ЗАСТАВА

Семейство продуктов сетевой безопасности ЗАСТАВА

Описание решения

ЭЛВИС-ПЛЮС

Сеть передачи данных на сегодняшний день является основой для функционирования всех государственных организаций и коммерческих компаний. Для эффективного противодействия угрозам средства защиты каналов связи распределенной системы должны соответствовать ряду требований:

- Они должны быть эффективными и гарантировать всестороннюю безопасность защищаемой информации.
- Они не должны существенно снижать производительность инфраструктуры.
- Они должны быть максимально удобными, а лучше, совсем незаметными, «прозрачными» для пользователей и приложений.
- Они должны быть сертифицированными, чтобы соответствовать требованиям и стандартам.
- Управление средствами защиты должно быть гибким, унифицированным и удобным для персонала, который обслуживает их.

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

С самого начала разработки семейства продуктов ЗАСТАВА большое внимание уделялось удобству и продуманности централизованного управления, поэтому в настоящий момент продукт ЗАСТАВА-Управление по функциональным возможностям не уступает ведущим мировым аналогам. Это позволяет компании ЭЛВИС-ПЛЮС реализовывать крупные проекты федерального и регионального уровня.

Продукты ЗАСТАВА сертифицированы ФСТЭК по 2-му классу защищенности межсетевых экранов и 3-му уровню контроля отсутствия недекларированных возможностей, согласно руководящим документам ФСТЭК России. Также продукты ЗАСТАВА сертифицированы в качестве средства криптографической защиты информации (СКЗИ) в системе ФСБ России по классам КС1 и КС2 (на этапе сертификации КС3).

Цели создания системы на базе продуктов ЗАСТАВА

- Создание защищённой системы обеспечения безопасности информации (СОБИ) государственных и корпоративных информационных систем с функцией централизованного управления в режиме реального времени.
- Минимизация рисков информационной безопасности при передаче информации между объектами компании.
- Создание надежной и отказоустойчивой защищенной корпоративной сети.
- Реализация требований российского законодательства и соответствующих нормативных актов в части криптографической защиты информации, передаваемой по каналам связи.

Области применения

- Создание защищенной корпоративной сети (объединение всех территориально распределенных подразделений компании в единую виртуальную сеть).

  Семейство продуктов ЗАСТАВА позволяет реализовать технологии создания виртуальных частных сетей (Virtual Private Network - VPN) на базе стандартных протоколов IPsec и IKE с использованием сертифицированных российских криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94/ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012. ЗАСТАВА поддерживает все технологии создания защищенных сетей, включая построение туннелей между узлами сети (site-to-site VPN) и методы удаленного доступа (remote access VPN), что позволяет реализовывать различные конфигурации и топологии защищенных сетей для наших заказчиков.

- Обеспечение безопасного доступа в Интернет.

  Продукты ЗАСТАВА включают встроенные функции межсетевого экранирования и трансляции сетевых адресов (Network Address Translation — NAT), что позволяет использовать их для защиты корпоративной сети при подключении к сети общего пользования Интернет. Наши решения сертифицированы ФСТЭК по 2-му классу защищенности межсетевых экранов и 3-му уровню контроля отсутствия недекларированных возможностей.

- Защищенный доступ удалённых и мобильных пользователей к корпоративной сети (предоставление защищенного доступа клиентов к сервисам компании).

  Программные агенты ЗАСТАВА-Клиент позволяют обеспечить защищенное подключение мобильных пользователей к корпоративной сети компании через сеть общего пользования Интернет. Для защиты соединения используются стандартные протоколы IPsec и IKE с шифрованием трафика с помощью сертифицированных российских криптографических алгоритмов ГОСТ 28147-89. Наши продукты позволяют работать в архитектуре, где криптографический шлюз расположен за межсетевыми экранами и реальный адрес шлюза транслируется с помощью механизмов NAT. ЗАСТАВА-Клиент также имеет встроенные функции межсетевого экрана, что позволяет обеспечить защиту мобильных пользователей.

- Защита каналов связи между центрами обработки данных.

  Продукты ЗАСТАВА могут функционировать на различных аппаратных конфигурациях, в том числе и на высокопроизводительных модульных платформах. Использование стандартной аппаратной платформы HP позволяет осуществлять параллельную обработку и обеспечивать производительность ПАК «ЗАСТАВА» при шифровании трафика до 4 Гбит/сек. Решения с применением функций распределения нагрузки дают возможность защищать широкополосные каналы связи, в том числе связывающие основной и резервный центры обработки данных федеральных и региональных органов власти, компаний корпоративного масштаба, операторов, предоставляющих услуги ЦОД.

- Внутреннее сегментирование корпоративной информационной системы для обработки информации разной степени конфиденциальности.

  ЗАСТАВА может использоваться в качестве межсетевого экрана в сетях компаний и организаций для сегментирования информационной системы. МЭ ЗАСТАВА работает на основе механизмов фильтрации пакетов с контролем соединения, что даёт необходимую гибкость в настройках политики безопасности. ЗАСТАВА сертифицирована ФСТЭК по 2-му классу защищенности межсетевых экранов и 3-му уровню контроля отсутствия недекларированных возможностей, что позволяет использовать наш продукт для

сегментирования сетей, обрабатывающих информацию различных уровней конфиденциальности (вплоть до государственной тайны).

- Межведомственное взаимодействие (подключение сетей организаций-партнеров).

  Продукты ЗАСТАВА могут использоваться для подключения отдельных компьютеров или сетей других организаций к корпоративной сети. Таким образом может быть построено межсетевое взаимодействие между разными ведомствами и государственными организациями.

Ключевые преимущества

- Высокий уровень масштабирования системы.

  Решение ЗАСТАВА является одним из самых масштабируемых решений, обеспечивающих защиту сетевого трафика с использованием сертифицированных российских криптографических алгоритмов. В рамках проектов у наших заказчиков один сервер ЗАСТАВА-Управление управляет защищённой сетью, содержащей более 10 000 агентов ЗАСТАВА. При этом нет ограничений по масштабу, количеству и форме подчинения узлов корпоративной сети.

- Централизованное иерархическое управление в режиме реального времени всей защищенной сетью из одной географической точки.

  ЗАСТАВА изначально создавались с акцентом на централизованное управление с помощью интуитивно понятного графического интерфейса. Программный продукт ЗАСТАВА-Управление имеет самый удобный, функциональный и простой интерфейс администрирования среди всех сертифицированных российских продуктов криптографической защиты сетевого трафика. Графический интерфейс продукта позволяет управлять всеми наборами правил (глобальной политикой безопасности) на основе бизнес-объектов и ролей. Политика безопасности может быть представлена в трех разных представлениях — в виде графа, таблицы и «проекции» политики на топологию сети. Также ЗАСТАВА-Управление позволяет построить иерархическое управление в больших корпоративных сетях с разграничением полномочий по управлению сетью между центром и регионами.

- Низкая стоимость приобретения, внедрения и владения.

  Применение продуктов линейки ЗАСТАВА обеспечивает низкую совокупную стоимость владения. Благодаря применению ЗАСТАВА-Управление снижаются расходы на эксплуатацию системы: удалённое администрирование отменяет необходимость содержания в штате территориально распределённой организации системных администраторов в региональных подразделениях.

- Разделение полномочий по управлению системой.

  ЗАСТАВА-Управление имеет функцию доменного управления, которая особенно актуальна для крупных корпоративных сетей, включающих в себя объекты в масштабах нескольких регионов и часовых поясов. Это позволяет выделить группы управляемых агентов по произвольным признакам (например, по региональному признаку или по принадлежности к определенным подразделениям в организационной структуре) и объединить их в логические домены. Для каждого домена можно задать собственные параметры и политики безопасности, а также передать полномочия по управлению региональные подразделения компании или межрегиональные центры компетенции.

- Высокая надежность системы.

  Продукты ЗАСТАВА позволяют обеспечить высокую доступность (High Availability, HA) защищаемых информационных систем и надежность функций защиты сетевого трафика. ПАК «ЗАСТАВА» могут объединяться в кластеры, которые работают как единый логический шлюз. 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 сбоя происходит автоматическое переключение на резервный узел кластера. Процесс смены активного узла полностью прозрачен для пользователей и приложений корпоративной сети.

- Высокая производительность.

  ЗАСТАВА функционирует на различных аппаратных платформах и поддерживает несколько типов операционных систем, что позволяет выбрать оптимальное техническое решение с учетом требований к производительности и стоимости. Эффективная реализация многопоточных вычислений позволяет достичь высоких показателей скорости шифрования даже для стандартных серверных архитектур (4 Гбит/сек). Используя опыт уже реализованных проектов, ЭЛВИС-ПЛЮС может предложить решение, позволяющее обеспечить производительность 10 Гбит/сек.

- Использование международных стандартов и протоколов сетевой защиты.

  Решение ЗАСТАВА использует международные протоколы и стандарты IPsec и IKE, что позволяет реализовать интеграцию с другими продуктами, как в части создания защищенных туннелей, так и в управлении устройствами. ЗАСТАВА на сегодняшний день является единственным российским решением, в котором реализован протокол IKEv2. В отличие от других отечественных решений, построенных на собственных (proprietary) форматах защищенных сетевых пакетов, в ЗАСТАВЕ существует возможность устанавливать защищенные VPN туннели с ведущими зарубежными решениями, а также с российскими разработками, которые реализуют стандарты IPsec. Кроме того, ЗАСТАВА-Управление может управлять конфигурациями продуктов сетевой защиты других производителей: Cisco IOS Router, МЭ Cisco ASA, Check Point VPN/FW, встроенных в ОС Microsoft Windows 2000/XP/Vista/7/8 агентов IPsec Agent, а также свободно распространяемым ПО strongSwan.

- Поддержка механизмов качества обслуживания (QoS).

  Продукты ЗАСТАВА обеспечивают возможность обработки параметров качества обслуживания, на основе значений кода DSCP содержащихся в заголовке IP пакета. Это позволяет эффективно использовать продукты ЗАСТАВА для защиты приложений, чувствительных к пропускной способности канала связи, задержкам, джиттеру (например, IP-телефонии и видеоконференций).

- Гибкость поставки системы.

  Заказчики не ограничены минимальным набором стандартных платформ. Продукты ЗАСТАВА могут поставляться как программное обеспечение, которое может устанавливаться на аппаратные серверные платформы, являющиеся стандартом у заказчика. Также мы можем поставить продукты ЗАСТАВА как программно-аппаратный комплекс с полной технической поддержкой программного обеспечения и аппаратной платформы. На сегодняшний день продукты ЗАСТАВА поддерживают все современные версии операционных систем MS Windows 7/8, MS Windows Server 2008/2012 и ALT Linux (в 32 и 64 разрядных версиях). Также ЗАСТАВА может работать под управлением операционной системы МСВС.

Архитектура и основные функции Системы

Продуктовая линейка ЗАСТАВА включает в себя следующие компоненты:

- **ЗАСТАВА-Офис** — программный шлюз, обеспечивающий защиту периметра корпоративной сети, объединение филиалов и удаленных подразделений компании в единую защищенную корпоративную сеть. Существует реализация в виде программно-аппаратных комплексов (ПАК ЗАСТАВА).
- **ЗАСТАВА-Клиент** — программный агент, обеспечивающий защищенный удаленный доступ в корпоративную сеть из любой географической точки.
- **ЗАСТАВА-Управление** — компонент централизованного управления системой защиты каналов для распределенной корпоративной сети, включая управление всеми криптографическими шлюзами и агентами (в том числе ПАК), формирование политик безопасности. 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 (принципов функционирования топологий).

ЗАСТАВА-Офис

Программный комплекс ЗАСТАВА-Офис (может быть реализован в виде ПАК ЗАСТАВА) реализует все функции по созданию защищенных туннелей с филиалами и удаленными подразделениями компании (site-to-site VPN), а также мобильными пользователями (remote access VPN). Для создания защищенных туннелей и шифрования данных ЗАСТАВА-Офис использует протоколы IPsec и сертифицированные российские СКЗИ. Весь трафик между узлами корпоративной сети шифруется в соответствии с ГОСТ 28147-89. Управление криптографическими ключами и установление IPsec соединений со шлюзами ЗАСТАВА-Офис или агентами ЗАСТАВА-Клиент производится в соответствии со стандартами IKEv2 или IKEv1. На сегодняшний день протокол IKEv2 является самым современным стандартом, который поддерживается всеми ведущими мировыми производителями оборудования и программного обеспечения, которое обеспечивает защиту каналов связи. Продукты ЗАСТАВА являются первым и единственным российским средством защиты каналов связи, которые поддерживают протокол IKEv2. Реализация нового стандарта IKEv2 в продуктах ЗАСТАВА позволила повысить производительность и безопасность работы всей системы в целом, ведь IKEv2 обладает целым рядом ключевых преимуществ по сравнению с прошлой версией протокола IKEv1:

- более гибкое использование криптографических алгоритмов;
- улучшена защита от DoS-атак;
- снижена нагрузка на сетевую инфраструктуру и аппаратное обеспечение;
- существенно повышена надёжность работы протокола в условиях, когда велика вероятность потери сетевых пакетов;
- реализована возможность использования расширений IKEv2 (например, Quick Crash Detection — QCD и IKE Fragmentation).

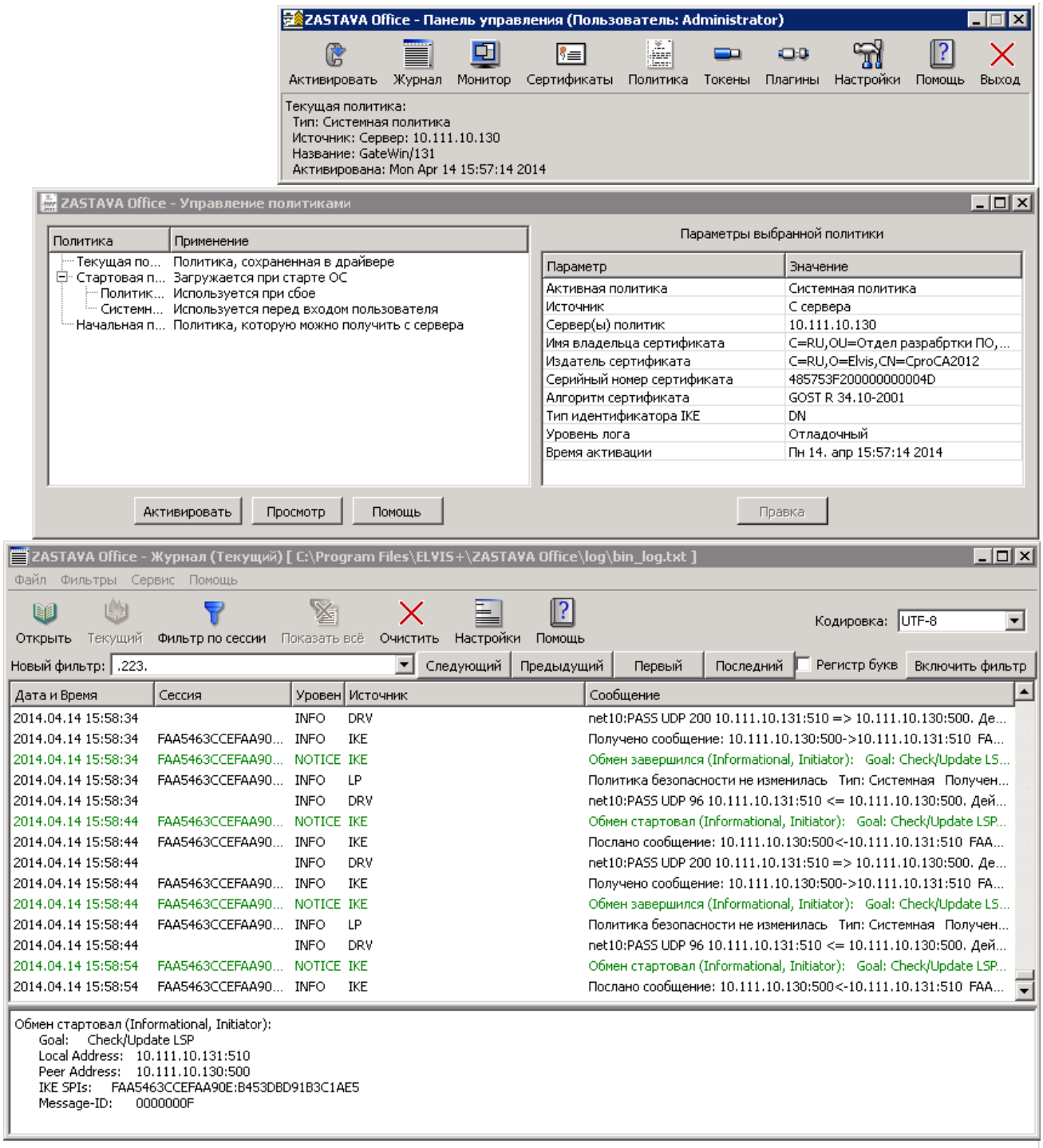

Рисунок 1. Интерфейс ЗАСТАВА-Офис

ЗАСТАВА-Офис также является и сертифицированным межсетевым экраном, который работает на основе механизма фильтрации сетевых пакетов с контролем TCP/UDP-соединений (Stateful Packet Inspection). Дополнительно межсетевой экран ЗАСТАВА-Офис включает механизмы проксирования соединений популярных сетевых сервисов и приложений (FTP, SMTP, HTTP), поддерживает протокол SOCKS, а также функции преобразования сетевых адресов (NAT).

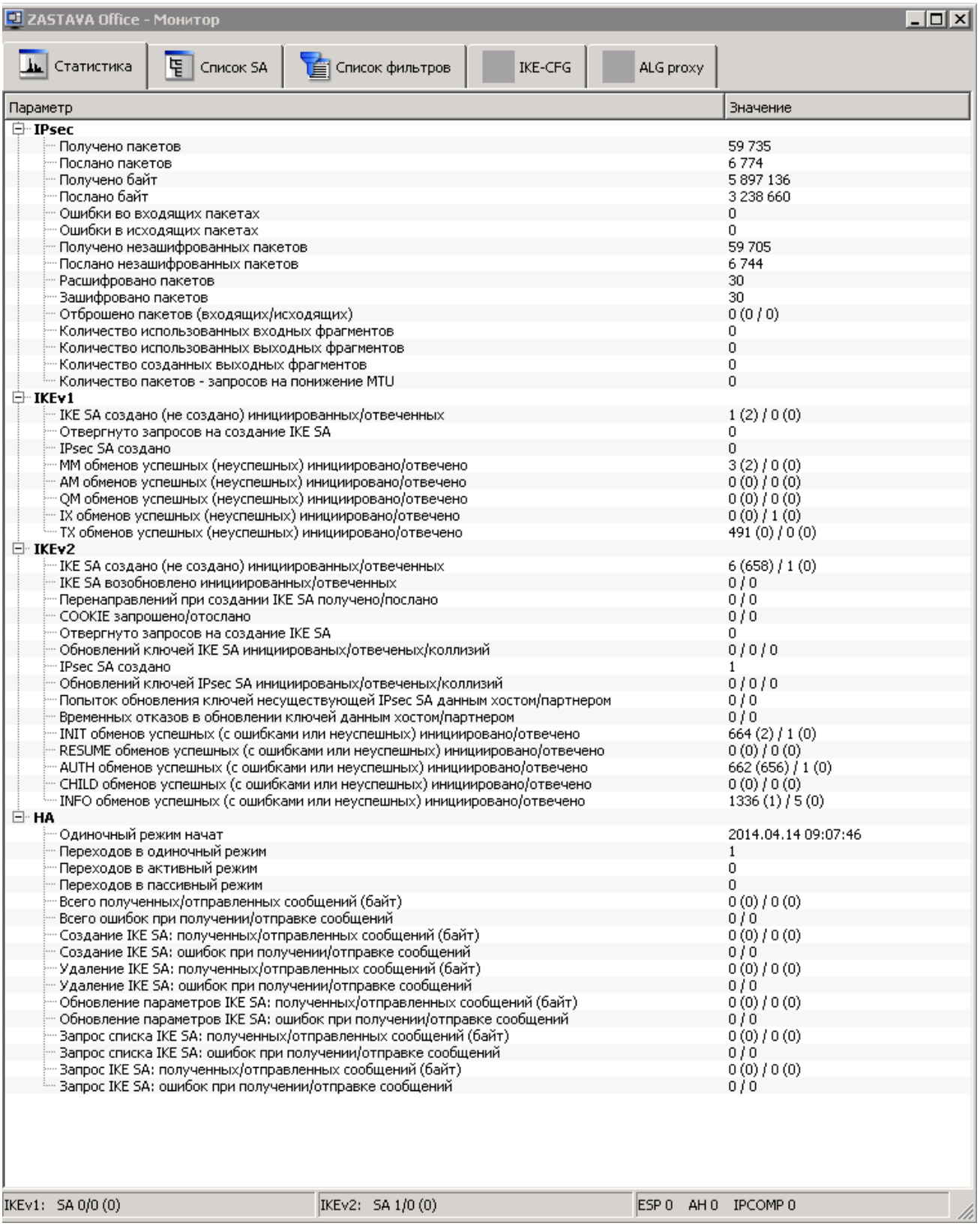

Рисунок 2. Монитор ЗАСТАВА-Офис

ЗАСТАВА-Клиент

Для организации защищенного доступа удаленных пользователей к корпоративным ресурсам на мобильных рабочих станциях устанавливаются программные агенты ЗАСТАВА-Клиент,

которые поддерживают версии операционных систем MS Windows XP/7/8, а также ALT Linux (32 и 64 разрядные). ЗАСТАВА-Клиент имеет встроенные функции межсетевого экранирования, что позволяет обеспечить защиту мобильного компьютера пользователя от несанкционированного доступа и сетевых атак в сети общего пользования Интернет, а также при подключении к публичным точкам беспроводного доступа.

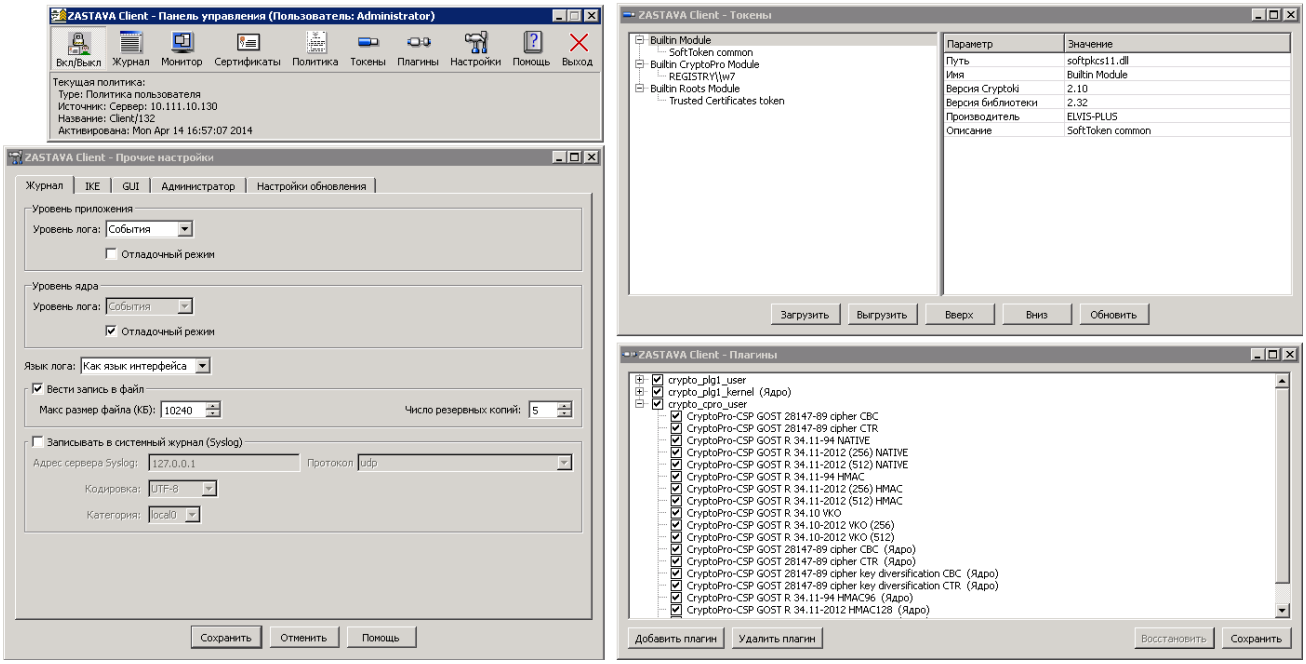

Рисунок 3. Пример защищенной корпоративной сети

ЗАСТАВА-Управление

Система централизованного управления ЗАСТАВА-Управление является наиболее функциональным, удобным и эффективным инструментом управления среди всех сертифицированных российских разработок систем защиты каналов связи.

Одним из ключевых преимуществ ЗАСТАВА-Управление является возможность масштабирования с точки зрения управления, которая достигается благодаря использованию доменной системы. Эта возможность особенно актуальна для масштабных корпоративных, географически распределенных сетей, включающих до нескольких тысяч криптографических шлюзов и удаленных агентов. Система управления позволяет объединить часть работающих узлов сети в домены по произвольным признакам, например, по географическому местоположению сетевых узлов или по принадлежности к определённому подразделению, а затем задать параметры работы для каждого домена в отдельности. ЗАСТАВА-Управление также позволяет назначать администраторов, которые будут обладать полномочиями только в своём домене, это позволит передать часть процессов управления сертификатами, хранение ключей и регистрацию событий на уровень домена (см. Рисунок **4**).

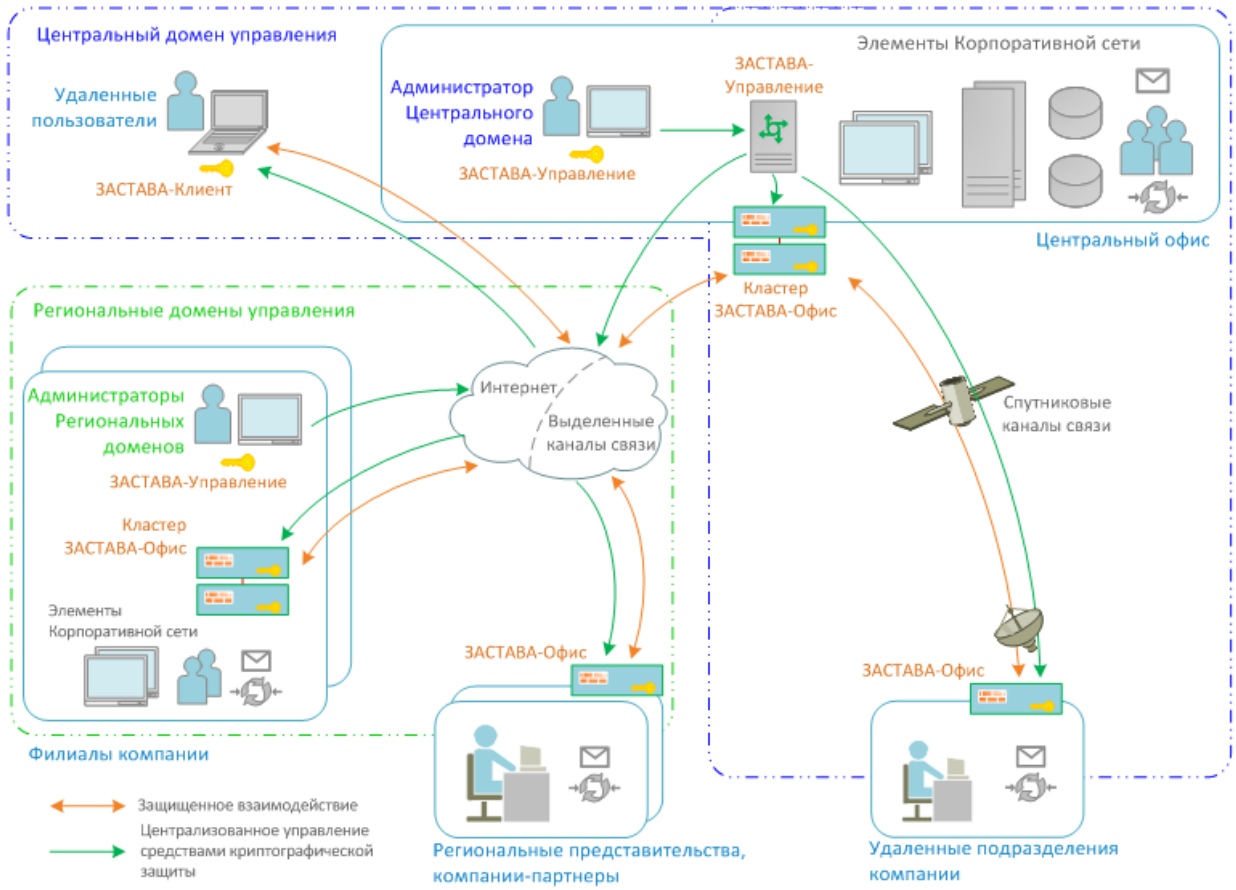

Рисунок 4. Пример защищенной корпоративной сети

ЗАСТАВА-Управление позволяет создавать единую политику безопасности — набор правил для защищаемой сети на уровне бизнес-объектов и ролей. Политика формируется в графической консоли и включает в себя сведения о топологии сети (описания объектов с их идентификационной информацией) и правила взаимодействия объектов. Создаваемая политика 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. Поддерживается несколько ролей администраторов безопасности.

Гибкие правила в компоненте ЗАСТАВА-Управление предоставляют возможность изменения свойств объектов политики межсетевого экранирования в различных представлениях (во вкладках Группы, Сетевые объекты, Пользователи, Топология, Монитор) при работе с разграниченными сегментами сети (пример интерфейса см. Рисунок). В окне Монитор можно просмотреть локальную политику безопасности любого объекта, лог-файл, лог активации, а также просмотреть и изменить свойства объекта политики.

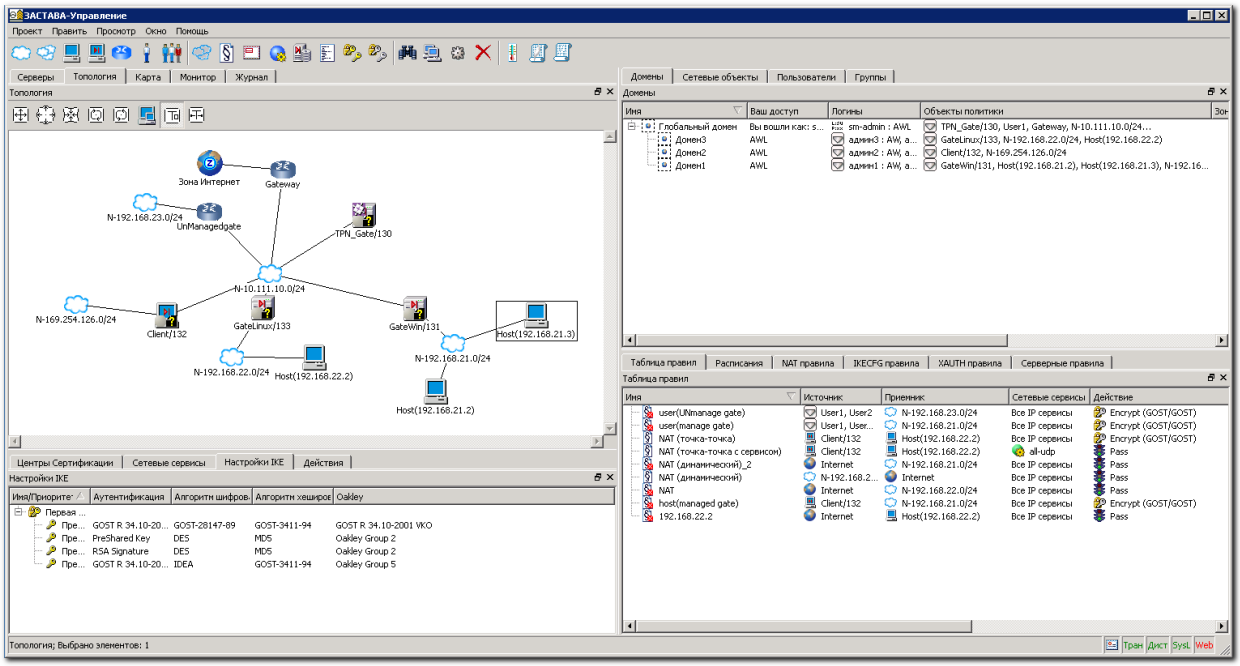

Рисунок 5. Пример графического интерфейса компонента ЗАСТАВА-Управление

В компоненте ЗАСТАВА-Управление поддерживается несколько ролей администраторов безопасности, реализована активация политик по конфигурируемому расписанию, встроена функция импорта политик VPN/FW агентов третьих производителей.

Уникальный режим представления топологии сети — наложение на географическую карту. Этот режим будет особенно удобен администраторам системы в территориально-распределённых организациях.

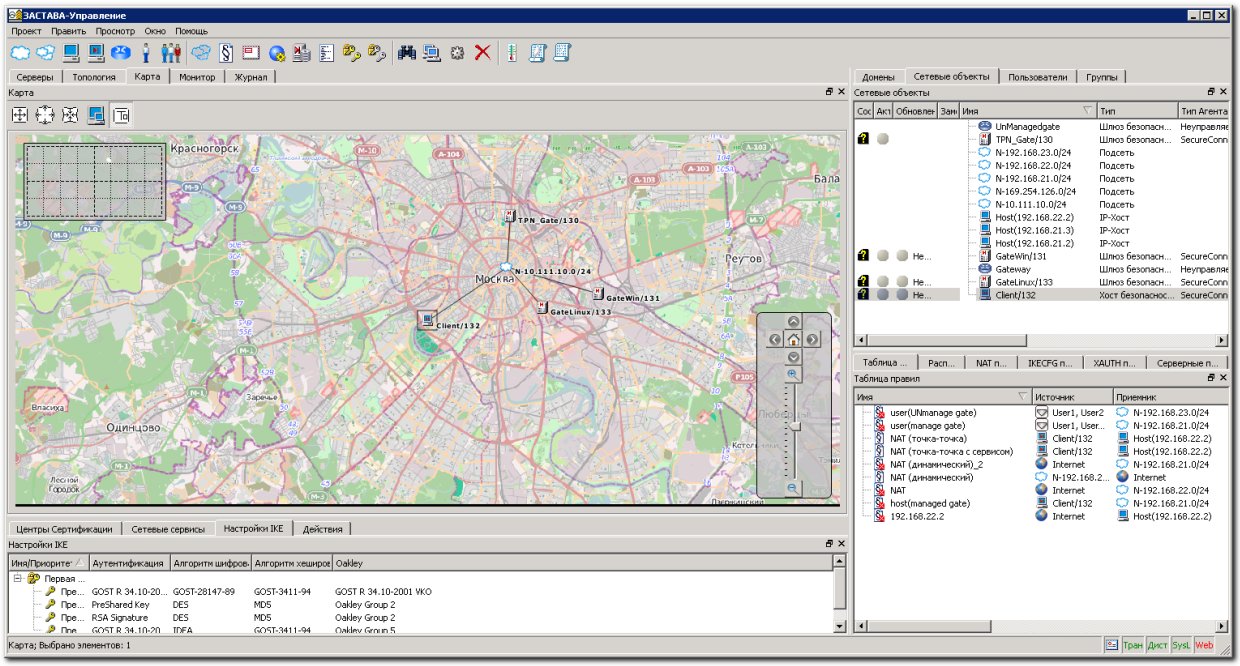

Рисунок 6. Пример графического интерфейса компонента ЗАСТАВА-Управление

Мониторинг и анализ событий ИБ

Продукты ЗАСТАВА поддерживают полноценные функциональные возможности по мониторингу работы всех компонентов защищенной сети. Компонент ЗАСТАВА-Управление собирает события со всех управляемых криптографических шлюзов и агентов мобильных пользователей. Система позволяет гибко настраивать параметры фиксации событий, имеет возможности использования глобальных и локальных настроек аудита. Журнал событий ЗАСТАВА может быть передан в SIEM-системы различных производителей для дальнейшего анализа.

Программный комплекс ЗАСТАВА также включает возможности мониторинга и управления текущими соединениями в режиме реального времени: просмотр параметров активных IKE и ESP соединений, удаление активных соединений, сортировка и выборка активных соединений. Также существует возможность мониторинга ПАК ЗАСТАВА по протоколу SNMP.

Возможности аутентификации в продуктах ЗАСТАВА

Продукты ЗАСТАВА могут использовать следующие механизмы аутентификации при установлении IPsec туннеля: разделяемый ключ (Pre-Shared Key) и сертификаты открытого ключа X.509. В сетях крупных компаний и организаций, как правило, используются сертификаты, которые выпускаются корпоративным удостоверяющим центром. Продукты ЗАСТАВА совместимы со всеми ведущими центрами сертификации российских и зарубежных производителей.

Компоненты ЗАСТАВА-Офис и ЗАСТАВА-Клиент поддерживают многофакторную аутентификацию пользователей с помощью токенов стандарта PKCS#11 (например, Aladdin eToken и JaCarta, Рутокен, SafeNet iKey и пр.). Кроме того, для аутентификации пользователей удаленных ЗАСТАВА-Клиентов шлюз ЗАСТАВА-Офис может использовать протокол EAP и внешние RADIUS-совместимые серверы аутентификации.

Обеспечение надежности

Продукты ЗАСТАВА поддерживают 2 способа обеспечения отказоустойчивых защищенных соединений в корпоративной сети.

Первый способ реализуется созданием отказоустойчивого кластера из нескольких ПАК ЗАСТАВА, которые функционируют как единый логический шлюз. Кластер может включать 2 и более шлюза ЗАСТАВА-Офис, что обеспечивает автоматическое восстановление работоспособности в случае:

- аппаратного отказа оборудования одного из узлов кластера;
- отказа каналов связи с одним из узлов.

Работу кластера поддерживает компонент ЗАСТАВА-Управление, который формирует и транслирует глобальную политику безопасности, отслеживает состояние узлов комплекса.

Каждый из узлов кластера работает в одном из двух режимов — активном или 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, переключая активный узел на один из резервных узлов.

Процесс смены активного узла не влияет на работу систем и приложений в защищаемой зоне, поскольку все параметры туннелей и соединений сохраняются и синхронизируются между узлами кластера.

Второй способ используется для обеспечения надёжности подключения мобильных пользователей и реализуется с помощью стандартных протоколов DPD (Dead Peer Detection), QCD (Quick Crash Detection) и IKE redirect . С их помощью ЗАСТАВА-Клиент автоматически в реальном масштабе времени определяет недоступность шлюза на втором конце VPN-туннеля и создает новый VPN-туннель с другим криптографическим шлюзом.

Опыт внедрения

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 нефтяной промышленности, телекоммуникационной отрасли, предприятия оборонного комплекса, региональные и федеральные органы власти, государственные учреждения и организации. Среди наших заказчиков: ФСТЭК России, Министерство обороны, Единый Информационный Расчетный Центр города Москвы, Федеральная служба государственной регистрации, кадастра и картографии (Росреестр), Единая мультисервисная телекоммуникационная сеть Санкт-Петербурга, Государственные учреждения Республики Татарстан, ФСК ЕЭС, Российский Союз Автостраховщиков, медицинские учреждения Ханты-Мансийского Автономного округа, Ямало-Ненецкого Автономного округа, Тамбовской области и Республики Калмыкии.

Росреестр

Сотрудничество с Управлением Росреестра началось в 2009 г. Продукты линейки ЗАСТАВА выбраны в качестве основного FW/VPN-решения. За прошедшее время был выполнен проект по защите каналов связи Федеральной системы Росреестра и её региональных подразделений. В настоящий момент успешно функционирует более 5000 ПАК ЗАСТАВА и центр управления ЗАСТАВА-Управление. В данный момент в этой системе федерального уровня планируется более 15 000 агентов.

Проекты в Санкт-Петербурге

Сотрудничество с Комитетом Информатизации и Связи Правительства Санкт-Петербурга началось в 2006 г. Первоначально Санкт-Петербургский Информационно-Аналитический центр провел тестирование ряда FW/VPN-решений, представленных на российском рынке. По его итогам продукты линейки ЗАСТАВА были выбраны основным решением для обеспечения безопасности на сетевом уровне при взаимодействии государственных и муниципальных структур г. Санкт-Петербурга.

За прошедшее время выполнен ряд проектов в разных структурах правительства Санкт-Петербурга, в том числе:

- Организация защищенного взаимодействия в ЕМТС Санкт-Петербурга.
- Подключение АИС ЗАГС Санкт-Петербурга.

- Подключение к ЕМТС ИОГВ Санкт-Петербурга.

В настоящий момент установлено около 1 200 экземпляров ЗАСТАВА-Офис и 400 экземпляров ЗАСТАВА-Клиент.

Проекты в Республике Татарстан

Сотрудничество с Республикой Татарстан началось в 2005 г. За прошедшее время выполнен ряд проектов в разных структурах Республики, в том числе:

- В систему казначейского распределения бюджета Республики Татарстан проведена поставка и установка ПО ЗАСТАВА-Офис — 132 шт., ПО ЗАСТАВА-Клиент — 786 шт. и ПО ЗАСТАВА-Управление. Общее количество инсталляций в Системе составляет около 6 000 клиентов.
- Центр Информационных Технологий Республики Татарстан закупил ПО ЗАСТАВА для защиты органов государственной власти. В настоящее время в ЦИТ РТ работает 246 ПО ЗАСТАВА-Офис и 1809 ПО ЗАСТАВА-Клиент.
- В Администрацию Президента Республики Татарстан провидена поставка ПО ЗАСТАВА-Управление, ПО ЗАСТАВА-Офис, ПО ЗАСТАВА-Клиент для удаленного доступа с последующим присоединением к ЗСПД органов государственной власти Республики Татарстан.

В 2013 году стартовал проект защиты медицинской информационной системы Республики Татарстан: 12 000 рабочих мест.

Проекты в Москве

Сотрудничество с правительством города Москвы началось в 2007 г. За прошедшее время был выполнен проект по защите каналов связи Единого Информационно-расчетного центра города Москвы. В настоящий момент успешно функционирует 4 300 экземпляров ЗАСТАВА-Клиент и центр управления ЗАСТАВА-Управление.

В 2013 году стартовал проект защиты сети многофункциональных центров г. Москвы. За счет применения продуктов ЗАСТАВА в данном проекте удалось существенно сократить стоимость проекта и обеспечить простоту дальнейшей эксплуатации системы.

Технические параметры и характеристики

Параметр	Описание
Шифрование трафика (VPN)	
Поддерживаемые алгоритмы шифрования	ГОСТ 28147-89, AES (256, 192, 128 бит), 3DES, DES
Поддерживаемые алгоритмы хэширования	ГОСТ Р 34.11-94/ГОСТ Р 34.11-2012, MD5, SHA-1
Поддерживаемые алгоритмы электронной подписи	ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012, RSA, DSA
Поддерживаемые сертифицированные криптопровайдеры	КриптоПро CSP (Крипто-Про)
Возможность подключения криптографических библиотек	Открытый интерфейс CryptoApi, который позволяет подключить любые библиотеки (например, Крипто-КОМ (Сигнал-КОМ), Верба (МО ПНИЭИ) и пр.)
Возможность подключения токенов (смарт-карт)	Стандартный интерфейс PKCS#11 (API Cryptoki - cryptographic token interface), включая поддержку российской криптографии в соответствии с PKCS#11 2.30
Поддерживаемые протоколы IPsec	Encapsulating Security Payload (ESP), Authentication Header (AH), Internet Security Association and Key Management Protocol (ISAKMP), IKEv1/2
Стандарты обмена ключами и установления туннелей	IKEv1, IKEv2
IPSec VPN ГОСТ 28147-89, максимальная производительность	4 Гбит/сек с одного ПАК ЗАСТАВА
Максимальное количество туннелей IPSec VPN (site-to-site)	Ограничений нет
Максимальное количество туннелей IPSec VPN (remote access)	Ограничений нет
Поддержка функций установки туннелей через промежуточные NAT-устройства	Да, инкапсуляция IPsec в UDP
Обеспечение отказоустойчивости	High Availability кластер криптошлюзов ЗАСТАВА-Офис (режим active-passive) Протоколы DPD (Dead Peer Detection), QCD (Quick Crash Detection), и IKE redirect
Поддержка сертификатов X.509	Да
Аутентификация пользователей	Сертификаты X.509 Pre-shared keys Предварительно распределенные ключи XAUTH, EAP

Функции межсетевого экранирования	
Технология межсетевого экранирования	Фильтрация сетевых пакетов с контролем TCP/UDP-соединений (Stateful Packet Inspection)
Фильтрация на транспортном уровне протокола IP	Да
Возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети	Да
Поддержка протоколов прикладного уровня	FTP, SMTP, HTTP, SOCKS
Возможность включения ограничения по времени в правила фильтрации	Да
Максимальное количество одновременных соединений	Не ограничено
Сетевые функции	
Поддержка механизмов качества обслуживания (QoS)	Обработка параметров качества обслуживания, на основе значений кода DSCP
Поддержка механизмов сжатия IP-пакетов	Да, IP Payload Compression Protocol (IPComp)
Поддержка механизма трансляции сетевых адресов	NAT (Network Address Translation), PAT (Port Address Translation)
Статическая маршрутизация	Да
Поддержка динамических протоколов маршрутизации	Да
Поддержка протоколов групповой передачи (Multicast)	Да
Функции управления и мониторинга	
Наличие системы централизованного управления	Да
Возможность локального управления	Да
Возможность построения иерархической системы управления	Да, поддерживается иерархия управления – доменная структура
Возможность управления сторонними устройствами и ПО	Да, Cisco IOS Router, МЭ Cisco PIX (Cisco ASA), Check Point VPN/FW, Microsoft IPsec Agent, strongSwan
Разграничение прав доступа к интерфейсу управления на основе ролей	Да
Возможности разграничения доступа по устройствам/группам	Да, на основе доменной структуры

устройств	
Аудит действий по управлению системой	Да
Наличие встроенного журнала событий	Да
Возможность интеграции с Security Information and Event Management (SIEM) системами	Да (Syslog)
Поддержка протоколов сетевого управления	SNMP
Возможность централизованного обновления ПО	Да
Поддерживаемые ОС	
ЗАСТАВА-Офис	MS Windows Server 2003/2008/2012, ALT Linux 6.0 СПТ, ALT Linux 6.0 Centaurus, ALT Linux BC
ЗАСТАВА-Клиент	Windows XP/7/8, ОС ALTLinux 6.0 СПТ/6.0 Centaurus и ОС ALTLinux BC (32 и 64 разрядные версии для всех ОС)
ЗАСТАВА-Управление	ОС Microsoft Windows Server 2008/2012