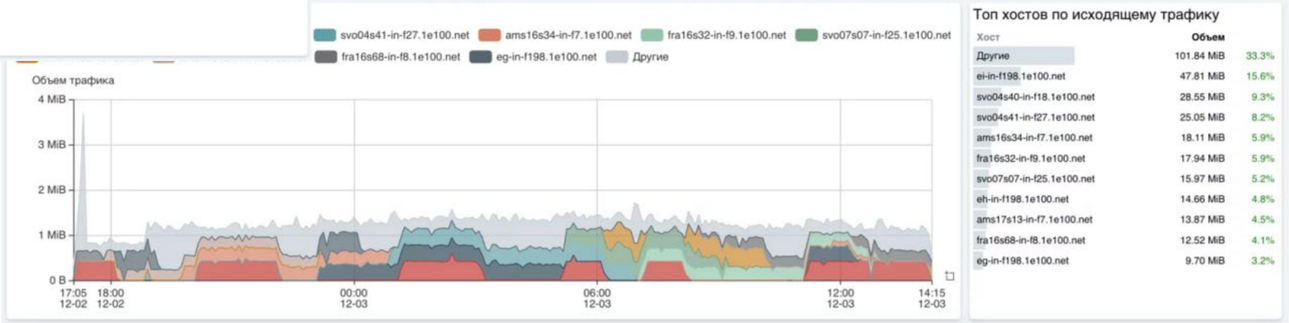


Сетевая Безопасность

Netflow анализаторы

Помогут сформировать политику доступа и выявить аномалии





Возможные продукты:
- Open Source проекты
- Neutrino Foresight, Efros DefOps*, Гарда NDR*

Как поддерживать политику когда тысячи «правил» и несколько устройств?

Сетевая Безопасность

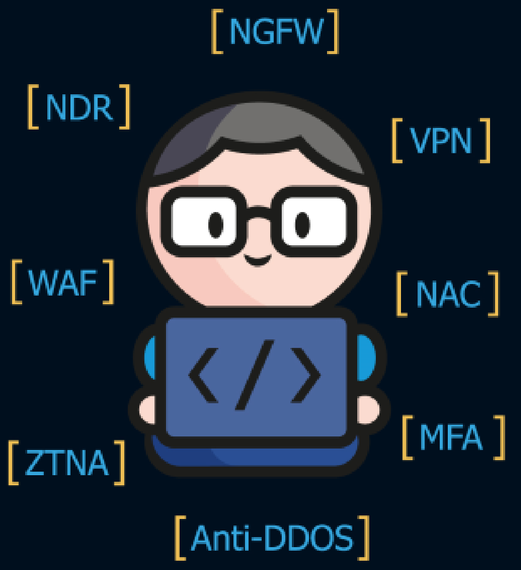
Тренд на микросегментацию...

Как:
1) Найти дубликаты
2) Найти неиспользуемые правила
3) Найте перекрывающиеся правила
4) Найти несооветствие стандартам (Compliance)
5) Найти более оптимальные правила
6) И т.д.

tufin

algosec

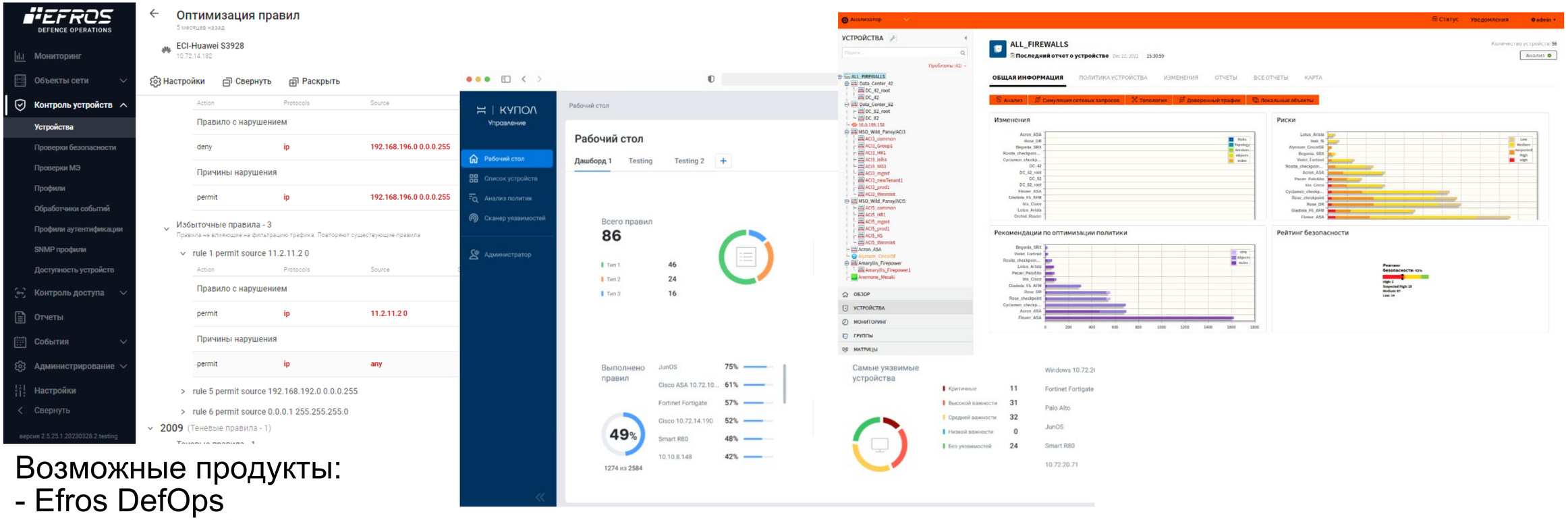
FIREMON



Сетевая Безопасность

Network Security Policy Management (NSPM)

Управление политиками NGFW, FW, L3 коммутаторов



Возможные продукты:
- Efros DefOps
- Нота Купол Управление
- Нетхаб

Access Lists на сегментах это хорошо... Но они статические!

Сетевая Безопасность

Как подстраивать политику для динамичной инфраструктуры и особенно динамичных пользователей?

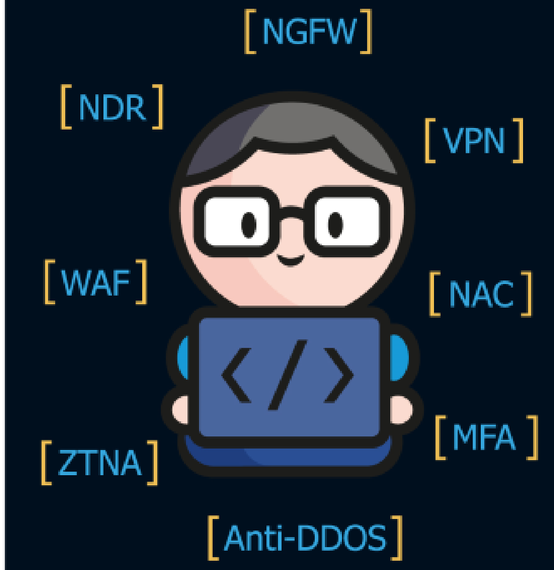
1) Пользователи могут подключаться по проводу или по wifi.

2) Пользователи могут подключаться со своих устройств (BYOD).

3) Есть удаленные пользователи.

4) Удаленные пользователи могут использовать разные устройства.

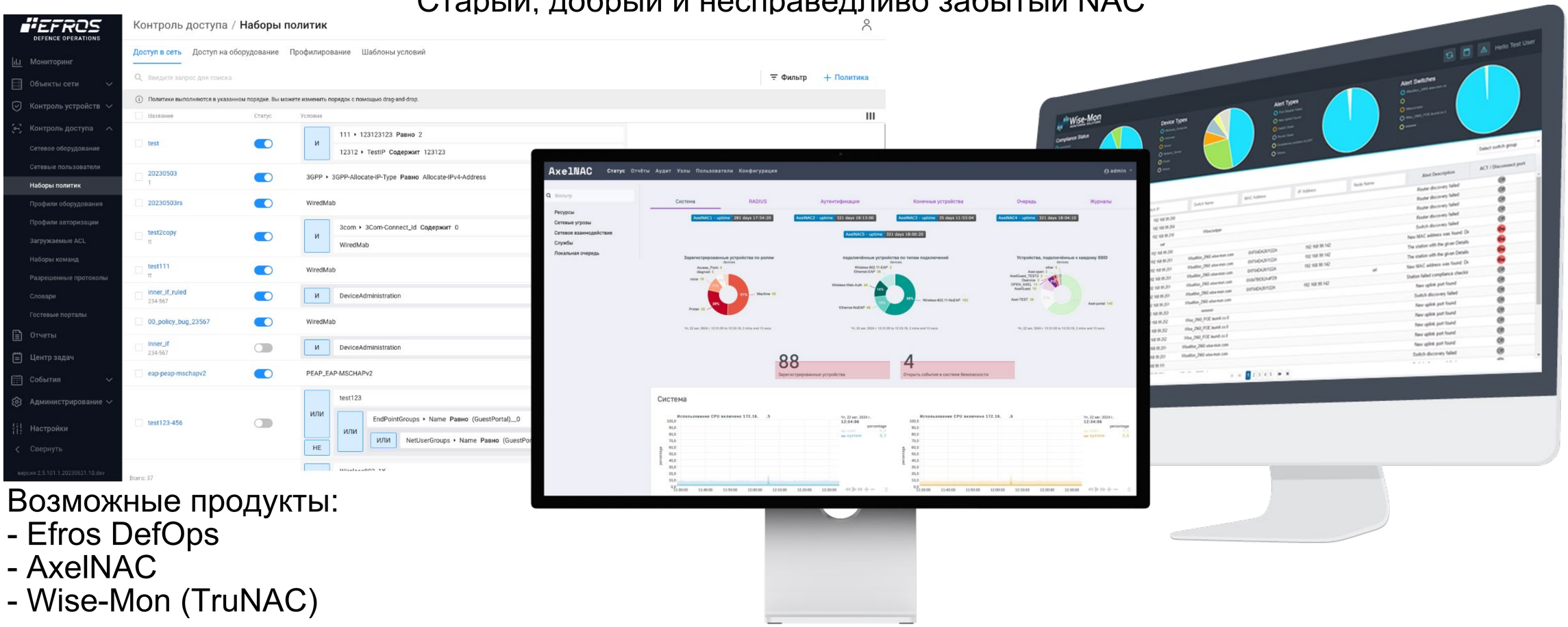
Динамический ZTNA?



Сетевая Безопасность

Network Access Control (NAC)

Старый, добрый и несправедливо забытый NAC



Возможные продукты:
- Efros DefOps
- AxelNAC
- Wise-Mon (TruNAC)

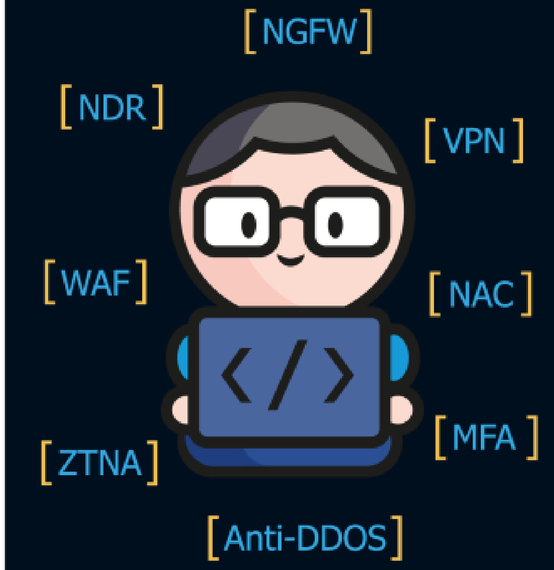
Самый критичный трафик сети - Management трафик

Сетевая Безопасность

Out of band Management это хорошо, но не всегда достаточно!

Как контролировать подключения по:
1) SSH
2) RDP/VNC
3) HTTP/HTTPS
4) MySQL/Postgres
5) API (Kubernetes)
6) И т.д.

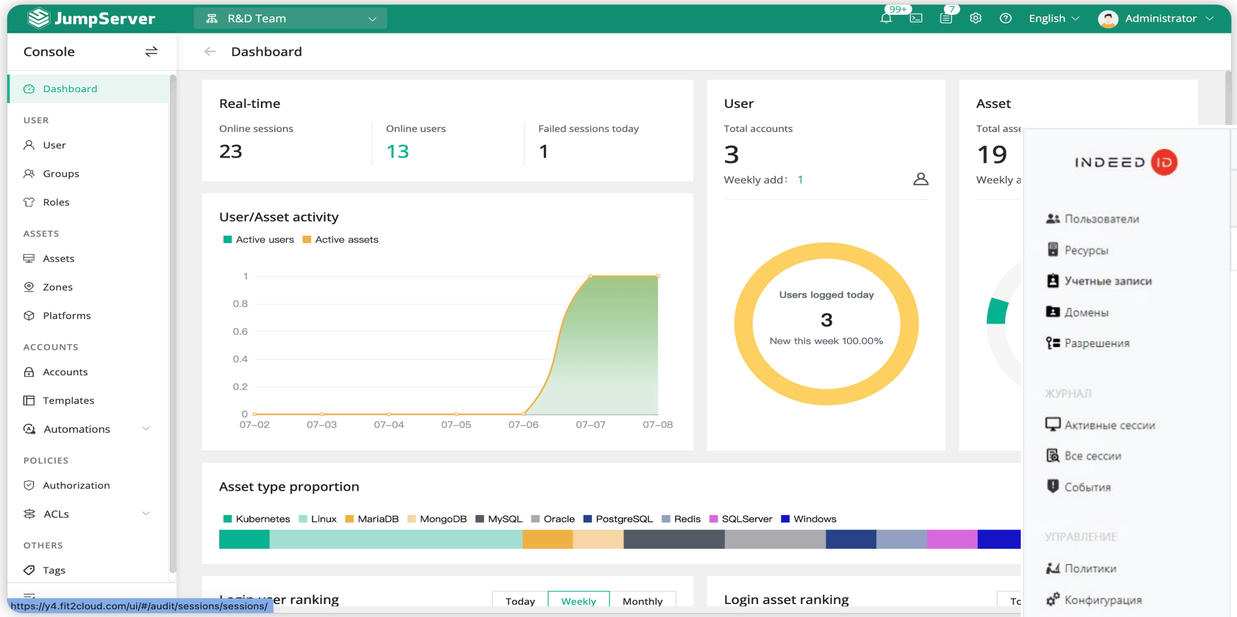
Что значит контроль?
1) Контроль учетных записей
2) Логирование/запись всех действий
3) Запрещение команд
4) Сброс/заморозка сессий
5) Двухфакторная аутентификация
6) Доступ к управлению без доступа ко всей сети (Jump Host)
7) И т.д.

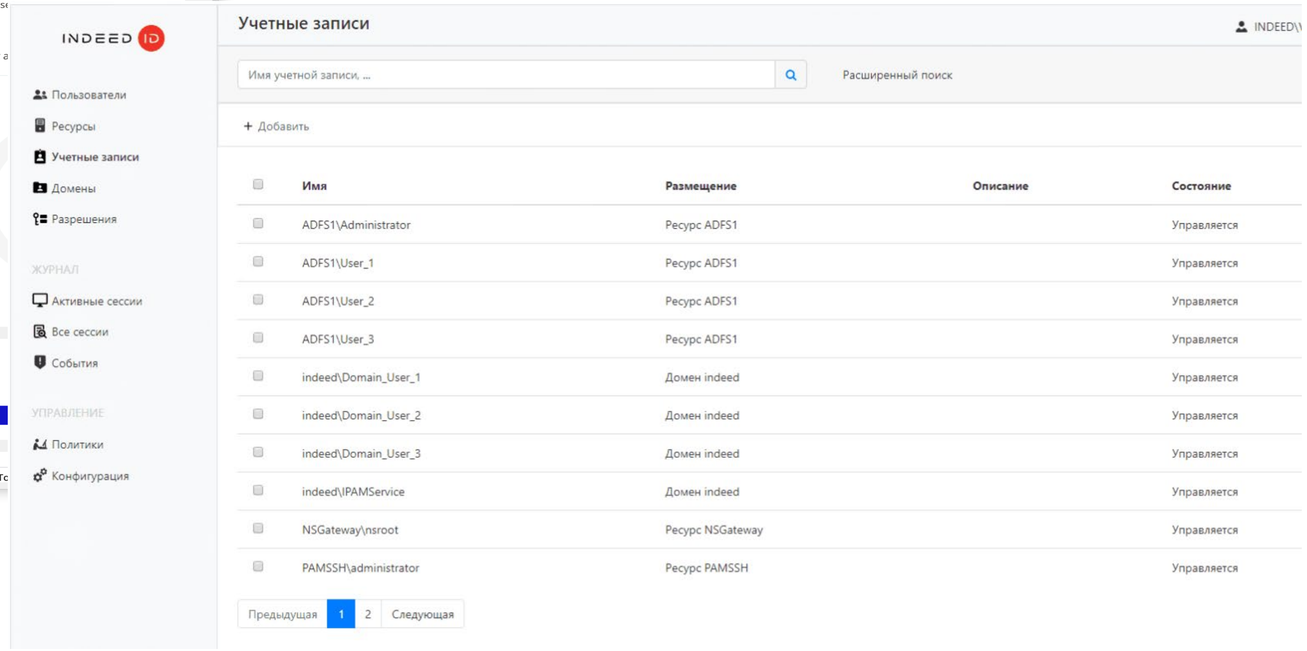


Сетевая Безопасность

Privileged Access Management (PAM)

Максимальный контроль привилегированного доступа к наиболее критичным система





Возможные продукты:
Indeed, АйТи Бастион, Infrascope, Solar SafeInspect,
Контур PAM, Bi.Zone PAM, Zecurion PAM,
JumpServer и многие другие...

Сетевая Безопасность

Резюме по Access Control (Харденинг)

Доверяй, но проверяй - Threat Detection

Сетевая Безопасность

Возможные варианты:

1) NGFW как ядро сети

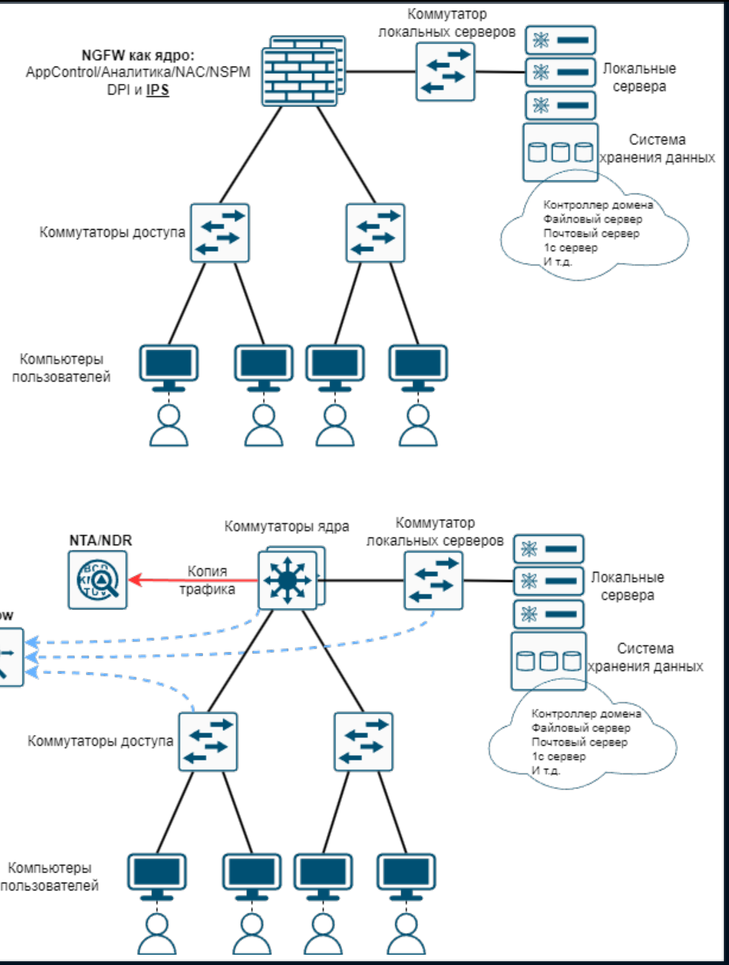
2) IPS/IDS

3) NTA/NDR

4) NetFlow?

5) HoneyPot/Deception

6) И т.д.



NGFW в ядре - закрываем сразу несколько задач

Сетевая Безопасность

Access Control:

1) Улучшаем видимость и контроль трафика на уровне приложений (L7)
2) Уже есть модуль аналитики или лайтовая замена NetFlow (не у всех!)
3) Уже есть базовый функционал NAC (не у всех!)
4) Уже есть NSPM и Compliance (не у всех!)

Threat PREVENTION:

1) DPI
2) IDS/IPS

*Важно!
По внутренним тестам, “хороший” NGFW детектит (а может и «превентить»!) известные сетевые угрозы НЕ хуже отчественных NTA решений!

NGFW в ядре - проблемы производительности как-будто больше нет?

Сетевая Безопасность

Учитывая предыдущий слайд - может быть дешевле, чем комплекс дополнительных средств (NetFlow, NAC, NSPM)

Большой выбор на рынке:

- IPS везде разный...
- Может не хватить сетевого функционала...

Если мы боимся False Positive...

Сетевая Безопасность

Когда выясняется, что IPS надо тоже «администрить»:

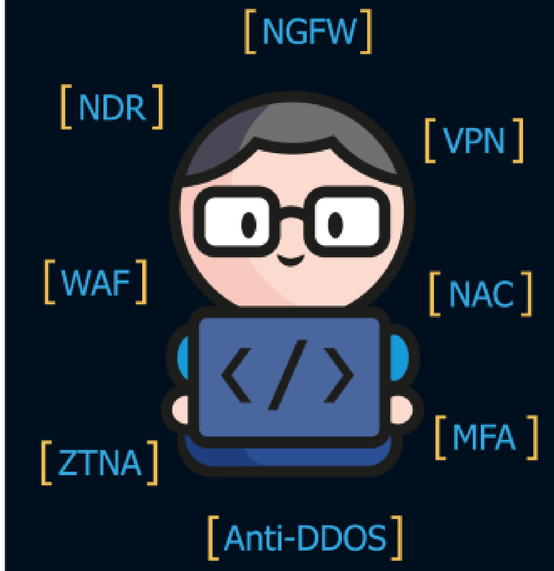
IPS -> IDS ... Тогда может сразу NTA?

1) Хранит «историю» трафика (не путать с сырым дампом!), что позволяет делать ретроспективный анализ
2) Позволяет «расследовать»
3) В теории позволяет выявлять злоумышленников на уровне аномалий (в принципе можно обойтись NetFlow)
4) Можно использовать как альтернативу NetFlow (безумно дорого)

positive technologies

ГАРДА

kaspersky



HoneyPot или когда «постучали снизу»

Сетевая Безопасность

Как «подстраховать» ваши ИБ бюджеты?

Помните нашу вторую идею в самом начале? - «вас все равно взломают»

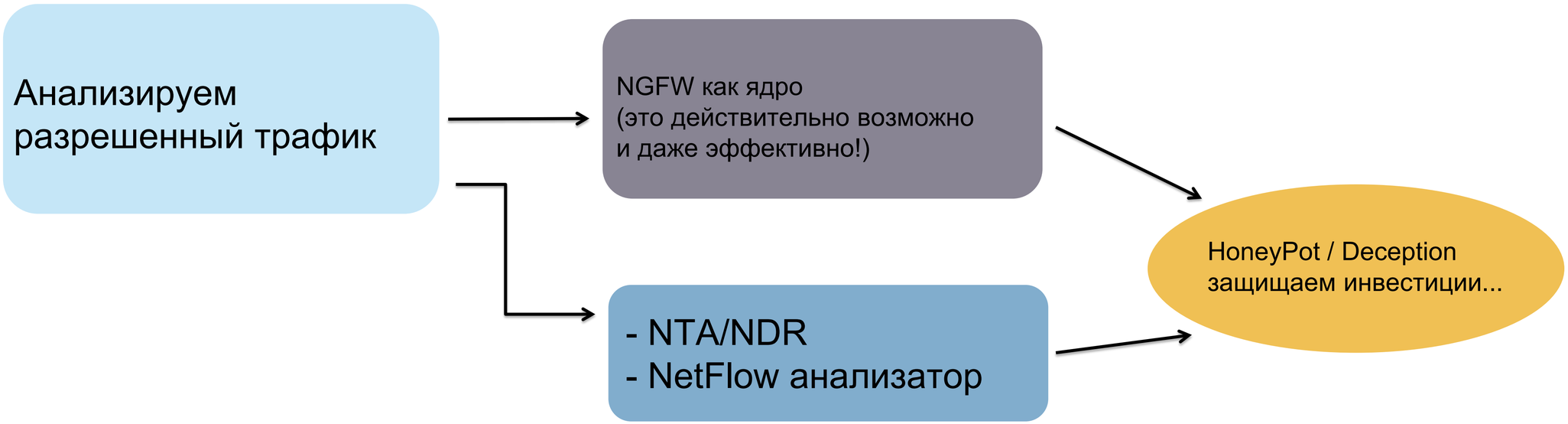
Мера последней надежды - HoneyPot или Deception

xello R-Vision ГАРДА

Часто в логи NTA идут после инцидента от Deception...

Сетевая Безопасность

Резюме по Threat Detection (проверяем разрешенный трафик)



Сетевая
Безопасность

Благодарю за внимание!