TrustAccess

Сертифицированная защита ключевых ресурсов локальной сети

TrustAccess – распределенный межсетевой экран высокого класса защиты с централизованным управлением и мониторингом.

- **Обеспечивает защиту конфиденциальной информации и персональных данных в соответствии с № 152-ФЗ.**
- **Позволяет сегментировать ИСПДн для снижения стоимости защиты персональных данных.**
- **Защищает серверы и АРМ от внешнихи внутренних сетевых угроз.**
- **Разграничивает сетевой доступ к информационным системам на основе должностей или уровней допуска пользователей.**
- **Защищает терминальные соединения и виртуальные машины.**

Назначение

- **Защита серверов и рабочих станций локальной сети от несанкционированного доступа.**
- **Разграничение сетевого доступа к информационным системам предприятия.**
- **Сегментация АС/ИСПДн.**

Достоинства

- **Наличие сертификата ФСТЭК МЭ 2/НДВ 4.**
- **Простота внедрения и удобство использования.**
- **Усиленная аутентификация пользователей и компьютеров.**
- **Широкий диапазон настроек правил фильтрации.**
- **Централизованное управление.**
- **Централизованный аудит событий ИБ.**
- **Интеграция с Secret Net 7 (сетевой вариант).**

Совместимо с Windows 7

Works with Windows Server 2008 R2

vmware READY

Код безопасности

ГК «Информзащита»

TrustAccess

Сертифицированная защита ключевых ресурсов локальной сети

Сертификат ФСТЭК России уровня МЭ 2/НДВ 4 позволяет использовать продукт для защиты автоматизированных систем до класса 1Г включительно (конфиденциальной информации с грифом «для служебного пользования») и ИСПДн всех классов до К1 включительно.

Функциональные возможности

Аутентификация сетевых соединений

Используется механизм двусторонней аутентификации пользователей и компьютеров, основанный на протоколе Kerberos. Механизмы защищены от прослушивания, попыток подбора и перехвата паролей. Для повышения эффективности процедуры аутентификации пользователей могут применяться eToken или iButton.

Фильтрация сетевых соединений

Правила фильтрации TrustAccess обладают широким диапазоном настроек. Сетевые соединения можно ограничивать на уровне служебных протоколов, периодов времени, пользователей или групп пользователей, параметров прикладных протоколов. Предусмотрен широкий выбор действий для определения реакции системы на срабатывание правил фильтрации — от регистрации в журнале до запуска программ или сценариев.

Защита сетевых соединений

Механизмы защиты сетевых соединений позволяют контролировать аутентичность, целостность и конфиденциальность передаваемых данных.

Централизованное управление

С рабочего места администратора безопасности возможно централизованное управление списком защищаемых объектов, механизмами защиты, правилами фильтрации и т.д.

Контроль целостности

Контролируется целостность как программной, так и информационной частей (правил фильтрации).

Централизованный сбор событий ИБ и отображение данных аудита

Реализованы возможности централизованного сбора событий ИБ со всех компьютеров, на которых установлены компоненты системы, а также просмотра событий в виде структурированных отчетов.

Варианты применения

Защита конфиденциальной информации и персональных данных

TrustAccess обеспечивает сертифицированную защиту конфиденциальной информации и ИСПДн любого класса в части межсетевого экранирования. Дополнительно TrustAccess позволит организовать сертифицированную защиту распределенных информационных систем при отсутствии в них собственных сертифицированных механизмов разграничения доступа.

Сегментирование АС (ИСПДн) без изменения конфигурации сети

Сегментирование АС (ИСПДн) средствами TrustAccess дает возможность отнести отдельные части ИСПДн (например, рабочие места пользователей) к более низкому классу. Данный способ также применим для логической изоляции нескольких ИСПДн в сети предприятия без изменения топологии локальной сети.

Разграничение сетевого доступа пользователей

С помощью TrustAccess можно построить систему разграничения сетевого доступа на основе уровней допуска или должностей пользователей. Также TrustAccess позволит ограничить доступ пользователей к файл-серверу на уровне общих папок.

Разграничение доступа в терминальной среде

Аутентификация сетевых соединений на уровне пользователей позволяет разграничить доступ в условиях работы пользователей в терминальной среде.

Защита виртуальных машин

TrustAccess может применяться для защиты виртуальных машин. Защищаются как внешние соединения, так и соединения между виртуальными машинами. Логотип VMware Ready подтверждает совместимость продукта с платформами VMware.

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетнего опыта в области создания средств защиты информации для государственных и коммерческих заказчиков.

Код Безопасности
ГК «Информзащита»

Тел.: +7 (495) 980-2345, E-mail: info@securitycode.ru
www.securitycode.ru