Построение защищенных технологических сетей в энергетических компаниях

ООО «АЛЬФА МЕТРОНИК»

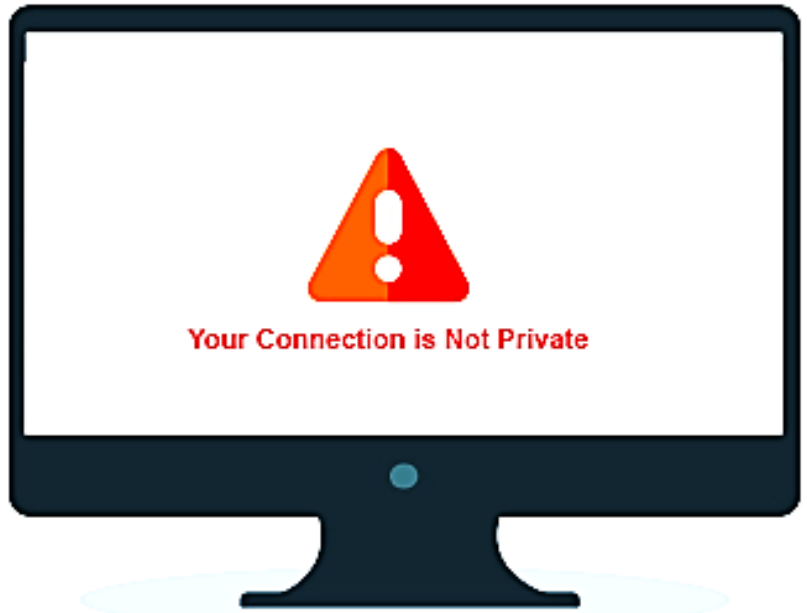
тел. +380 (44) 501-96-01
e-mail: info@alfa-metronik.ua
web: www.alfa-metronik.ua

Входные данные - с чем мы сталкиваемся

- Ситуативное построение технологической сети передачи данных
- Большое разнообразие каналов и технологий передачи данных
- Территориально распределенная структура предприятия с большим количеством удаленных подстанций без обеспечения климатических условий
- Промышленные протоколы передачи данных

Ситуативное построение технологической сети приводит

- Отсутствие контролируемого стыка сети между технологической сетью передачи данных и корпоративной
- Недостаточный контроль периметра в следствии отсутствия сетевых экранов периметра
- Недостаточный уровень аутентификации пользователей
- Отсутствие шифрования трафика
- Отсутствие систем выявления и предотвращения вторжений



Особенности технологической сети

- сеть используется для управления технологическим процессом
- кроме распространенных, используются специализированные операционные системы
- сложности обновлений ПО
- высокие требования к готовности
- критичность к задержкам и потере данных
- требования к резервированию и отказоустойчивости

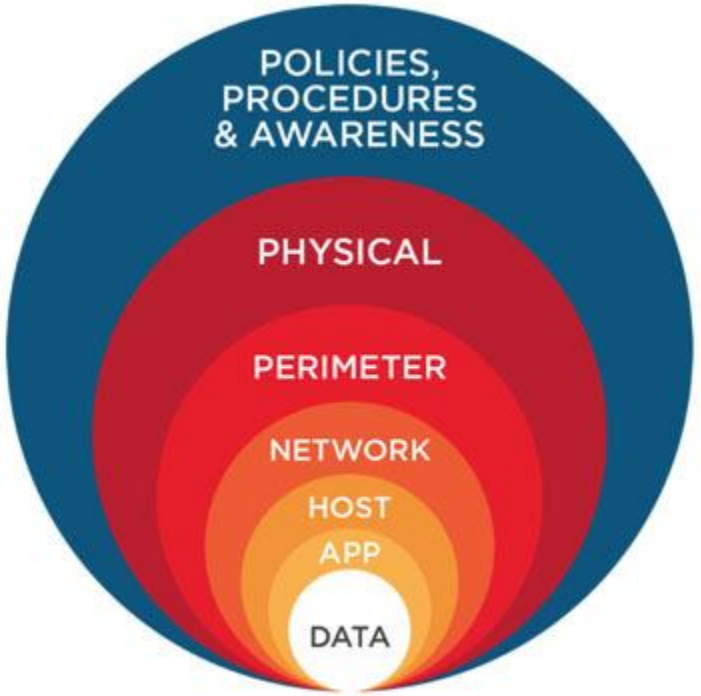
Подходы при построении защищенной технологической сети

Защита не сети, а активов и технологических процессов от несанкционированных действий третьих лиц

Для этого применяется подход в безопасной сетевой изоляции активов предприятия, сохраняя контроль технологического процесса

Теорию «defense in depth» внедряем на практике

1. План обеспечения защиты (аудит, активы, риски)
2. Отделение технологической сети (создание DMZ)
3. Защита периметра (использование Firewall и VPN)
4. Сегментация сети (отдельные зоны, сегменты)
5. Повышение защиты на устройствах
6. Мониторинг, аудит и обновление

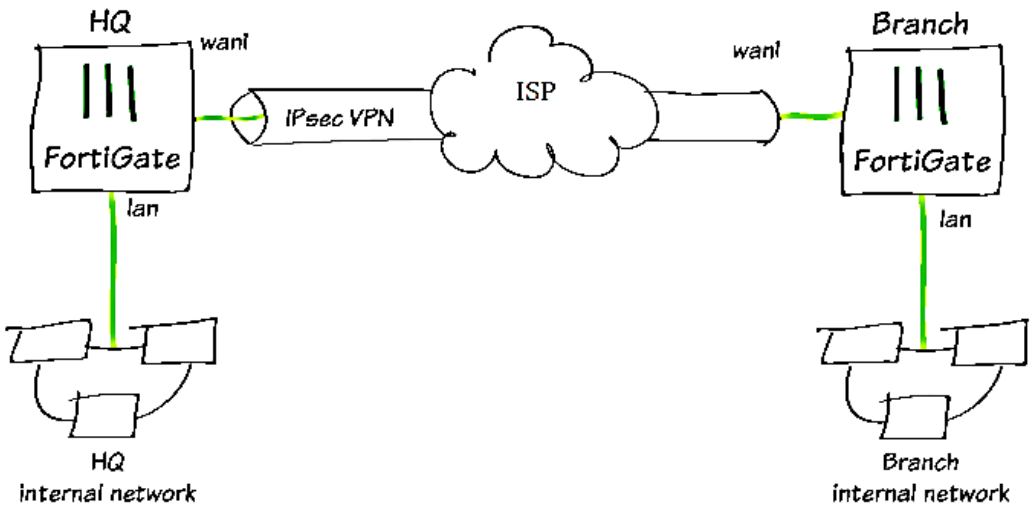


Основные процессы которые нужно выстроить

- нормативно правовое обеспечение
- административное обеспечение
- техническое обеспечение

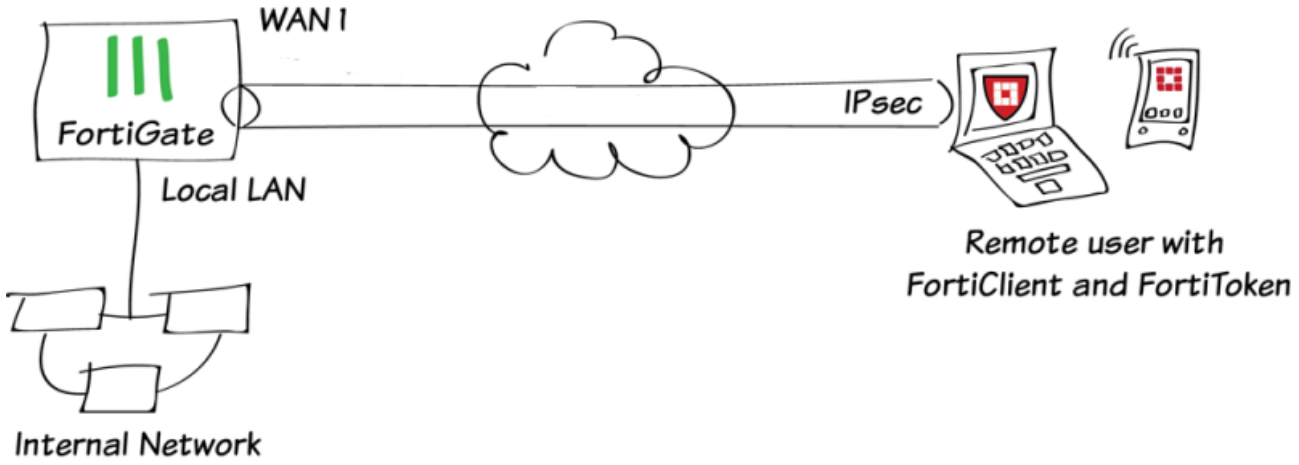
С помощью чего обеспечить защиту

- изоляция активов предприятия и разграничение сетей – сетевой экран нового поколения **FortiGate** от **Fortinet**
- безопасное использование сетей провайдеров для расширения сети **– Ipsec VPN** туннели



С помощью чего обеспечить защиту

- организация безопасного доступа для пользователей с двухфакторной аутентификацией - **IPsec VPN** туннель + **FortiClient** + **FortiToken**



- предотвращение атак на промышленные устройства - **IPS** на **FortiGate**
- контроль трафика в промышленных протоколах – **Application Control** + **Industrial** сигнатуры на **FortiGate**
- эксплуатация в широком диапазоне температур при электромагнитном воздействии – промышленные устройства **FortiGate** серии **Rugged**

Защита в реальном времени от Fortinet

- **FortiGuard Labs =** A Global Threat Research Team – over 200 top threat analysts

- **FortiGuard Services =** Security services offered on all Fortinet devices, deployed through FortiOS, receiving real-time updates with proactive threat defense and new signautes/updates

FORTINET

FORTINET
FortiGate 500E v6.0.4 build 0231
NEXT GENERATION FIREWALL
NSS LABS
RECOMMENDED
JULY 2019