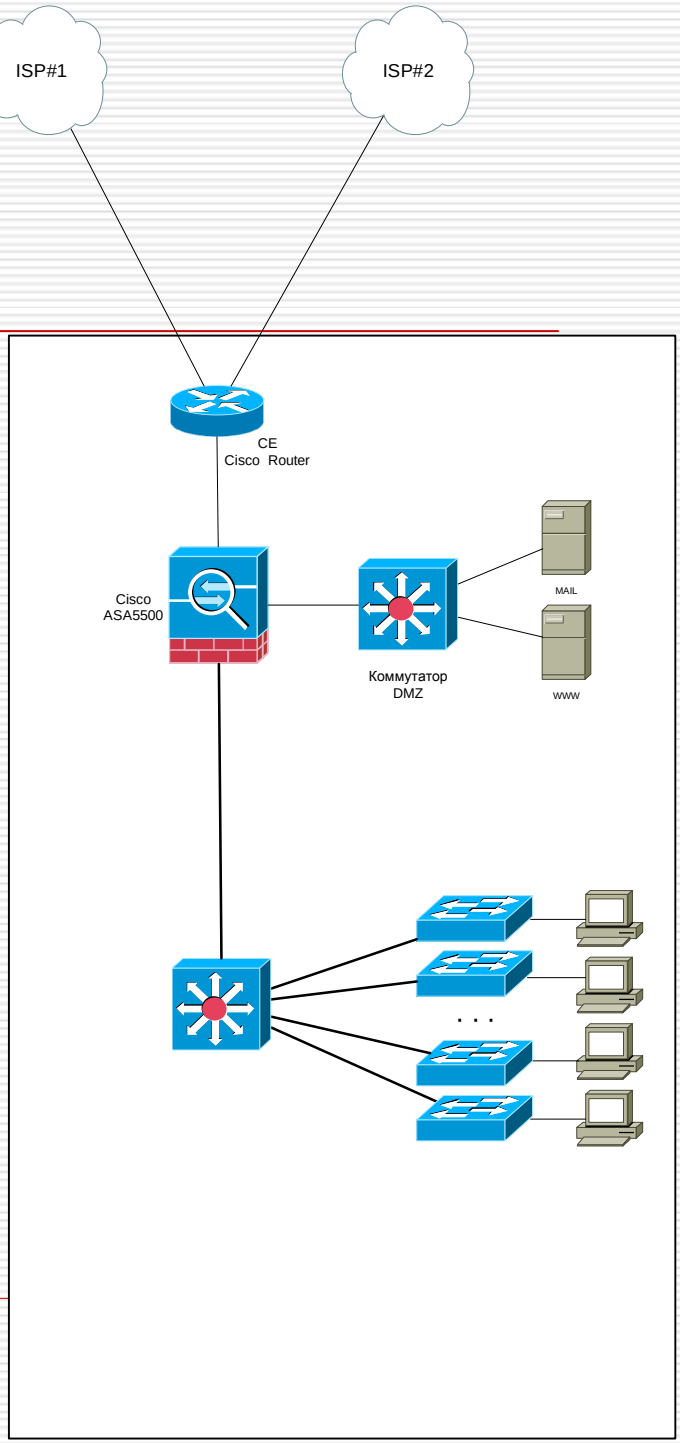
Cisco SDN

Решения **Cisc**о для обеспечения информационной безопасности ЛВС

Максим Краюшин
НетПроб
m.krayushin@net-probe.ru
+7 919 968 6404

Исходные данные

- ЛВС, в которой размещены рабочие станции пользователей
- Возможно наличие нескольких территориально разнесенных сегментов ЛВС
- Собственная **AS**
- Несколько подключений к Интернет **с BGP Multihoming**
- **DMZ** для размещения публичных сервисов: **e-mail, Web, DNS…**

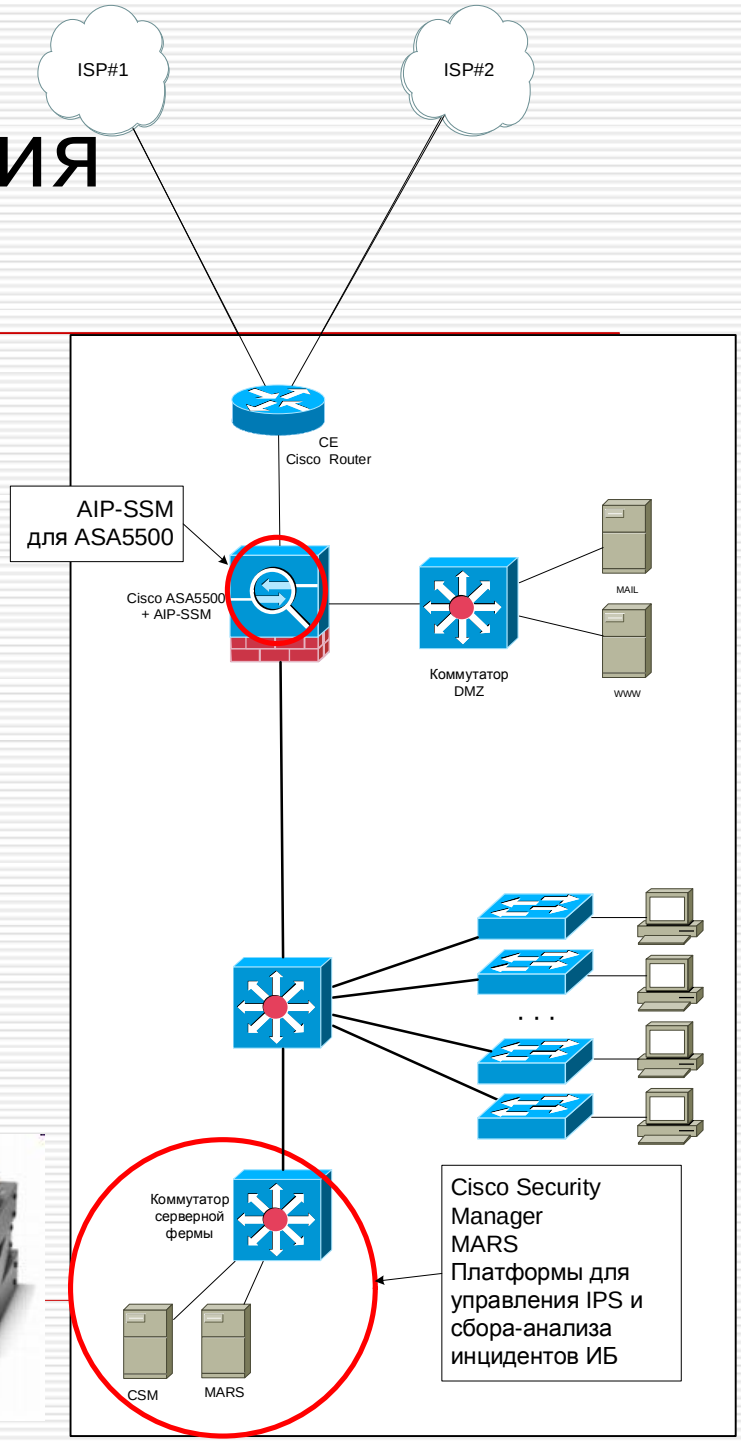


Задача: комплексная защита ЛВС

- Система предотвращения вторжений **(IPS)** в направлениях:
  - ЛВС-Интернет – сетевая и хостовая части **IPS**
  - **DMZ**-Интернет – сетевая и серверная части **IPS**
- Система контроля доступа в ЛВС
- Защита от **DDoS** на уровне оператора связи
- Контроль доступа пользователей к ресурсам **WEB (**фильтрация **URL)**
- Защита почтовых сообщений
- Система мониторинга и анализа событий безопасности
- Интеграция систем с контроллером домена

Система предотвращения вторжений **IPS**

- Интегрированное решение с **ASA5500**
- Реализуется на базе модуля **AIP-SSM,** обеспечивающих функционал **IPS** для двух **ASA5500**
- Аппаратное ускорение, не влияет на производительность **ASA**
- До **650 Mbps** для **SSM-40**
- Режим **bypass**
- Обнаружение большого спектра угроз
- Высокая точность обнаружения



IPS: обнаружение угроз

- Шпионское ПО
  - Контроль утечки
  - Блокирование **spyware** в сетевом трафике
- Сетевая разведка
- Черви, стетевые вирусы
- Анализ злоупотреблений на уровне протоколов
- Злоупотребления **P2P/IM**
- Троянцы
- Угрозы **VoIP**

IPS: множество методов обнаружения

- Обращение к существующим уязвимостям ПО
- Сигнатурный анализ
- Контроль протоколов
- Эвристические методы
- Обнаружение аномалий протоколов и потоков
  - Обучение
  - Контроль поведения
  - **zero-day**

IPS: качество и скорость

- Аккуратность и эффективность обнаружения
  - Рейтинг рисков
  - Рейтинг угроз
  - Корреляция событий
- Скорость реагирования
- Гибкость
  - Настройка сигнатур
  - Настройка реагирования
  - Пороги реагирования

IPS: Реагирование

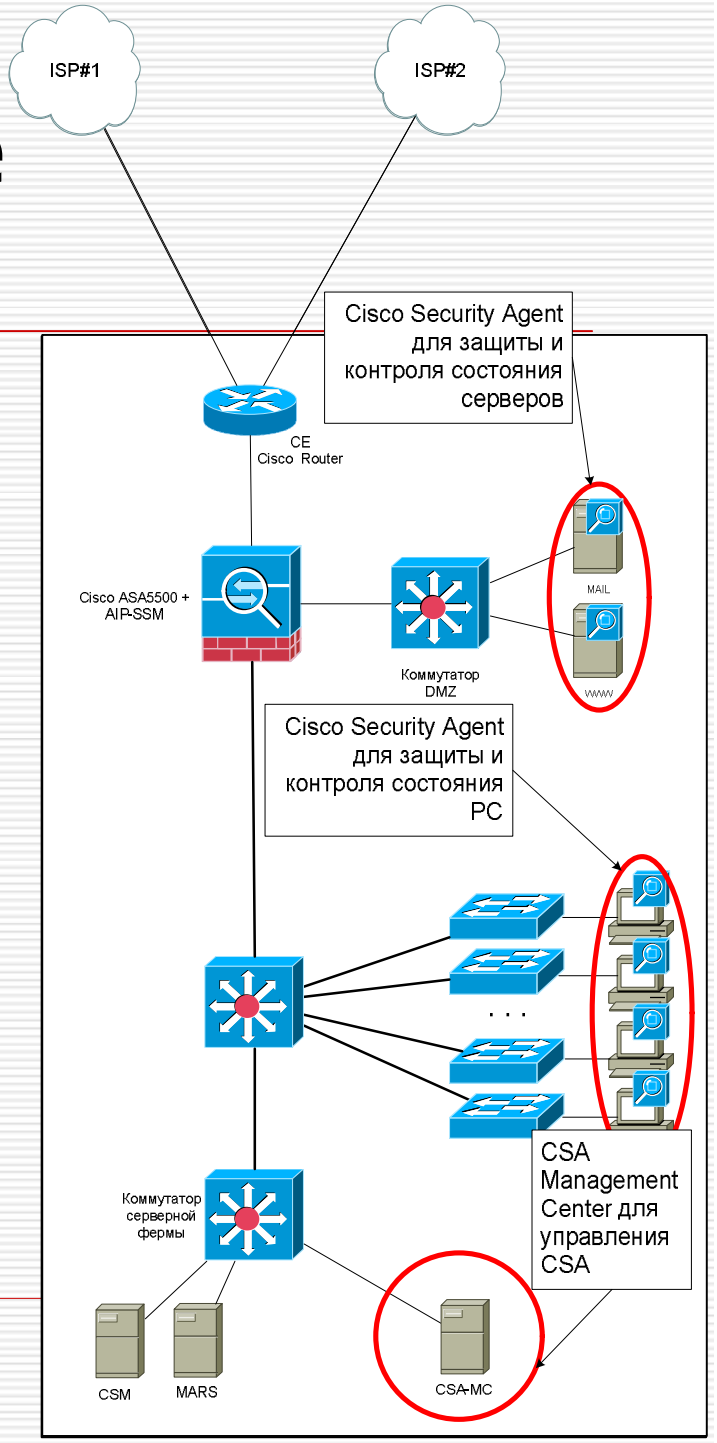
- Блокирование потоков, сервисов
- **ACL** на устройствах
- Завершение соединений
- Ограничение полосы
- Отключение портов
- Карантин

IPS: Контроль трафика

- туннелированный **IP in IP, GRE** трафик
- **MPLS**
- **802.1q**
- **IPv4** в **IPv6**
- анализ зашифрованного трафика

IPS: защита на уровне серверов

- Интеграция с **Cisco Security Agent (CSA)**
- Дополнительная информация об узле
  - ОС
  - Версии ПО
  - Установленное ПО, используемое ПО
  - Установленные патчи
  - И т.п.
- Дополнительная информация от **CSA** используется для выбора метода реагирования
- Корреляция событий на сети и серверах

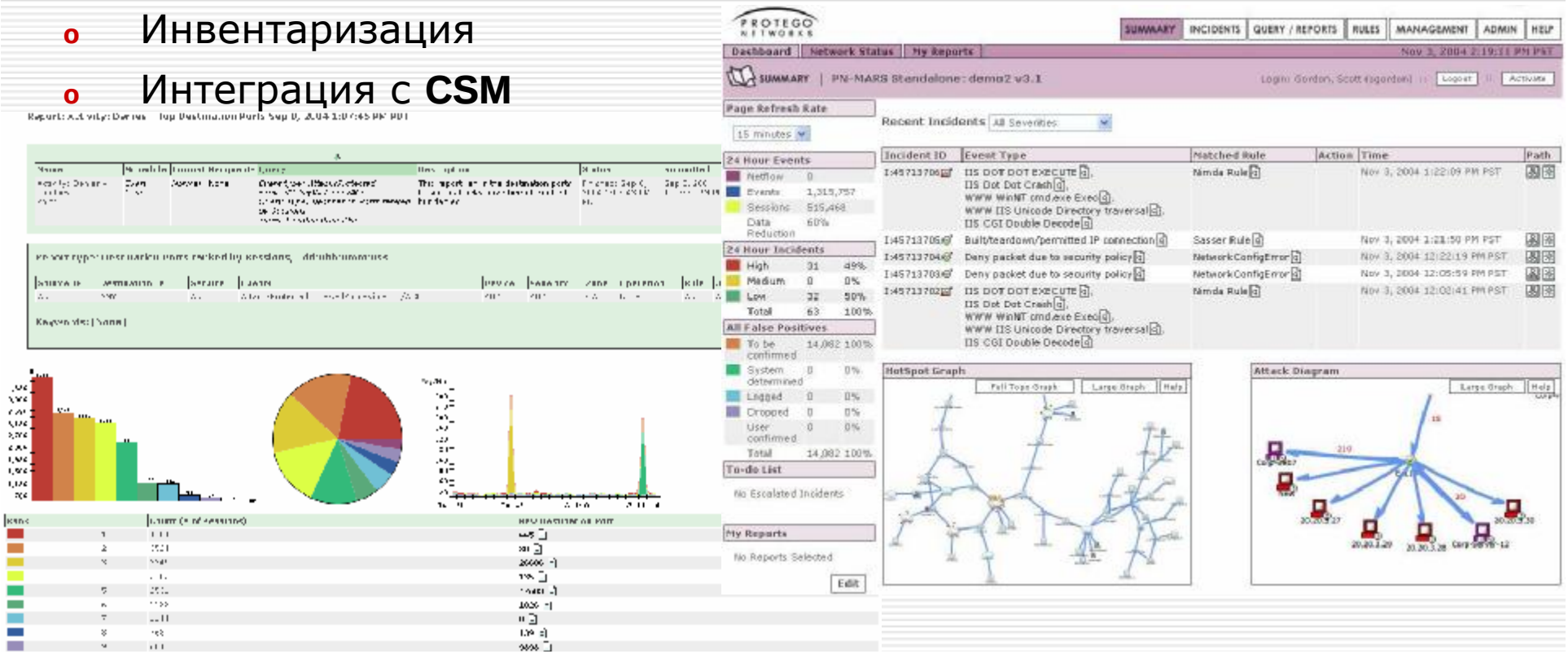


Система мониторинга и анализа событий безопасности

- **Cisco Security MARS**
- Мониторинг, анализ и реагирование на события ИБ
- Быстрая идентификация угроз
- Контекст топологии сети
- Корреляция событий

CS-MARS

- Множество поддерживаемых устройств
- Анализ и корреляция
- Визуализация инцидентов на карте
- Рекомендации и координация по отражению
- Инвентаризация
- Интеграция с **CSM**



IPS: управление

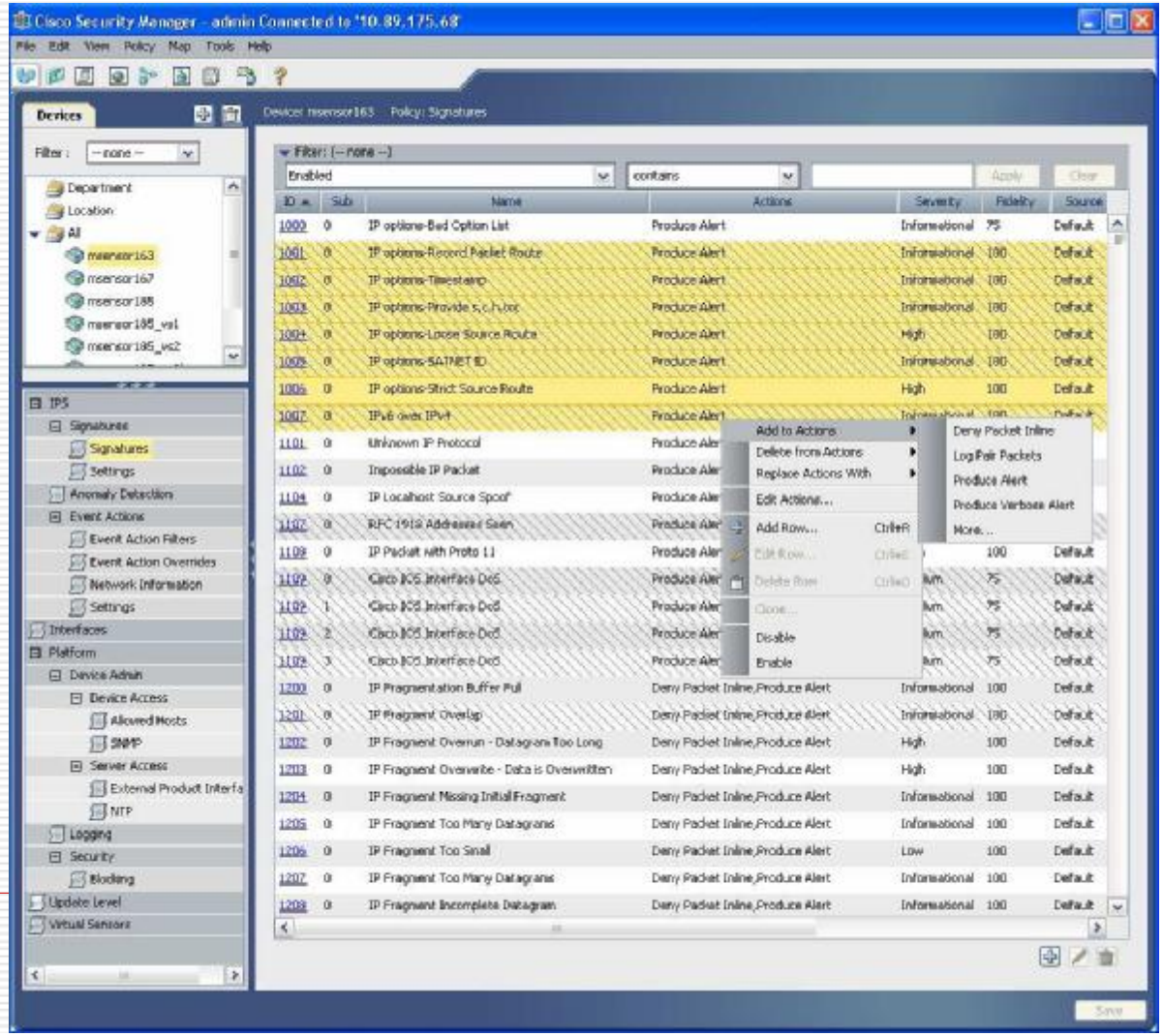
- Платформа **Cisco Security Manager (CSM)**
- Единое централизованное управление множеством **IPS, ASA, PIX**
- Управление на базе политик безопасности **FW, VPN** и **IPS**
- Распределенный **GUI**
- Эффективная визуализация

IPS: CSM

- Настройка, конфигурация, инвентаризация
  - Управление политиками
  - Анализ политик
  - Конфигурация устройств
  - Конфигурация групп
  - Автоматическое обновление **IPS**
  - Определение сигнатур

IPS: CSM: интерфейс

- Сортировка, скрытие столбцов
- Выбор множеств
- Связывание с действиями
- Фильтрация
- Клонирование
- Редактор сигнатур

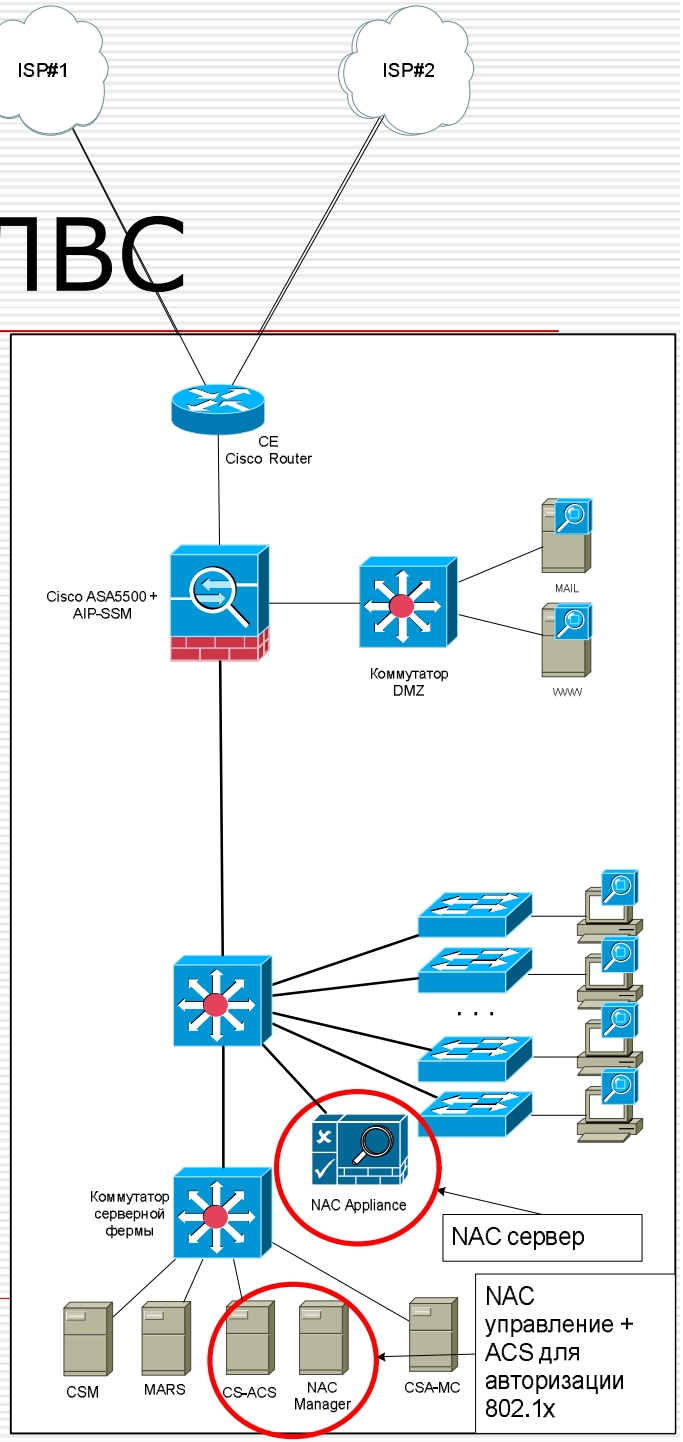


Cisco Services for IPS

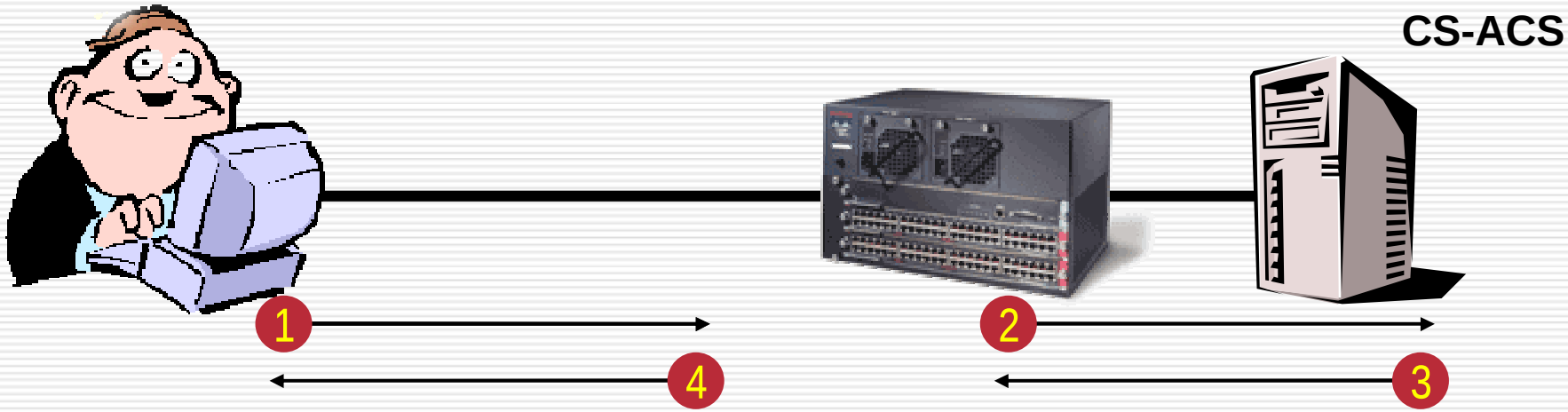
- Совместно с **TrendMicro**
- Обновление сигнатур и уведомления
- Обновление ПО
- Доступ **24**x**7**
- **Cisco IPS Alert Center**

Контроль доступа в ЛВС

- **802.1x** – контроль доступа к порту устройства, предоставляющего доступ к ресурсам сети (проводной, беспроводной, коммутируемой, широкополосной и т.д.)
- **Network Admission Control (NAC)** – контроль соответствия политики безопасности на рабочей станции (ПО, антивирусы, патчи и т.п.)



802.1x



1. Пользователь активирует линк
2. Коммутатор запрашиват **ACS** авторизацию доступа
3. **ACS** аутентифицирует пользователя и возвращает параметры доступа
4. Пользователь включается в сегмет ЛВС, права на доступ к которой у него есть

802.1x

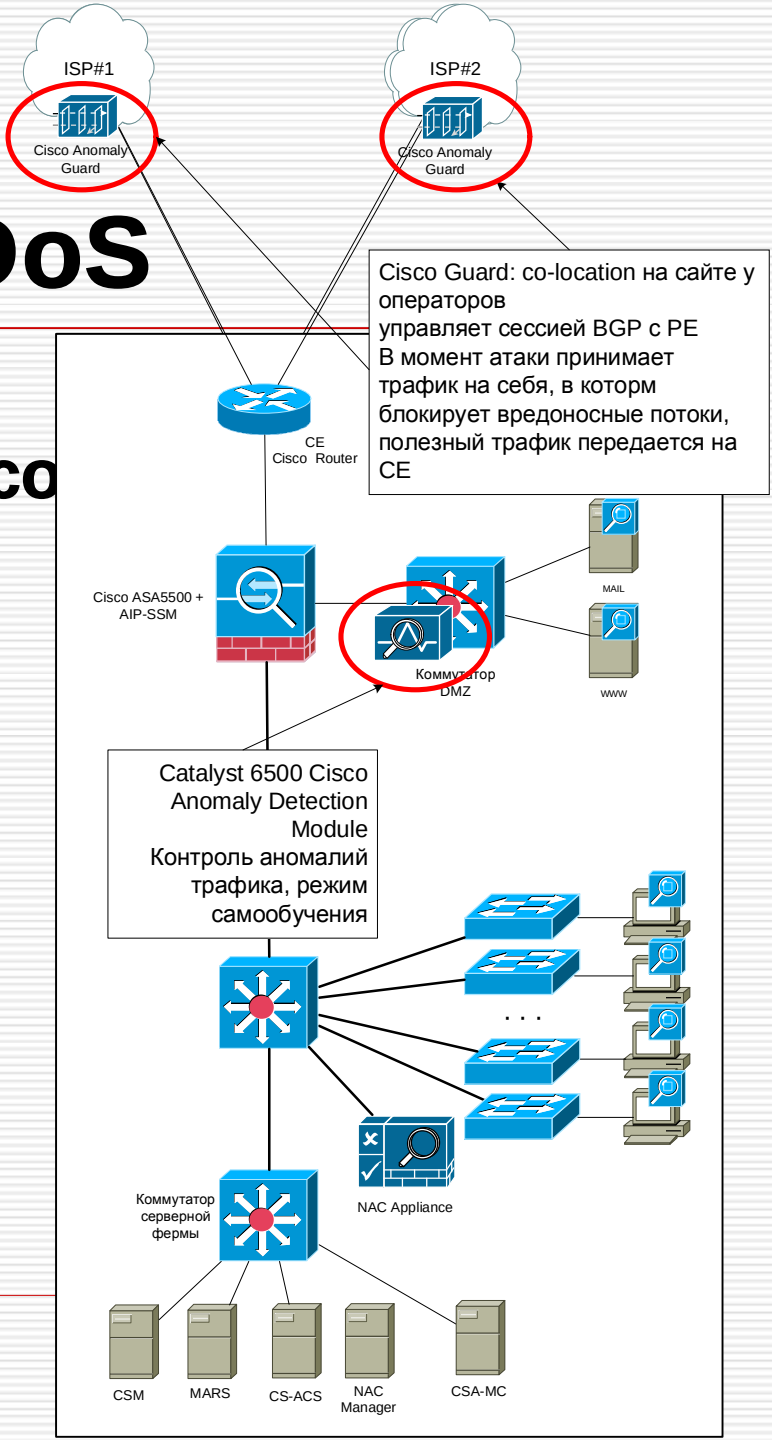
- Порт коммутатора с поддержкой **802.1x** ассоциируется с двумя виртуальными точками доступа
  - для авторизации
  - для авторизованных пользователей
  - Неавторизованных пользователей можно включить в гостевой **VLAN** имеющий доступ только к Интернет

Network Admission Control (NAC)

- Обеспечение соответсвия конфигурации клиентского ПК политике безопасности сети
- Прозрачность для пользователя
- Поддержка **802.1x**
- Агентское ПО под **Windows, Linux, Solaris**
- Помещение несоответствующего узла в карантинную сеть

Защита от **DoS & DDoS**

- Решение на базе **Cisco Guard** и **Catalyst 6500 Cisco Anomaly Detection Module**
- Защита от **DoS** и **DDoS** на уровне оператора связи
- В качестве детекторов атаки используются **IPS** и **Anomaly Detection,** размещенные в ЛВС
- **Guard** размещается на сайте у оператора на **co-location**



Защита от **DoS & DDoS**

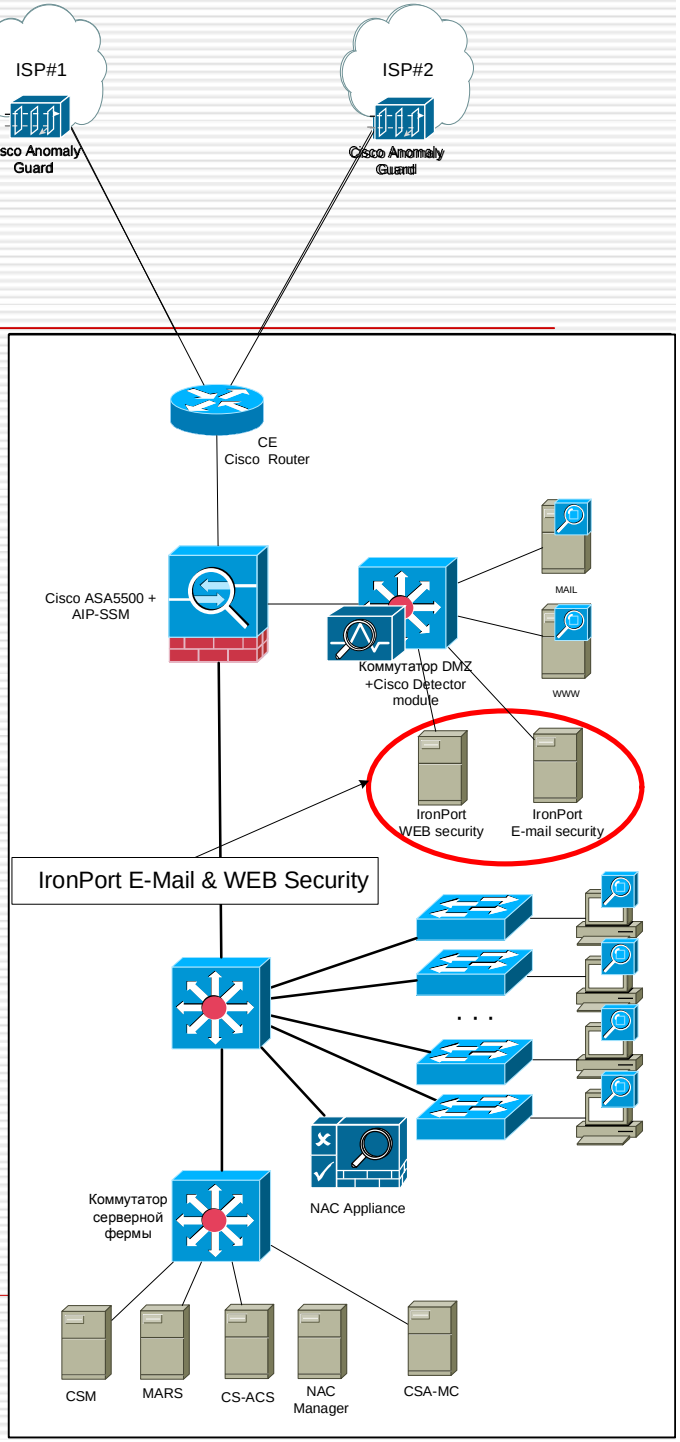
- **Guard** управляет сессией **BGP** с **PE** оператора
- В штатном режиме трафик маршрутизируется напрямую на **CE,** минуя **Guard**
- В момент атаки трафик направляется на **Guard. Guard** блокирует вредоносные потоки**,** полезный трафик передается на **CE.**

Защита от **DoS & DDoS**

- В нормальных условиях **(**отсутствие атак**)** не влияет на производительность защищаемой сети
- **3 Gbps; 1**мс**; 4,5M** одновременных сессий**;** защита от одновременной атаки**,** исходящей до **100K** узлов
- Защита от **DDoS** на **IP** телефонию
- Самообучающийся режим с профилированием трафика
- Поддержка множества зон безопасности

Защита **WEB & e-mail**

- Реализуется на базе продуктов **IronPort**
- **Web Security Appliance**
- **E-mail Security Appliance**



Контроль доступа к **WEB** с **IronPort Web Security Appliance**

- Защита **WEB-**трафика от вредоносного кода **(**вирусов**,** червей**)**
- Аудит и контроль обращений к **WEB** ресурсам
- **100M TCP** соединений**, 1Gbps**
- Категоризированная база **URL**
- Интеграция с **LDAP, AD**
- Система отчетов
- Может работать как **proxy,** прозрачный коммутатор или по **WCCP**

Защита электронной почты с **IronPort E-mail Security Appliance**

- Защита от спама, фишинга **(SenderBase, Reputation filters)**
- Отражение вирусов, червей **(McAffe, Sophos)**
- Применение политик (вложения, шифрование)
- Аутентификация почты
- Обеспечение целостности и конфиденциальности, защита от подмены сообщений
- Интеграция в инфраструктуру **LDAP** в т.ч. **Active Directory**
- Автоматические обновления вирусных баз, антиспам-правил

Свяжитесь с нами

- Компания ООО «НетПроб»
  - **http://www.net-probe.ru**
  - **info@net-probe.ru**
  - **+7 (495) 253 60 33**