Семейство продуктов ЗАСТАВА

Основные конкурентные преимущества

Введение

Настоящий документ описывает технические, функциональные, архитектурные и финансово-экономические преимущества комплекса программных продуктов FW/VPN ЗАСТАВА 5.3 (далее ЗАСТАВА 5.3).

Детальные технические характеристики продуктов линейки ЗАСТАВА 5.3 представлены в других документах, размещенных на продуктовом сайте www.zastava.ru.

Информация в документе приведена в виде таблиц с краткими тезисами и пояснениями к ним и ориентирована на: менеджеров IT-направлений, специалистов по информационной безопасности и внедрению.

Примечания:

Содержащиеся в тексте сокращения, названия продуктов и технологий являются общераспространенными и стандартными для рынка информационной безопасности. Все перечисленные торговые марки являются собственностью их правообладателей.

Используемые в тексте сокращения:

МЭ - Межсетевой Экран (FireWall);

FW/VPN-агент, **Агент** – средство обеспечения сетевой безопасности на конечном устройстве (рабочая станция, сервер, мобильный терминал) или транспортном устройстве, контролирующем сегмент сети (шлюз, МЭ). В состав линейки ЗАСТАВА 5.3 входит два типа FW/VPN-агентов: ЗАСТАВА-Клиент 5.3 и ЗАСТАВА-Офис 5.3;

IETF - открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, созданное IAB в 1986 году, которое занимается развитием протоколов и архитектуры Интернета.

end-to-end – «сквозная безопасность», защищённое соединение «точка-точка» (например, «сервер-Пользователь» - «сервер-База Данных»);

ГПБ – глобальная политика безопасности корпоративной сети – набор правил безопасности на уровне корпоративной сети;

ЛПБ - локальная политика безопасности конечного или транспортного устройства – набор правил безопасности на уровни конкретного устройства.

NAT — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

UDP - это транспортный протокол для передачи данных в сетях IP без установления соединения.

IPSec - набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.

LDAP - это сетевой протокол для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP.

PKI - технология аутентификации с помощью открытых ключей.

Технические преимущества

Преимущество	**Краткое описание**
Использование IPSec в качестве базовой технологии безопасности	Программные продукты семейства ЗАСТАВА 5.3 реализованы в полном соответствии со спецификациями комплекса протоколов сетевой безопасности IPSec/IKE. Как механизм образования защищённых соединений в открытых сетях, IPSec, де-факто, является наиболее совершенным средством безопасности.
Распределенная аутентификация пользователя	FW/VPN ЗАСТАВА 5.3. предлагает комплекс взаимосвязанных механизмов, поддерживающих многофакторную аутентификацию пользователей на сетевом уровне и обслуживающих защищаемую часть информационной системы. Если пользователь прошел аутентификацию локально на ЗАСТАВА-Клиент 5.3., то он автоматически считается аутентифицированным во всех других защищенных частях системы, что усиливает общую ее безопасность.
Совместимость с сетями NAT	Работа с NAT (Network Address Translation) поддерживается с помощью IPSec-инкапсуляции в UDP на базе стандарта IETF. Это свойство позволяет использовать агенты ЗАСТАВА 5.3 для защиты сетей с собственным пространством внутренних IP-адресов.
Дружественность к ресурсам ОС	FW/VPN-агенты ЗАСТАВА 5.3. поддерживают многопроцессную и многопоточную обработку информации на уровне используемых платформ.
Оптимизация под современные аппаратные платформы	Работы по повышению производительности продукта ЗАСТАВА-Офис проводились в тесном технологическом сотрудничестве с компаниями Intel, SUN Microsystems и IBM. Преимуществом является то, что для каждого заказчика подбирается аппаратная платформа с необходимыми техническими характеристиками. Скорость шифрования может варьироваться от 40 Мбит/сек (мини-компьютер) до 2 Гбит/сек (мощный сервер).
Поддерживаемые операционные платформы	Операционные платформы ЗАСТАВА-Офис: компьютеры на базе процессоров Intel или SPARC, и ОС Microsoft Windows 2003, Windows 2008/VISTA, Solaris 9/10 и Linux. ЗАСТАВА-Клиент работает на компьютерах на базе процессоров Intel, на которых установлены ОС семейства Microsoft Windows и Linux. Компоненты ЗАСТАВА-Управление могут быть установлены на одном или отдельных компьютерах и работают под управлением ОС Microsoft Windows Server 2003/2003 SP1/2003 R2, Windows 2008/VISTA. Поддерживаются как 32-разрядные так и 64-разрядные операционные системы.
Совместимость со сторонними продуктами ИБ	При работе по протоколам IPSec ЗАСТАВА-Агенты совместимы с VPN-продуктами сетевой безопасности известных зарубежных и российских производителей. Также, ЗАСТАВА-Управление обеспечивает управление конфигурациями VPN и МЭ таких продуктов, как: Cisco IOS Router, МЭ Cisco PIX Firewall, шлюзов Check Point VPN-1/FireWall- 1 Gateway а также встроенных в ОС семейства Microsoft Windows агентов IPSec Agent. Это обеспечивает автоматическую согласованность политик сетевой безопасности в многовендорных VPN-сетях и – как следствие – более высокий уровень защищенности.

Решение высокой доступности	Кластерная реализация программно-аппаратных комлексов ЗАСТАВА обеспечивает высокую доступность (High Availability, HA) защищаемых информационных систем. Комплекс обеспечивает автоматическое восстановление работоспособности агентов Застава в случае: аппаратного отказа оборудования одного из узлов кластера; отказа каналов связи с одним из узлов; отказа программного обеспечения Застава на одном из узлов. Работу кластера поддерживает Застава-Управление, которое формирует и транслирует глобальную политику безопасности, отслеживает состояние узлов комплекса.

Функциональные преимущества

Преимущество	**Краткое описание**
Централизованное управление в режиме реального времени	FW/VPN-агенты ЗАСТАВА 5.3. централизованно управляются продуктом ЗАСТАВА-Управление по протоколу управления политиками (PMP) в реальном масштабе времени. При этом процесс управления заключается не в формировании ЛПБ для каждого конкретного Агента, а в задании общей логики взаимодействия Агентов и необходимого для каждого взаимодействия сервиса безопасности.
Сквозная безопасность соединений	Кроме контроля доступа и защиты соединений средствами IPSec (туннелирование и расширенная пакетная фильтрация), со стороны ЗАСТАВА-Агентов осуществляется непосредственный контроль TCP/UDP-соединений, обеспечивающий дополнительную низкоуровневую защиту сетевого доступа. При этом могут быть заданы различные политики безопасности, включая фильтрацию пакетов для каждого соединения. Это дает возможность управлять доступом с точностью до конкретного пользователя конкретного приложения, а также обеспечить сквозную (end-to-end) безопасность между пользователем и сервером приложений.
Распределенный межсетевой экран	FW/VPN-агенты ЗАСТАВА 5.3. содержат встроенный МЭ с расширенной пакетной фильтрацией и контролем TCP/UDP-соединений. ЗАСТАВА-Управление централизованно управляет распределенным МЭ в реальном масштабе времени, тем самым обеспечивая защиту соединений между всеми типами Агентов, а также между Агентами и внешними хостами.
Поддержка роуминга пользователей	Все FW/VPN-агенты ЗАСТАВА 5.3 поддерживают работу с динамическими IP-адресами, назначенными провайдерами услуг Интернета, или временными IP-адресами, полученными через DHCP-сервер локальной сети. Поддержка режима работы с динамическими адресами – свойство всех агентов ЗАСТАВА 5.3, поэтому защищаемой единицей может быть не только рабочая станция, но и мобильный офис или небольшой филиал, подключающийся к Интернету на сеансовой основе. ЗАСТАВА-Управление снабжает Агентов ЛПБ вне зависимости от их физического нахождения. Благодаря этому могут формироваться защищённые виртуальные сообщества, периметр которых определяется не физическими критериями, а текущим местонахождением управляемого объекта вне зависимости от топологии защищаемых сетей.

Использование персональных средств аутентификации	Полная поддержка многофакторной аутентификации пользователей с помощью токенов eToken и Rutoken (PKCS#11 2.10 и выше), а также программной эмуляции токена на носителе или жестком диске. Реализована поддержка российской криптографии в соответствии с PKCS#11 2.30.
Ограничение «человеческого фактора»	Привилегии пользователей по изменению ЛПБ полностью контролируются Администратором безопасности. Исключение в управлении безопасностью пользователей сделано только в самостоятельной аутентификации в ЗАСТАВА-Клиенте 5.3 и изменении PIN – кода при использовании токена. Типичная для других IPSec-клиентов степень свободы, когда пользователь может вносить изменения в локальную политику безопасности, в ЗАСТАВА-клиент 5.3. не практикуется, так как это значительно повышает уязвимость системы в целом.
Открытый криптоинтерфейс	FW/VPN-агенты ЗАСТАВА 5.3 используют подключаемые внешние модули шифрования, цифровой подписи и хэширования. Обычно это продукт КриптоПро CSP компании Крипто-Про, однако, по выбору пользователя, это могут быть другие модули шифрования. Также ЗАСТАВА может использовать криптоалгоритмы RSA, AES, DES, 3DES, SHA1, MD5 и другие.
Наличие сертификатов регуляторов	Наличие сертификатов (№ 1586: МЭ 3-й класс, 3-й уровень НДВ; №1585: МЭ 2-й класс, 2-й уровень НДВ; №2288: МЭ 2-й класс, 3-й уровень НДВ; №2289: МЭ 2-й класс, 3-й уровень НДВ) ФСТЭК позволяет использовать линейку продуктов ЗАСТАВА для защиты информационных систем обработки персональных данных до класса К1 включительно. Наличие сертификата МО ВС РФ №1482 (МЭ 2-й класс, 2-й уровень НДВ) позволяет применять продукт «ЗАСТАВА-М» в информационных системах Министерства обороны. Получено положительное заключения ФСБ о соответствии ЗАСТАВЫ 5.3 требования ФСБ России к шифровальным средствам класса КС1 (для исполнения КС1), КС2 (для исполнения КС2). Планируется сертифицировать продукты ЗАСТАВА на соответствие требованиям ФСБ к межсетевым экранам.

Архитектурные преимущества

Преимущество	**Краткое описание**
Полное соответствие промышленным стандартам безопасности	Благодаря поддержке популярных международных стандартов FW/VPN-агенты ЗАСТАВА 5.3. совместимы с большинством известных средств обеспечения безопасности: PKI-платформами (RSA Keon, SunONE, Microsoft CA, Baltimore UNICERT, Entrust/PKI, КриптоПро, Верба), LDAP-директориями (NDS, AD и др.), системами NMS (HP OpenView, Cisco MARS), средствами строгой аутентификации (Aladdin, Rutoken и др.). IPSec-агентами (Cisco, CheckPoint, Microsoft, HP и др.), Поэтому ЗАСТАВА 5.3. «бесшовно» встраивается в существующую корпоративную архитектуру безопасности.
Интеграция с системами сетевого управления	В каждый FW/VPN-агенты ЗАСТАВА 5.3 включен SNMP-агент, предназначенный для сбора статистики (мониторинга) и подачи сигналов о нарушениях политики безопасности на внешнюю систему управления сетью NMS (Network Management System) - HP OpenView NNM, Cisco MARS, что позволяет унифицировать управление информационной системой в целом
Взаимодействие с оборудованием Cisco	ЗАСТАВА-Клиент 5.3. поддерживает протокол IKE CFG, используемый IPSec-шлюзами Cisco (маршрутизаторами Cisco IOS и МЭ Cisco PIX Firewall) для безопасной доставки IP-адреса из пула локальных адресов в LAN. IKE CFG облегчает обратную маршрутизацию (от сервера к вызывающему IPSec-клиенту, в пределах LAN) и присвоение имени для компьютера клиента, который установил VPN-туннель к LAN. Важная особенность состоит в возможности установки сессии IKE CFG с несколькими шлюзами Cisco IOS/PIX. Клиент получает несколько внутренних IP-адресов от шлюзов Cisco и, одновременно поддерживает с ними IPSec-туннели. Таким образом, ЗАСТАВА 5.3 может встраиваться в уже функционирующие информационные сети, построенные на оборудовании Cisco Systems без изменения архитектуры сети.

Финансово-экономические преимущества

Преимущество	**Краткое описание**
Снижение затрат на управление безопасностью	Управление доступом и защита соединений в ЗАСТАВА 5.3. реализованы с использованием идентификационных данных, полученных из сертификатов X.509 агентов. Это позволяет Администратору безопасности определять политику безопасности на уровне отдельных пользователей и групп пользователей (группировка пользователей осуществляется ссылкой на имя общего поля в их сертификатах). Например, группировка может производиться по полю, в котором указано конкретное подразделение организации. Перечисление всех сотрудников становится ненужным, что важно при относительно большой численности подразделений. Фильтрация по сходным полям сертификатов, значительно снижает затраты на формирование и изменение политики безопасности в крупномасштабных сетях. Продукт «ЗАСТАВА-Управление» обеспечивает успешное управление 5000 агентами из одного центра управления, что существенно снижает затраты на администрирование системы.
Снижение затрат на развертывание системы	ЗАСТАВА-Клиент 5.3 и его первоначальная конфигурация безопасности устанавливаются на рабочую станцию «одним щелчком мыши». При этом, дистрибутив может быть загружен из локальной сети, с переносного модуля FLASH-памяти или web-сайта в Интернете. Пакет инсталляции первоначально конфигурируется администратором для создания оптимального дистрибутива. Скорость развёртывания даже больших систем сокращается с нескольких недель до считанных часов.
Снижение затрат на администрирование	ЗАСТАВА-Управление предлагает графический интерфейс с удобной древовидной структурой управляемых объектов, а также мастер типичных сценариев ГПБ. Все правила ГПБ могут быть выведены на принтер в виде таблицы. Таким образом, создается оптимальные условия для удобства формирования глобальной политики безопасности и аналитической работы Администратора, что в свою очередь существенно снижает количество ошибок администрирования.
Прозрачность для инфраструктуры сети	Драйвер FW/VPN-агенты ЗАСТАВА 5.3. «расположен» на нижней границе IP-стека, тем самым обеспечивается полная независимость работы продукта от протоколов прикладного и канального уровней (приложения и сервисы ОС не нуждаются в интеграции со средой защиты на базе ЗАСТАВА 5.3.). Для реализации решений безопасности на базе ЗАСТАВА 5.3 не требуется специальных изменений или настроек программно-аппаратного комплекса, выполняющего бизнес-задачи. В результате, инвестиции в существующее оборудование и ПО полностью защищены.

ПРОДУКТЫ

КОМПАНИИ

ЭЛВИС-ПЛЮС

Основные конкурентные преимущества линейки продуктов ЗАСТАВА 5.3