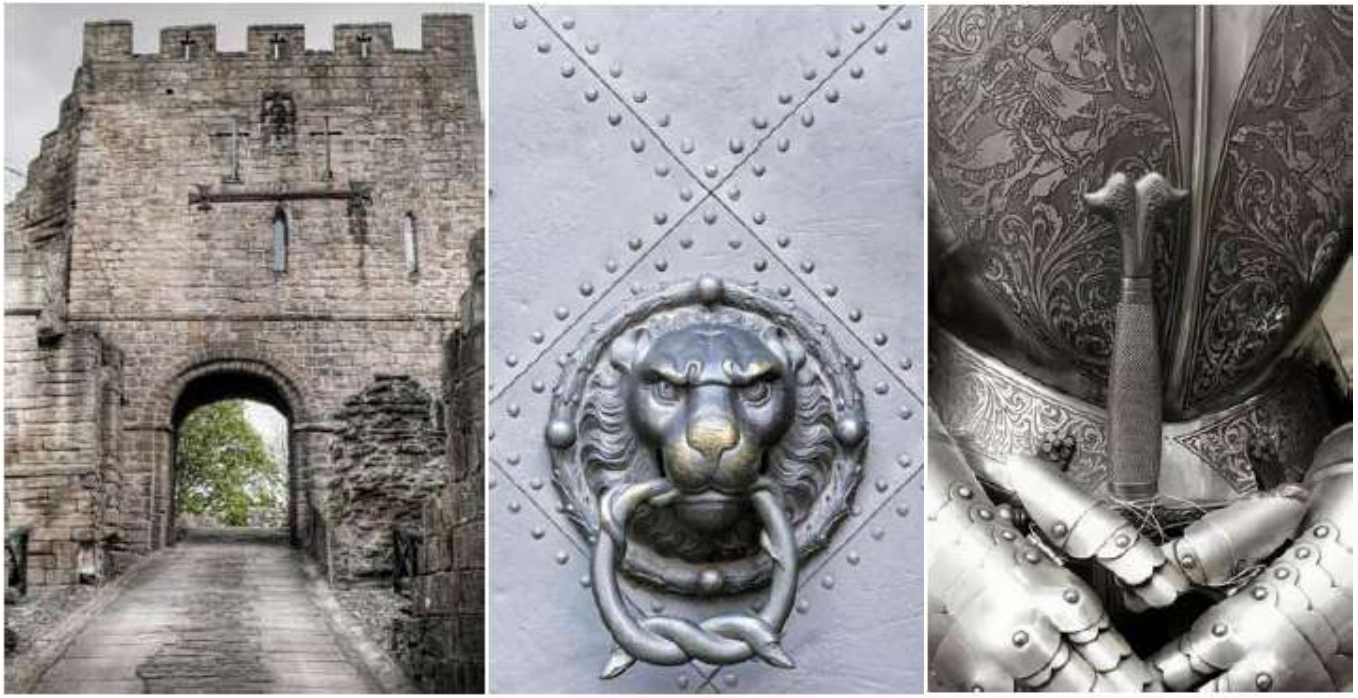
анализ | обучение | ит-архитектура | принятие решения

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY



Информационная безопасность технологических сегментов IP-сети (СКАДА, АСУТП и прочее)

управление рисками

SNITEGROUP

FOX-IT
информация о компании

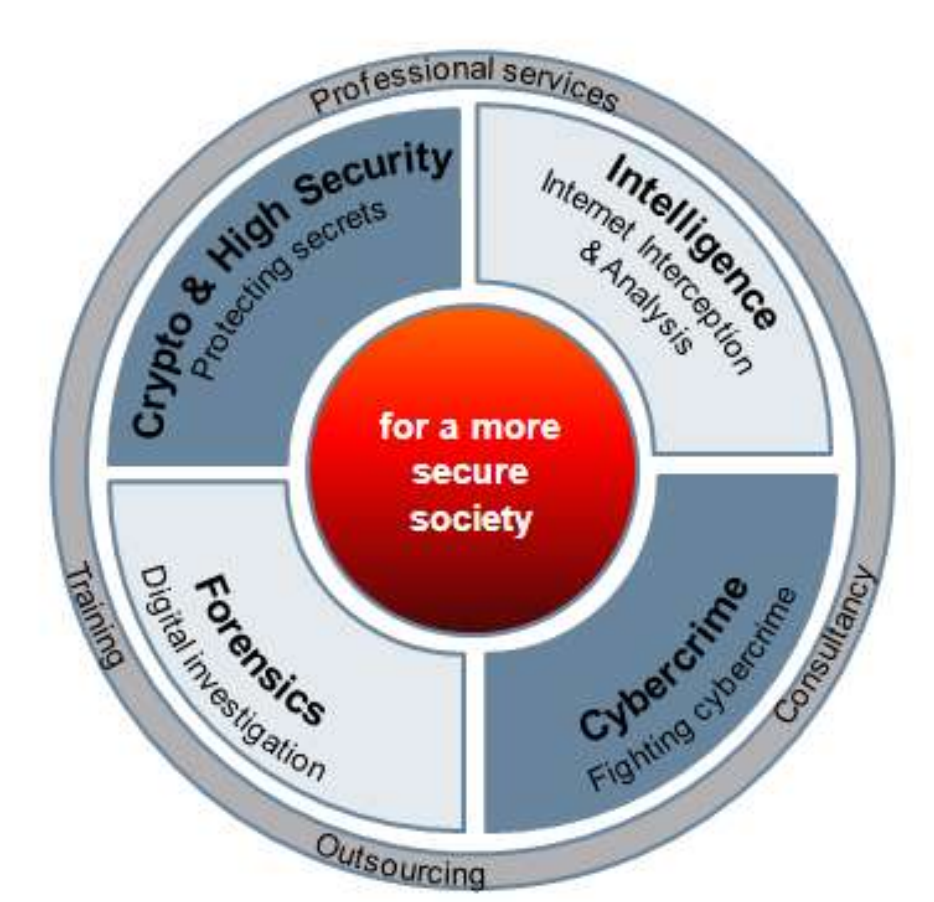
- Миссия: «Разработка инновационных решений для повышения уровня безопасности в обществе!»

- Компания создана в 1999 году
- Более100 инженеров-разработчиков
  - Все сотрудники лицензированы Правительством Нидерландов
- Штаб-квартира в городе Делфт, Нидерланды, офисы в США и Великобритании
- Партнерская сеть по всему миру

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

FOX-IT
направления деятельности



SNITEGROUP
Информация о компании

- SNITEGROUP – консалтинговая компания
- Экспертиза в области , решений по системам передачи данных, системам учета электроэнергии и информационной безопасности технологических сегментов сетей (SCADA, АСУТП и т.д.)
- Технологические партнеры – в 6 странах мира
- Штаб-квартира - г. Шлирен Швейцария

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Что такое риск?

- Риск – это комбинация вероятности события и его последствий (ISO/IEC Guide 73)

- Любые действия приводят к событиям и последствиям, которые могут представлять собой как потенциальные «положительные» возможности, так и «опасности»

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Перечень рисков

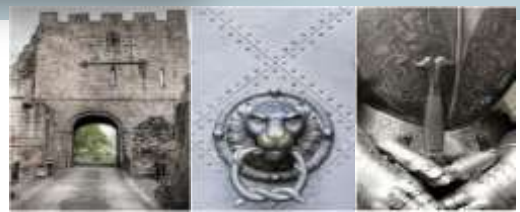
- Ошибки персонала
- Преднамеренные действия по сокрытию (изменению информации)
- Утечка информации
- Качество сервиса
- Ошибки программного обеспечения
- Некорректная работа программно-аппаратных комплексов
- Нарушения методологии работы
- Искажения отчетности

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

РИСК: Преднамеренные действия по сокрытию (изменению информации)

- Таблицы баз данных
- Экраны приложений
- Отчеты
- Системные и прикладные журналы событий



SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Как это работает?

- Запись и воспроизведение
  - Запись всех действий пользователей в контролируемом сегменте сети
  - Полное восстановление экранов пользовательских сессий
- Анализ содержания экрана
  - Автоматическое распознавание экранов и полей баз данных
  - Поиск по содержимому экрана (а-ля “Google”), например: кто открывал мнемосхему объекта в определенный период времени?
- Идентификация действий пользователя
  - Постоянный анализ действий пользователей
  - Восстановление последовательности действий пользователя, которая может включать в себя, в том числе, несколько экранов и приложений
- Аналитический процессор
  - Настраиваемые правила отслеживания и предупреждения действий пользователей в реальном времени
  - Гибкая система изменения правил
  - Управление инцидентами обеспечивает предупреждение аварий и расследование произошедших событий

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Информационные потоки

Current Impact or Likely Future Impact of the Incident	Criticality of Resources Currently Impacted or Likely To Be Impacted by the Incident		
	High (e.g., Internet Connectivity, Public Web Servers, Firewalls, Customer Data)	Medium (e.g., System Administrator Workstations, File and Print Servers, XYZ Application Data)	Low (e.g., User Workstations)
Root-level access	15 minutes	30 minutes	1 hour
Unauthorized data modification	15 minutes	30 minutes	2 hours
Unauthorized access to sensitive data	15 minutes	1 hour	1 hour
Unauthorized user-level access	30 minutes	2 hours	4 hours
Services unavailable	30 minutes	2 hours	4 hours
Annoyance[ff]	30 minutes	Local IT staff	Local IT staff

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

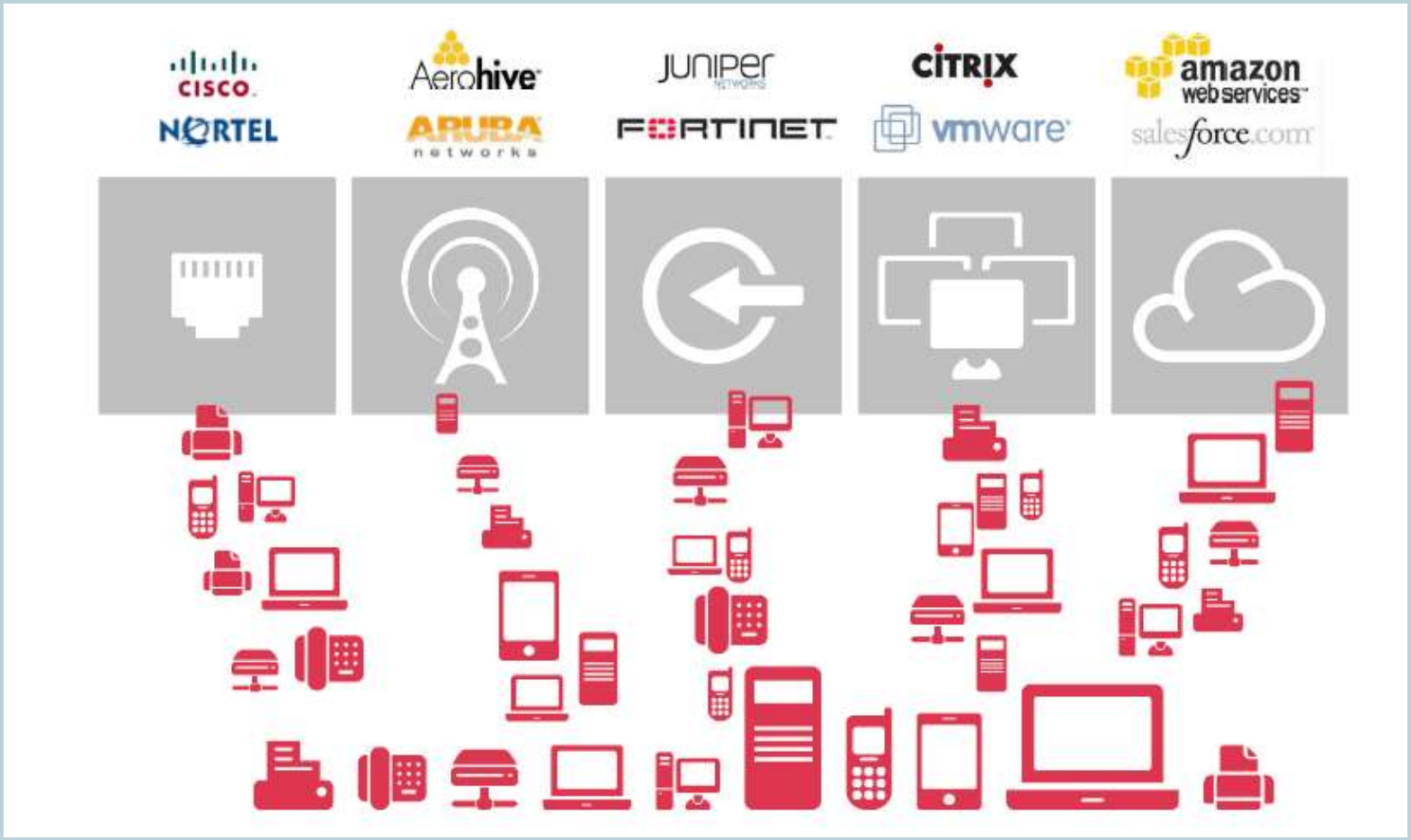
Риск: Некорректная работа программно-аппаратных комплексов

- Бесконечные сочетания вариантов доступа к сети
- Многочисленные виды устройств, пользователей и услуг

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Схема доступа к сети



SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Система управления доступом к сети

- Не требует установки агентов
- Стандартные протоколы (SNMP, SSH, HTTP)
- Интеграция с управляемыми и неуправляемыми устройствами доступа;
- Нет обработки трафика, не требует изменения топологии
- Интеграция с корпоративным каталогом и доменом
- Изменяемый белый список объектов для проверки подлинности
- Интегрируется в текущую сеть и существующую идеологию информационной безопасности

РИСК: Утечка информации…

- Собственные ОС и протоколы → открытые стандарты
- Централизованные вычисления → распределенные вычисления
- Сегментированные потоки данных → интегрированные потоки данных
- Замкнутые системы → открытые системы

В чем проблема ?

Если мы присоединены к сети, то более уязвимы

Должны быть отделены от сети → Нет реального времени

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

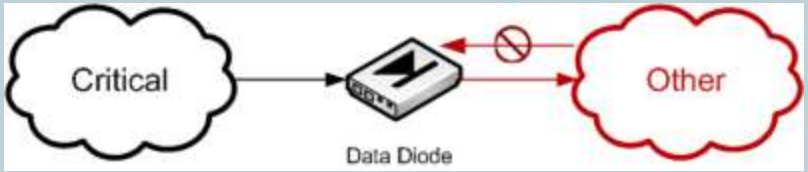
Варианты присоединения к сети

- Air Gaps

- Firewalls

До
После

- Data Diodes

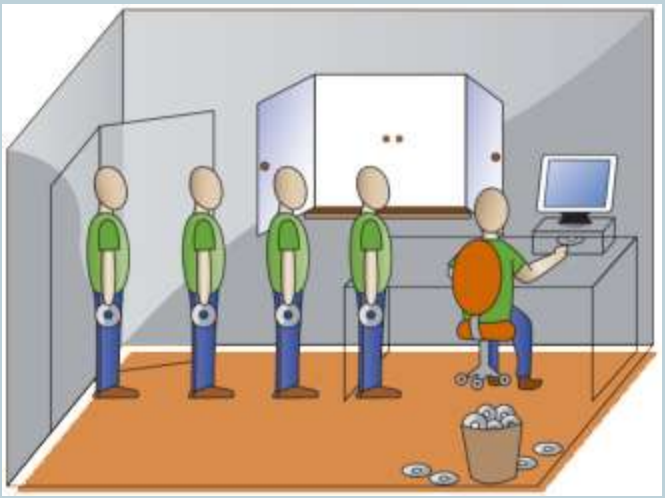


Вариант 1: Отсутствие соединения

- Ручной перенос данных на CD
- Подготовка данных по устным запросам

Преимущества:

- Нет соединения = нет потери уровня безопасности



Недостатки:

- Нет реального времени
- Ручной ввод данных
- Потеря информации
- Больше рисков технических ошибок

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

Вариант 2: Фаерволы

- Логическое разделение сетей
  - Блокировка неавторизованного доступа
  - Разрешение на авторизованные потоки данных
- **Преимущества:**
  - Проверенная технология
  - Автоматизированное и гибкое решение
- **Недостатки:**
  - Нет гарантии от ошибок пользователей, хакеров и недобросовестных пользователей

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

Вариант 3: ДатаДиоды

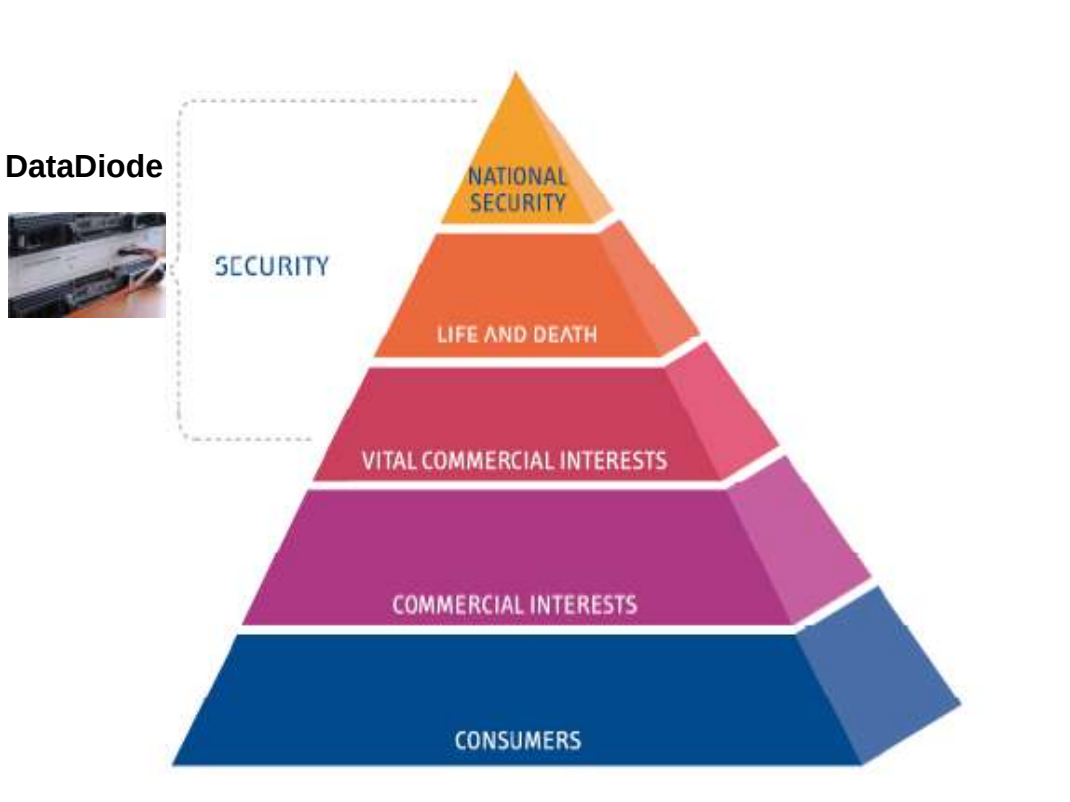
- Однонаправленное на физическом уровне, соединение сегментов сетей
- **Преимущества:**
  - Автоматическое и гибкое решение
  - Однонаправленное соединение
  - Взлом не возможен,
  - Нет возможности онлайн-атак и потерь данных 100% защита !
- **Недостатки:**
  - Однонаправленное соединение

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

История создания ДатаДиода

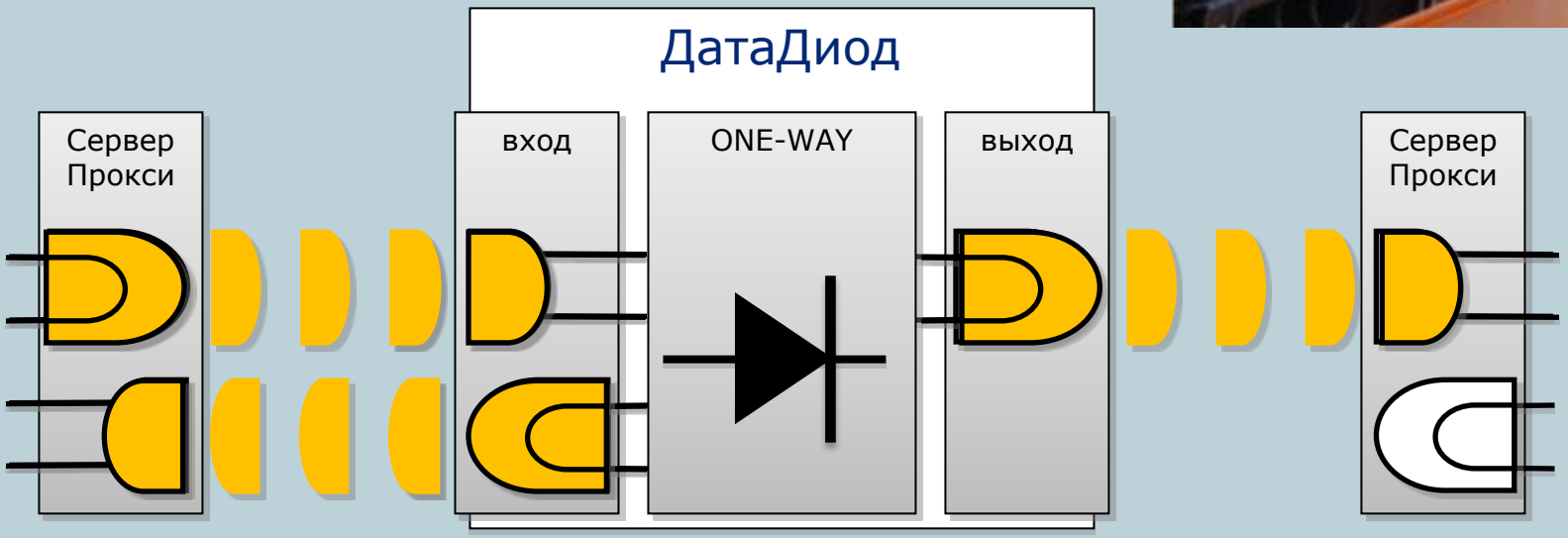
- ДатаДиод первоначально был разработан для использования в государственных организациях EU
- Однако со временем нашел широкое применение также в промышленности и коммерческой сфере



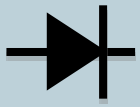
SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Как это работает?



Световой передатчик



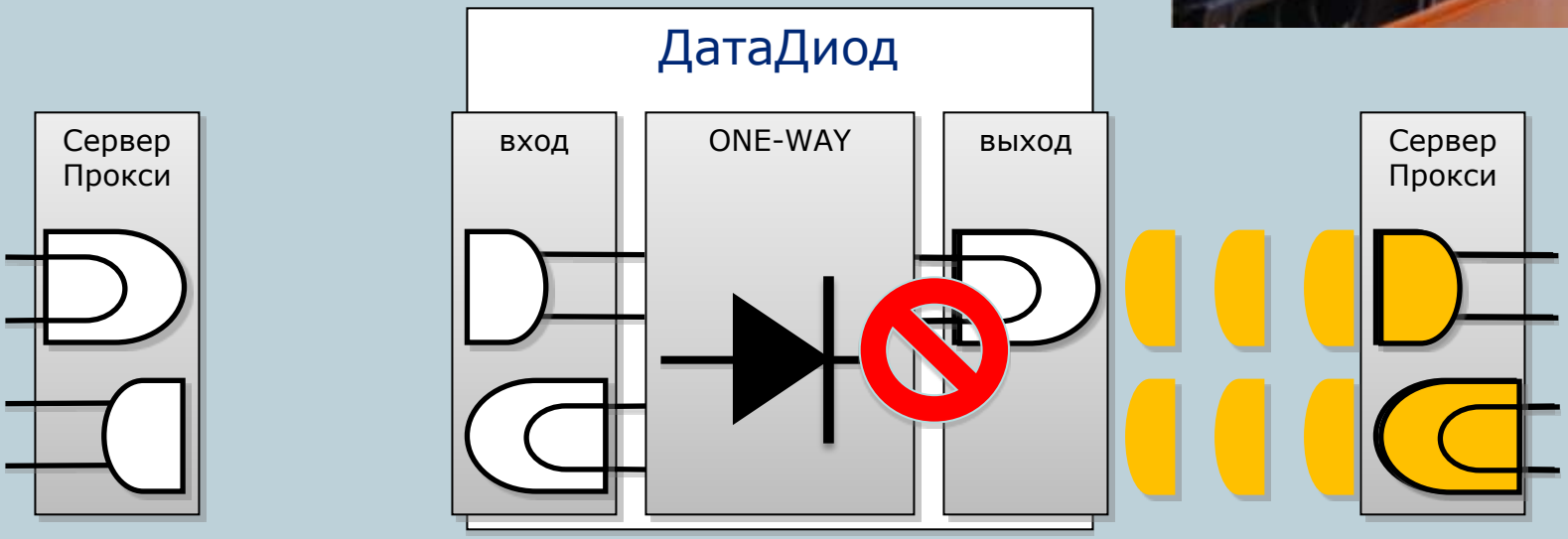
Световой приемник

Допустимо

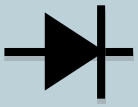
SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Как это работает?



Световой передатчик



Невозможно

Световой приемник

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

ДатаДиод

Однонаправленное коммуникационное устройство:

- аппаратная реализация (нет ПО, прошивок)
- сертифицировано
- не может быть взломано
- большое количество внедрений по всему миру

Более 300 поддерживаемых протоколов, например:

Matrikon, ORACLE, GE Energy, Kepware, OPC OLE for Process Control, MITSUBISHI ELECTRIC, OSIsoft., SIEMENS, dnp Distributed Networks Protocol

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Сертификация решения

- Сертификаты
  - Common Criteria **EAL 7+** (Европейский союз)
  - Национальные стандарты
    - NL-NCSA (Голландия)
    - BSI (Германия)
  - NATO Secret (NS)
  - ФСТЭК (Россия)

- NERC (US)
  (North American Electric Reliability Corporation)

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Внедрения

- Правительственные структуры
- Службы безопасности
- Армия
- Полиция
- NASA
- НАТО
- Банки
- Промышленность
- Телекоммуникации

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

Типичные приложения

- **Передача данных СКАДА/Process Control Security**
- Передача файлов (FTP/CIFS/SMB)
- Работа с электронной почтой (SMTP)
- Аудио/Видео поток (UDP)
- Удаленная печать
- Репликации баз данных: Oracle, mysql, MSSQL, etc
- Синхронизация LDAP/Active Directory
- Синхронизация данных
- Сервис обновления Windows Server (WSUS)
- Обновление антивирусов: McAfee, Symantec etc...
- Синхронизация веб-страниц
- Мониторинг удаленных сетей (SNMP)/ Nagios

ORACLE

McAfee

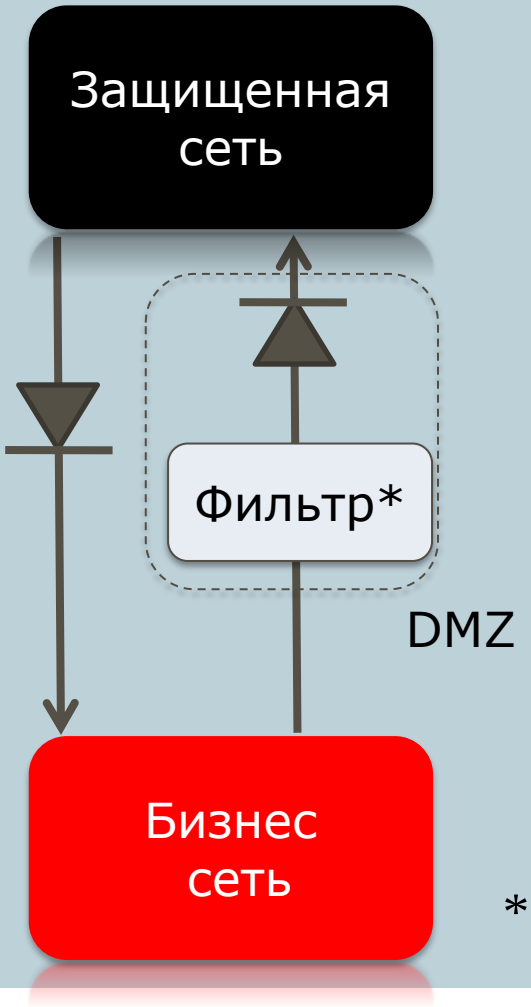
symantec.

Nagios®

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Комплексные решения



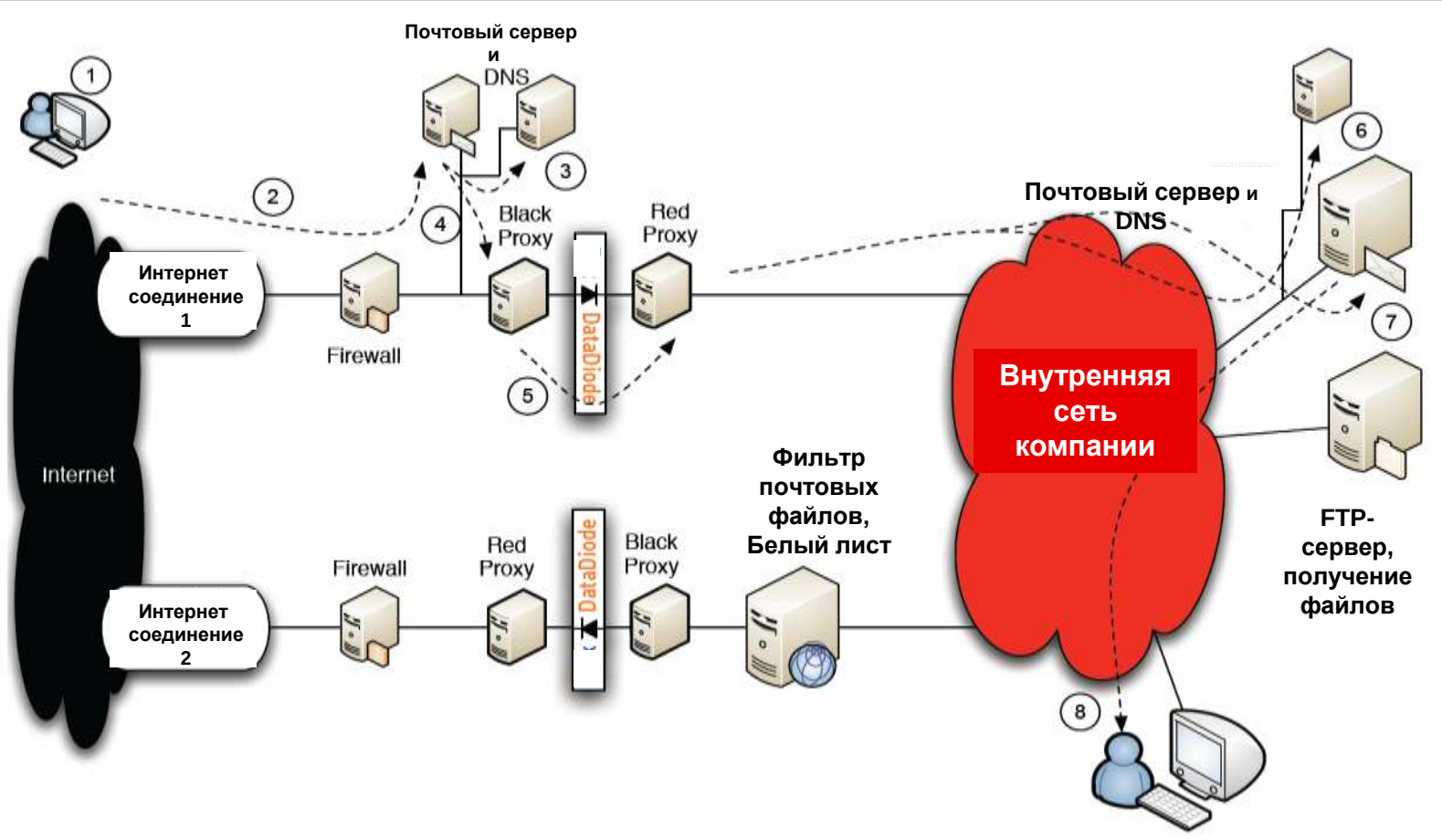
- Контролируемое двунаправленное соединение
- Исходящие файлы изолируются прежде чем они поступят в защищенный сегмент сети
- DMZ и Фильтр обеспечивают контроль файлов поступающих в защищенный сегмент сети

* приложение другого производителя

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Пример комплексного решения: Электронная почта

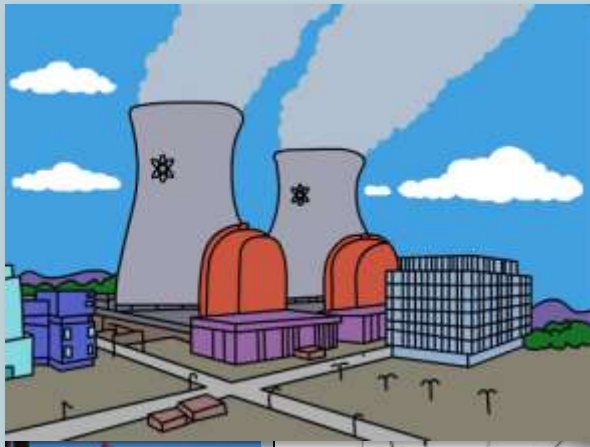


SNITEGROUP

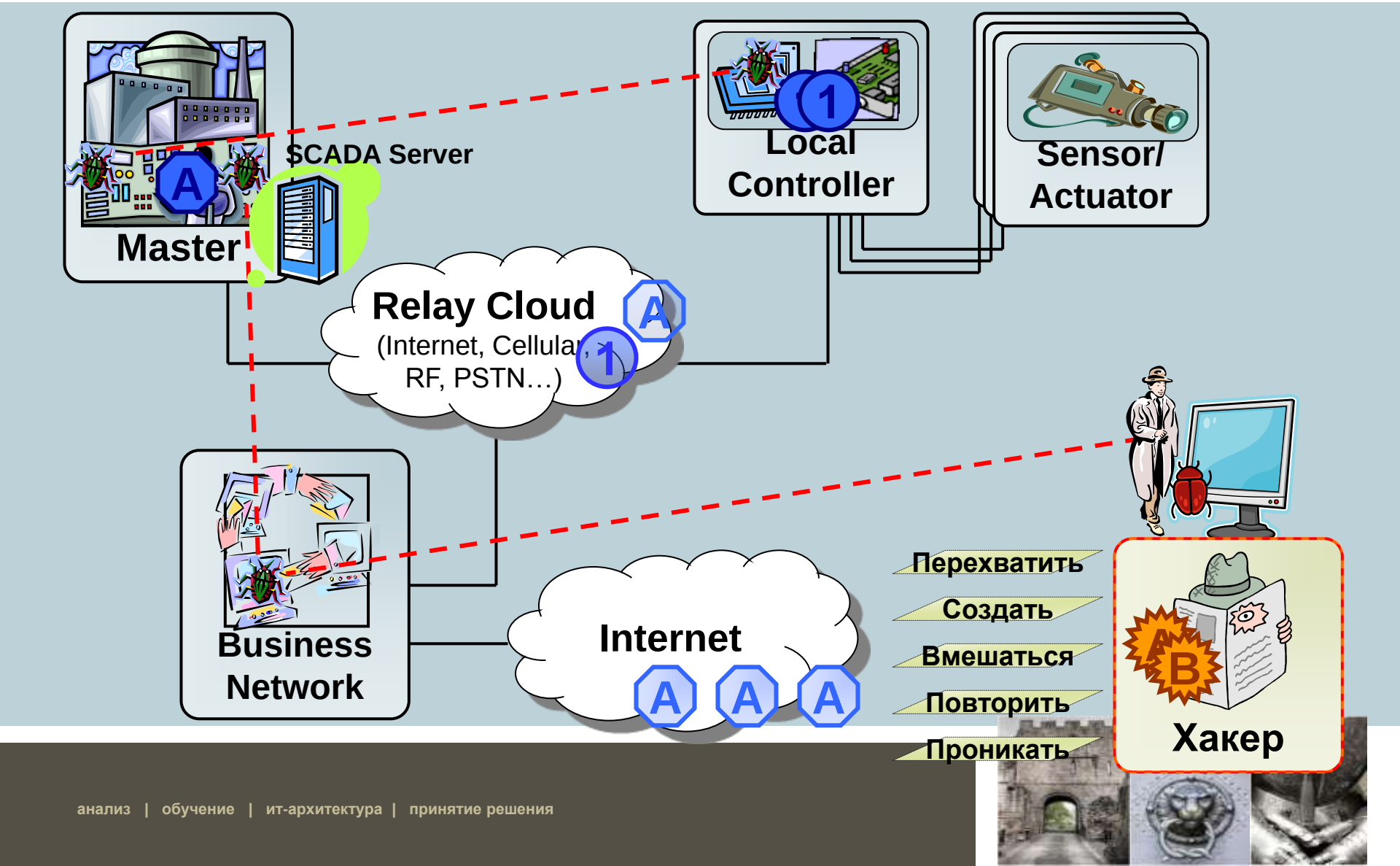
FOX-IT
EXPERTS IN IT SECURITY

Промышленность

- Электроэнергетика (сети, сбыты, генерация, включая атомные станции)
- Нефть и Газ (добыча, переработка)
- Водоканалы
- Оборонная промышленность
- Автомобильные и железнодорожные системы управления
- Инфраструктура портов
- Контроль воздушного движения
- Налоговые органы
- Телеком компании

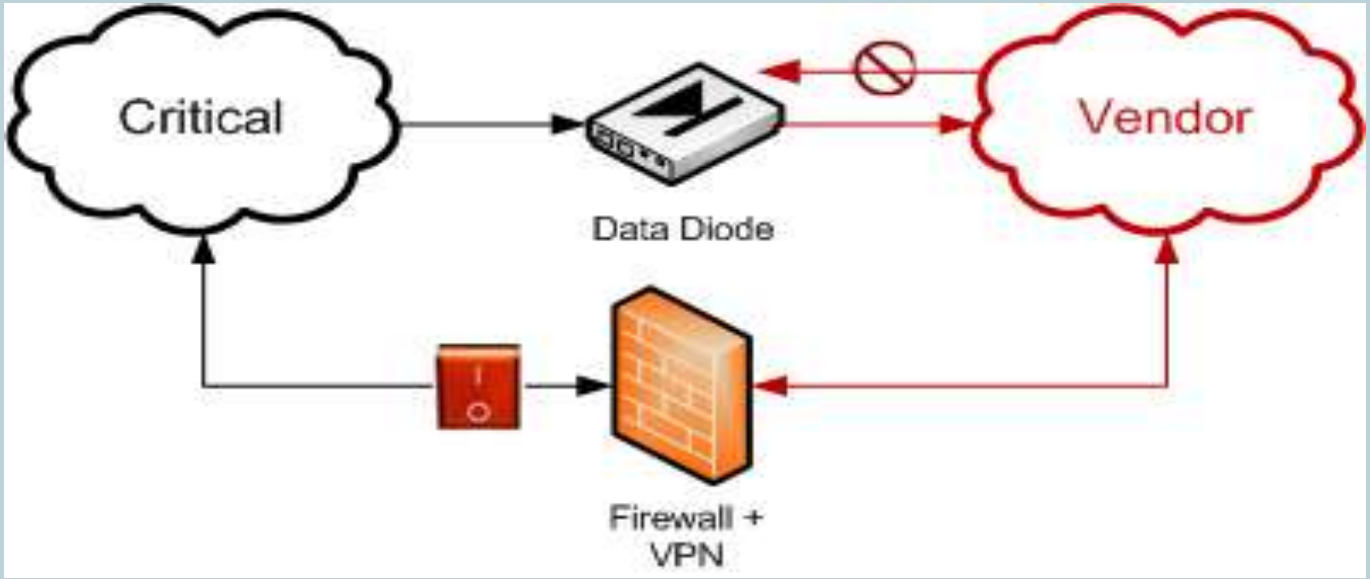


Критическая инфраструктура: Угрозы!



Пример: Решение для сервисных компаний

- Возможность безопасно мониторить работоспособность системы управления через удаленный доступ
- Обратный канал по умолчанию отключен, но может быть активирован по запросу



SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Пример: Атомные станции (до)

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

Пример: Атомные станции (после)

Все требуемые данные через корпоративную сеть направляются регулятору.

Защищенность корпоративной сети обеспечена ДатаДиодами

SNITEGROUP

FOX-IT
EXPERTS IN IT SECURITY

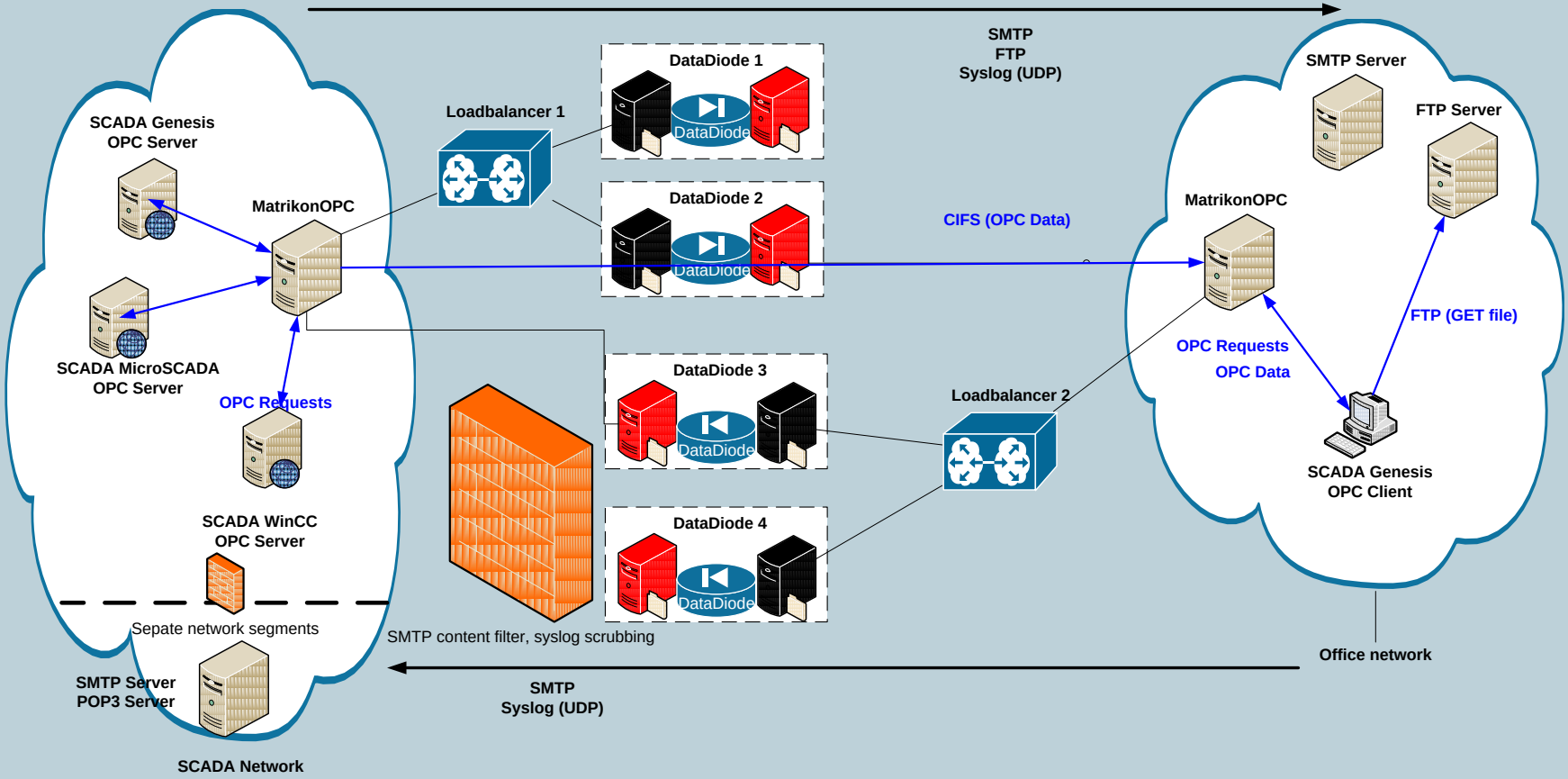
Пример: Электроэнергетика

- **Голландия/Евросоюз**
  - Регулятор контролирует производство и потребление электроэнергии
  - Получает данные от всех энергетических компаний страны
  - ДатаДиод позволяет Регулятору сохранять уровень защищенности своей сети
- **ОАО «Русгидро»/Россия**
  - Взаимодействие СКАДА и Бизнес сегментов сетей на станционном уровне
  - ДатаДиод обеспечивает безопасный доступ к данным контура оперативного управления

SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

Пример: Типовое решение для ОАО «Русгидро»



SNITEGROUP

FOX-IT EXPERTS IN IT SECURITY

Спасибо за внимание!

FOX-IT EXPERTS IN IT SECURITY

ДатаДиод

Система управления доступом в сеть

Система контроля за действиями персонала

Evgeny Gengrinovich
Executive Director SNITEGROUP GmbH
tel. +7(985) 9288602, E-mail: gel@snitegroup.com