Семейство продуктов ЗАСТАВА

Описание решения

1. Введение

Семейство продуктов информационной безопасности ЗАСТАВА™ успешно применяется для защиты информации с 1997 года. В России продукты ЗАСТАВА используют крупные компании и структуры из кредитно-финансового сектора, энергетики, газо и нефтедобывающей промышленности, телекоммуникационной отрасли, предприятий оборонного комплекса, региональных и федеральных органов власти, государственных учреждений и организаций. Все больший интерес к ней проявляют учебные учреждения, организации здравоохранения и социальной сферы, предприятия среднего и малого бизнеса. За рубежом ЗАСТАВА используется на территории некоторых стран постсоветсткого пространства.
Продукты ЗАСТАВА 5.3 обеспечивают защиту корпоративных информационных систем на сетевом уровне с помощью технологий виртуальных частных сетей (Virtual Private Networks - VPN) и распределенного межсетевого экранирования (МЭ). Они работают на различных аппаратных платформах, под управлением практически всех популярных операционных систем.

2. Семейство продуктов ЗАСТАВА 5.3

Семейство ЗАСТАВА 5.3 включает программные агенты ЗАСТАВА-Клиент и ЗАСТАВА-Офис, которые устанавливаются, соответственно, на персональные компьютеры и шлюзы защищаемой информационной системы. Третий продукт семейства, ЗАСТАВА-Управление, в удаленном режиме обеспечивает централизованное администрирование и оперативное управление агентами, их политиками безопасности.
Семейство продуктов ЗАСТАВА 5.3 обеспечивает:

- Защиту отдельных компьютеров, в том числе мобильных, от атак из сетей общего пользования и Интернет;
- Защиту корпоративной информационной системы или ее частей от внешних атак;
- Внутреннее сегментирование информационной системы для обработки информации разной степени конфиденциальности;
- Организацию доверенных, защищенных каналов связи между сегментами территориально распределенной информационной системы, а также с мобильными пользователями;
- Ограничение доступа с рабочих станций к внешним информационным ресурсам и интернет-сайтам;
- Соответствие информационной системы Российскому законодательству и нормативным требованиям в сфере информационной безопасности и защиты персональных данных;
- Централизованное, в режиме реального времени управление сетевой безопасностью в информационных системах масштабом более 5000 защищенных узлов;
- Высокую производительность и прозрачность для пользователей и приложений.
- централизованный мониторинг состояния управляемых агентов и событийных журналов сетевой безопасности;

- автоматическую координацию конфигураций VPN и МЭ для всех управляемых агентов, что снижает риски несанкционированного доступа либо недоступности сервисов КИС, возникающие из-за ошибок и несогласованностей при раздельном конфигурировании;
- Совместимость с существующими VPN-продуктами, работающими на базе стандартов IPsec, с устройствами и системами аутентификации пользователей, платформами инфраструктуры открытых ключей (PKI) а также системами сетевого управления;

Для выполнения криптографических функций ЗАСТАВА использует внешние, сертифицированные криптомодули производства ведущих российских компаний, реализующие отечественные стандарты ГОСТ Р 34.11-94, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ 28147-89. Обычно это продукт КриптоПро CSP компании Крипто-Про, однако, по выбору пользователя, это могут быть Крипто-КОМ (Сигнал-КОМ), Верба (МО ПНИЭИ). Также ЗАСТАВА может использовать криптоалгоритмы RSA, DES, 3DES, SHA1, MD5 и другие.
Продукты ЗАСТАВА сертифицированы ФСТЭК, по 2-му классу защищенности межсетевых экранов и 2-му уровню контроля отсутствия недекларированных возможностей, а также по 3-му классу защищенности межсетевых экранов и 3-му уровню контроля отсутствия недекларированных возможностей, согласно РД Гостехкомиссии. Продукты могут быть использованы (и рекомендованы некоторыми ведомствами) для защиты персональных данных до 1 категории включительно.

3. ЗАСТАВА-Агенты

Программные агенты - ЗАСТАВА-Офис 5.3, ЗАСТАВА-Клиент 5.3 предназначены для использования в качестве межсетевых экранов с функциями расширенной пакетной фильтрации, и организации защищенных VPN-соединений в сетях связи общего пользования. На их основе строятся территориально распределенные, защищенные корпоративные информационные системы, обеспечивающие конфиденциальность, целостность и аутентичность сетевого трафика на базе стандартных протоколов IPSec. Строгая аутентификация пользователей, а также взаимная аутентификация агентов, производится с использованием сертификатов цифрового ключа.

ЗАСТАВА-Агенты нечувствительны к наличию в сети промежуточных NAT-устройств, обеспечивают «прозрачное» прохождение через них VPN-трафика с помощью стандартных методов протокольной инкапсуляции IPsec в UDP.

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

Поддержка приоритезации типов трафика (QoS) позволяет эффективно использовать продукты ЗАСТАВА для защиты приложений, чувствительных к задержкам, например, IP-телефонии и видеоконференций.

При работе по протоколам IPSec ЗАСТАВА-Агенты совместимы с VPN-продуктами сетевой безопасности известных зарубежных и российских производителей: Cisco IOS Router, Cisco PIX Firewall, Check Point VPN-1/FW-1 Gateway, Microsoft 2000/XP/2003 IPSec Agent.

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

ЗАСТАВА-Агенты поддерживают многофакторную аутентификацию пользователей с помощью PKCS#11 совместимых токенов: Aladdin eToken, Rutoken, Rainbow iKey1000/iKey2000, ActiveCARD Gold, 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.

Межсетевой экран и VPN-агент ЗАСТАВА-Офис реализует функции прикладного проксирования популярных сетевых сервисов и протоколов (Telnet, FTP, SMTP, HTTP, SOCKS), а также маскирование топологии защищаемой сети в режиме VPN-туннелирования, либо с использованием встроенного централизованно управляемого NAT-сервера.
ЗАСТАВА поддерживает ряд типовых сценариев применения VPN и МЭ:

- защита внешнего сетевого периметра КИС и сегментирование КИС;
- обеспечение безопасного доступа в Интернет для внутренних пользователей сети;
- объединение нескольких удаленных офисов в единую виртуальную сеть;
- защищенный удаленный доступ мобильных пользователей к корпоративной ИС;
- защищенный доступ мобильных пользователей в Интернет (централизованно управляемый распределенный МЭ);
- "сквозная" (end-to-end) защита клиент-серверных коммуникаций в локальных и глобальных сетях;
- "полносвязная" VPN с поддержкой всех типов защищенных соединений: клиент-шлюз, клиент-сервер, клиент-клиент, сервер-шлюз, сервер-сервер;
- сетевая защита "виртуальных рабочих групп", включая группы мобильных пользователей в проводных и беспроводных локальных сетях;
- централизованная онлайн-активация аварийных политик сетевой безопасности на всех типах управляемых агентов.

Гибкое сочетание технологий VPN-IPSec и МЭ обеспечивает разные степени защиты трафика и индивидуальные политики безопасности – аутентификации и/или шифрования – для каждого защищенного соединения. Используется множество параметров, включая сетевые адреса и порты, направление соединения а также идентификационные данные отправителя и получателя. При этом правила защиты трафика для каждого сетевого интерфейса могут задаваться раздельно.

Эффективная реализация многопоточных вычислений и использование возможностей многопроцессорных и многоядерных архитектур позволили шлюзу ЗАСТАВА-Офис достичь высоких показателей производительности VPN-каналов. В конце 2011 года совместно с Hewlett-Packard было проведено тестирование программного комплекса ЗАСТАВА-Офис. В качестве аппаратной платформы использовались серверы HP ProLiant DL380 G7, каждый с двумя шестиядерными процессорами IntelE XeonR X5660 (2.80 Ггц) и 10 гигабитными сетевыми картами. При шифровании трафика по алгоритму ГОСТ 28147-89 средняя пропускная способность защищенного канала передачи данных составила **1740 Мбит/сек**, максимальная доходила до **2260 Мбит/сек**.

Операционные платформы ЗАСТАВА-Офис: компьютеры на базе процессоров Intel или SPARC, и ОС Microsoft Windows 2003/2008/VISTA/7, Solaris 9/10 и Alt Linux.

Персональный межсетевой экран и VPN-агент ЗАСТАВА-Клиент обеспечивает полный набор функций сетевой защиты для отдельных рабочих станций и мобильных пользователей – например, при работе из Интернет, включая режим выделения мобильному пользователю внутреннего локального адреса для удаленного VPN-доступа в защищенную корпоративную сеть.

Работа программы ЗАСТАВА-Клиент на персональных компьютерах не требует обучения пользователей, или какого-либо их участия в администрировании продукта. Не менее важно, что пользователи не могут ни блокировать работу ЗАСТАВА-Клиент, ни изменить централизованно задаваемые для их компьютеров политики безопасности – включая конфигурации VPN и МЭ – вне зависимости от того, работают ли они в корпоративной сети или удаленно.

Затраты на эксплуатацию системы ИБ значительно 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. Конфигурирование режимов обновления может выполняться как через локальные настройки Клиента, так и с центра ЗАСТАВА-Управление.
ЗАСТАВА-Клиент работает на компьютерах на базе процессоров Intel, на которых установлены ОС семейства Microsoft Windows и Linux

4. ЗАСТАВА-Управление 5.3

Центр Управления Политиками (ЦУП) безопасности ЗАСТАВА-Управление обеспечивает удаленное, централизованное, гибкое управление всей совокупностью агентов ЗАСТАВА-Офис и ЗАСТАВА-Клиент на основе бизнес-логики и бизнес-ролей. Это позволяет координировать корпоративную политику сетевой безопасности с бизнес- процессами и организационной структурой защищаемой информационной системы.

ЦУП ЗАСТАВА-Управление в составе компонентов ЦУП-Сервер, ЦУП-Консоль и База Данных ЦУП предназначен для централизованного оперативного управления конфигурациями VPN и МЭ, правилами NAT и прикладным проксированием на ЗАСТАВА-Агентах в локальных и глобальных IP сетях. Дополнительно на шлюзах ЗАСТАВА-Офис поддержано управление аутентификацией пользователей по протоколу XAUTH с использованием внешних RADIUS серверов а также выделением ЗАСТАВА-Клиентам локальных IP адресов по протоколу IKE-CFG.

ЗАСТАВА-Управление позволяет создавать, редактировать, транслировать, хранить, подписывать, доставлять по защищенным каналам и активировать политики сетевой безопасности на управляемых агентах. Ведется мониторинг состояния агентов, есть возможность собирать и просматривать данные событийных журналов по протоколу SYSLOG, вести и контролировать внутренний журнал регистрации событий, поддерживать базу управляющей информации SNMP (MIB). ЗАСТАВА-Управление может использовать отчуждаемые носители информации (PKCS#11-совместимые токены) для хранения критической информации пользователей, цифровых ключей и их сертификатов.

ЗАСТАВА-Управление работает не только с агентами ЗАСТАВА-Офис и ЗАСТАВА-Клиент, но и обеспечивает управление конфигурациями VPN и МЭ продуктов сетевой защиты лидеров

зарубежного рынка информационной безопасности: 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.

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.

В ЗАСТАВА-Управление поддержаны несколько ролей администраторов безопасности, реализована активация политик по конфигурируемому расписанию, встроена функция импорта политик VPN/FW агентов третьих производителей. Гибкий лицензионный механизм позволяет без приобретения лицензии опробовать полный процесс конфигурирования, редактирования, трансляции и отображения политик безопасности в графическом интерфейсе пользователя (ГИП).

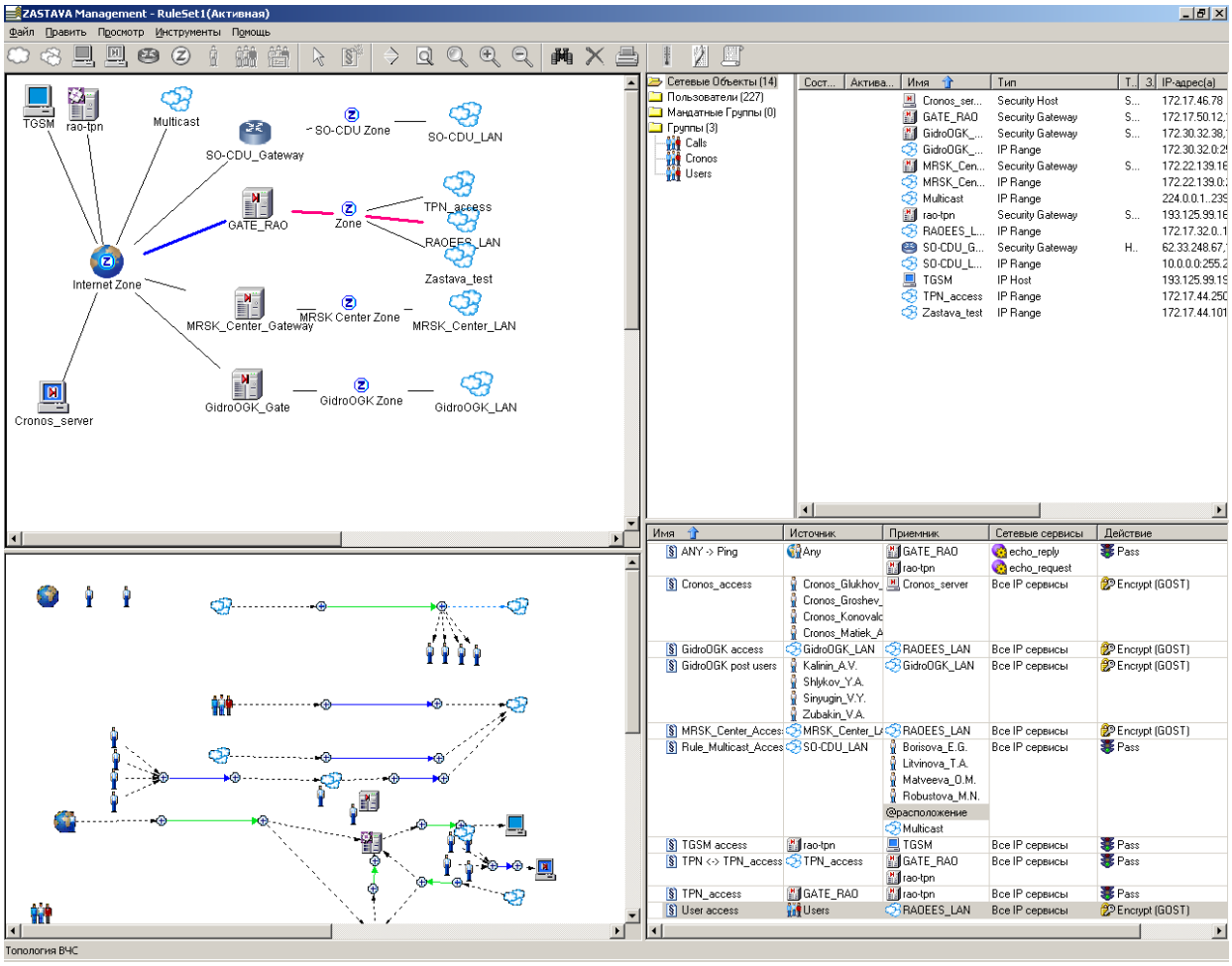
ЗАСТАВА-Управление генерирует Глобальную Политику Безопасности (ГПБ) – набор правил для КИС как единого целого на уровне бизнес-объектов и ролей. ГПБ-проект создается в ЦУП-Консоли и включает в себя сведения о топологии сети (описания объектов с их идентификационной информацией), и правила взаимодействия объектов. ГПБ соответствует бизнес-процессам и основывается на бизнес-ролях защищаемых объектов в структуре организации, что позволяет удобным для администраторов безопасности способом задавать и отображать правила защищенного взаимодействия пользователей и информационных ресурсов.

Результирующие конфигурации VPN и МЭ – Локальные Политики Безопасности (ЛПБ) – для всех управляемых агентов сетевой защиты автоматически генерируются из ГПБ. При этом производится контроль непротиворечивости и согласованность конфигураций VPN и МЭ всех 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.

Эффективность и простоту работы с ЗАСТАВА-Управление обеспечивает графический интерфейс администратора. В нем ГПБ представлена в трех различных «измерениях» – в виде графа, таблицы и «проекции» политики на сетевую топологию. Каждое из представлений эффективно для управления различными этапами создания, модификации и отладки политики.

Табличное представление политики сетевой безопасности в окне «Таблица ГПБ» позволяет упорядоченно и компактно отобразить *полный набор данных* (атрибутов) правил ГПБ, нужных для ее тонкой настройки, детального аудита и эксплуатации, включая регламентные процедуры и отработку нештатных ситуаций.

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



Для эффективной эксплуатации системы сетевой безопасности обслуживающий персонал должен иметь удобный инструмент оперативного визуального соотнесения исполняемой политики с ее важнейшими инфраструктурными компонентами: сетевой топологией а также топологией исполнительных агентов и защищаемых объектов сетевого типа (подсетей, диапазонов, хостов и их групп). В ГИП ЗАСТАВА-Управление таким графическим инструментом является окно «Топология ВЧС», в котором «проецируется» весь сетевой контекст политики безопасности, ее объектов и агентов на топологию защищаемой сети.

Помимо задания топологических данных сети, в окне «Топология ВЧС» администратор может создавать и удалять защищаемые объекты, управляемые и неуправляемые агенты безопасности и их параметры. При этом ЗАСТАВА-Управление автоматически вычисляет и отображает на графе все сетевые связи и взаиморасположение объектов, позволяя наблюдать за их состоянием и корректировать работу в привычном для сетевых администраторов топологическом представлении.

Еще один инструмент автоматизированной отладки и аудита политики ЗАСТАВА-Управление – трассировщик правил ГПБ на сетевую топологию системы. Полезный как при первоначальном создании и изменении политики, так при анализе нештатных ситуаций, этот уникальный инструмент позволяет администратору визуально проверять возможные сетевые маршруты трафика, подпадающего под действие того или иного правила ГПБ, а также и выявлять агенты безопасности, участвующие в его защите.

5. Комплексы высокой готовности на основе продуктов ЗАСТАВА

Комплексы высокой готовности могут иметь в своей основе любой из описанных продуктов семейства ЗАСТАВА, но уже установленный на аппаратную платформу и в максимальной степени сконфигурированный силами производителя.

Программно-Аппаратный Комплекс ЗАСТАВА

Программно-Аппаратный Комплекс ЗАСТАВА, (ПАК ЗАСТАВА), предназначен для тех же целей, что и продукт ЗАСТАВА-Офис, а именно для использования в качестве межсетевого экрана с функциями пакетной фильтрации, трансляции адресов, и в качестве VPN устройства, обеспечивающего защиту трафика по протоколам IKE/IPsec. Комплекс поставляется в типовых конфигурациях, отличается повышенной надежностью и удобством разворачивания и эксплуатации.

Комплексом можно управлять через консоль (монитор, клавиатура подключены непосредственно к ПАК) или через терминал, подключенный через com порт. Управление ПАК осуществляется пользователем с полномочиями администратора, удаленное администрирование возможно по протоколу SSH2, может быть обеспечено использование протокола HTTPS.

Программная часть ПАК ЗАСТАВА базируется на продукте ЗАСТАВА-Офис и обеспечивает всю его функциональность. Комплекс обычно поставляется под управлением ОС Солярис X86 32 бит, однако доступны и другие конфигурации. Предусмотрен интерфейс для администрирования ОС в части редактирования пароля пользователя, возможность администрирования сетевых настроек ОС стандартными средствами ОС в части:

- конфигурирования сетевых интерфейсов (адрес, маска);
- таблицы маршрутизации;
- служб DHCP и DNS клиента.

ПАК автоматически восстанавливает работоспособность после перезагрузки, вызванной внезапным выключением питания. При этом восстанавливается последняя загруженная конфигурация. Имеется возможность быстрого начального конфигурирования ЗАСТАВА-Офис по сети от ЗАСТАВА-Управление, включая настройку сертификатов, в том числе сертификатов, установленных СКЗИ с алгоритмами GOST, интерфейсов, политики и протокола конфигурирования. Сертификаты с ключами передаются в PKCS11/12 конверте или в предусмотренном разработчиками СКЗИ защищенном виде (для КриптоПРО – контейнер, закрытый паролем). Ключ и сертификат могут быть созданы и доставлены на ПАК внешними средствами.

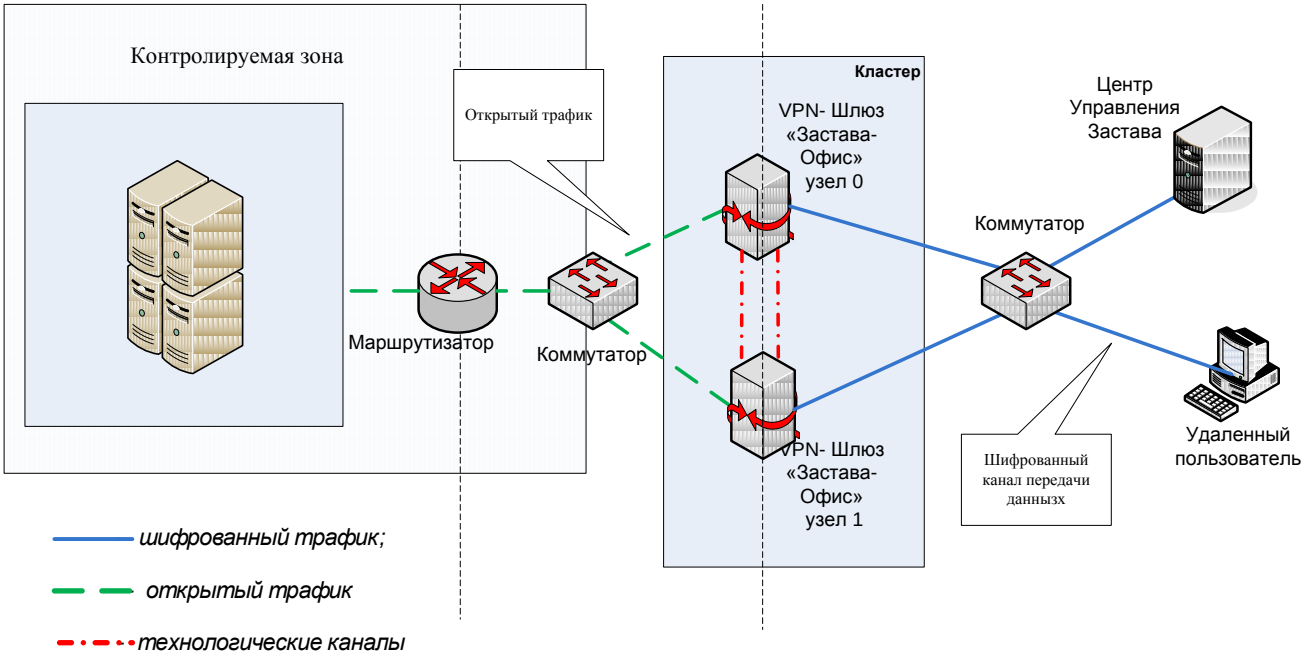
Кластерная реализация ПАК обеспечивает высокую доступность (High Availability, HA) защищаемых информационных систем.
Комплекс обеспечивает автоматическое восстановление работоспособности агентов ЗАСТАВА в случае:

- 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.

Каждый из узлов кластера работает в двух режимах - активном и пассивном. В один момент времени работает только активный узел, а пассивный узел не участвует в сетевом взаимодействии. При возникновении нештатной ситуации кластер автоматически восстанавливает работоспособность, за несколько секунд заменяя вышедший из строя узел или канал связи на резервный, пассивный. Процесс смены активного узла практически не влияет на работу систем и приложений в защищаемой зоне.

Серверные узлы кластера работают под управлением операционных систем SUN Solaris (SPARC и x86), Linux и Windows.



В качестве аппаратной платформы для VPN-шлюзов ЗАСТАВА-Офис, установленных на кластерном узле, могут использоваться как SPARC - серверы SUN Microsystems, так и компьютеры других производителей на Intel процессорах, иначе говоря, любые серверы на которых работает ОС SUN Solaris (SPARC и x86). В состав кластера могут входить до четырех однотипных узлов.

Использование комплексов высокой доступности Застава позволяет обеспечить стабильный удаленный доступ к корпоративной информационной системе и организовать надежное разделение ее на зоны, в которых обрабатывается информация разной степени секретности. Высокая производительность системы и автоматическая замена активных узлов кластера в случае отказа делают работу средств защиты практически незаметной для пользователя. Наличие сертификатов ФСТЭК на основное программное обеспечение и криптоалгоритмы позволяет применять кластерные комплексы высокой доступности ЗАСТАВА для защиты конфиденциальной информации на предприятиях оборонного комплекса, в региональных и федеральных органах власти, в государственных учреждениях и организациях.

ПРОДУКТЫ КОМПАНИИ ЭЛВИС-ПЛЮС

Семейство продуктов информационной безопасности ЗАСТАВА 5.3