Федеральное государственное унитарное предприятие
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР «АТЛАС»

название изделия

Система обнаружения сетевых атак программно-аппаратный комплекс «Тор»

назначение, область применения

Программно-аппаратный комплекс «Тор» предназначен для обнаружения сетевых компьютерных атак на компоненты информационной системы, а также для мониторинга соблюдения политики безопасности внутренней сети (Сертификат соответствия ФСБ России – СФ/129-1818 от 01.05.2012).

ПАК "Тор" позволяет выявлять подозрительные действия, которые могут нанести вред наиболее критичным компонентам информационной системы — операционным системам и приложениям, реализующим сетевые сервисы информационной системы.

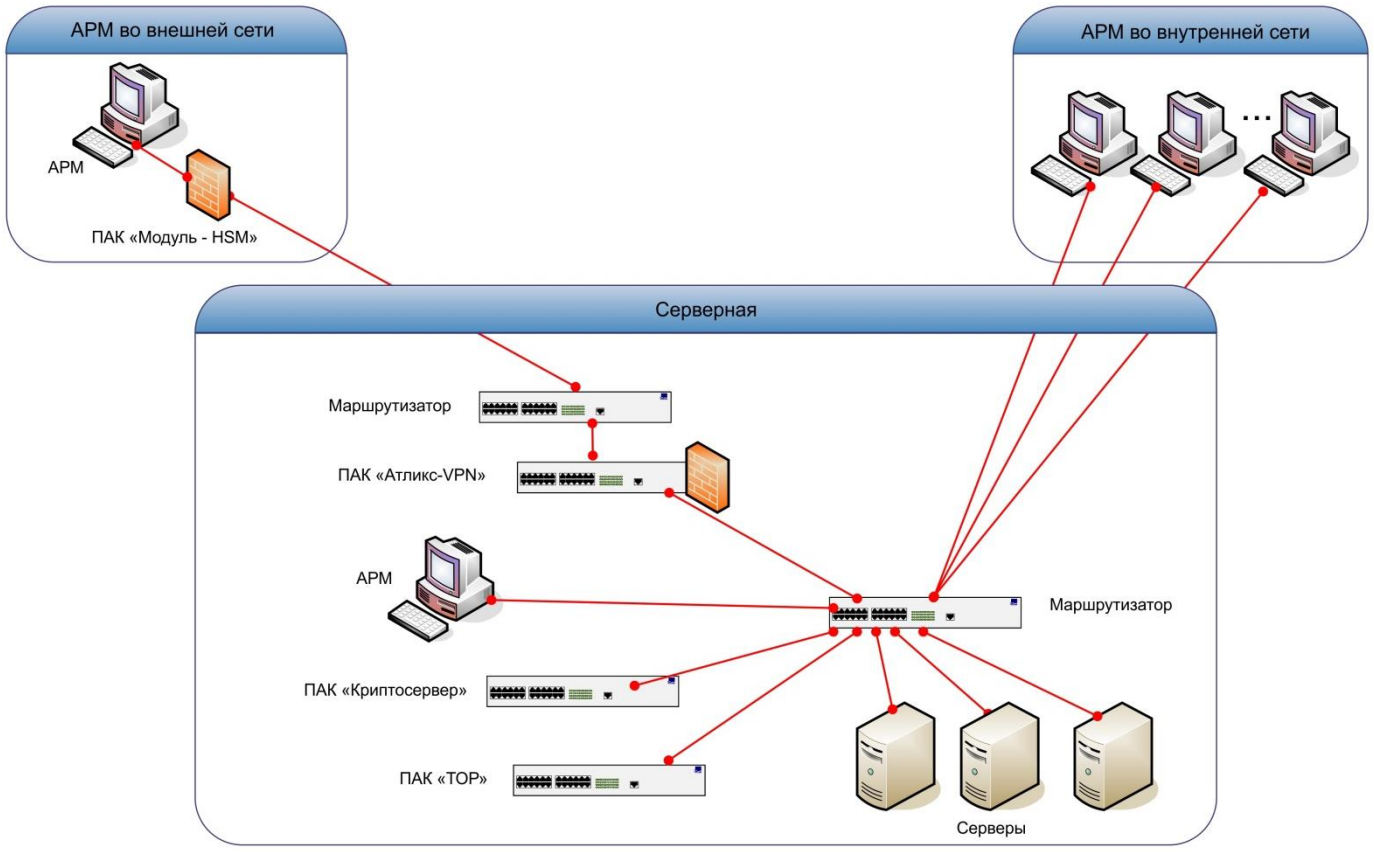
Отличительной особенностью ПАК «Тор» как средства обнаружения атак является реализация функций мониторинга соблюдения политики безопасности внутренней сети информационной системы, что обеспечивает его эффективное применение для корпоративных информационных систем.

Областью применения ПАК «Тор» является область информационной безопасности компьютерных сетей. Изделие предназначено для использования в автоматизированных информационных системах органов государственного управления и других организаций Российской Федерации, обрабатывающих сведения, составляющие конфиденциальную информацию.

Целевая функция ПАК «Тор» заключается в автоматическом выявлении воздействий на контролируемую им АИС, которые могут быть классифицированы как сетевые компьютерные атаки, а также для мониторинга соблюдения политики безопасности внутренней сети.

ПАК «Тор» – как система обнаружения атак, по способу сбора информации относится к сетевым СОА, по способу выявления опасных воздействий – к системам обнаружения сигнатур (используется метод сигнатурного анализа сетевого трафика).

ПАК «Тор» встраивается в информационную сеть (см. рисунок) и становится частью комплексной системы ее информационной безопасности.



ПАК «Тор» удовлетворяет стандартам: IEEE 802.2 (Logical Link Control); IEEE 802.3 (CSMA/CD, 10Base-T); 802.3u (1000Base-TX); EIA RS-310-C (монтаж в стойку).

Управление ПАК «Тор», а также его мониторинг осуществляются с консоли управления или удаленно из единого центра безопасности распределенной информационной системы.

В качестве консоли управления может использоваться ПЭВМ, подключенная к ПАК «Тор» одним из следующих способов:

- локально – через COM-порт;
- удаленно при помощи защищенного протокола администрирования.

Подключение консоли управления к порту локального управления ПАК «Тор» (последовательному асинхронному COM-порту), осуществляется через нуль-модемный кабель. Последовательный асинхронный порт соответствует стандарту EIA RS-232C (DTE-DCE).

ПАК «Тор» обеспечивает:

- сбор данных аудита и параметров функционирования средств, функционирующих в контролируемом сегменте;
- выявление воздействий на контролируемый сегмент IP-сети и факты нарушения (попыток нарушения) политики безопасности на основе анализа сетевого трафика и сканирования контролируемых хостов IP-сети с использованием баз данных сигнатур компьютерных атак и шаблонов штатного функционирования контролируемого сегмента IP-сети;
- сканирование хостов контролируемого сегмента IP-сети (задается администратором) и выявление:
  - Функционирования несанкционированных служб (демонов);
  - Отклонений от штатных режимов работы серверов;
- перехват сетевого трафика контролируемого сегмента IP-сети (задается администратором) и выявление:
  - Появления несанкционированных хостов или шлюзов в другие сегменты;
  - Использования несанкционированных протоколов взаимодействия и/или портов;
  - Отклонений от штатных режимов работы пользователей (клиентов).
- реализацию механизмов аутентификации и авторизации пользователей СОА;
- возможность выполнения локального и удалённого обновления программного обеспечения СОА;
- возможность выполнения локального и удалённого обновления базы данных сигнатур компьютерных атак;
- контроль целостности программной части и конфигурации;
- уведомление администратора сети о наступлении заданного множества событий, определяемых шаблонами анализа первичных данных о работе контролируемого сегмента;
- синхронизацию собственного системного времени с общим источником единого времени с использованием сетевого протокола Network Time Protocol (NTP);
- настройку выборочного контроля ресурсов АИС на уровне отдельных объектов сети (ПЭВМ, активное сетевое оборудование).

контакты

127018, г. Москва, ул. Образцова, 38
телефон: (495) 689-14-64
e-mail: info@stcnet.ru
http://web.stcnet.ru