

Семейство продуктов ЗАСТАВА 5.2

Семейство продуктов ЗАСТАВА 5.2 обеспечивает защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (Virtual Private Networks - VPN) и распределенного межсетевое экранирования (МЭ).

Безопасность информации, хранимой, передаваемой и обрабатываемой в корпоративных системах, существенно влияет на общую эффективность бизнеса. Однако угрозы этой безопасности постоянно растут, вместе с ростом возможностей карманных компьютеров и смартфонов, распространением беспроводных технологий и IP телефонии, все большей распределенностью корпоративных вычислительных процессов. Для эффективного противодействия угрозам средства защиты информации должны соответствовать ряду требований.

В первую очередь, они должны быть эффективными, гарантируя всестороннюю безопасность защищаемой информации. Работа средств защиты, как части корпоративной информационной системы, не должно снижать ее производительность и надежность, логично встраиваться в систему информационной безопасности.

Средства защиты должны быть максимально удобными, а лучше, совсем незаметными, «прозрачными» для пользователей и приложений.

Управление средствами защиты должно быть гибким, унифицированным и удобным для персонала, который обслуживает их.

И наконец, финансовая сторона проблемы защиты информации. Важен не только факт обеспечения безопасности информации в системе, но и цена, которую за это приходится платить, важна минимизация общей стоимости владения системой защиты.

Всем этим требованиям соответствует семейство продуктов ЗАСТАВА™ 5.2 производства компании ЭЛВИС-ПЛЮС.

На российском рынке продукты ЗАСТАВА пользуются заслуженной популярностью у крупных заказчиков из финансового сектора, энергетики, газо- и нефтедобывающей промышленности, телекоммуникационной отрасли, на предприятиях оборонного комплекса, в региональных и федеральных органах власти, в государственных учреждениях и организациях.

Состав и характеристики продуктов ЗАСТАВА 5.2

Семейство ЗАСТАВА 5.2 состоит из набора исполнительных агентов (ЗАСТАВА-Клиент, ЗАСТАВА-Сервер и ЗАСТАВА-Офис), и координирующего комплекса ЗАСТАВА -Управление.

Агенты устанавливаются на персональные компьютеры, серверы и шлюзы защищаемой информационной системы. ЗАСТАВА-Управление обеспечивает централизованное администрирование и оперативное управление политикой безопасности, контроль состояния агентов и взаимодействие с ними.

Решения на базе продуктов ЗАСТАВА 5.2 характеризуются:

- поддержкой полного набора сценариев VPN-топологий и межсетевое экранирования, в том числе – в условиях применения трансляции сетевых адресов (NAT);
- реализацией технологии распределенного МЭ с поддержкой протокольных автоматов на всех типах агентов, включая ЗАСТАВА-Клиент, что позволяет обеспечить принципиально более высокий уровень защищенности персональных компьютеров пользователей как внутри периметра КИС, так и за ее пределами;
- централизованным управлением политикой сетевой безопасности защищаемой КИС – топологией VPN туннелей и конфигурациями МЭ – в режиме реального времени;
- возможностью задания интегральной политики сетевой защиты всей КИС как единого целого на уровне бизнес-объектов и ролей, что позволяет наиболее удобным и наименее трудоемким

для администраторов безопасности способом отображать общую логику защищенного взаимодействия пользователей и информационных ресурсов КИС;

- автоматически обеспечиваемой координированностью VPN и МЭ конфигураций всех управляемых агентов сетевой безопасности, что значительно снижает риски несанкционированного доступа либо – наоборот – недоступности сервисов КИС, возникающие из-за ошибок и несогласованностей при раздельном конфигурировании;
- централизованным оперативным мониторингом состояния и событийных журналов управляемых агентов сетевой безопасности;
- "прозрачностью" для конечных пользователей, которые не вовлечены в процедуры инсталляции, обновления и администрирования продукта ЗАСТАВА-Клиент;
- "прозрачностью" для прикладной и системной инфраструктуры - для использования продуктов не требуется встраивание VPN в программное обеспечение и изменение работы приложений или сервисов операционных систем;
- хорошим взаимодействием с существующими VPN-продуктами на базе стандартов IPsec, устройствами и системами аутентификации пользователей, платформами инфраструктуры открытых ключей (PKI) а также системами сетевого управления;
- высокими масштабируемостью, производительностью и надежностью.

Для организации защищенного VPN соединения продукты ЗАСТАВА используют сертифицированные криптомодули, подключаемые через открытый программный интерфейс. Это продукты ведущих российских разработчиков: КриптоПро CSP 2.0 и КриптоПро CSP 3.0 компании Крипто-Про, Крипто-КОМ 3.1 компании Сигнал-КОМ, Верба компании "МО ПНИЭИ", реализующие отечественные стандарты ГОСТ Р 34.11-94, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ 28147-89.

В качестве инфраструктуры открытых ключей продукты ЗАСТАВА могут использовать PKI-платформы RSA Keon, SunONE, Microsoft CS, Baltimore UNICERT, Entrust/PKI, КриптоПро, Верба.

ЗАСТАВА-Агенты 5.2

Программные продукты ЗАСТАВА-Офис 5.2, ЗАСТАВА-Клиент 5.2 и ЗАСТАВА-Сервер 5.2 (ЗАСТАВА-Агенты) обеспечивают конфиденциальность, целостность и аутентичность информации, передаваемой по каналам связи, на основе протокола IPsec. Они решают задачи аутентификации пользователей и VPN-узлов (в том числе внешними средствами двухфакторной аутентификации) и межсетевого экранирования на базе расширенной пакетной фильтрации.

ЗАСТАВА-Клиент обеспечивает защиту мобильных пользователей – например, при работе из Интернет, включая режим выделения мобильному пользователю внутреннего локального адреса для удаленного VPN-доступа в защищенную корпоративную сеть. ЗАСТАВА-Клиент не требует обучения пользователей или какого-либо их участия в администрировании продукта. Не менее важно, что пользователи не могут ни заблокировать работу ЗАСТАВА-Клиент, ни изменить централизованно задаваемые политики сетевой безопасности – включая конфигурации VPN и МЭ – вне зависимости от того, работают ли они в корпоративной сети или удаленно.

Межсетевой экран ЗАСТАВА-Офис решает задачи защиты периметра корпоративной информационной системы, и ее деления на сегменты с регламентированным доступом. Кроме того, он реализует функции прикладного проксирования наиболее популярных сетевых сервисов и протоколов (Telnet, FTP, SMTP, HTTP, SOCKS), а также сокрытие топологии защищаемой сети.

ЗАСТАВА-Сервер предназначен для защиты и фильтрации входящего и исходящего трафика на компьютере с одним или несколькими интерфейсами, выполняющем роль корпоративного сервера. Обеспечение целостности, аутентичности и шифрования передаваемых данных производится в соответствии с загружаемой в ЗАСТАВА-Сервер Локальной Политикой Безопасности (ЛПБ), созданной с помощью ЗАСТАВА-Управление

Совместное использование агентов ЗАСТАВА обеспечивает:

- защищенный удаленный VPN-доступ мобильных пользователей к корпоративным информационным ресурсам и сервисам;

- защиту мобильных пользователей от атак из Интернета (централизованно управляемый распределенный МЭ);
- защиту внешнего периметра корпоративной системы и сетевое сегментирование;
- обеспечение безопасного доступа в Интернет для внутренних пользователей сети;
- объединение нескольких удаленных офисов защищенными VPN - каналами, организованными в общедоступных сетях связи;
- поддержку всех типов защищенных VPN-соединений: клиент-шлюз, клиент-сервер, клиент-клиент, сервер-шлюз, сервер-сервер;
- организацию защищенных "виртуальных рабочих групп", включая офисных пользователей и удаленных мобильных клиентов, с использованием проводных и беспроводных сетей;

Сочетание технологий VPN - IPSec и МЭ позволяет ЗАСТАВА-Агентам обеспечивать разные степени защиты трафика и индивидуальные политики безопасности (аутентификации и/или шифрования) для каждого защищенного соединения. При этом учитываются сетевые адреса и порты, направление соединения, идентификационные данные отправителя и получателя. Для каждого сетевого интерфейса правила защиты могут задаваться отдельно.

В гетерогенных сетях ЗАСТАВА-Агенты совместимы с VPN-продуктами известных зарубежных и российских производителей: Cisco IOS Router, Cisco PIX Firewall, Check Point VPN-1/FW-1 Gateway, Microsoft 2000/XP/2003 IPSec Agent, NME-RVPN компании "С-Терра СиЭсПи".

Эффективная реализация многопоточных вычислений позволили шлюзу ЗАСТАВА-Офис достичь высокой пропускной способности VPN-каналов при использовании алгоритма ГОСТ 28147-89. К примеру, 280 Мбит/с на однопроцессорном Intel компьютере, 440 Мбит/с на двухпроцессорной машине, 640 Мбит/с на сервере с двумя двухъядерными процессорами и 800 Мбит/с на системе с двумя четырехъядерными процессорами.

ЗАСТАВА-Клиент работает на компьютерах в конфигурации не хуже Intel Pentium 200MHz и 50MB НЖМД, на которых установлены ОС Microsoft Windows XP SP1/SP2, Windows 2000 Professional SP4, Windows 2003/2003 SP1.

ЗАСТАВА-Офис: компьютеры в конфигурации не хуже Intel Pentium 200MHz или SPARC с 50MB НЖМД и ОС Microsoft Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003/2003 SP1, а также Solaris 8/9 (64-bit).

ЗАСТАВА-Управление 5.2

Центр Управления Политикой безопасности (ЦУП) ЗАСТАВА-Управление включает компоненты ЦУП-Сервер, ЦУП-Консоль и База Данных ЦУП. Он предназначен для централизованного оперативного управления конфигурациями VPN и МЭ, правилами NAT и прикладным проксированием на ЗАСТАВА-Агентах в локальных и глобальных IP сетях.

ЗАСТАВА-Управление обеспечивает взаимодействие и защиту трафика между управляемыми агентами и внешними компонентами – серверами регистрации, системами сетевого управления и продуктами сетевой защиты третьих производителей

ЗАСТАВА-Управление позволяет создавать, редактировать, транслировать, хранить, подписывать, доставлять по защищенным каналам и активировать политики сетевой безопасности на управляемых агентах, осуществлять оперативный мониторинг их состояния, собирать и просматривать данные их событийных журналов, вести и контролировать внутренний журнал регистрации системных событий.

В ЗАСТАВА-Управление предусмотрены несколько ролей администраторов безопасности, реализована активация политик по заданному Администратором расписанию, возможен импорт политик VPN/FW агентов третьих производителей.

ЗАСТАВА-Управление управляет защитой КИС на основе набора правил - Глобальной Политики Безопасности (ГПБ). ГПБ отражает бизнес-процессы корпоративной информационной системы и основывается на бизнес-ролях защищаемых объектов. Это позволяет удобным способом отображать логику защищенного взаимодействия пользователей и информационных ресурсов.

ГПБ включает в себя как сведения о топологии КИС (описания всех объектов с их идентификационной информацией), так и правила взаимодействия объектов.

На основе Глобальной Политики Безопасности генерируются Локальные Политики Безопасности (ЛПБ) для управляемых агентов. Этим обеспечивается согласованность VPN и МЭ конфигураций управляемых агентов, что значительно снижает риски несанкционированного доступа либо – наоборот – недоступности сервисов КИС, возникающие из-за несогласованностей или ошибок при раздельном или ручном конфигурировании агентов.

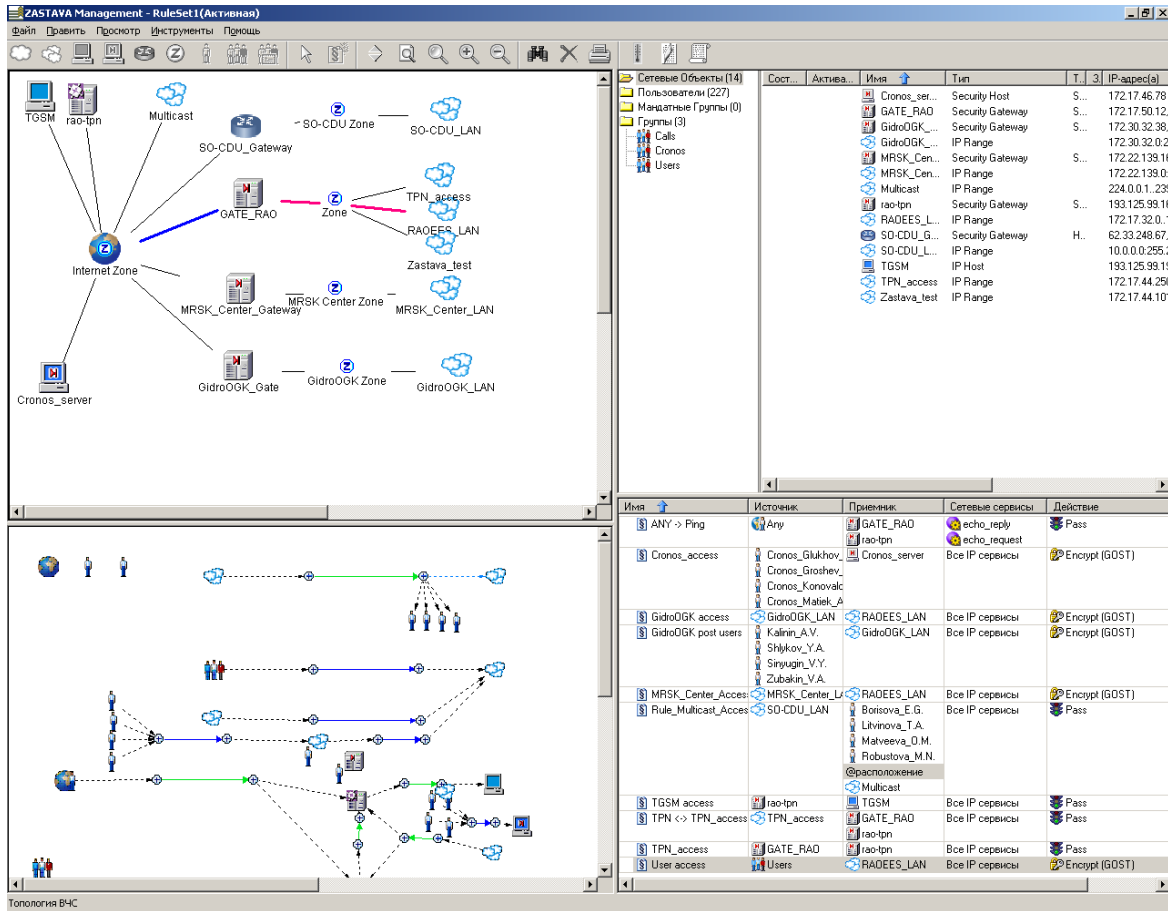
ЗАСТАВА-Управление позволяет работать не только с агентами ЗАСТАВА, но и обеспечивает управление конфигурациями VPN и МЭ, принадлежащих лидерам рынка информационной безопасности: Cisco IOS Router, МЭ Cisco PIX Firewall, шлюзов Check Point VPN-1/FireWall-1 Gateway, а также встроенных в ОС Microsoft 2000/XP/2003 агентов IPSec Agent. Технология трансляции политик обеспечивает автоматическую согласованность политик сетевой безопасности в гетерогенных VPN-сетях и – как следствие – значительно более высокий уровень защищенности информационных ресурсов.

Компоненты ЗАСТАВА-Управление 5.2 могут быть установлены на одном или отдельных компьютерах и работают под управлением ОС Microsoft Windows Server 2000 SP4, Windows Advanced Server 2000 SP4, Windows XP SP2, Windows Server 2003/2003 SP1/2003 R2. В качестве платформы Базы Данных сервера ЗАСТАВА-Управление используется Microsoft SQL Server 2000 или Microsoft SQL 2000 Server Desktop Engine (MSDE 2000).

Графический интерфейс. Главное окно консоли

Простоту работы с ЗАСТАВА-Управление обеспечивает графический интерфейс администратора. Он обеспечивает целостное представление ГПБ в виде графа, таблицы и «проекции» политики на сетевую топологию, каждое из которых удобно на разных этапах создания, модификации и отладки политики. Интерфейс обеспечивает оперативную и наглядную работу с масштабными ГПБ-проектами (десятки тысяч объектов).

Главное окно состоит из строки меню, инструментальной линейки и окна просмотра. Окно просмотра – это набор из четырех секций, каждая из которых отображает информацию в своем формате. Графический интерфейс позволяет эффективно управлять политикой как из графического, так и табличного видов ее представления, обеспечивая синхронизацию внесенных изменений вне зависимости от того, в какой из секций ГИП они сделаны.



Графический интерфейс. Топология ВЧС

В секции «Топология ВЧС», содержание политики безопасности, ее объектов и агентов «проецируется» на топологию Виртуальной Частной Сети. Здесь администратор может создавать и удалять защищаемые объекты, управляемые и неуправляемые агенты безопасности, а также задавать их параметры.

При этом ЗАСТАВА-Управление автоматически вычисляет и отображает сегменте «Граф ГПБ» все сетевые связи и взаиморасположение объектов, позволяя наблюдать за их состоянием и корректировать работу в привычном для сетевых администраторов топологическом представлении.

Секция «Топология ВЧС», используется также для онлайн мониторинга текущего состояния локальных политик управляемых агентов.

Графический интерфейс. Объекты политики

Секция **Объекты Политики** представлена в виде дерева папок, отражающего Сетевые Объекты (слева), и таблицы Политик (справа), в которой отображаются все *Объекты Политики*, включенные в выбранную справа папку.

Графический интерфейс. Таблица ГПБ

Секция «Таблица ГПБ» представляет глобальную политику безопасности в виде таблицы, компактно отображая *полный набор данных* (атрибутов) правил ГПБ. Табличный вид эффективен для тонкой настройки ГПБ, аудита и эксплуатационной поддержки, включая регламентные процедуры и обработку нештатных ситуаций.

Графический интерфейс. Граф ГПБ

В секции «Граф ГПБ» правила отображается в виде графа, который обеспечивает *структурное* представление всей политики или ее части «с одного взгляда». Такой формат удобен для создания, оперативного анализа, отладки и модификации ГПБ.

Граф ГПБ содержит ссылки (ярлыки) для быстрого вызова объектов Политики, созданных в секциях *Топология ВЧС* и *Объекты Политики*, которые участвуют в Правилах. Объекты Политики можно скопировать в *Граф ГПБ* и тогда можно интуитивно создавать Правила ГПБ прямо в секции *Граф ГПБ*.

Преимущества семейства продуктов ЗАСТАВА 5.2

ЗАСТАВА-Агенты нечувствительны к наличию в сети промежуточных NAT-устройств, и обеспечивают «прозрачное» прохождение через них VPN-трафика.

Высокая устойчивость ЗАСТАВА-Агентов к отказам VPN-шлюзов обеспечивается поддержкой стандартного протокола DPD (Dead Peer Detection) разработки компании Cisco Systems, с помощью которого ЗАСТАВА-Агенты могут автоматически и в реальном масштабе времени детектировать недоступность шлюза на втором конце VPN-канала и создавать дублирующие каналы с другими VPN-шлюзами на том же сетевом периметре.

Поддержка приоритезации типов трафика (QoS) посредством модификации поля DiffServ при туннелировании IP-пакетов позволяет эффективно использовать продукты ЗАСТАВА для защиты коммуникаций приложений, чувствительных к задержкам, например, IP-телефонии.

ЗАСТАВА-Агенты поддерживают многофакторную аутентификацию пользователей с помощью PKCS#11 совместимых токенов Rainbow iKey1000/iKey2000, Eutron Cryptoidentity, ActiveCARD Gold, Aladdin eToken, смарт-карт Gemplus MPCOS-EMV а также программной эмуляции токена на дискете или жестком диске. Кроме того, для аутентификации пользователей удаленных ЗАСТАВА-Клиентов шлюз ЗАСТАВА-Офис может использовать протокол XAUTH и внешние RADIUS-совместимые серверы аутентификации. ЗАСТАВА-Управление поддерживает базу управляющей информации SNMP (MIB) и использовать возможности встроенного SNMP-агента для отработки SNMP-запросов и отправки оперативных SNMP-сообщений к внешним Системам Сетевого Управления (NMS), использовать специальные носители информации (PKCS#11-совместимые токены) для хранения критической служебной информации пользователей.

На шлюзах ЗАСТАВА-Офис обеспечено управление аутентификацией пользователей по протоколу XAUTH с использованием внешних RADIUS серверов а также выделением ЗАСТАВА-Клиентам локальных IP адресов по протоколу IKE-CFG.

Использование продуктов ЗАСТАВА 5.2 существенно сокращает расходы на создание и эксплуатацию комплексных систем ИБ. В частности, затраты снижаются благодаря поддержке ЗАСТАВА-Клиентами процедуры удаленного автоматического обновления, при которой загрузка и установка новых патчей и версий продукта осуществляется без участия пользователей и без перезагрузки компьютеров.

Используя ЗАСТАВА-Управление, администратор может эффективно распределять выполнение различных по своей природе задач управления на разные окна ГИП и в процессе работы мгновенно переходить от одного окна к другому, не теряя при этом синхронизации между операциями, выполненными в разных окнах, и при этом постоянно контролировать систему управления «с одного взгляда» в главном окне ГИП.