SafeTechnologies

SafeRoute

Программно-технический комплекс защиты управления и мониторинга сетевого оборудования

В настоящее время базовые методы защиты телекоммуникационного оборудования успешно реализуются и на первый план выходят угрозы, связанные с недекларированными возможностями самого оборудования и программного обеспечения, а также несанкционированными действиями внутренних нарушителей, то есть сотрудников, которым принято доверять (администраторы, операторы, инженеры). Кроме того, к управлению телекоммуникационным оборудованием зачастую привлекаются аутсорсинговые компании (в том числе иностранные), что повышает риски неконтролируемого изменения конфигурации сетей и создает потенциальные угрозы утечки информации ограниченного доступа.

Компании «НИИ СОКБ» и «Национальный Инновационный Центр» предлагают российским заказчикам программно-технический комплекс SafeRoute, предоставляющий возможность централизованного управления, мониторинга телекоммуникационного оборудования в интересах обеспечения устойчивости его функционирования, а также обеспечение защиты от несанкционированного доступа к нему.

Назначение системы SafeRoute

Программно-технический комплекс SafeRoute разработан с целью предоставления заказчикам возможностей централизованного управления, мониторинга телекоммуникационного оборудования в интересах обеспечения устойчивости его функционирования, а также обеспечение защиты от несанкционированного доступа к оборудованию.

Решение SafeRoute обеспечивает:

- снижение рисков от атак на телекоммуникационное оборудование, связанных с получением несанкционированного доступа к нему и средствам управления им;
- сокращение времени, требуемого на восстановление корректной работоспособности телекоммуникационного оборудования при авариях или ошибках персонала;
- обеспечение устойчивости функционирования телекоммуникационного оборудования.

Программно-технический комплекс SafeRoute представляет собой серийно выпускаемый продукт, предназначенный для эксплуатации в структурных подразделениях, ответственных за развитие и эксплуатацию ИТ-инфраструктуры, а также подразделениях, отвечающих за обеспечение информационной безопасности в организации.

Операторы связи могут использовать программно-технический комплекс SafeRoute как основное средство защиты информации, обеспечивающее устойчивость функционирования сети связи и защищающее телекоммуникационного оборудования от несанкционированного доступа.

Задачи, решаемые с помощью системы SafeRoute

Программно-технический комплекс SafeRoute предназначен для решения следующих задач:

1. обеспечение доверенной загрузки телекоммуникационного оборудования;

2. защита от несанкционированного подключения к портам управления, включая консольные порты телекоммуникационного оборудования;

3. реализация механизма безопасного Outbound-управления телекоммуникационным оборудованием;

4. сбор и передача информации о конфигурации телекоммуникационного оборудования и ее изменениях во внешние системы мониторинга его состояния;

5. удаленное управление политиками информационной безопасности и авторизацией администраторов и операторов на телекоммуникационном оборудовании;

6. сбор и корреляция событий информационной безопасности, связанных с эксплуатацией телекоммуникационного оборудования;

7. контроль действий администраторов и операторов телекоммуникационного оборудования.

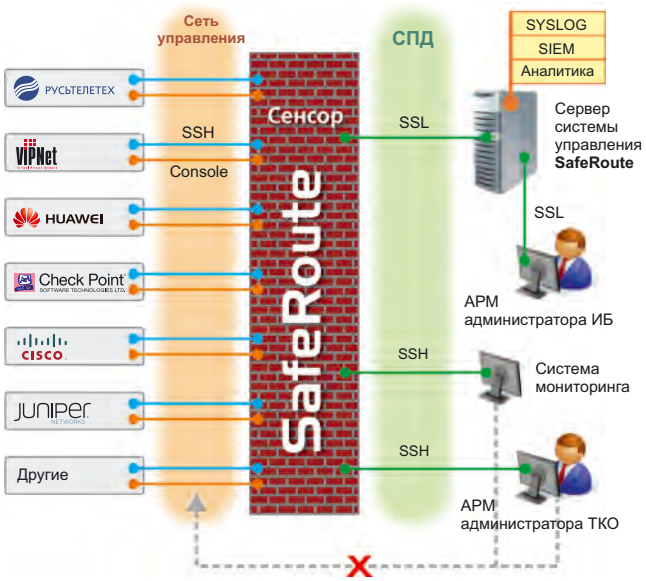
Уникальная особенность, выгодно отличающая программно-технический комплекс SafeRoute от аналогов, — это ее отечественная разработка, а также реализация в программно-аппаратном исполнении, что позволяет контролировать порты управления на физическом уровне. SafeRoute реализован в виде специализированного модуля, устанавливаемого непосредственно в телекоммуникационное оборудование, кроме этого имеется исполнение в виде самостоятельного устройства, которое позволяет контролировать сразу несколько единиц оборудования.

Архитектура и возможности использования SafeRoute

В программно-техническом комплексе SafeRoute субъектами доступа являются инженеры и операторы, эксплуатирующие телекоммуникационное оборудование, а также администраторы, управляющие самим SafeRoute. Объектами доступа являются телекоммуникационное оборудование.

Субъекты доступа по отношению к телекоммуникационному оборудованию разграничиваются:

- конкретным оборудованием или группой единиц оборудования, к которым могут иметь доступ;
- IP-адресом, с которого разрешено удаленное управление;



- типом доступа на телекоммуникационное оборудование: удаленный по протоколу SSH или локальный по консольному порту;
- перечнем команд, которые могут выполняться от имени субъекта.

Данные ограничения позволяют каждой группе телекоммуникационного оборудования присвоить одну или несколько групп пользователей. В свою очередь, группа пользователей формируется из инженеров и операторов, которые имеют схожие ограничения по работе с оборудованием, а именно: тип доступа (по SSH, с консоли), перечень выполняемых команд и могут подключаться к оборудованию только из конкретной сети.

Программно-технический комплекс SafeRoute может использоваться либо автономно, либо в рамках системы управления сетью.

При автономном использовании групповая политика реализуется встроенными механизмами операционной системы SafeRoute. Пользователю ставится в соответствие IP-адреса, с которого разрешено удаленное управление, список команд, которые ему разрешены и типы доступа (по SSH, с консоли).

Групповая политика в рамках системы управления сетью реализуется централизовано средствами сервера управления SafeRoute, сервера аутентификации, использующему протокол RADIUS. В рамках использования RADIUS реализуется двухфакторная аутентификация. Групповые политики хранятся на сервере SafeRoute, на каждом модуле могут храниться локальные настройки, которые являются копией центральной базы данных групповых политик. В случае подключения комплекса SafeRoute к портам управления оборудованием появляется возможность контролировать подключенные порты как на предмет несанкционированного подключения к ним, так и на предмет запуска и исполнения команд, которые через них передаются на оборудование. Кроме этого имеется возможность контролировать изменения конфигурационного файла, обеспечивается возможность двухфакторной аутентификации инженера и администратора, управляющего телекоммуникационным оборудованием, а также доверенная загрузка оборудования.

Основные функции системы SafeRoute:

- централизация управления телекоммуникационным оборудованием на узлах связи с аутентификацией администраторов и сетевых операторов на устройстве;
- контроль несанкционированного отключения (подключения) кабелей от (к) консольных портов(-ам) управления оборудованием связи;
- контроль конфигурации оборудования путем сравнения конфигурационного файла с эталонным образом, с возможностью принудительного восстановления рабочей конфигурации, то есть обеспечения целостности конфигурации;
- защита самого программно-технического комплекса SafeRoute, реализуемая подсистемой управления доступом, регистрацией и протоколированием всех действий пользователей (в том числе привилегированных);
- запрет ввода неразрешенных для данного пользователя команд управления телекоммуникационным оборудованием.

Сценарии использования SafeRoute:

1. Обеспечение контролируемого управления оборудования аутсорсинговыми организациями. Реализуется посредством развертывания специализированного узла доступа администраторов сервисной компании в сеть заказчика. Узел оснащается средствами SafeRoute, разрабатывается политика доступа, которая позволяет для части администраторов ограничить возможность исполнения только разрешенных команд, а для отдельных администраторов запретить исполнение определенного списка команд.

2. Организация доверенного Outband-канала управления сетью. Реализуется посредством установки средств SafeRoute на узлах сети, объединением их в единую выделенную сеть и обеспечение доступа администраторов к оборудованию только через эту сеть. Обеспечивается полный контроль действий администраторов, порты управления контролируются на физическом уровне.

3. Защита конкретного оборудования. Реализуется за счет установки в телекоммуникационное оборудование специализированного модуля SafeRoute, который обеспечивает доверенный доступ к «каналу управления». Управление оборудование минуя SafeRoute блокируется.