Обзор угроз

Кибер Атаки на ИТ-инфраструктуру – это не миф

Hackers Break Into Power Station, In Less Than A Day

Next news

6:04 AM - April 10, 2008 by Humphrey Cheung

Email | Print | Comment | Share

San Francisco (CA) - It took hackers less than a day to take over several desktops at a major power company. Ira Winkler, a penetration testing consultant, and his team were able to trick company employees into clicking false links which contained self-installing Trojan horse software. Winkler says his team had complete control of the computers and could have caused even more damage to the company's power production and distribution systems.

Schoolboy hacks into city's tram system

By Graeme Baker
Last Updated: 2:48am GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.

The teenager, who was not named by police, told them

Hackers Break Into Water Processing Plant Network

Darknet spilled these bits on December 14th 2006 @ 7:52 am

When things like this happen it's kinda of scary, like a while back when someone managed to get into a highly secure power station network through a stupid contractors laptop that was connected to the net via dialup and to the uber 'secure' power station LAN.

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Article | Video | Comments (144)

Email | Print | Save This | Like 1,218 | + More | Text

By SIOBHAN GORMAN

Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

DataDiode

Официальный доклад о вирусных атаках на SCADA, промышленные системы управления

Ожидается рост целевых замаскированных атак, таких как Stuxnet и APT, на промышленные системы управления

Mar 07, 2011 | 04:06 PM | 0 Comments

By Kelly Jackson Higgins

Darkreading

На вредоносные программы приходится почти одна треть всех реальных инцидентов в промышленных системах управления, в соответствии с новым докладом, опубликованным SIO.

"Цена / качество решений [атак] сосредоточены на передовой постоянных угроз ... Мы начинаем видеть, преобладание очень тихих, тонких атак, таких как Stuxnet, GhostNet, NightDragon", которые являются более эффективными и прибыльными, говорится в докладе.

Одна крупная государственная компания США, которая работает с оборудованием Siemens PLC, попала под перекрестный огонь Stuxnet вируса в июле 2010 года, 43 операторских станции были заражены червем. Вирус сделал незначительные, случайные изменения в конфигурационных файлах, результаты их изменения не должны были быть разрушительными, но этого было достаточно, чтобы возникли проблемы, а через месяц, полностью потеряна информация всей системы. Эксперты в области безопасности опасаются, что Stuxnet прообраз будущих вирусов с моделью загрузки для всех систем управления технологическими процессами. "Если вы посмотрите на Stuxnet, это был типичный пример о том, как уничтожить процесс ... ", говорится в докладе.

... .. Стоимость одного такого инцидента может достигать10 миллионов долларов!

DataDiode

Общие угрозы

Электроника и ИТ-системы в составе критических производственных инфраструктур и конфиденциальные данные находятся под постоянной угрозой, в следствии:

- Ошибки оператора
- Саботаж со стороны недовольных сотрудников
- Хакеры
- Террористы
- Киберпреступники (например, финансовое вымогательство)
- Шпионаж
- ….

Быстрые изменения

- Из прошлого в будущее:
  - Собственные ОС и протоколы → открытые стандарты протоколов
  - Сегментированные потоки данных → интегрированные потоки данных
  - Замкнутые системы → открытые системы
  - Централизованные вычисления → распределенные вычисления

В чем проблема ?

Если мы присоединены к сети

- Более уязвимы
- Опасность взлома

- Должны быть отделены от сети → Нет реального времени

DataDiode

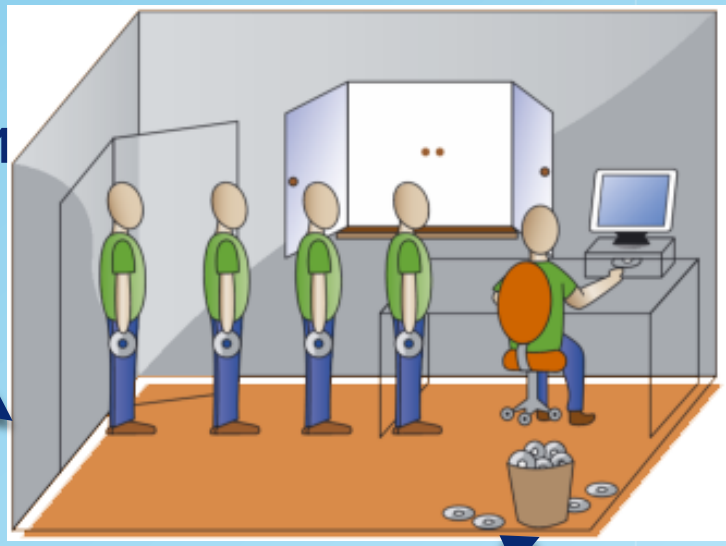
Вариант 1: Отсутствие соединения

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

Преимущества:

- Нет соединения=

нет потери уровня безопасности



Недостатки:

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

DataDiode

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

DataDiode

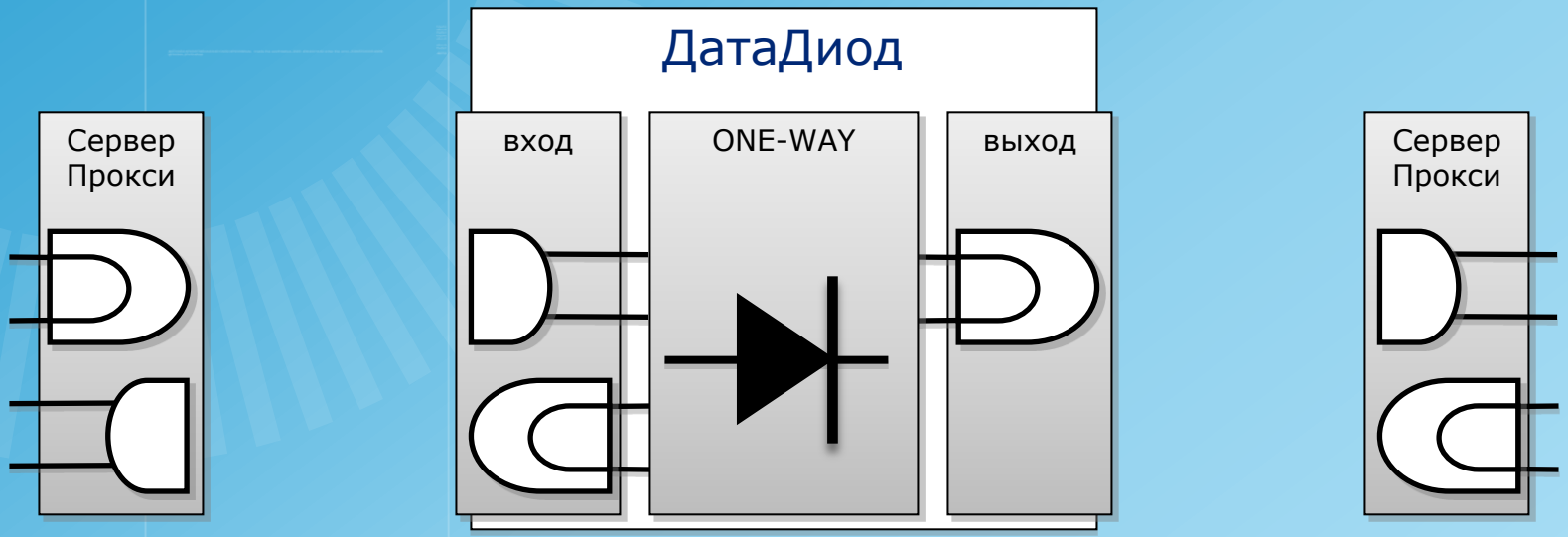
ДатаДиоды

- Однонаправленное, на физическом уровне, соединение сегментов сетей
  - Данные могут быть переданы но не получены или наоборот
- Преимущества:
  - Автоматическое и гибкое решение
  - Однонаправленное соединение
  - Взлом не возможен
  - Нет возможности онлайн-атак
  - Нет потерь данных
- 100% защита !
- Недостатки:
  - Однонаправленное соединение

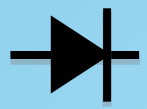
DataDiode

Технология ДатаДиода

Как это работает?



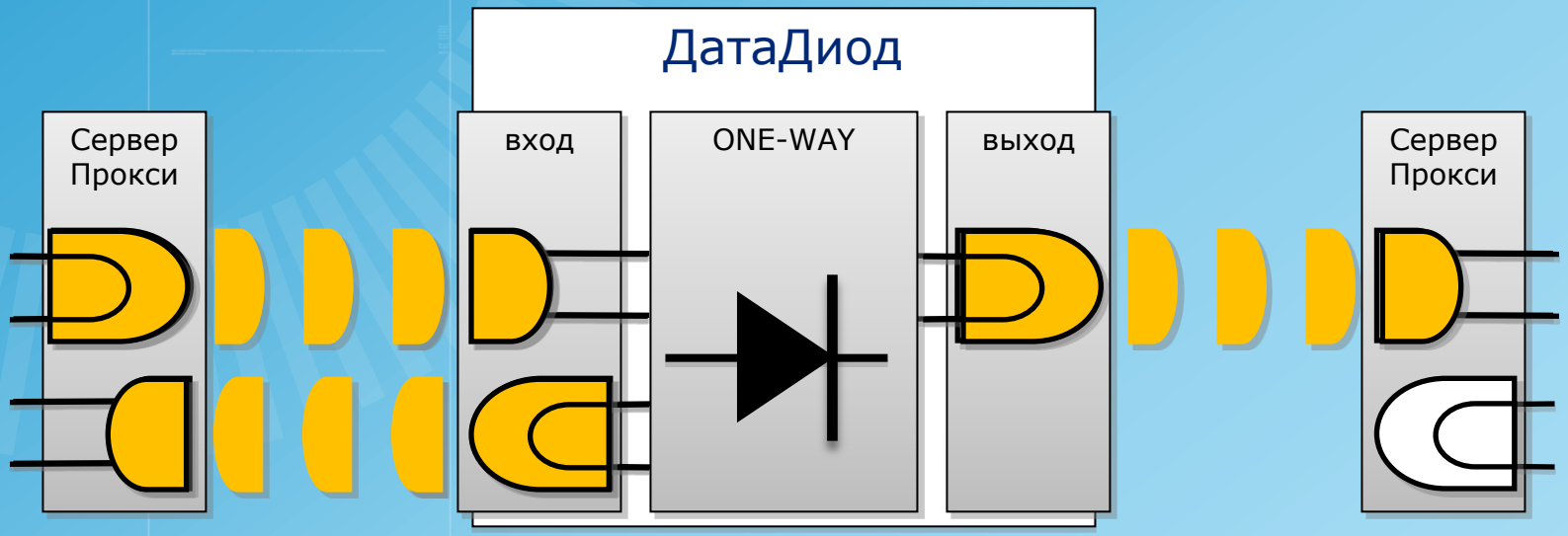
Световой передатчик



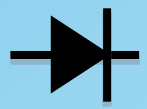
Световой приемник

DataDiode

Как это работает?



Световой передатчик

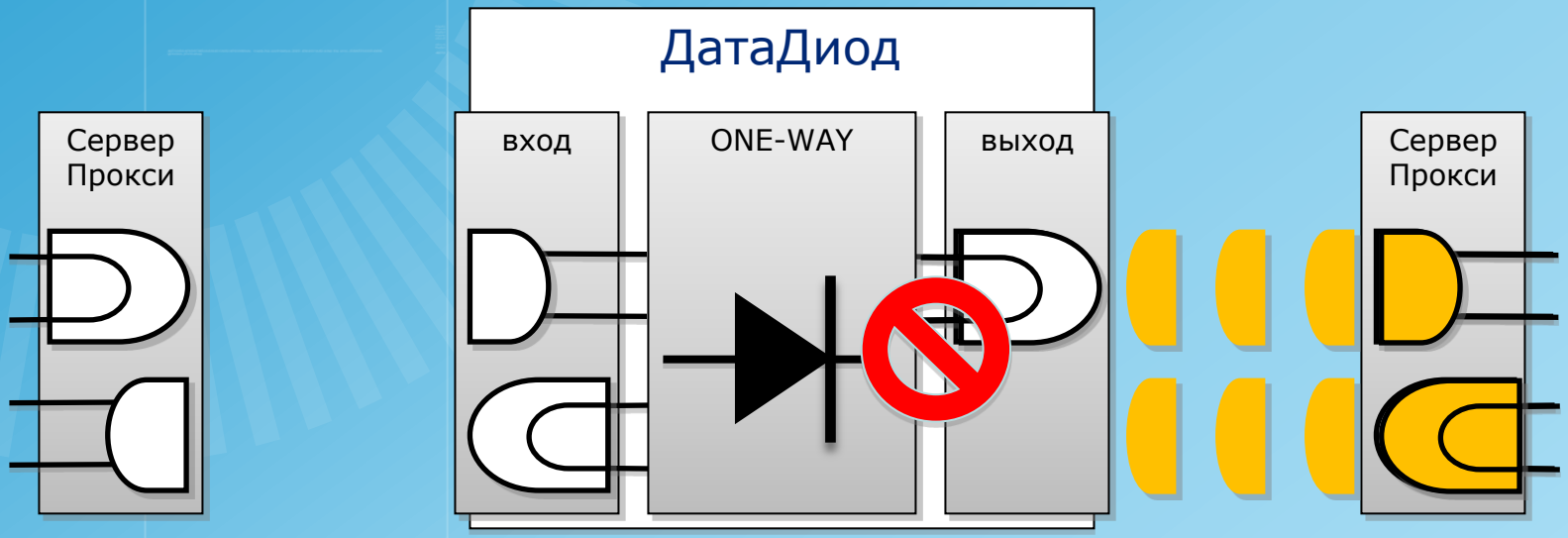


Световой приемник

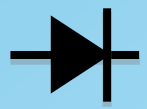
Допустимо

DataDiode

Как это работает?



Световой передатчик



Световой приемник

Невозможно

DataDiode

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)

Прокси сервера

Критическая сеть

Данные получены или извлечены

Протокол ДатаДиода

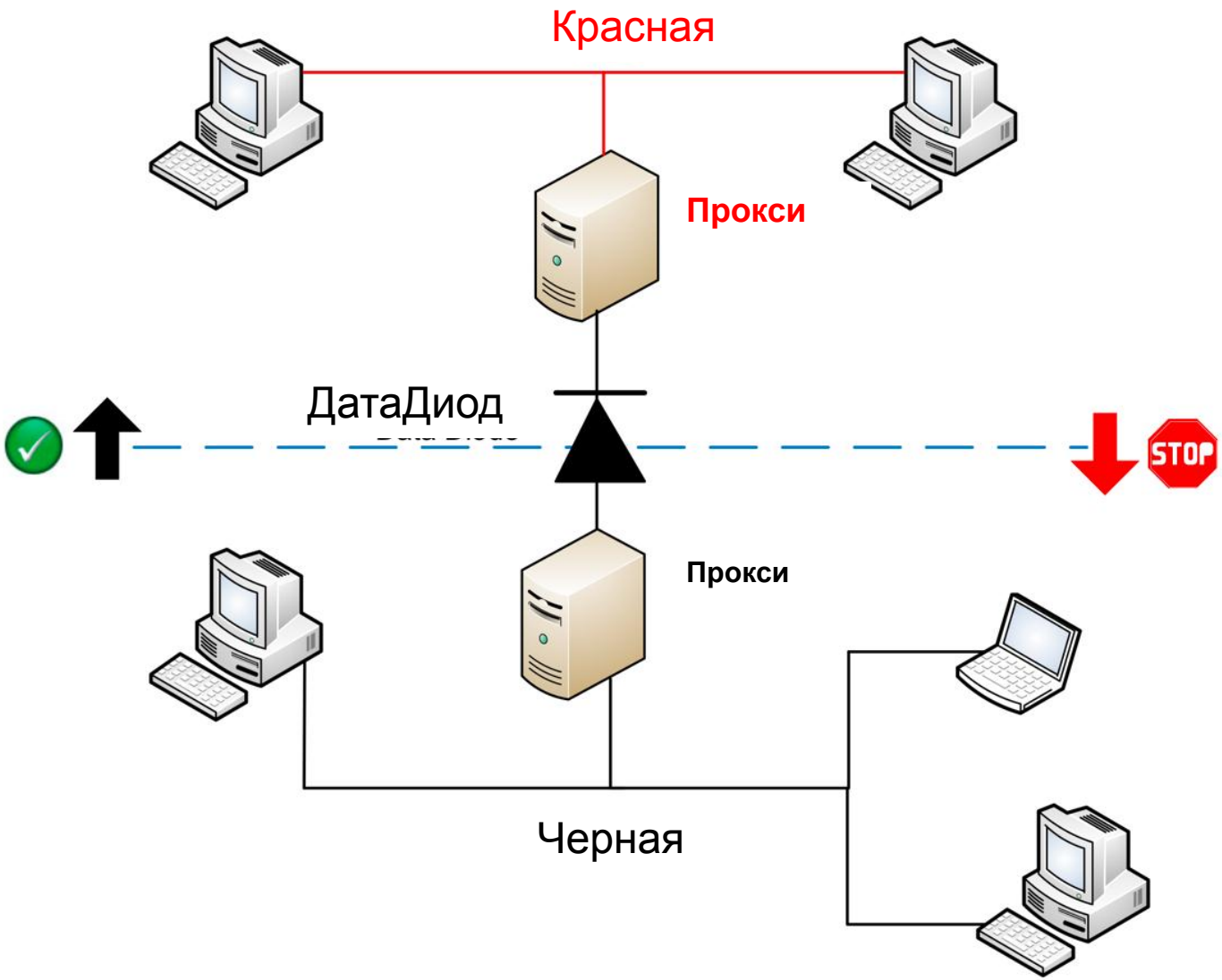
Протокол ДатаДиода

Данные переданы или стали доступны

Бизнес сеть

DataDiode

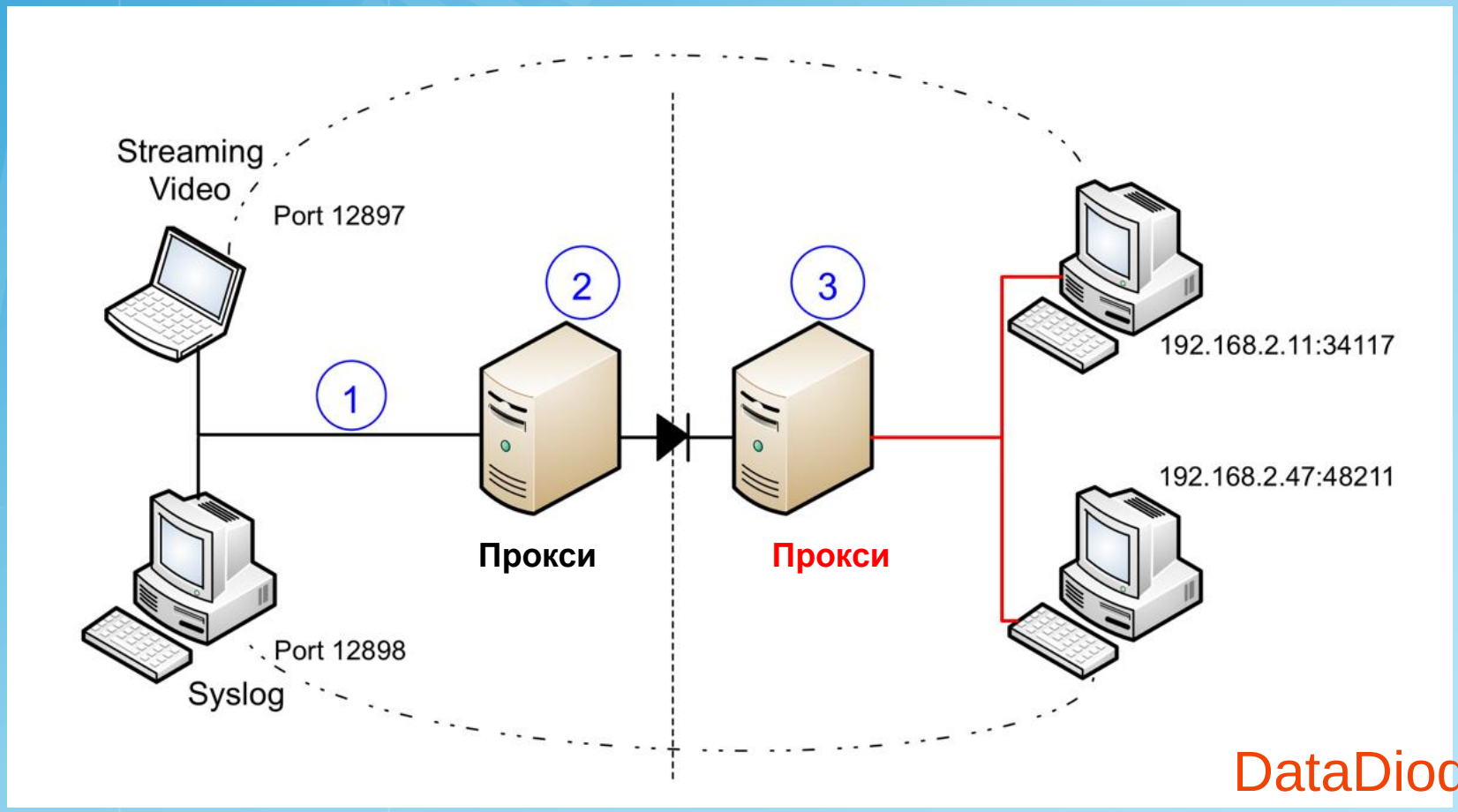
Передача файлов



DataDiode

Потоки данных

- UDP
- TCP



Сценарий: Электронная почта

Доступ к электронной почте из защищенной сети

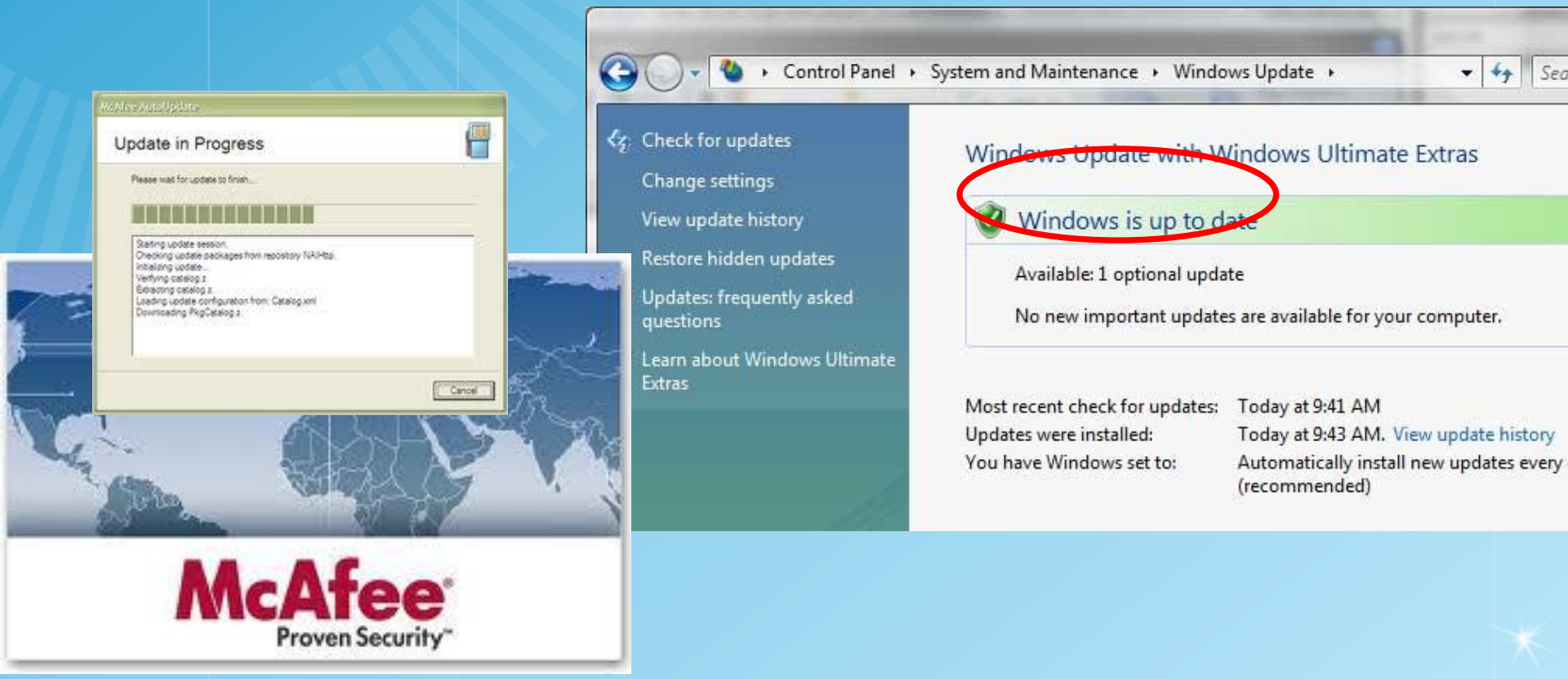
Преимущества:

- SMTP
- Отсутствие временных задержек
- 24/7

DataDiode

Сценарий: обновление ПО

Обновление ПО в автоматическом режиме в защищенной сети



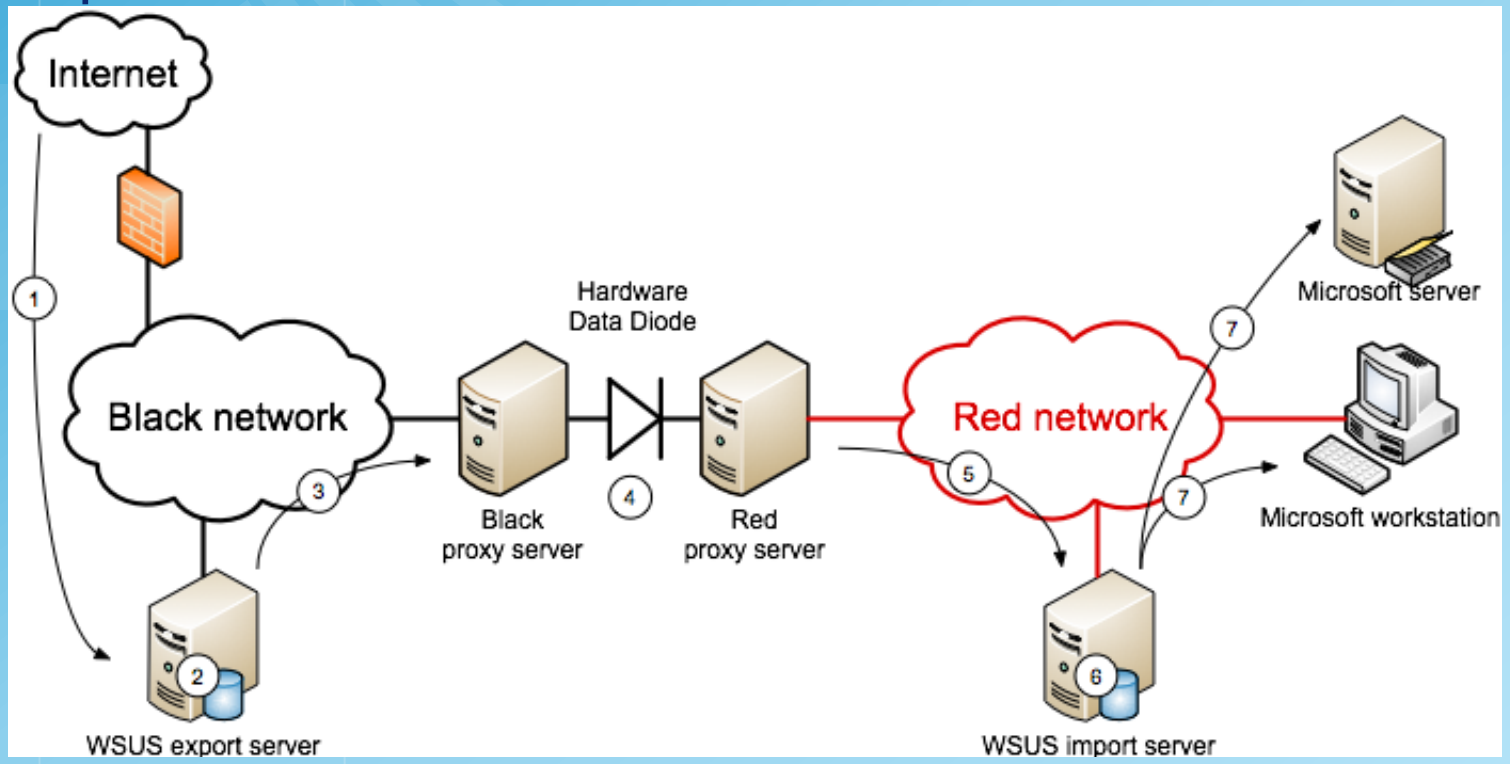
DataDiode

Сервис - обновление Windows Server

Преимущества:

Windows Server Update Services

Нет больше уязвимости защищенной сети в процессе обновления ПО



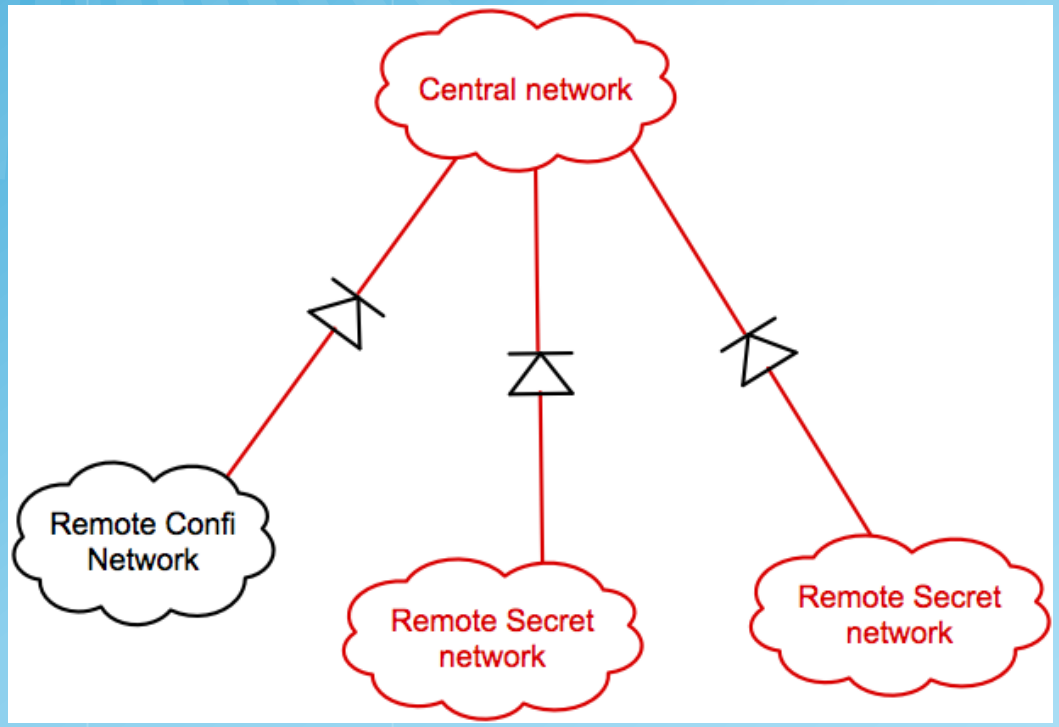
DataDiode

Централизованный сетевой мониторинг

Nagios®

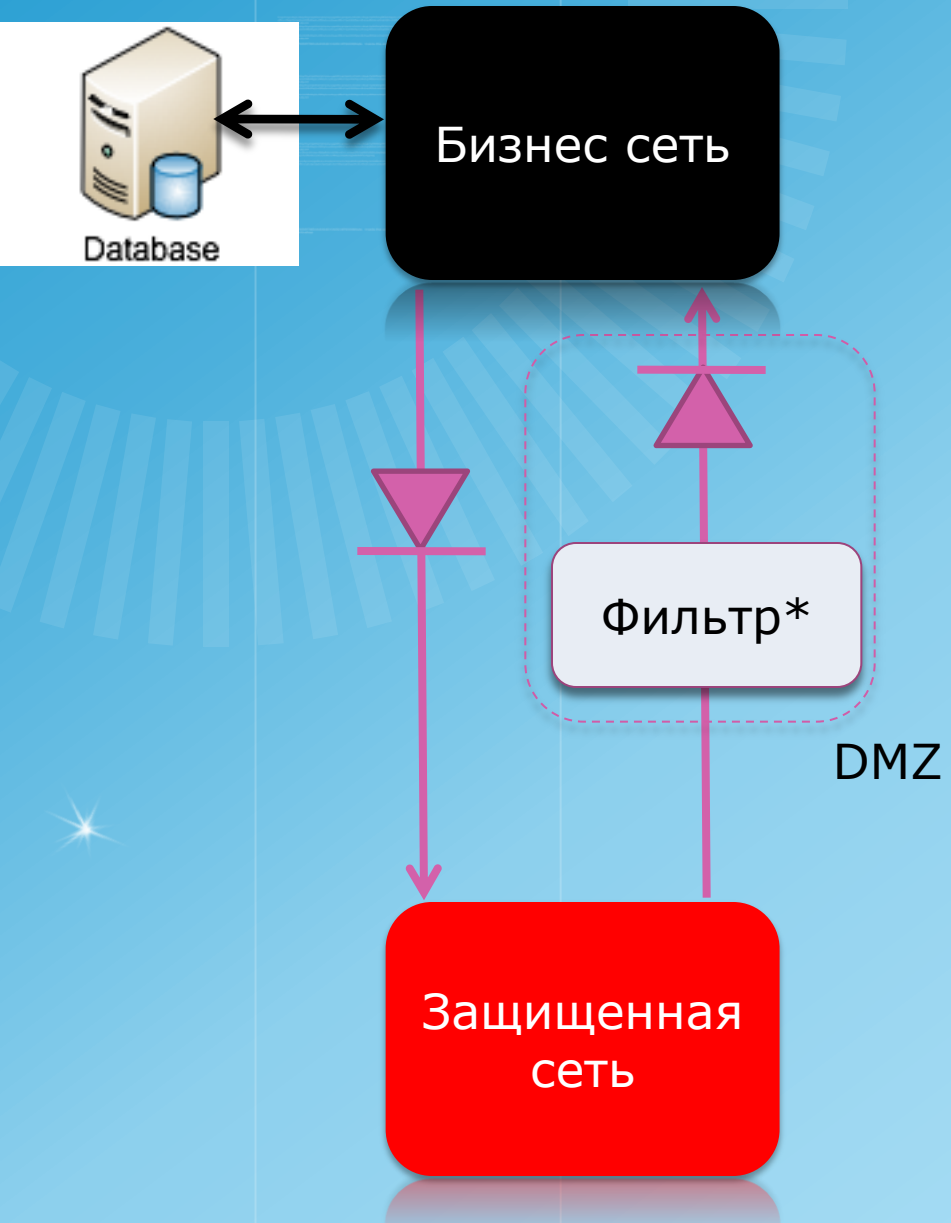
Мониторинг каждого сегмента сети в отдельности очень громоздкая процедура, централизованный мониторинг более эффективен и защищен.

(syslog, SNMP Traps)



DataDiode

Комплексные решения с ДатаДиодом

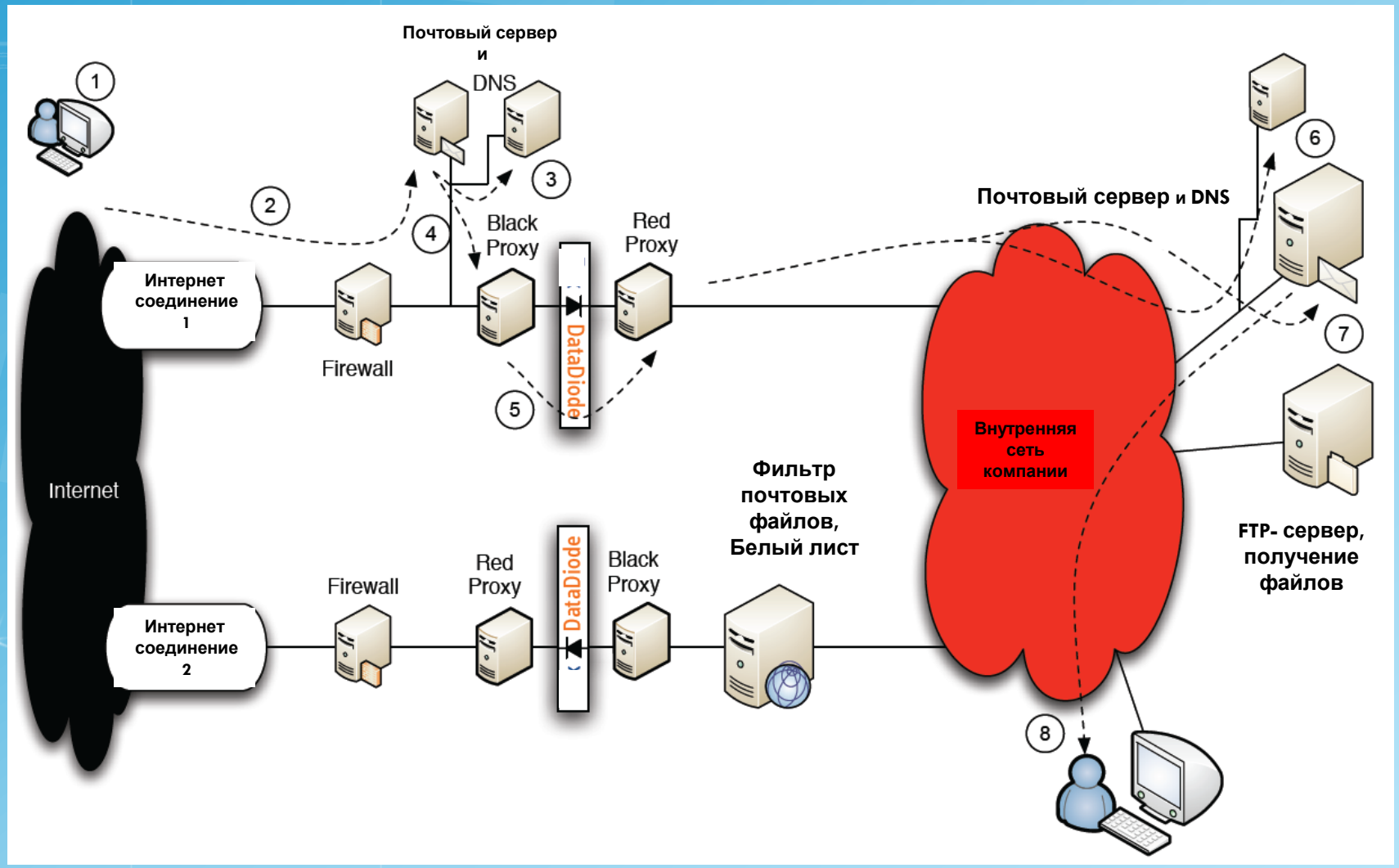


- Контролируемое двунаправленное соединение
- Исходящие файлы изолируются прежде чем они покинут сеть
- DMZ и Фильтр обеспечивают контроль файлов покидающих защищенную сеть

* приложение другого производителя

DataDiode

Комплексное решение для электронной почты



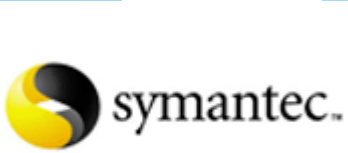
DataDiode

Типичные приложения

- 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

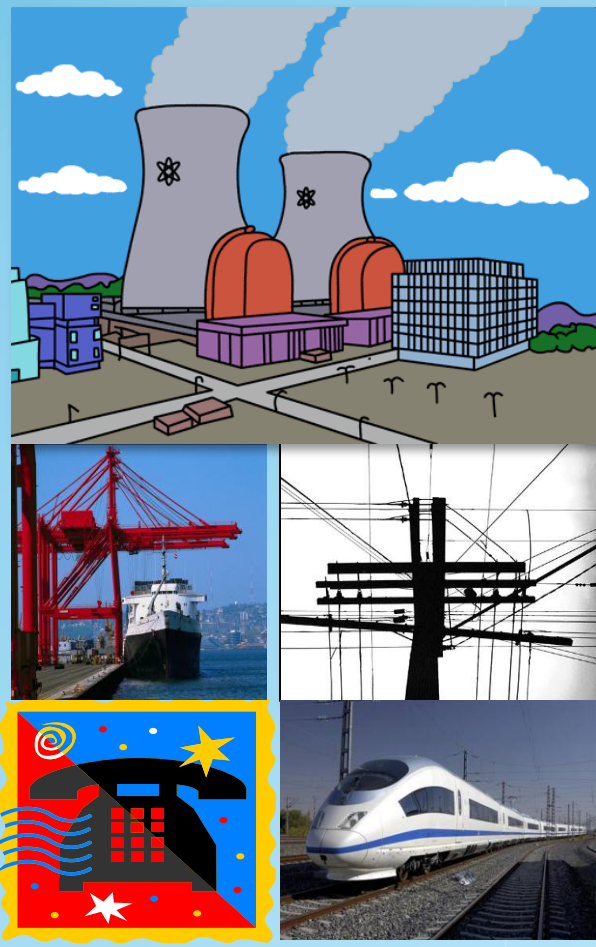
- **СКАДА/Process Control Security**



DataDiode

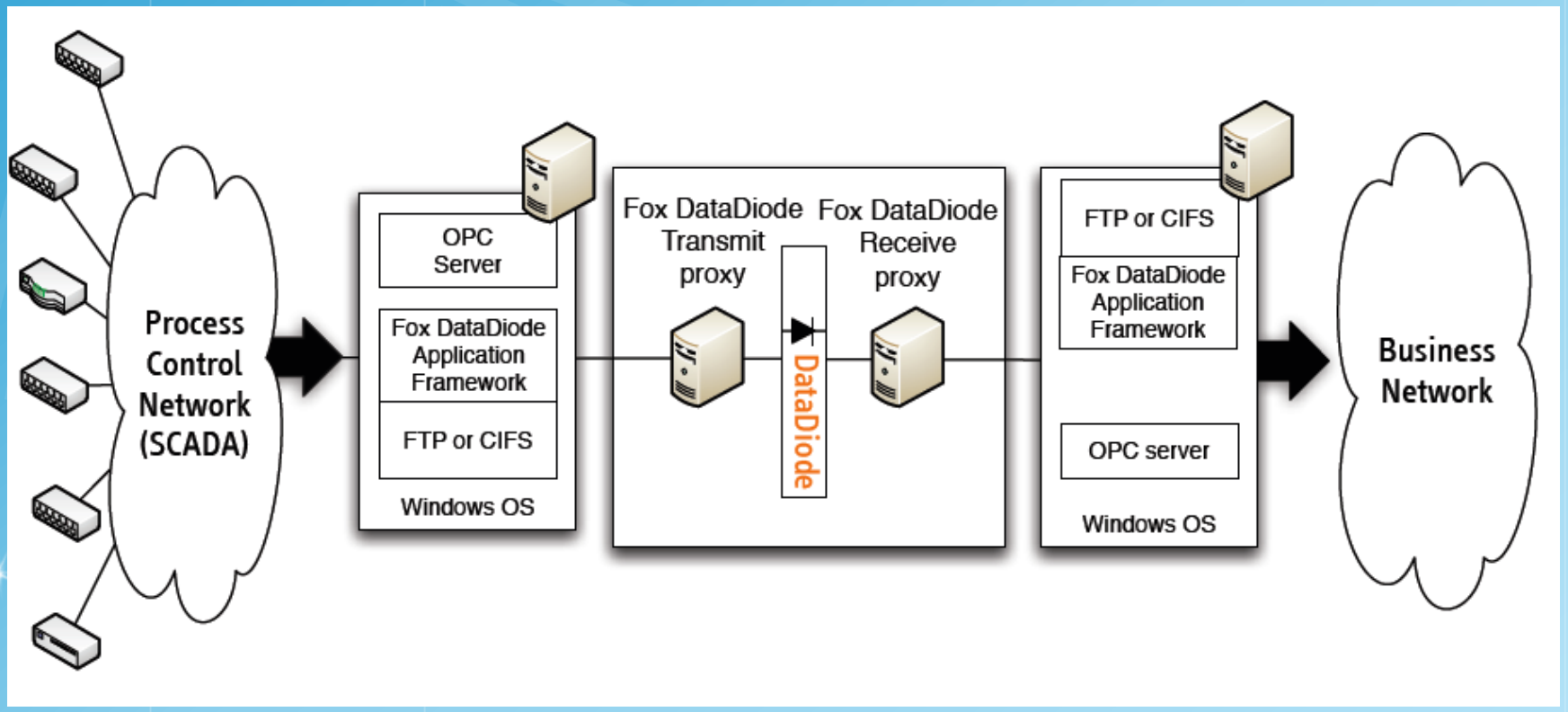
Промышленность

- Электроэнергетика
- Газ и нефть/переработка
- Водные станции
- Атомные станции
- Авто и железные дороги
- Инфраструктура портов
- Контроль воздушного трафика
- Налоговый контроль
- Телекоммуникации



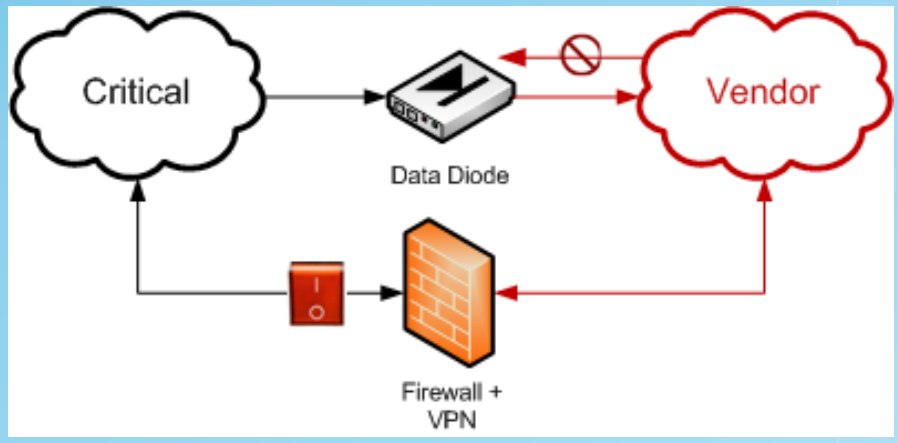
DataDiode

Типовая конфигурация



Решение для сервисных компаний

- Чаще всего используется для аутсорсинговых компаний или компаний производителей оборудования
- Возможность мониторить работоспособность оборудования через удаленный доступ
- Обратный канал по умолчанию отключен, но может быть активирован по запросу



DataDiode

Безопасность NASA

Данные получены или извлечены

Протокол ДатаДиода

Протокол ДатаДиода

Данные переданы или стали доступны

DataDiode

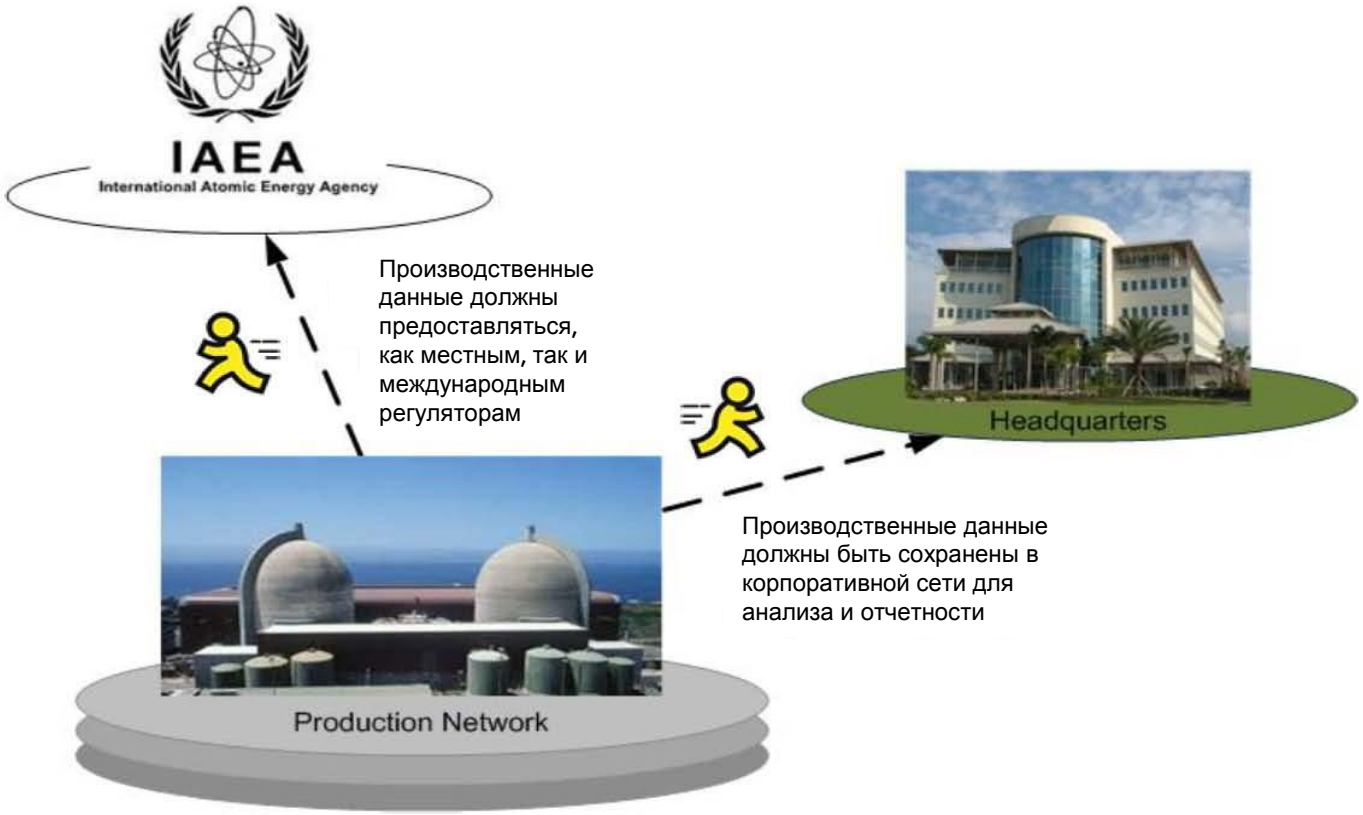
Транспорт (до)

DataDiode

Транспорт (после)

DataDiode

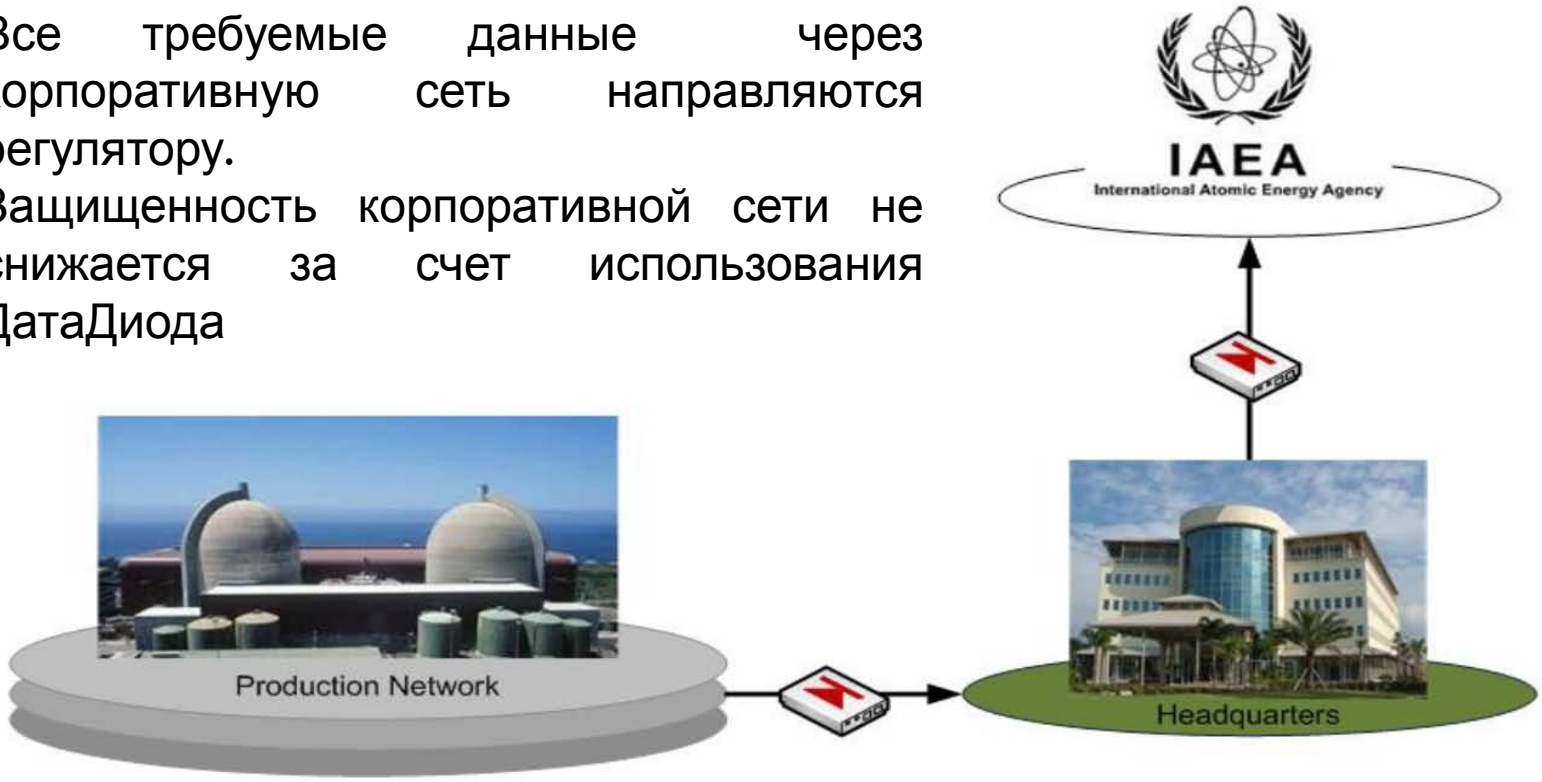
Атомные станции (до)



DataDiode

Атомные станции (после)

Все требуемые данные через корпоративную сеть направляются регулятору.
Защищенность корпоративной сети не снижается за счет использования ДатаДиода



DataDiode

Электроэнергетика

- Голландия/Евросоюз
  - Регулятор контролирует производство и потребление электроэнергии
  - Получает данные от всех энергетических компаний страны

- ДатаДиод позволяет Регулятору сохранять уровень защищенности своей сети

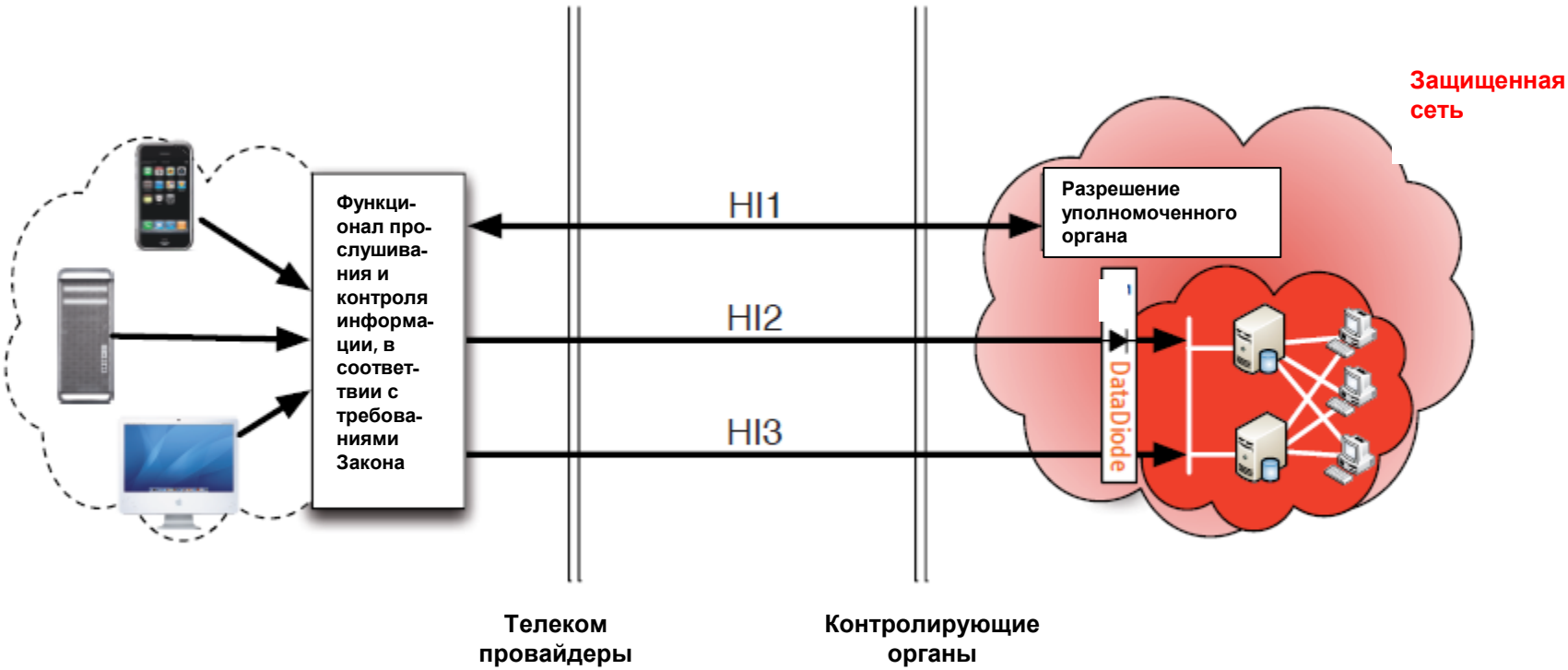
DataDiode

Телеком компании

- Изолируй и присоединяй свою операционную сеть (GSM) одновременно!
- Изолируй конфиденциальную информацию!!!
- Изолируй сегмент разработчиков.
- Присоедени Internet к защищенной сети
- Изолируй защищенную сеть от публичных сетей, сетей филиалов, сетей партнеров

DataDiode

Телеком и контролирующие органы



DataDiode

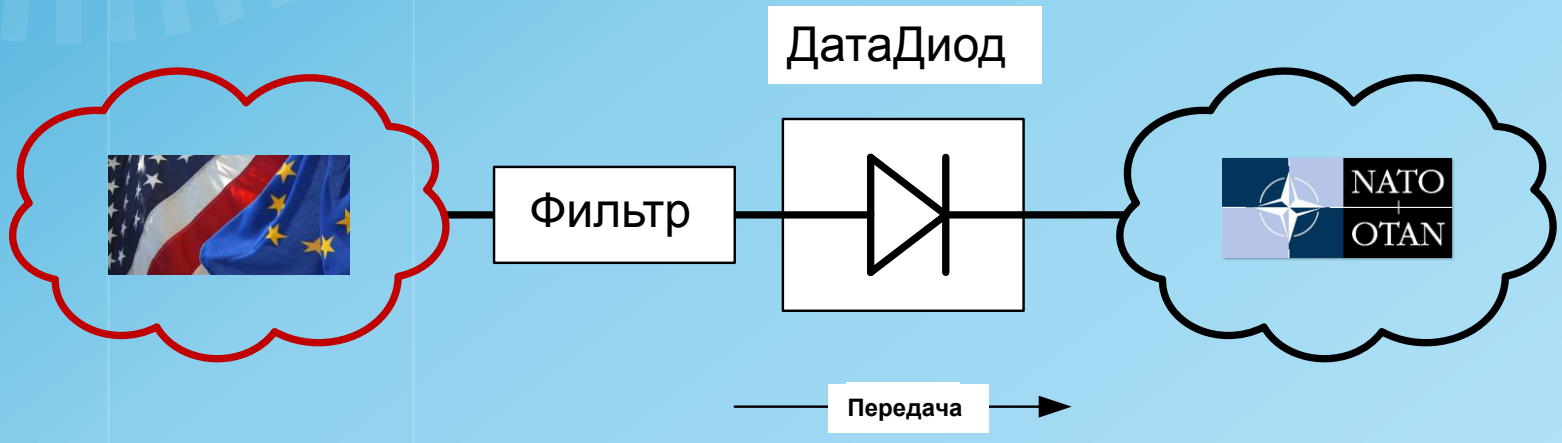
Банки

- Изолируйте Ваши конфиденциальные данные!!!
- Обеспечьте работу с Internet в защищенной сети
- Изолируйте Вашу конфиденциальную сеть от публичных сетей
- Изолируйте управленческую сеть от сетей филиалов
- Обеспечьте безопасное соединение с сетью банкоматов

DataDiode

Пример: NATO

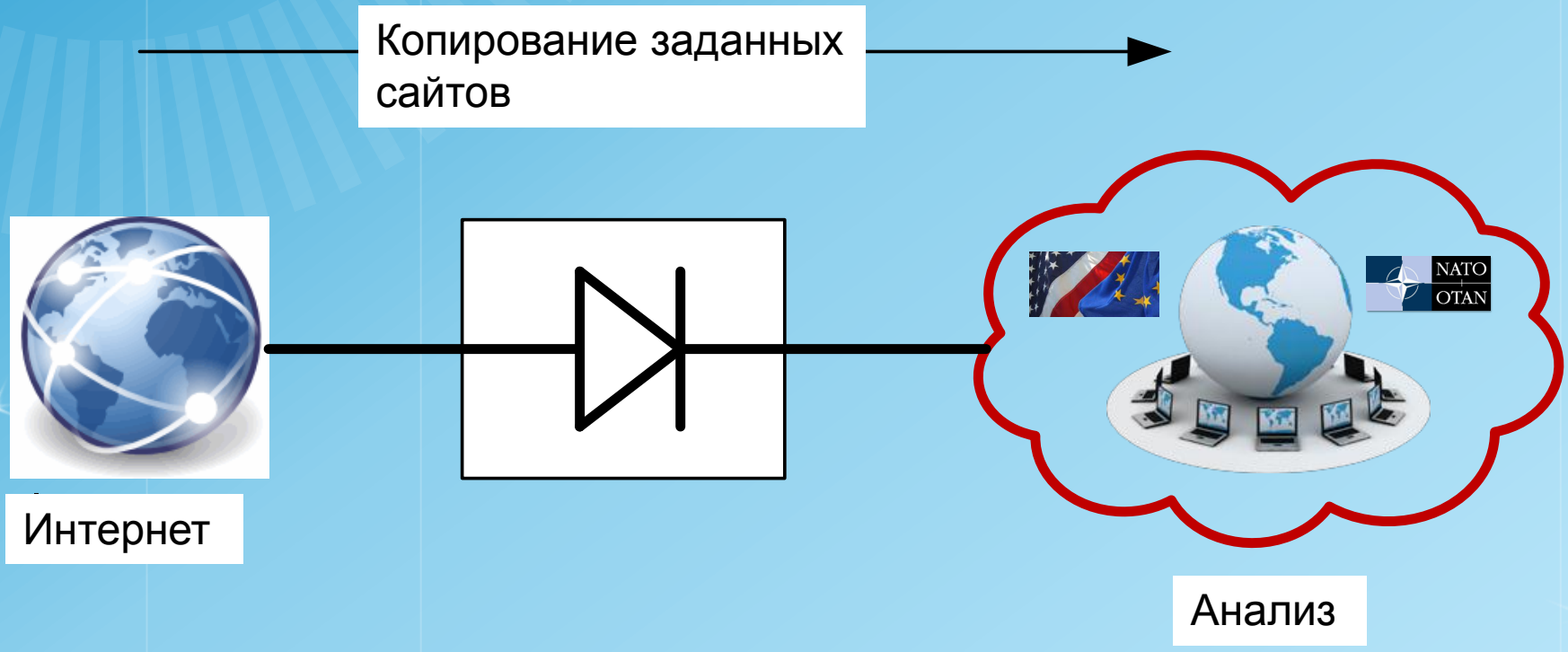
- Передача информации от партнеров по NATO
- И предотвращение доступа к информации в сетях партнеров



DataDiode

Пример: NATO

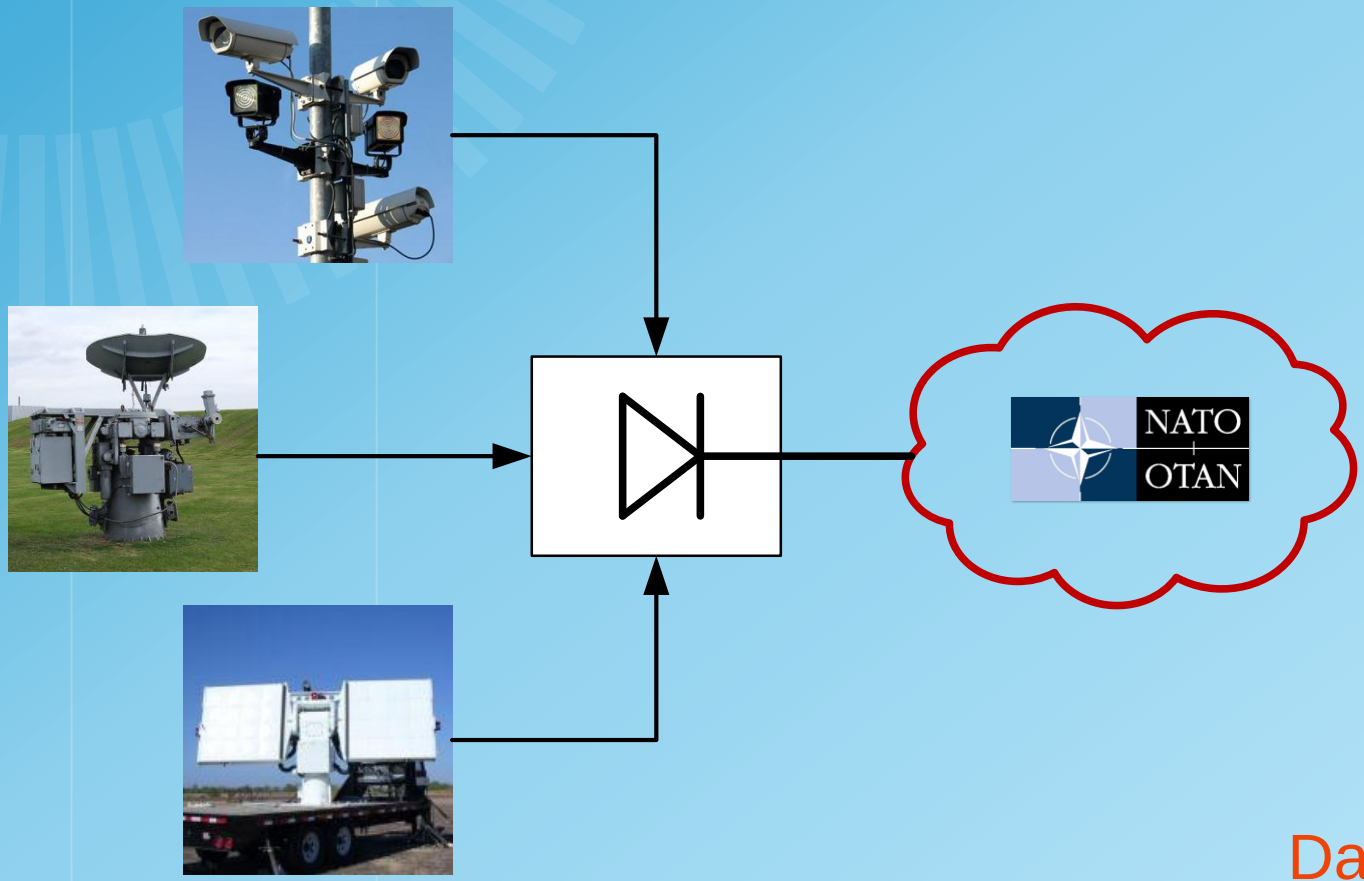
- Соединение защищенной сети с Интернетом и сбор информации 24/7



DataDiode

Пример: NATO

- Прием или передача сигналов с первичных датчиков, с гарантией невозможности воздействия на них по обратному каналу



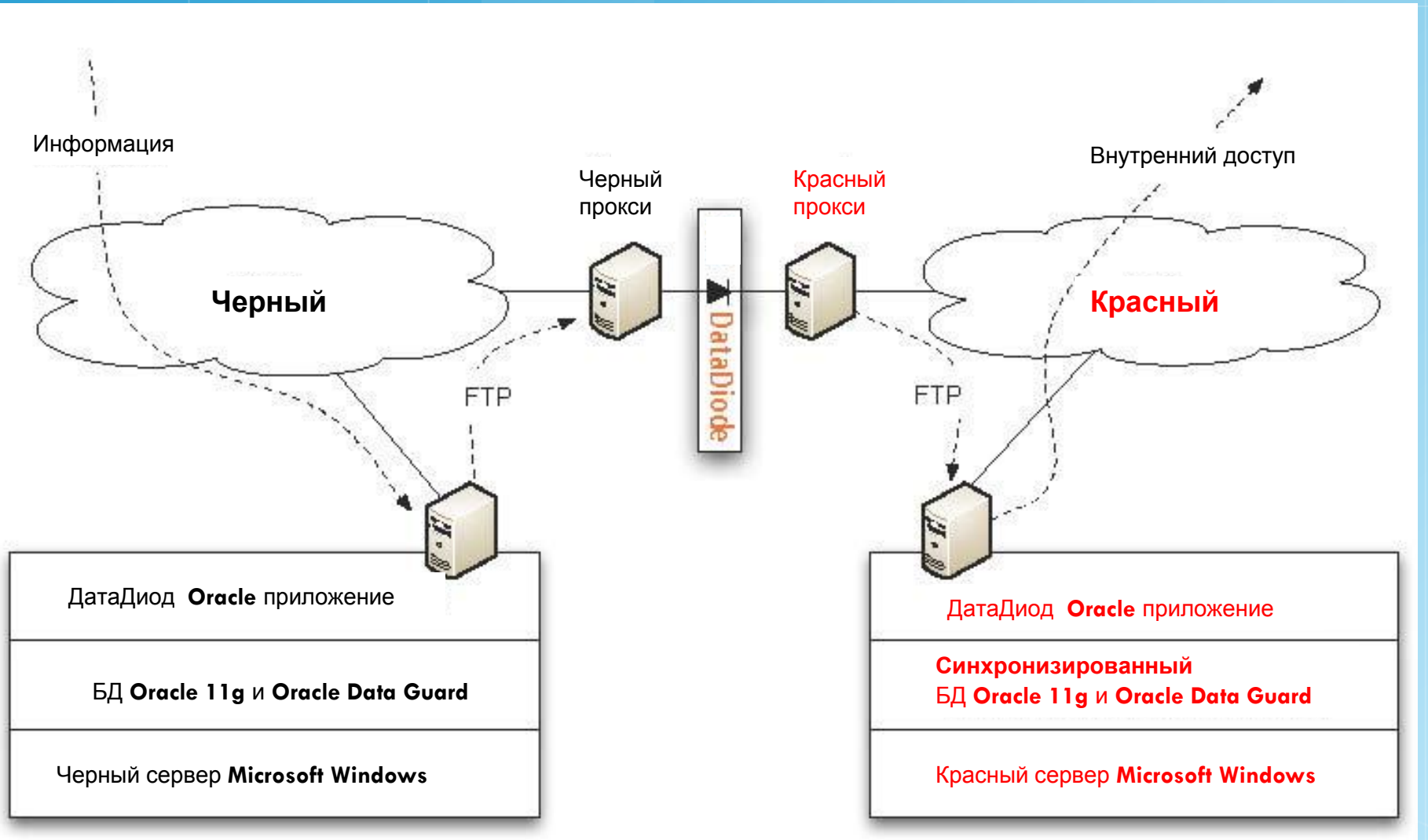
DataDiode

Пример: NATO

- Распределение информации во время совместных операций

DataDiode

Пример: BBC (Европа)



Пример: ВМФ (Европа)

Navy/
Air Force

DataDiode

ДатаДиод

Однонаправленное коммуникационное устройство:

- аппаратная реализация (нет ПО, прошивок)
- сертифицировано (CC EAL7+, NATO Secret, NERC, …)
- не может быть взломано

Много поддерживаемых протоколов

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

DataDiode

Спасибо за внимание!