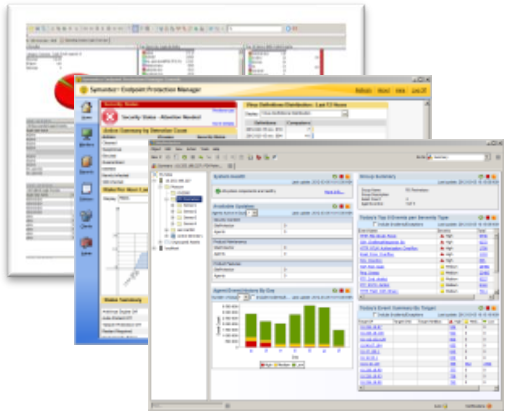
Быть лучше каждый день

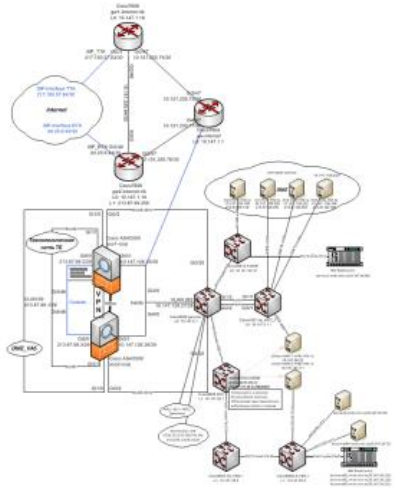
Более пяти лет – полет нормальный

Андрей Дугин
Начальник отдела обеспечения информационной безопасности
Руководитель SOC

Предпосылки



Большое количество критичных систем



Внедрение новых сервисов

Зависимость от поставщиков и аутсорсеров

МТС

Базовые меры по защите критичных систем:

- Архитектурно:
  - Выделение сегментов сети за firewall
  - Разнесение компонентов по сегментам с разными уровнями безопасности
- Протоколирование и анализ на внешних системах (SIEM):
  - Событий ОС/БД/ПО
  - Сессий firewall/VPN
  - Привязки IP-адреса ПК/VPN к пользователю
- Дополнительный контроль и аудит:
  - Сетевой доступ по принципу «default deny»
  - Аутентификация, авторизация и учет доступа в ОС/БД/ПО
  - Формализация доступов/работ
  - Анализ сетевого трафика
  - Генерация и обработка инцидентов ИБ в случае нарушений

Дополнительные меры контроля

Базовые меры не обеспечивают полный контроль:

- Использования недокументированных возможностей
- Отключения протоколирования (частично)
- Мошенничества
- Сокрытия истинных причин инцидентов (частично)

Требования к средству контроля

- Интеграция без существенной доработки критичных систем
- Масштабируемость
- Независимость от поставщика системы
- Контроль сессий управления
- Видеозапись и хранение терминальных сессий
- Поиск по вводимым командам
- Возможность контроля/запрета дополнительных функций:
  - Проброс дисков, принтеров (RDP, ICA)
  - SCP, SFTP (SSH)
  - Проброс портов (SSH)
- Возможность допуска к работе в «четыре руки»

Интеграционные требования

- Связность по IP с системами
- Изменение архитектуры доступа
- Изменение логики администрирования
- Не требуется доработка ПО/БД систем
- Закрытие прямого сетевого доступа
- Отсутствие простоя систем и потери управления

Терминальный сервер собственной сборки

Поколение 1:

- Hardened Windows
- Customized Putty
- ScreenAnytime
- Поддержка RDP, SSH

Транзитный терминальный сервер собственной сборки

Поколение 2:

- Customized Windows (shell = mstsc)
- ScreenAnytime
- Поддержка RDP

Транзитный терминальный сервер

Поколение 3:

- Balabit SCB
- Поддержка RDP, SSH, ICA (proxy)

Транзитный терминальный сервер

Дополнительные возможности:

- Дисциплинирование;
- Контроль SLA;
- Получение подробной хроники действий.

Дополнительные затраты:

- Выделение терминальных серверов для систем;
- Переобучение администраторов новой логике работы;
- Добавление новой точки отказа и этапа отладки.

Схема организации прямого доступа к системам

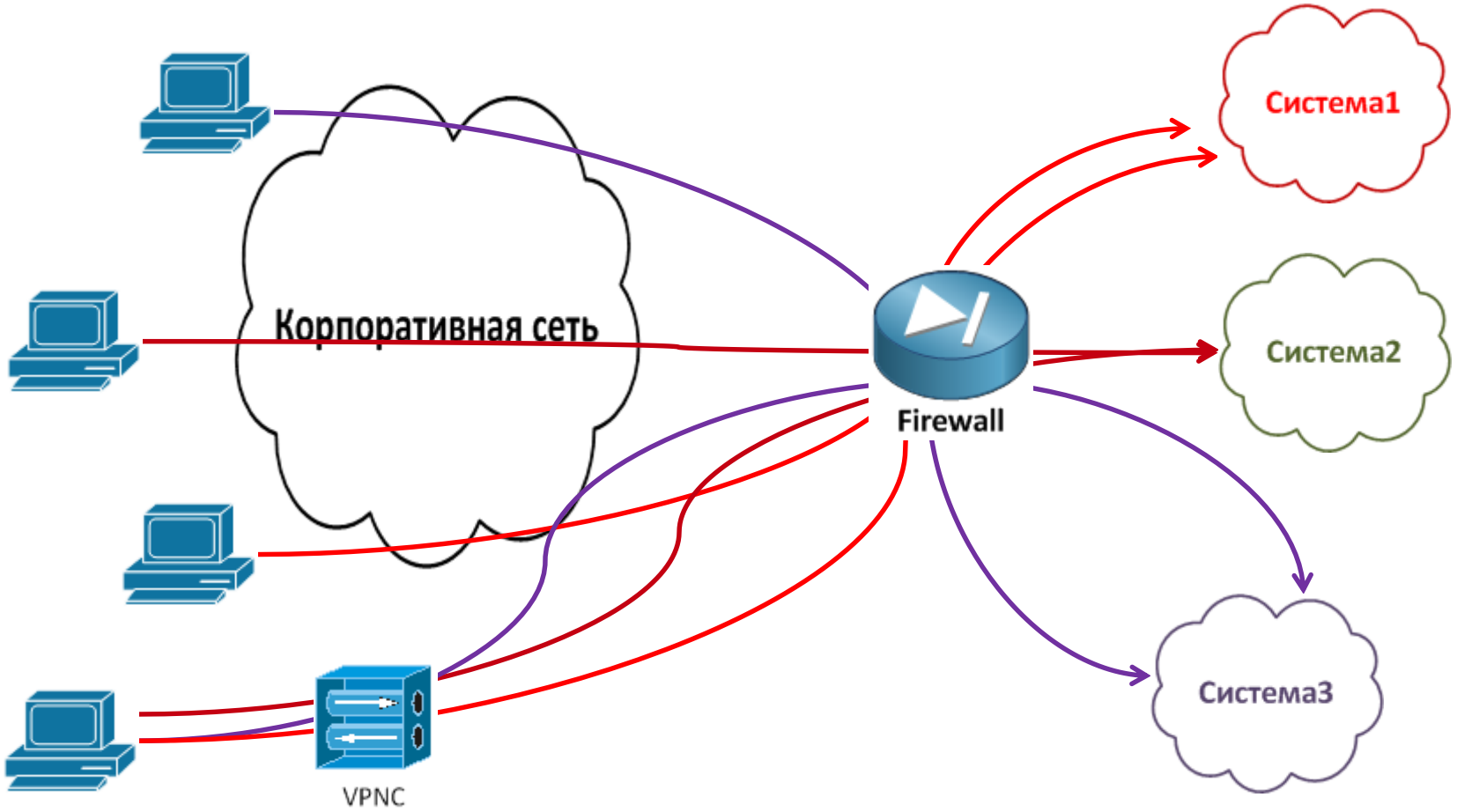
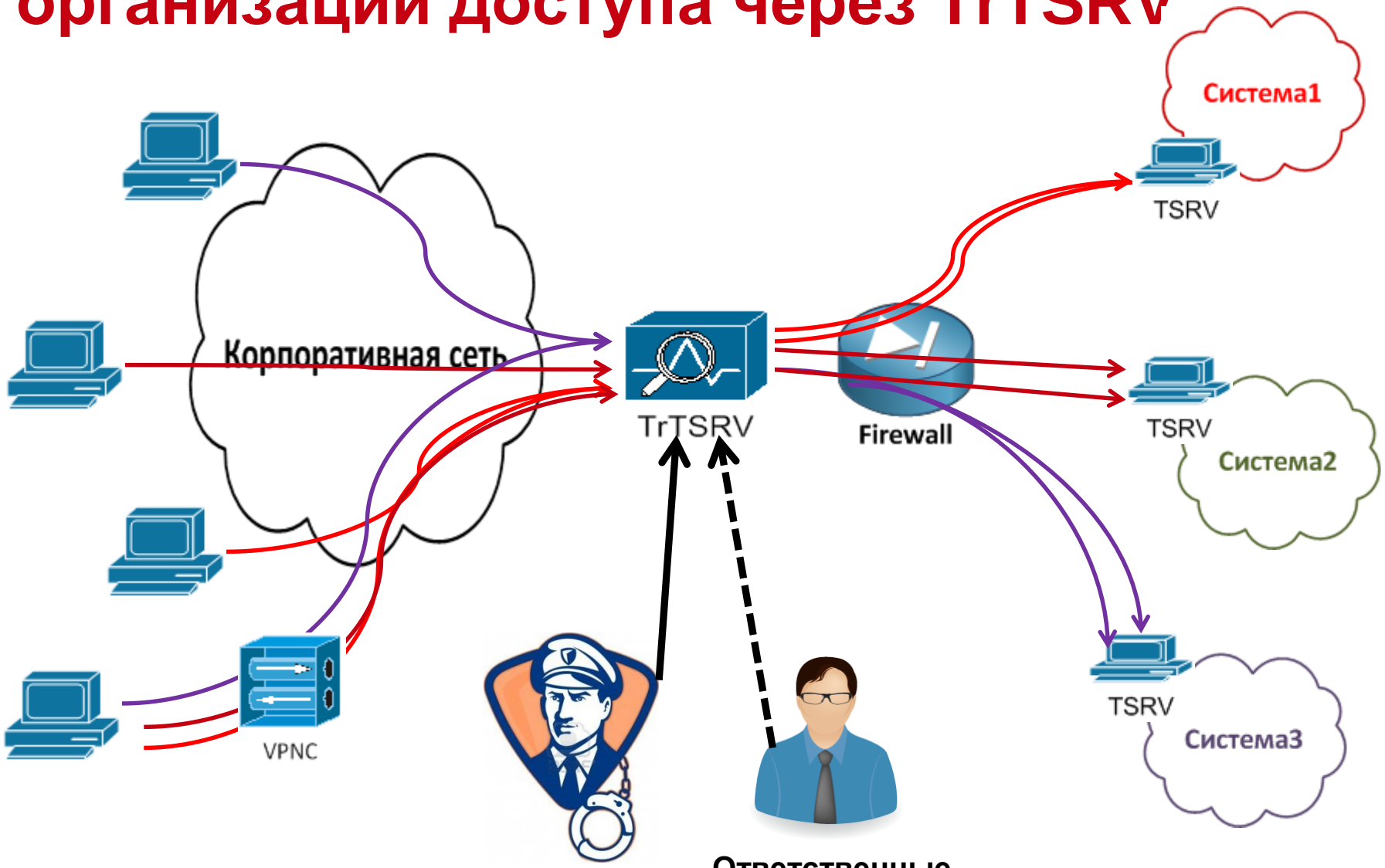


Схема организации доступа через TrTSRV



Транзитный терминальный сервер Balabit SCB

Схема работы:

- ПК/VPN → TrTSRV:port1 → TSRV_SYSTEM1:RDP
- ПК/VPN → TrTSRV:port2 → TSRV_SYSTEM2:SSH
- ПК/VPN → TrTSRV:port3 → TSRV_SYSTEM3:ICA

Порядок действий для безболезненного перехода:

- Выделение терминальных серверов на критичных системах
- Развертывание и настройка транзитного терминального сервера
- Открытие сетевого доступа ПК/VPN → TrTSRV и от TrTSRV к терминальным серверам бизнес-критичных систем
- Переобучение администраторов новой логике работы
- Тестирование и отладка взаимодействия по новой схеме
- Закрытие прямого сетевого доступа пользователей к критичным системам по управляющим протоколам
- Эксплуатация
- Контроль на SIEM подключения к терминальным серверам в обход TrTSRV

Balabit SCB – ложка дёгтя

- Проигрывание видеозаписей большого объема
- Ресурсоемкость индексации видеозаписей
- Синхронизация нод кластера N10K
- Смена интерфейсов кластера после обновления
- DoS полуоткрытыми сессиями mRemote
- Остановка модулей обработки RDP, SSH, ICA

Balabit SCB – интересные сценарии

- 1xvCPU vs 8xvCPU
- Техподдержка Balabit работает через Balabit
- Использование Balabit SCB в «Противостоянии» на PHDays