

NGFW

УНИВЕРСАЛЬНОСТЬ ИЛИ РЕАЛЬНОСТЬ?

Алексей Петухов

Руководитель отдела развития InfoWatch ARMA

Лидер центра компетенций

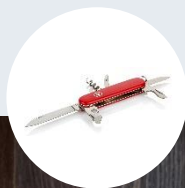
«Кибербезопасность» НТИ Энерджинет

А у вас есть швейцарский нож?

INFOWATCH®



Он хорош, если под рукой
нет ничего другого



Какие задачи решает NGFW и почему так получилось?



Межсетевое экранирование

Сегментирование сетей с возможностью фильтрации и ограничения доступа на основе списков доступа и политик обмена данными

DPI пром. протоколов

Обнаруживает вторжения по специализированным промышленным протоколам благодаря глубокому разбору трафика до уровня команд

Потоковый антивирус

Сканирует и анализирует трафик промышленной сети в реальном времени. При обнаружении вредоносных объектов блокирует их на сетевом уровне

СОВ

Обнаруживает и блокирует вредоносное ПО, компьютерные атаки и попытки эксплуатации уязвимостей ПЛК на сетевом и прикладном уровнях. Сигнатурные базы обновляются регулярно

QoS

Позволяет настроить приоритизацию трафика, тем самым управлять нагрузкой и обеспечить стабильную работу сети

Контроль приложений

Позволяет создавать правила для разрешения, ограничения или блокировки использования приложений разными группами пользователей

NAT / PAT

Позволяет обеспечить сокрытие инфраструктуры в защищённом от злоумышленника периметре. Обеспечивает доступ за счёт преобразования частных и публичных адресов

Контроль удалённого подключения

Обнаруживает любую попытку подключения по протоколам удалённого доступа Telnet и RDP, позволяет фильтровать возможность доступа пользователя

Веб-фильтрация

Позволяет создавать правила для разрешения, ограничения или блокировки веб-ресурсов разными группами пользователей

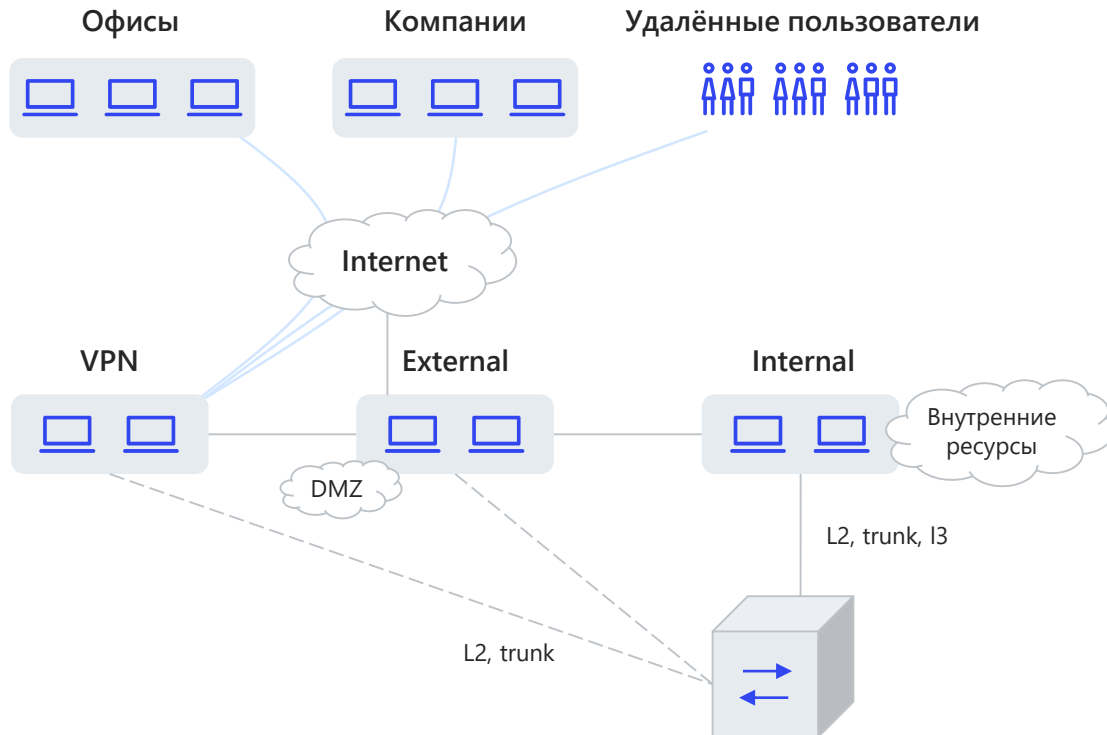
VPN-ГОСТ

Построение безопасного, зашифрованного туннеля связи между объектами при удалённом подключении, объединении филиалов или подключении технической поддержки

Proxu

Анализ проходящего через межсетевой экран веб-трафика и интеграция со смежными системами защиты информации (DLP, Sandbox, Antivirus и т. д.)

Какие задачи бывают?



- ✓ Пограничная защита и создание безопасных удалённых подключений
- ✓ Выявление и противодействие атакам внутри сети
- ✓ Глубокое сегментирование внутри сети
- ✓ Защита внутри промышленного сегмента
- ✓ Защита пользователей телеком оператором
- ✓ и другие

Какие ещё есть факторы?



Технические

- Размер пакетов в трафике
- Количество пакетов
- Прикладной смысл этих пакетов
- Многообразие приложений
- Наличие шифрования
- Поведение устройств и пользователей в сети
- Реакция NGFW на «перегруз»
- Взаимодействие с другими средствами защиты



Организационные

- Кто будет администрировать их
- Кто будет настраивать политики ИБ
- Кто будет выявлять атаки и реагировать

Что ещё влияет на принятие решения?



Стандартизация

- Государственное регулирование
- Отраслевая сертификация



Сервисы

- Стоимость покупки и владения
- Скорость приобретения
- Техподдержка



Корпоративные особенности

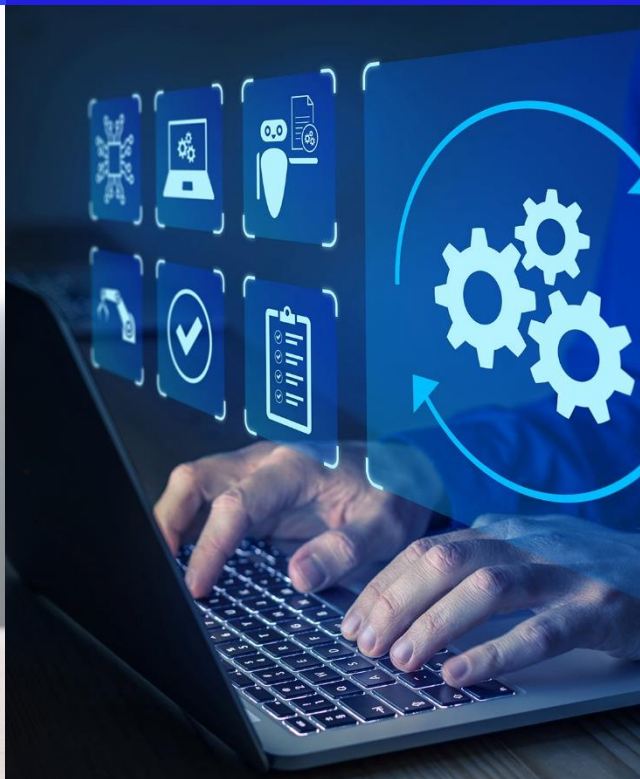
- Особенности созданных ключевых систем
- Существующие ИБ- и ИТ-процессы

Что мешает сделать один уже сейчас?

ВРЕМЯ



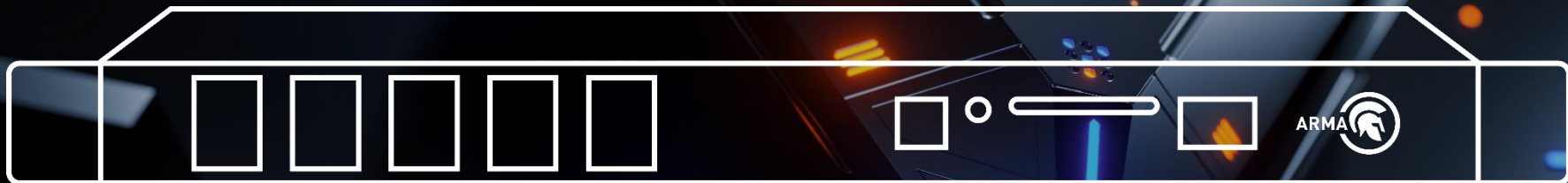
ТЕХНОЛОГИИ



СПРОС



Так каким должен быть идеальный NGFW?



Какие могут быть типы NGFW?

- 1** Для пограничной защиты малого бизнеса (до 1 Гб/с без требований к ФСТЭК)
Основные угрозы: UserGate, Ideco, Smartsoft
- 2** Для пограничной защиты среднего и крупного бизнеса (до 10 Гб/с + требования ФСТЭК)
Основные угрозы: UserGate, Ideco, InfoWatch ARMA
- 3** Для защиты промышленного сегмента (до 1 Гб/с + требования ФСТЭК)
Основные угрозы: InfoWatch ARMA, Инфотекс
- 4** Для безопасного удалённого доступа особых систем (до 10 Гб/с + требования ФСТЭК + ФСБ)
Основные угрозы: Инфотекс, Код безопасности
- 5** Для защиты телеком-операторов (100 Гб/с + требования ФСТЭК)

NGFW может быть универсален,
но для каждого по-своему



Может быть, стоит вообще посмотреть заново?



Датацентричный подход

Обновлённый взгляд на классы решений

Безопасные разработка и модернизация ключевых систем



NGFW уже есть
на российском рынке
и их всегда будет
несколько



Развитие каждого
из существующих
NGFW — долгосрочный
процесс (в сторону
своей универсальности)



Решение задач
сетевой безопасности
в кооперации

ОБСУДИМ?



Алексей Петухов


Руководитель отдела развития InfoWatch ARMA

Лидер ЦК «Кибербезопасность» НТИ Энерджинет

 @PA_my_mind

arma.infowatch.ru

 /InfoWatchOut

 /InfoWatch