Экз. № _____

ЗАО «Энвижн Груп»

УТВЕРЖДАЮ

Директор филиала
ЗАО «Энвижн Груп» Энвижн-Сибирь

_____ Д.Г. Гоков
«___» _____ 2011 г.

Руководитель технического отдела
филиала ЗАО «Энвижн Груп» Энвижн-Сибирь

_____ А.В. Шовкун
«_____» _____ 2011 г.

УТВЕРЖДАЮ

Ректор ФГАОУ ВПО «Сибирский федеральный университет»

_____ Е.А. Ваганов
«___» _____ 2011 г.

_____
«_____» _____ 2011 г.

Создание защищенной сети отдела бухгалтерии в составе задачи по защите персональных данных, обрабатываемых в ФГАОУ ВПО «Сибирского федерального университета»

Технический проект

Пояснительная записка

NV.01. 011422.СФУ.БУХ.П2

2011

Инв. № подл.	Подпись и дата	Взамен инв. №	Инв. № дубл.	Подпись и дата

Содержание

Подпись и дата | Инв. № дубл. | Взамен инв. № | Подпись и дата | Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата	NV.01. 011422.СФУ.БУХ.П2		
Разработал		Гасенко		02.2011	Пояснительная записка	Стадия	Лист	Листов
Проверил		Кочетков		02.2011		ТП	2	61
Н. контр.		Соломагин		02.2011				
Утвердил		Шовкун		02.2011				

NVisionGroup

Список сокращений и условных обозначений

Сокращение	Расшифровка
СА	Certification Authority (Центр сертификации)
АРМ	Автоматизированное рабочее место
ВОЛС	Волоконно-оптическая линия связи
ИС	Информационная система
МЭ	Межсетевой экран
ОС	Операционная система
ПО	Программное обеспечение
СКС	Структурированная кабельная система

1 Общие положения

1.1 Наименование проектируемой системы: создание защищенной сети отдела бухгалтерии в составе задачи по защите персональных данных, обрабатываемых в «Сибирском федеральном университете».

1.2 Сокращённое наименование системы: защищенная сеть бухгалтерии.

1.3 Перечень организаций, участвующих в разработке

Заказчиком проекта является ФГАОУ ВПО «Сибирский федеральный университет» (далее – Заказчик).

Исполнитель работ: ЗАО «Энвижн Груп».

1.4 Перечень работ

Создание защищенной сети бухгалтерии включает следующие работы:

- обследование, анализ исходных данных по объектам Заказчика;
- разработка технического проекта по созданию защищенной сети бухгалтерии;
- закупка оборудования;
- установка и настройка оборудования;
- приемо-сдаточные испытания.

1.5 Назначение, цели создания и функции защищенной сети бухгалтерии

1.5.1 Назначение защищенной сети бухгалтерии

В настоящее время в сети бухгалтерии Заказчика обрабатывается информация ограниченного доступа, в том числе персональные данные. Для защиты этой информации и с целью соблюдения требований № 152-ФЗ «О персональных данных» предлагается выделить часть общей сети СФУ в отдельный изолированный сетевой сегмент и внедрить систему усиленной аутентификации пользователей.

1.5.2 Цели создания

Целью создания защищенной сети бухгалтерии является обеспечение комплексной защиты информации, передаваемой, накапливаемой и обрабатываемой во всех информационных системах Заказчика. Цель создания защищенной сети бухгалтерии достигается применением соответствующей архитектуры сети и программно-технических средств обеспечения безопасности, противодействующих актуальным угрозам информационной безопасности.

Работы по созданию защищенной сети бухгалтерии проводятся с учетом требований законодательства Российской Федерации и действующих руководящих и нормативных документов по защите конфиденциальной информации и персональных данных.

Основные цели защиты информации в защищенной сети бухгалтерии предусматривают:

- предотвращение несанкционированного доступа к информации со стороны внешних нарушителей;

- предотвращение несанкционированного доступа к информации со стороны внутренних нарушителей;
- сохранение возможности управления процессом обработки, хранения и использования информации в условиях несанкционированных воздействий на защищаемую информацию.

1.7 Функции защищенной сети бухгалтерии

Компоненты защищенной сети бухгалтерии комплексно выполняют следующие функции по защите информации:

- идентификация и аутентификация пользователей;
- разграничение доступа к информационным и техническим ресурсам;
- межсетевое экранирование;
- регистрация и учёт показателей состояния информационной безопасности;
- обнаружение вторжений.

1.8 Сведения об использовании при проектировании нормативно-технических документов

Работы по созданию защищенной сети бухгалтерии проводятся в соответствии с федеральными законами, стандартами и действующими руководящими и нормативными документами уполномоченных органов исполнительной власти, основные из которых следующие:

- Федеральный закон от 27.07.06 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.06 года № 152-ФЗ «О персональных данных»;
- Указ Президента РФ от 12 мая 2004 года N 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указ Президента РФ от 23 сентября 2005 года N 1111 «О внесении изменения в перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 г. N 188»;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России;
- Приказ ФСТЭК России от 5.02.2010 N 58, зарегистрирован в Минюсте России 19.02.2010 № 16456;
- Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций
- Приказ Роскомнадзора «Об утверждении образца формы уведомления об обработке персональных данных»;
- Административный регламент проведения Роскомнадзором проверок соблюдения законодательства о персональных данных.
- «Доктрина информационной безопасности Российской Федерации» от 9.09.2000 года;
- ГОСТ 34.601-90. «Автоматизированные системы. Стадии создания»;

- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
- ГОСТ Р 51583-2000. «Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 50922-96. «Защита информации. Основные термины и определения»;
- ГОСТ 34.602–89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ Р 50739-95. «Средства вычислительной техники. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»;
- ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ 50922-2006. «Защита информации. Основные термины и определения»;
- ГОСТ 51583-2000. «Порядок создания АС в защищенном исполнении»;
- «Положение о сертификации средств защиты информации по требованиям безопасности информации». Приказ Председателя Гостехкомиссии России от 27.10.1995 г. №199. Зарегистрировано Госстандартом России в Государственном реестре 20.03.1995 г. (Свидетельство №РОСС 1Ш.0001.01БИОС MS Windows SPR);
- «Положение по аттестации объектов информатизации по требованиям безопасности информации». ФСТЭК России (Гостехкомиссии России), 1994.
- РД ФСТЭК России (Гостехкомиссии России). «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30 марта 1992 г.;
- РД ФСТЭК России (Гостехкомиссии России). «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992 г.;
- РД ФСТЭК России (Гостехкомиссии России). «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 года;
- РД ФСТЭК России (Гостехкомиссии России). «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 30 марта 1992 г.;
- РД ФСТЭК России (Гостехкомиссии России). «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25 июля 1997 г.;
- РД ФСТЭК России (Гостехкомиссии России). «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» от 4 июня 1999 г. № 114.;
- РД ФСТЭК России (Гостехкомиссии России). «О защите информации при вхождении России в международную информационную систему Интернет» от 21 октября 1997 г № 61.;

- РД ФСТЭК России (Гостехкомиссии России) «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.» Части 1, 2 и 3» и ГОСТ 15408 «Критерии оценки безопасности информационных технологий»;
- Инструкция ФСБ России (ФАПСИ). «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Утверждена приказом ФАПСИ от 13 июня 2001 г. № 152, зарегистрирована Минюстом России от 6 августа 2001 г. № 2848);
- Выписка из «Требований к средствам криптографической защиты конфиденциальной информации» ФСБ России (ФАПСИ);
- Выписка из «Временных требований к информационной безопасности удостоверяющих центров» ФСБ России (ФАПСИ);
- Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности ISO/IEC 17799:2005.

2 Характеристика объекта информатизации, требования к системе

2.1. Характеристика объекта информатизации

2.1.1. Общие сведения об объекте информатизации

ИС Заказчика представляет собой совокупность сетевого коммутационного оборудования, серверной платформы и АРМ пользователей. В настоящее время сегмент сети бухгалтерии не отделен от общей сети СФУ. Кроме того, на АРМ пользователей настроена локальная однофакторная аутентификация на основе связки логин/пароль.

2.1.2. Объекты защиты

Объектами защиты являются:

- сегмент сети, относящийся к бухгалтерии;
- АРМ пользователей;
- серверная платформа.

2.2. Общие требования к построению решения

Требования к построению защищенной сети бухгалтерии приведены в техническом задании, которое является неотъемлемой частью данной проекта.

2.2.1. Требования к вычислительной технике

Должны быть выполнены организационно-технические мероприятия, исключающие возможность несанкционированного изменения пользователями состава программно-аппаратных средств.

Компьютеры АРМ пользователей должны отвечать следующим минимальным требованиям:

- процессор Pentium III 500 МГц;
- ОЗУ 256 Мбайт;
- сетевой адаптер Ethernet 10/100 Мбит/сек;
- порт USB.

2.2.2. Требования к программному обеспечению

На всех АРМ пользователей, входящих в состав ИС должна быть установлена операционная система Windows XP/Vista/7.

На сервере безопасности защищенной сети бухгалтерии должна быть установлена операционная система Windows Server 2008 R2.

2.2.3. Требования к сетевой инфраструктуре

Для нормального функционирования защищенной сети бухгалтерии необходимо, чтобы все вычислительные средства взаимодействовали между собой по протоколу IP.

Особые требования к коммутационному оборудованию не предъявляются.

3 Основные технические решения по изменению сетевой части

3.1. Состав проектируемой системы

В соответствии с требованиями проектируемая сеть состоит из восьми коммутаторов уровня доступа, коммутатора агрегации и межсетевого экрана. Размещение оборудования осуществляется в учебных корпусах в специализированных помещениях Сибирского федерального университета, отвечающих необходимым требованиям.

3.2. Назначение настоящего раздела документа

Данный раздел технического проекта содержит детальное описание технических решений и архитектуры сети передачи данных отдела бухгалтерии. Технический проект документирует выбранный дизайн сети, ее конфигурацию, описание функционирования и возможностей.

3.3. Характеристика состава структуры сооружений и линий связи

В помещении 32-00 установлены существующие коммутаторы Cisco 2960G-24 и 2960G-24.

В помещении 22-05 установлены существующие коммутаторы Cisco 3560, 2960G-48 и 2960G-24. Проектом предусматривается высвобождение коммутатора Cisco 3560. В коммутаторы 2960G-48 и 2960G-24 добавляются SFP модули 1GE BX-U по 1шт.

В помещении 12-00 установлены существующие коммутаторы Cisco 3560, 2960G-24. Проектом предусматривается высвобождение коммутатора Cisco 3560. В коммутатор 2960G-24 добавляется один SFP модуль 1GE BX-U.

В помещении 21-03 установлен существующий коммутатор Cisco 2960G-24.

В помещении Дата центра 30-00 установлены - существующий модульный коммутатор Cisco 6500 и сервера HP Blade System. Проектом предусматривается добавление коммутатора Cisco 3750G с оптическими трансиверами 1GE BX-D и брандмауэра Stonegate FW-1030.

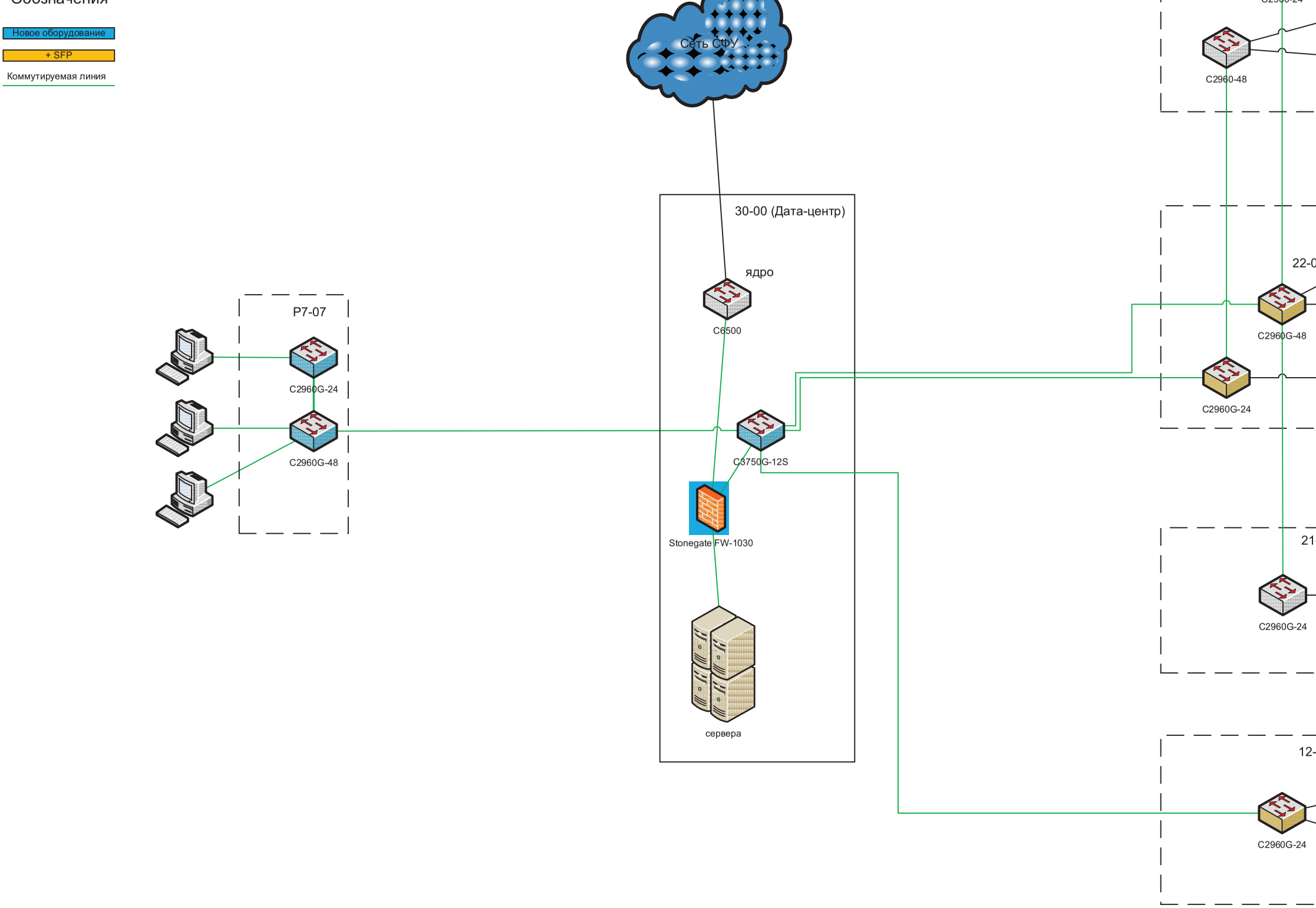


Рис. 1. Структурная схема решения

В помещении библиотеки Р7-07 установлен модульный коммутатор Cisco 4500. Проектом предусматривается установка коммутаторов Cisco 2960G-24 и 2960G-48 с одним SFP модулем 1GE BX-U.

Серверное оборудование подключено в коммутатор Cisco Cat6500. Проектом предусматривается переключение серверного оборудования в брандмауэр Stonegate. Брандмауэр подключается в существующий коммутатор С6500 и в новый С3750G. Коммутаторы рабочих групп переключаются в коммутатор С3750G.

3.4. Логическая структура сети

Рабочие группы пользователей подключаются в коммутаторы доступа Cisco 2960G в определенные VLAN из таблицы 1. Порты рабочих групп настраиваются в режим switchport access.

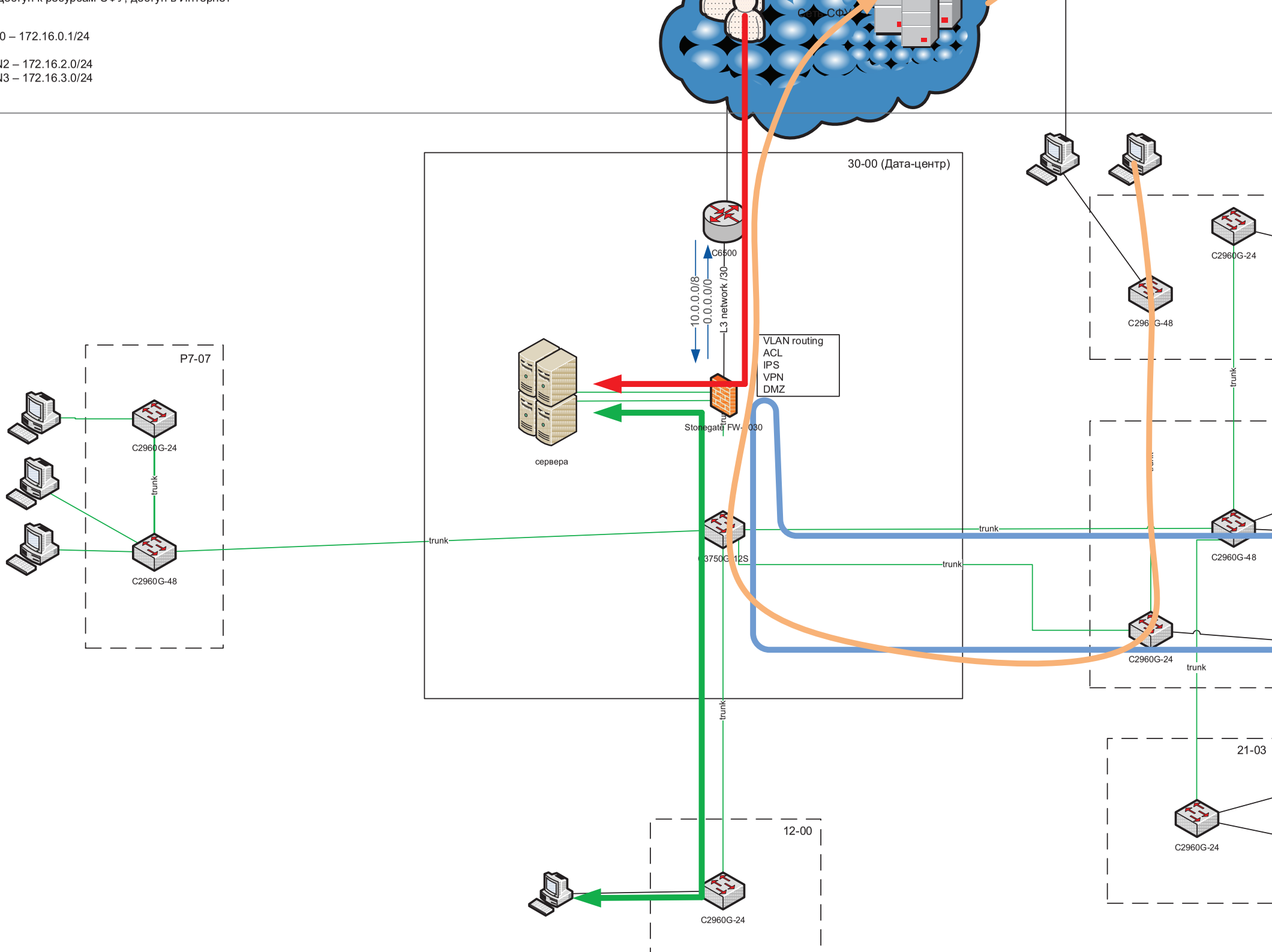
Коммутаторы доступа подключаются в С3750G в режиме trunk с инкапсуляцией 802.1q. На портах разрешается использование VLAN, которые используются на коммутаторе доступа. Все пользовательские и служебные VLAN терминируются на брандмауэре StoneGate.

Брандмауэр Stonegate является центром изолированной сети бухгалтерии СФУ. Обеспечивает непосредственное подключение серверов, связь с сетью СФУ (через С6500), отвечает за маршрутизацию и фильтрацию трафика, предоставляет доступ к серверам бухгалтерии по VPN для пользователей из других сетей.

Доступ к ресурсам СФУ, доступ в Интернет

DMZ – VLAN100 – 172.16.0.1/24

ROUP2 – VLAN2 – 172.16.2.0/24
ROUP3 – VLAN3 – 172.16.3.0/24



3.5. Организация VLAN

В данном проекте используется схема организации VLAN, максимально учитывающая особенности существующей схемы разделения на VLAN. Основные VLAN, используемые в сети, приведены в Табл. 1.

Табл. 1. VLAN, используемые в сети

Номер VLAN	Название VLAN	Проект VLAN	Сущ. подсеть	Проект. подсеть	Описание
0	--	-	-	-	Недоступен для использования.
1	--	сущ.	-	-	Используется различными служебными управляющими протоколами (Spanning Tree, VTP, etc).
245	MGMT	сущ.	10.0.245.0/24	172.16.245.0/24	Технологическая сеть для управляющих интерфейсов существующих устройств (порты/интерфейсы управления коммутаторов, серверов и т.д.).
244	ASU	сущ.	10.0.244.0/24	172.16.244.0/24	Рабочие станции администраторов АСУ
240	SERVERS	сущ.	10.0.240.0/24	172.16.240.0/24	Серверы
242	BUH	сущ.	10.0.242.0/24	172.16.242.0/24	Бухгалтерия
241	KADR	сущ.	10.0.241.0/24	172.16.241.0/24	Отдел кадров
100	YURIST	сущ.	10.0.100.0/24	172.16.100.0/24	Юридический отдел
73	LOGIST	сущ.	10.0.73.0/24	172.16.73.0/24	Отдел логистики
239	RASCH	нов.	-	172.16.239.0/24	Расчетчики
238	RUK	нов.	-	172.16.238.0/24	Руководители
237	PFU	нов.	-	172.16.237.0/24	ПФУ
236	SED	нов.	-	172.16.236.0/24	СЭД
235	MAT	нов.	-	172.16.235.0/24	Материальная группа
234	3112	нов.	-	172.16.234.0/24	3112
233	PODOTCH	нов.	-	172.16.233.0/24	Подотчет

Использование технологического VLAN 1 для создания интерфейсов управления и мониторинга, а так же использование данного VLAN в любых других целях не рекомендуется по соображениям безопасности. Все неиспользуемые порты коммутаторов рекомендуется назначать в VLAN 1001 и исключать этот VLAN из списка разрешенных VLAN на транковых портах, что позволит не допустить несанкционированный обмен трафиком между указанными портами на разных коммутаторах.

3.6. Переключение по этапам

Необходимо обеспечить плавную миграцию пользователей с минимально возможным перерывом сервиса. Перевод пользователей будет проводиться в несколько этапов.

Этап №1. Предварительный.

Между проектируемым коммутатором C3750G и коммутатором ядра C6500 организовывается физическое подключение по каналу Ethernet. Подключаемые порты настраиваются в режим trunk 802.1q. На портах разрешается обмен информации в существующих VLAN бухгалтерии СФУ – 245, 244, 240, 242, 241, 100, 73. Указанные VLAN должны быть созданы на коммутаторе C3750G.

В помещении P7-07 устанавливаются новые коммутаторы C2960G и коммутируются к коммутатору C3750G по оптическому Ethernet каналу согласно схеме подключений. Выполняется настройка коммутаторов C2960G.

Брандмауэр Stonegate подключается к коммутатору C3750G по каналу Ethernet. Дополнительные настройки не применяются.

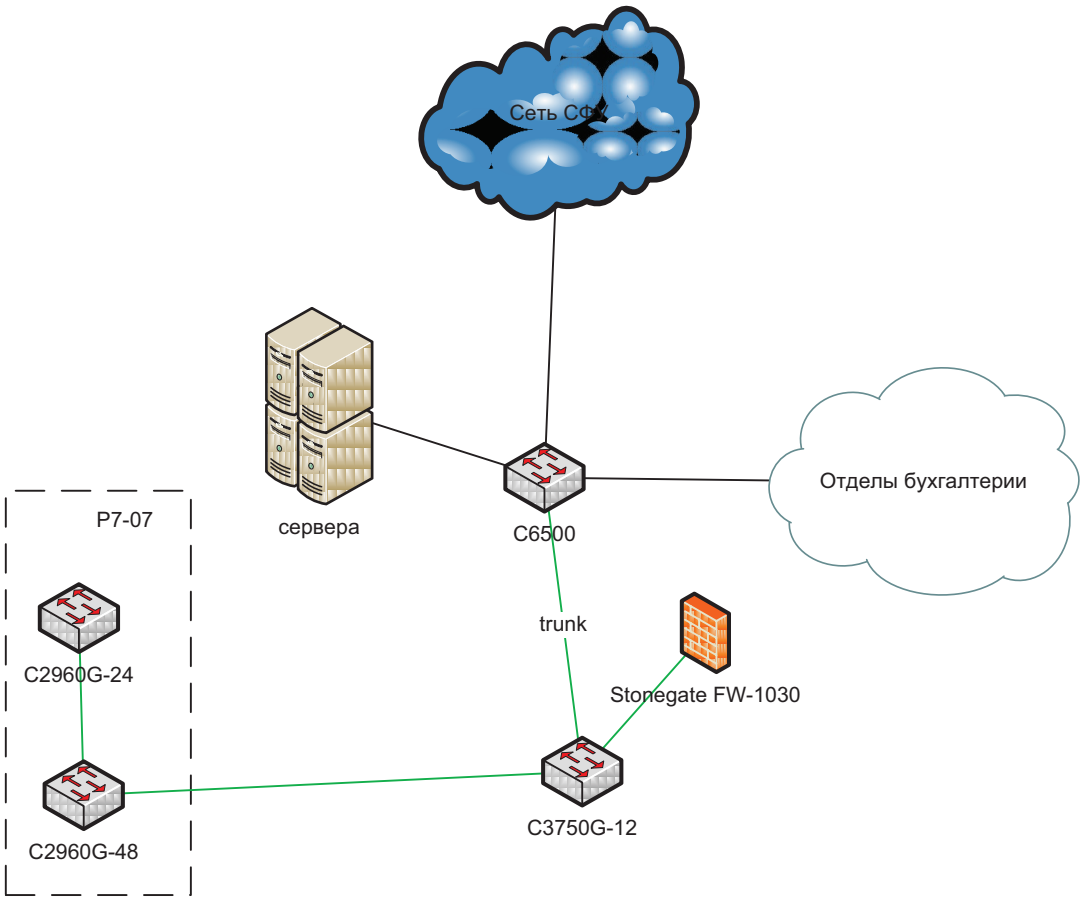


Рис. 3. Схема подключения этапа №1

Этап №2. Переключение пользователей и коммутаторов.

1. В помещении Р7-07 по мере необходимости производится переключение пользователей отдела бухгалтерии с коммутатора С4500 на новые коммутаторы С2960G-24 и С2960G-48.
2. В помещении 12-00 коммутатор С2960G-24 переключается по новой ВОЛС в коммутатор С3750. Выполняется настройка оптических интерфейсов коммутаторов. Связь между С2960G и С3560 расформировывается.
3. В помещении 21-03 коммутатор С2960G-24 переключается в коммутатор С2960G-48 в 22-05 с выполнением соответствующих настроек устройств.
4. В помещении 22-05 расформировывается линия связи между коммутатором С3560 и С2960G-48. Расформировывается линия связи между С2960G-24 и С2960G-48. От каждого из коммутаторов С2960G-24 и С2960G-48 организовывается по одной ВОЛС до коммутатора С3750G с выполнением соответствующих настроек интерфейсов.
5. В помещении 32-00 расформировывается линия связи между коммутаторами С2960G-24 и С2960G-48. Коммутатор С2960G-24 подключается в коммутатор С2960G-48 находящийся в комнате 22-05 с выполнением соответствующих настроек интерфейсов.
6. Расформировывается линия связи между коммутатором С2960G-48 находящимся в помещении 32-00 и коммутатором С3560 (22-05). Коммутатор С2960G-48 (32-00) подключается по новой линии связи в коммутатор С2960G-24 (22-05) с выполнением соответствующих настроек оптических интерфейсов.

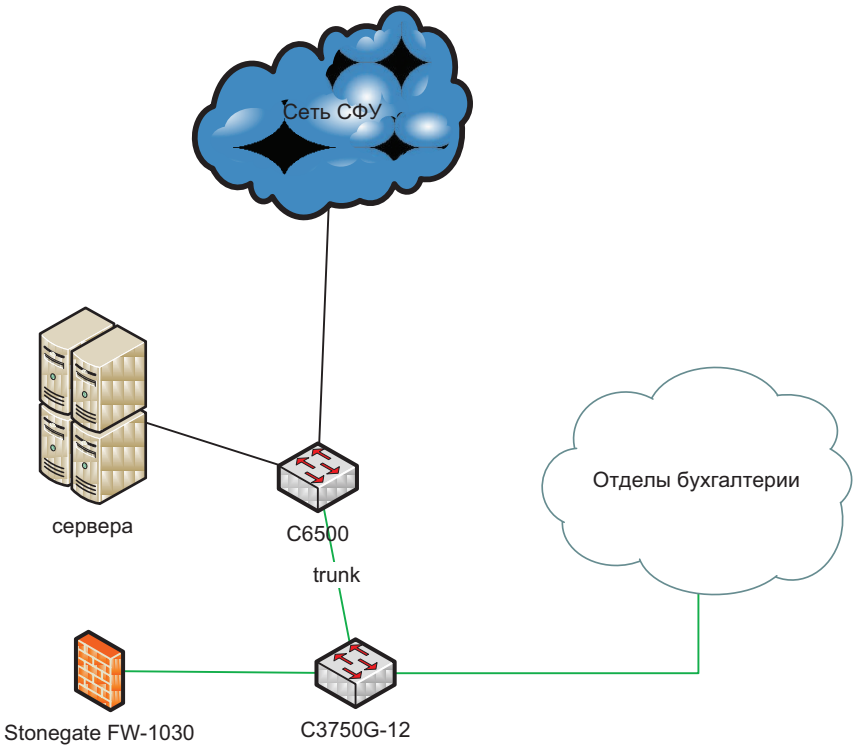


Рис. 4. Коммутаторы отдела бухгалтерии переключены в C3750G

Коммутатор C3750 обеспечивает прохождение трафика до серверов, позволяя в дальнейшем переключить сервера в брандмауэр с минимальным перерывом сервиса.

Этап №3. Переключение серверов. Подключение брандмауэра.
Этап №3.1

1. Расформировывается линия связи между коммутаторами C3750G и C6500.
2. На брандмауэре Stonegate создаются логические интерфейсы существующих VLAN (из табл. №1) для полноценной маршрутизации трафика в изолированном сегменте. Например, интерфейс VLAN 245 с IP адресом 10.0.245.1/24.
3. Сервера переключаются в брандмауэр Stonegate.

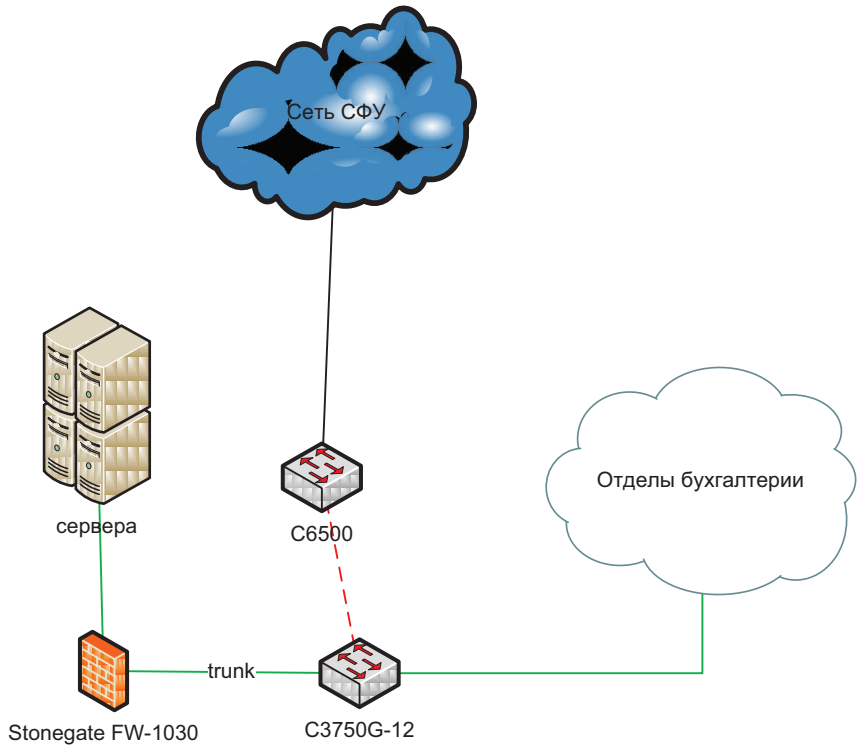


Рис. 5. Сервера переключены, сетевой сегмент отдела бухгалтерии изолирован

После этого переключения за всю маршрутизацию трафика в сегменте будет производить брандмауэр Stonegate. Сетевой сегмент отдела бухгалтерии становится полностью автономным. В последующем можно будет сменить сетевую адресацию и организовать связность с сетью СФУ (оборудованием ядра сети).

Этап №3.2

Пользователи, находящиеся за пределами сети бухгалтерии, в сети СФУ должны иметь контролируемый доступ к серверам и прочим ресурсам изолированной сети. Пользователи отдела бухгалтерии так же должны иметь доступ в сеть СФУ. Для этого между брандмауэром Stonegate и коммутатором ядра C6500 организовывается линия связи Ethernet. Тип соединения IP Layer3. На брандмауэре настраивается маршрут по умолчанию в сторону сети СФУ – 0.0.0.0/0, на коммутаторе ядра настраивается маршрут в сторону IP сетей бухгалтерии.

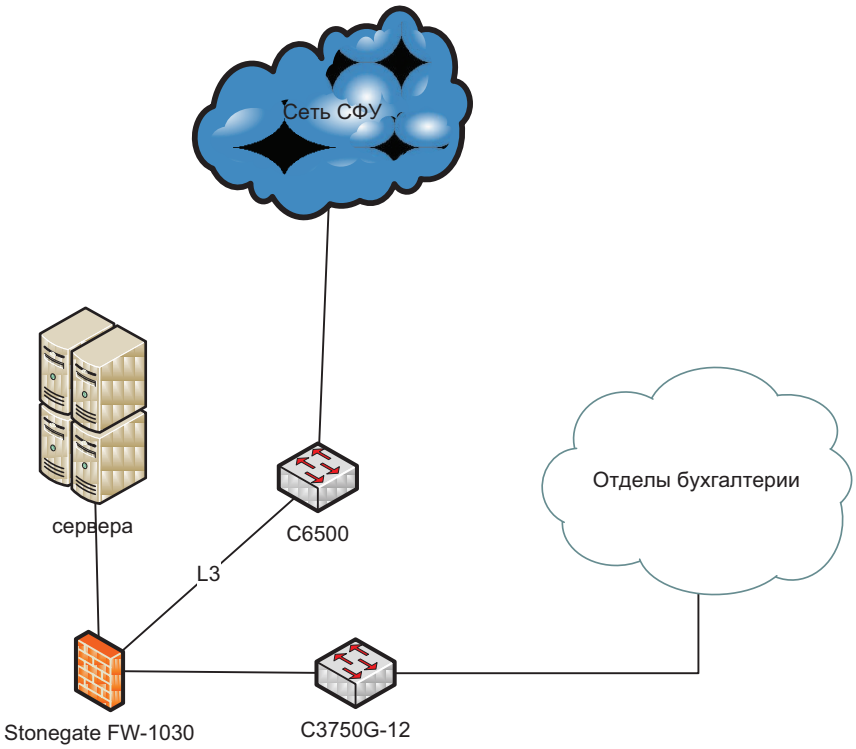


Рис. 6. Подключение сети бухгалтерии к общей сети СФУ

Этап №4. Смена адресного пространства сети.

Теперь, имея центральную точку маршрутизации трафика в сети в виде брандмауэра можно сменить существующее адресное пространство. Новая подсеть – 172.16.0.0/16. Пользователи каждого отдела поочередно переводятся в свой новый VLAN на коммутаторах доступа, которые соответствующим образом настраиваются. На брандмауэре создаются новые логические интерфейсы соответствующие VLAN'ам из таблицы №1. Брандмауэр обеспечивает прозрачную маршрутизацию трафика между подсетями 10.0.0.0 и 172.16.0.0, позволяя постепенно переводить пользователей из старого IP сегмента сети в новый. Сервера так же переводятся в новый сетевой сегмент, IP связность между пользователями и серверами не нарушается. DNS-имена устройств не меняются.

3.7. Политики безопасности.

Для обеспечения безопасности брандмауэр фильтрует трафик между всеми VLAN. Разрешается прохождение трафика из любой сети (отдела бухгалтерии/кадров и т.д.) в сеть серверов. Разрешается прохождение трафика из сети администраторов АСУ в сеть серверов и сеть управления.

На коммутаторах доступа будет использоваться привязка аппаратного адреса компьютера MAC к порту коммутатора (технология port-security). Это позволит запретить доступ в сеть для неизвестных рабочих станций.

Для автоматизации и упрощенного администрирования рабочими станциями предлагается использовать DHCP сервер. Например, на базе операционной системы Windows

Server или DHCP ISC под ОС Linux. IP адрес рабочей станции должен быть обязательно закреплен за ее аппаратным адресом (MAC).

3.8. Удаленный доступ.

Брандмауэр Stonegate обеспечивает защищенный удаленный доступ через VPN соединение к серверам. Для этого используются аппаратные ключи eToken. Удаленные пользователи после успешной авторизации имеют право работать только с серверами, доступ в сеть бухгалтерии для них запрещен.

Предоставление доступа из внешней сети так же возможно без использования VPN соединения. Разрешается доступ из подсетей, на сервера по определенным портам. Для этого нужно создать списки контроля доступа ACL на внешнем интерфейсе.

3.9. Управление.

Для настройки МЭ, а также с целью мониторинга и регистрации событий используется система централизованного управления StoneGate Management Center (SMC). Администратор со своего рабочего места, используя веб-браузер, имеет возможность получить доступ к графическому интерфейсу системы, в которой собирается статистика с МЭ Stonegate FW-1030. Здесь отображаются все событий, связанные с устройством, в том числе аутентификация внешних пользователей VPN-туннелей.

Посредством SMC выполняется как первоначальная настройка МЭ, так и его последующее администрирование.

В дальнейшем возможно подключение к платформе других используемых сетевых устройств для создания единого центра мониторинга, регистрации и управления.

3.10. Защита серверной платформы.

Поскольку основные процессы обработки информации у Заказчика связаны с использованием серверной платформы, в том числе и в терминальном режиме, ключевое значение имеют вопросы, связанные с защитой этой среды.

Безопасный доступ к Blade-платформе достигается использованием отдельных коммутаторов и линий связи для разного контекста.

Для предотвращения НСД к защищенным серверам, находящимся в этой же Blade-корзине, второй сетевой интерфейс от лезвий к коммутаторам блокируется на уровне шасси.

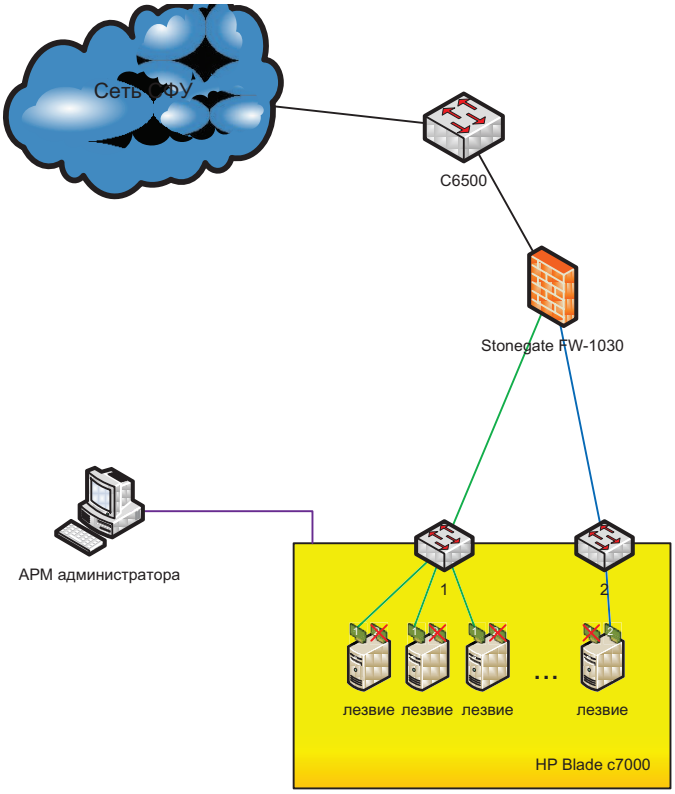


Рис. 7. Коммутация серверов

Часть лезвий платформы предоставляет ресурсы для внешней по отношению к защищаемой сети. Так как каждое лезвие имеет два сетевых интерфейса к коммутаторам шасси, для изолирования защищенной сети бухгалтерии от возможного доступа со стороны общего сегмента сети СФУ один из имеющихся сетевых интерфейсов (2) отключается от коммутатора. На лезвиях, находящихся в другом контексте отключаются интерфейсы 1. Таким образом, коммутаторы шасси 1 и 2 физически разделяют разные контексты и исключают взаимный доступ между ними в обход МЭ. Используемая платформа виртуализации используется только соответствующие контексту физические ресурсы.

Порт управления шасси подключается к АРМ администратора и недоступен извне защищенной сети бухгалтерии.

4 Основные технические решения по изменению кабельной части

4.1. Состав проектируемой системы

В рамках настоящего раздела под СКС понимается комплекс инженерных средств и сооружений, обеспечивающий доступ выделенного в отдельную группу распределенного по зданиям абонентского оборудования, к ресурсам защищенной вычислительной сети. В этом смысле в СКС входят следующие подсистемы:

- административная подсистема;
- горизонтальная подсистема.

Горизонтальная кабельная подсистема используется существующая и модернизации не подвергается, она обеспечивает доступ распределенного по объекту абонентского оборудования к активному оборудованию распределительного пункта.

Абонентское оборудование (рабочая станция либо телефонный аппарат) подключается к СКС абонентским шнуром, который связывает гнездо RJ45 розеточного модуля с гнездами RJ45.

В состав «горизонтальной подсистемы» входят розеточные модули информационных розеток и кабель (в данном случае 4-х парный кабель «витая пара» категории 5е, далее UTP). Эта подсистема связывает административную подсистему распределительного пункта с рабочим местом. Каналообразующее оборудование (корпуса розеток, лотки, кабельные желоба, крепежные принадлежности) в состав горизонтальной подсистемы не входят, но обеспечивают требования к условиям прокладки кабеля «горизонтальной подсистемы» в условиях офиса (механическая фиксация, степень защиты, внешний вид).

В состав «административной подсистемы» входят пассивное коммутационное оборудование (коммутационные шнуры и панели RJ45, оптические кроссовые панели и коммутационные шнуры, оптические и медные магистральные кабели), расположенное в телекоммуникационных шкафах расположенных в серверных помещениях организации.

Административная подсистема служит для подключения активного сетевого оборудования кроссовыми шнурами к информационным каналам, предоставляемыми горизонтальной кабельной подсистемой.

Путем перераспределения кабельной ёмкости административная подсистема определяет структуру локальной СКС. При этом также формируется способ использования каждого конкретного слаботочного канала. Схема кабельной системы представлена в Приложении 2.

4.2. Назначение настоящего раздела документа

Перестроение выделенной кабельной инфраструктуры предназначено для отделения локальной вычислительной системы отдела бухгалтерии от существующей СКС уровня организации на физическом уровне.

4.3. Характеристика объекта и исходные данные

Учебно-административные корпуса Университета, соединенные отапливаемыми галереями.

Тип зданий – многоэтажное здание.

Несущие стены – кирпич, внутренние перегородки – кирпич.

Горизонтальная система строится по принципу «звезда».

Все горизонтальные кабели сводятся в локальные телекоммуникационные шкафы в промежуточных распределительных пунктах, содержащий активное оборудование и патч-панели для коммутации пользователей (см. рис. 8).

Магистральная кабельная система построена на основе оптических и медных кабелей.

В качестве горизонтального кабеля используется кабели категорий 5е и 7.

На рабочих местах устанавливаются розетки с портами типа RJ-45.

Все кабели укладываются в короб.

4.4. Горизонтальная подсистема

В качестве среды передачи горизонтальной подсистемы используется существующий 4-х парный кабель «витая пара» категории 5е и 7.

4.5. Распределительные пункты

В существующих серверных помещениях и кроссовых узлах (обозначения – Р7-07, Б0-00, 20-00, 30-00, 32-00, 22-05, 12-00, 21-03) согласно вновь разработанной структурной схемы, основанной на данных о существующей кабельной системе предполагается произвести перекоммутацию оптических каналов (жил). Путем перекоммутации оптических сегментов, создается физически выделенная информационная подсеть, использующая общие (существующие) магистральные кабели. Для реализации канала связи между серверной (Р7-07 библиотеки) и серверным помещением (Б0-00) требуется проложить отдельный оптический кабель. Использование существующего канала данных затруднено в связи с его большой заполненностью. Для сегмента Р7-07 – Б0-00 предусмотрено использование одномодового кабеля емкостью 8 жил.

Терминирование вновь прокладываемого оптического кабеля производится на существующие оптические коммутационные панели.

Для обеспечения гибкой, быстрой и наглядной коммутации оптических каналов, запроектированы коммутационные шнуры отличающиеся по цвету от существующих и использующихся в данной организации.

Маркировка каналов связи на оптических панелях и шнурах производится цветными наклейками по следующей схеме: хх-уу, где хх – условное обозначение центра коммутации согласно структурной схеме, уу - порядковый номер оптической жилы для выделенной подсистемы в существующих кабелях,

Для размещения кроссовых кабелей в шкафах проектируются установка горизонтальный организаторы в виде 19" панелей с разрезными пружинными монтажными кольцами.

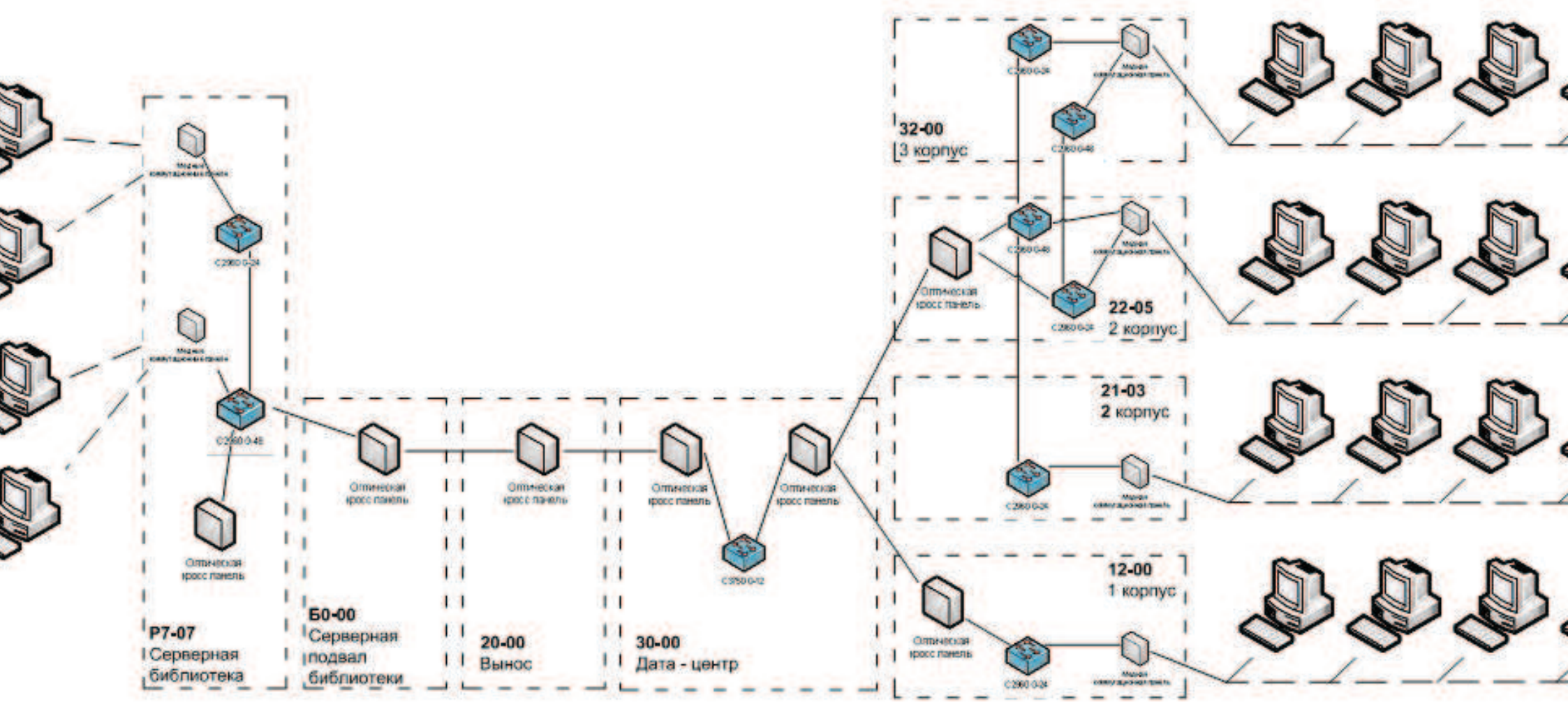


Рис. 8. Схема каналов связи

4.6. Кабельные каналы, каналообразующее оборудование.

Монтаж создаваемой оптической линии связи производится по существующим лоткам и коробам, а так же в пленумном пространстве между подвесным потолком и плитами перекрытия.

Для обеспечения удобства обслуживания, оптический кабель маркируется обозначением «оптический кабель Р7-07 – Б0-00» размещаемым на открытых для обзора местах через каждые 10 метров.

4.7. Применяемые виды кабельных соединений

Модернизированная кабельная коммуникационная система включает в себя проводные кабельные соединения, необходимые для обеспечения функционирования информационного оборудования.

Проводные кабельные соединения (далее, кабельные соединения) включают в себя следующие элементы:

- кроссовое оборудование;
- магистральные информационные кабели, соединяющие кроссовое оборудование;
- соединительные кабели для магистральных коммутаций.

Все применяемые компоненты для построения кабельных соединений имеют характеристики, соответствующие требованиям стандартов ISO 11801 -2002 и EIA/TIA 568A или превышающие их.

Кабельные соединения обеспечивают прохождение протоколов:

- 10 Base–T;
- 100 Base–TX;
- 1000 Base–T.

4.8. Маркировка кабельных соединений

Все вновь прокладываемые кабельные линии маркируются согласно Европейским и Международным стандартам. Маркировка элементов кабельных соединений наносится в доступном для наблюдения месте и позволяет идентифицировать данные элементы согласно документации.

4.9. Документация на кабельную систему

Разрабатываемая документация на кабельную коммуникационную систему включает:

- структурную схему информационных проводных кабельных соединений;
- результаты испытаний вновь создаваемых проводных кабельных соединений;
- кабельный журнал выделенной кабельной системы.

4.10. Состав и содержание работ по модернизации СКС

План производства работ и этапность реализации проекта, производится согласованно и параллельно с проведением работ по реконструкции архитектуры сети передачи данных бухгалтерии. Далее этапность будет представлена в соответствии с работами по установке и переключениям активного сетевого оборудования.

Этап №1. Предварительный.

1. Подготовка кабельных трасс и инсталляция оптического кабеля на участке «серверная Р7-07» - «кроссовая Б0-00».
2. Терминирование оптических жил вновь проложенного магистрального кабеля в существующих оптических кроссовых панелях.
3. Тестирование вновь проложенного кабельного сегмента.

Этап №2. Переключение пользователей и коммутаторов.

1. Перекоммутация свободных оптических жил существующих и вновь проложенных оптических кабелей с целью создания отдельной, физически выделенной магистральной кабельной инфраструктуры.
2. Подключение (переподключение) активного оборудования к физически выделенной магистральной кабельной инфраструктуре согласно схеме коммутаций (Приложение 2).

Этап №3. Переключение серверов. Подключение брандмауэра.

Подготовка кабельного журнала и исполнительной документации на СКС.

Этап №4. Смена адресного пространства сети.

Выдача Исполнительной документации на смонтированную СКС.

5 Основные технические решения по развертыванию системы усиленной аутентификации пользователей

5.1. Усиленная аутентификация для доступа внешних пользователей ИС

В целях аутентификации пользователей, получающих доступ к ресурсам ИС через VPN-туннели, терминирующиеся на МЭ Stonegate FW-1030 используются электронные идентификаторы «eToken».

Для установления VPN-канала между АРМ пользователя и МЭ пользователь предъявляет «eToken» с сертификатом. МЭ посредством SMC настраивается на распознавание необходимых ключей. На АРМ пользователя должен быть установлен драйвер «eToken». Кроме того, для использования VPN-туннеля с шифрованием по ГОСТ 28147-89 необходимо установить на АРМ крипто-провайдер КриптоПро CSP.

МЭ настраивается на использования внешнего центра сертификации (CA), разворачиваемого на выделенном лезвии в составе серверной платформы.

5.2. Усиленная аутентификация для доступа внутренних пользователей ИС

Для решения проблемы «слабых» паролей пользователей сети бухгалтерии используется программно-аппаратный комплекс усиленной аутентификации на основе электронных идентификаторов «eToken» и ПО «eToken Network Logon». Данное решение позволяет организовать двухфакторную аутентификацию сотрудников при входе в ОС на основе сертификатов.

На все защищаемые АРМ должно быть установлен драйвер «eToken» и ПО «eToken Network Logon» для реализации усиленной аутентификации. После установки «eToken Network Logon» стандартное приглашение для входа в Microsoft Windows заменяется новым, которое расширяет возможности по входу пользователя в систему. Для входа пользователь должен предъявить сертификат, записанный на электронном ключе, и ввести PIN-код.

Кроме того, на АРМ устанавливается пользовательская часть ПО «eToken TMS» для информирования о сроках истечения сертификата.

ПО «eToken Network Logon» помимо строгой аутентификации обеспечивает функции регистрации и учета предъявляемых ключей. Эти данные могут быть использованы в дальнейшем для анализа, в том числе, как и для обнаружения попыток НСД, так и для их предотвращения.

5.3. Управление ключевой информацией

Для централизованного управления жизненным циклом устройств eToken и обеспечения целостности связей между учетными записями пользователей, средствами аутентификации и приложениями безопасности в проекте используется ПО «eToken TMS», имеющее сертификат соответствия ФСТЭК России №1700 от 16 октября 2008 года.

TMS решает важнейшую проблему корпоративной безопасности: обеспечение связи между пользователями, их средствами идентификации и организационными политиками с приложениями безопасности.

TMS отвечает за выпуск и отзыв ключи, сбрасывание значение пароля, автоматическое копировать и восстанавливать идентификационные данные пользователя, позволяет оперативно решать проблемы, связанные с неисправностью или утратой ключа eToken.

Кроме того система обеспечивает регистрацию и учет всех действий как администраторов, так и пользователей, что очень важно при проектном количестве пользователей.

Для размещения сервера «eToken TMS» используется выделенный виртуальный сервер из состава серверной платформы HP Blade c7000. Сервер по аналогии с терминальными серверами и серверами приложений физически подключен через коммутатор шасси в МЭ Stonegate FW.

Для предоставления сервиса генерации сертификатов для ключей eToken здесь же находится сервис Microsoft Certificate Services, выполняющий функцию центра сертификации (Microsoft Certification Authority – MS CA). Совместно с «eToken TMS» администратором или самим пользователем осуществляется выпуск и перевыпуск сертификатов, хранящихся на электронных идентификаторах.

«eToken TMS» тесно интегрируется со службой каталогов, поэтому для полнофункциональной работы ПО необходимо предварительное развертывание на площадке одной из поддерживаемых служб.

Помимо всего прочего, администраторы безопасности должны осуществлять анализ информации, собираемой на основе системных журналов и сообщений используемых в проекте средств, с целью выявления критических, с точки зрения безопасности информации, событий. При обнаружении последних должен существовать типовой регламент реагирования на инциденты с целью минимизации угроз.

6 Ввод в эксплуатацию

Перечень конкретных мероприятий может уточняться с учетом изменения конфигурации и состава технических средств объекта и уровнем подготовки имеющегося персонала.

6.1. Мероприятия по обеспечению физической безопасности оборудования

Должны быть выполнены работы по обеспечению физической безопасности оборудования, размещаемого на коммуникационных узлах и помещении дата-центра. Все используемое оборудование должно быть опечатано для предотвращения несанкционированного вскрытия.

6.2. Мероприятия по обучению и проверке квалификации персонала

Мероприятия по обучению и проверке квалификации персонала должны включать в себя обучение всех пользователей работе со средствами защиты «eToken» и «eToken Network Logon» на специализированных тренингах, проводимых администратором безопасности, при этом знания пользователей должны быть проверены на испытании по окончании тренинга.

6.3. Мероприятия по созданию необходимых подразделений и рабочих мест

Для дальнейшей эксплуатации выбранных средств, в штатную структуру Заказчика должна быть ведена штатная единица администратора безопасности в количестве двух человек. Допускается совмещение обязанностей.

Администратор безопасности должен иметь квалификацию, необходимую для настройки и сопровождения:

- «eToken TMS»;
- «eToken Network Logon»;
- Stonegate FW-1030;
- Stonegate SMC.

Кроме этого, администраторы безопасности должны знать и выполнять требования действующего законодательства в области защиты информации.

6.4. Мероприятия по изменению объекта автоматизации

При подготовке объекта автоматизации необходимо провести комплекс организационно-технических мероприятий.

В результате данных мероприятий должны быть:

- развернут один из каталогов пользователей (AD или NMAS);
- отключены вторые интерфейсы на серверной платформе;

- интерфейс управления серверной платформой скоммутирован на АРМ администратора;
- выделен виртуализованный ресурс под сервер безопасности из состава серверной платформы.

7 Заключение

В ходе проектирования защищенной сети бухгалтерии были разработаны технические решения, реализующие предлагаемую модель защиты и функции назначения системы.

Для защиты информации в ИС были выбраны следующие средства защиты:

- архитектура сети;
- Stonegate FW;
- Stonegate SMC;
- электронные идентификаторы USB «eToken»;
- ПО строгой аутентификации «eToken Network Logon»;
- «eToken TMS».

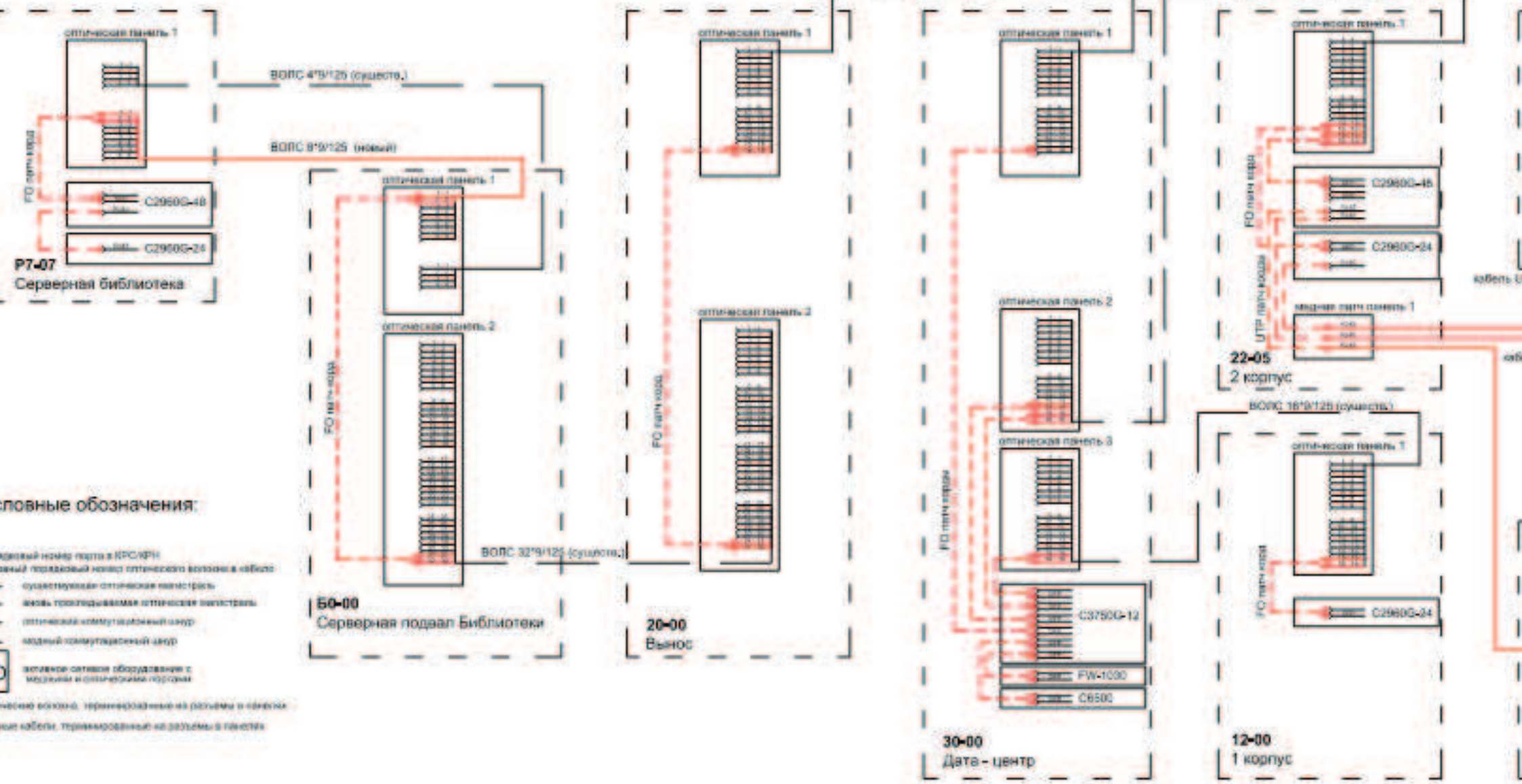
Также были приведены требования к инженерно-техническим средствам защиты от физического доступа и организационным мерам защиты.

Приложение 1: Спецификация оборудования и ПО

№ п\п	Код	Наименование товара	Кол-во
Межсетевой экран			
1.	DEV-FW-1030-C2-P-R	StoneGate FW Hardware Platform FW-1030-C2-P 6 x 10/100/1000 FE interfaces Max 1,3 Gbps throughput	1
2.	LIC-FW-1030-C2-P-R	StoneGate FW License FW-1030-C2-P Max 1,3 Gbps throughput	1
3.	M-APP-FW-1030-C2-P	Basic (8/5) Support and Maintenance for FW-1030-C2-P Including Hardware Replacement Service 15 Months	1
Пакет сертификации для МЭ			
4.		Лицензия на право использования СКЗИ "КриптоПро CSP" версии 3.6 для Stonegate Firewall/VPN на FW-1050/1030 p/1060/SSL-1060	1
5.	SG-SPO-FW1	Базовый пакет сертифицированного ПО StoneGateFW для модели 1030P, в состав, которого включены: – верифицированный установочный комплект ПО; – абонемент на получение сертифицированных online-обновлений; – техническая поддержка (информационные и консультационные услуги); – Формуляр на сертифицируемое ПО, промаркированный голографическим специальным знаком соответствия ФСТЭК России; – копия Сертификата ФСТЭК России на поставляемое ПО, заверенная печатью Заявителя; – Медиа-Кит (CD-диск), содержащий: – Руководство по настройке и администрированию ПО; – Руководство по получению сертифицированных обновлений; – набор информационных материалов по сертифицированному ПО.	1
Подсистема управления МЭ			
6.	LIC-SG-SMC-2	StoneGate Management Center License for 2 nodes. A node (either a single unit or a cluster) can be a FW/VPN, a FW, or a VPN gateway, or an IPS sensor. Includes both a Management Server and a Log Server, which can be installed on a single server or on separate servers	1
7.	M-SG-SMC-2	Basic (8/5) Support and Maintenance for SMC-2 15 Months	1
Электронные ключи			
8.	eToken PRO (Java)/72K/CERT-1883	USB-ключ eToken PRO (Java), защищённая память 72КБ, сертификат ФСТЭК №1883	260
9.	eToken Media-kit/CERT-1883	Комплект документации и ПО для сертифицированных электронных ключей и смарт-карт eToken (сертификат ФСТЭК №1883).	1
10.	ACS-USB-CBL-180	Фирменный удлинительный USB-кабель с присоской (Delux)	210
ПО строгой аутентификации			
11.	ETSW/NL/5/EU/CERT-1961	Лицензия на использование сертифицированной версии eToken Network Logon на одном рабочем месте.	210
12.	ETSW/NL/5/MK/CERT-1961	Комплект документации и дистрибутив eToken Network Logon, сертифицированная версия, на компакт-диске.	1
Система учета, управления и аудита средств аутентификации и хранения ключевой информации			
13.	ETTMS2-Serv-CERT-L	Программный комплекс «Система учета, управления и аудита средств аутентификации и хранения ключевой информации eToken TMS 2» (Token Management System). Сертифицированная версия. Лицензия на использование в рамках одного домена Microsoft Windows	1
14.	ETTMS2-User-1Y-L	Лицензия на использование eToken TMS 2.0 для одного пользователя на 1 год.	240
15.	ETTMS2-Support-1	Оперативная квалифицированная помощь и консультации сертифицированного специалиста с возможным выездом к заказчику для решения возникших проблем на месте, возможным прямым обращением в Aladdin и к разработчикам	1

		системы (до 4-х инцидентов в год). Срок действия – 1 год. Приобретается отдельно на каждый домен.	
Сетевое оборудование			
16.	WS-C2960G-24TC-L	Catalyst 2960 24 10/100/1000, 4 T/SFP LAN Base Image	1
17.	WS-C2960G-48TC-L	Catalyst 2960 48 10/100/1000, 4 T/SFP LAN Base Image	1
18.	WS-C3750G-12S-S	Catalyst 3750 12 SFP + IPB Image	1
19.	GLC-BX-D=	1000BASE-BX SFP, 1490NM	5
20.	GLC-BX-U=	1000BASE-BX SFP, 1310NM	5
21.	GLC-T=	1000BASE-T SFP	3
22.	CON-SNTE-3750G12S	SMARTNET 8X5X4 Cat 3750 12 SFP Std Multilayer Image	1
Патч-корды и расходные материалы*			
23.	EX9F-L1D	Комм шнур, ВО, LC-FC, 9/125, Duplex, 1м	1
24.	EX9F-F1D	Комм шнур, ВО, FC-FC, 9/125, Duplex, 1м	2
25.	EX9L-L2D	Комм шнур, ВО, LC-LC, 9/125, Duplex, 2м	2
26.	EX9C-C5D	Комм шнур, ВО, SC-SC, 9/125, Duplex, 5м	4
27.	EX9C-L2D	Комм шнур, ВО, LC-SC, 9/125, Duplex, 2м	3
28.	EX02-520	СКС"Exalan+" патч-корд UTP кат.5е, 2м PVC	6
29.	EX7F-F1Sd	Адаптер проходной FC-FC/SM, D-типа, СКС "ExaLan+"	16
30.	95M359A08B	Кабель ВО внутренний 8х9/125, MTD, FR PVC, усилен.	60
31.		Гильза КЗДС	20
32.		Полушнур оптический 9/125 FC	16
33.		Крепежный колмплект трассы оптического кабеля	1

*Тип, количество и длина может уточняться на этапе монтажа по месту


оптическая панель 1
ВОЛС 4*9/125 (существ.)
FO патч корд
ВОЛС 8*9/125 (новый)
C2960G-48
C2960G-24
P7-07
Серверная библиотека
оптическая панель 1
оптическая панель 2
FO патч корд
ВОЛС 32*9/125 (существ.)
Б0-00
Серверная подвал Библиотеки
оптическая панель 1
оптическая панель 2
FO патч корд
20-00
Вынос
оптическая панель 1
оптическая панель 2
оптическая панель 3
FO патч корды
C3750G-12
FW-1030
C6500
30-00
Дата - центр
оптическая панель 1
C2960G-48
C2960G-24
FO патч корд
UTP патч корды
медная патч панель 1
22-05
2 корпус
ВОЛС 16*9/125 (существ.)
оптическая панель 1
C2960G-24
FO патч корд
12-00
1 корпус
кабель U
ловные обозначения:
существующая оптическая магистраль
вновь прокладываемая оптическая магистраль
оптический коммутационный шнур
медный коммутационный шнур
активное сетевое оборудование с медными и оптическими портами

Приложение 3: Описание программно-аппаратных средств

1. StoneGate Firewall/VPN

Межсетевой экран с интегрированными функциями построения VPN StoneGate FW/VPN производства компании StoneSoft удовлетворяет всем современным требованиям к системам безопасности, при этом в его основе лежат уникальные архитектурные решения, не требующие применения вспомогательных специализированных дорогостоящих средств, как в ряде решений конкурентов.

В StoneGate Firewall используется собственная интегрированная защищенная операционная система, обеспечивающая высокий уровень безопасности решения. Это исключает необходимость выполнения каких-либо специализированных операций по настройке (все необходимые инсталляции выполняются в «один проход»), а также позволяет наращивать функциональность StoneGate лишь за счет добавления новых компонентов без изменения работающей инфраструктуры и без остановки в работе.

В StoneGate применены самые современные технологии анализа трафика и обеспечения отказоустойчивости. Запатентованная технология MultiLayer Inspection совмещает в себе достоинства фильтров Application proxy и Stateful Inspection, позволяя добиться большей безопасности соединений и гибкости фильтрации при отсутствии какого-либо значительного снижения скорости.

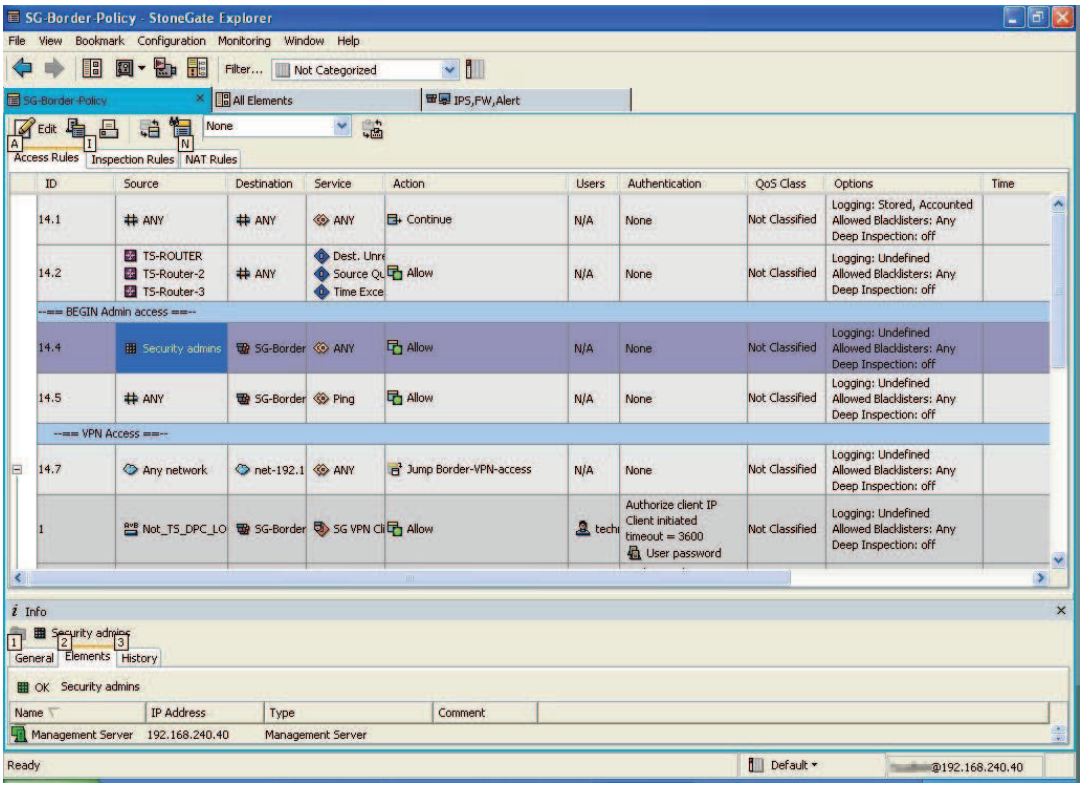
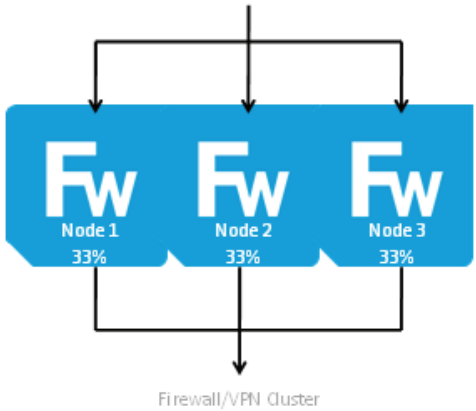


Рис. 9. Составление правил фильтрации трафика

При этом следует отметить, что фильтрация трафика с отслеживанием контекста устанавливаемых соединений возможна не только на 3-4 уровнях модели OSI, но и на уровне

приложений. На сегодняшний день для инспекции с использованием специализированных «агентов протоколов» доступно более 20 прикладных протоколов, таких как H.323, SIP, FTP, HTTP(S), SMTP, IMAP, POP3, SSH, NBT, MSRPC, Sun RPC, Oracle TNS и другие. Это означает, что StoneGate понимает последовательность установления соединения, умеет разбирать логику работы протокола и позволяет для них задавать такие параметры, как режим работы, набор разрешенных команд и т.п.

Производительность отдельно стоящего межсетевого экрана верхних модели может превышать 10Гб/с, что превосходит решения большинства конкурентов (при том, что в настоящий момент в решениях StoneGate, в отличие от конкурентов, используется 32-х разрядная архитектура, а переход на 64 бита запланирован на конец года – соответственно тогда же для уже существующих заказчиков можно будет ожидать еще большего прироста производительности путем простого программного апгрейда). Но ещё больший отрыв от них задает факт возможности кластеризации до 16 узлов. При этом создается «честный кластер», когда все устройства виртуального экрана, выглядящего для рядом стоящих сетевых устройств как одно логическое, работают одновременно, динамически балансируя нагрузку между собой. Особенностью решения компании StoneSoft является то, что производительность кластера растет практически линейно с увеличением количества добавляемых в него узлов (таким образом, пиковая производительность, которая может быть достигнута на сегодняшний день, составляет, с учетом «накладных расходов» порядка 150 Гб/с!). При этом администрирование кластера с точки зрения администратора полностью аналогично администрированию отдельно стоящего межсетевого экрана.



Ещё одной уникальной возможностью, реализованной в межсетевых экранах StoneGate Firewall, является поддержка запатентованной технологии MultiLink. Она позволяет обеспечить высокую степень доступности ресурсов путем использования динамической балансировки нагрузки по каналам связи. Суть технологии заключается в измерении загрузки и скорости передачи информации при одновременном задействовании нескольких каналов связи.

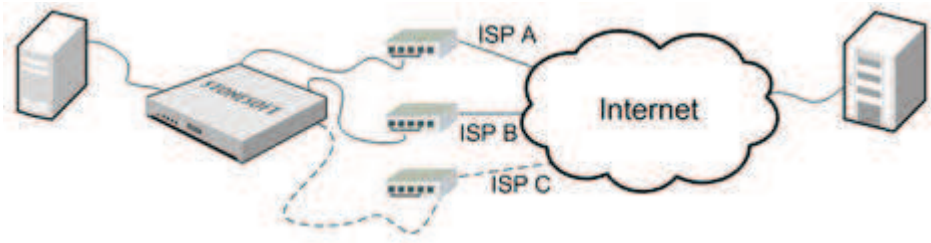


Рис. 10. Технология MultiLink в действии

Это позволяет без использования сложных протоколов маршрутизации или подписания договоров о совместном использовании схем маршрутизации трафика с провайдером в каждый конкретный момент времени использовать для передачи данных оптимальное соединение. Подобная технология позволяет добиться действительно динамической балансировки нагрузки, в отличие от решений конкурентов, которые не только более сложны в настройке и администрировании (за счет необходимости конфигурирования протоколов динамической маршрутизации и решения административных вопросов с провайдером), но и дают возможность реализовать только статическую балансировку по одному из выбранного множества каналов (настроив соответствующие метрики маршрутов).

Помимо действительно динамической балансировки, главным преимуществом данного решения является то, что ни один элемент оборудования или канал не простаивает – все элементы работают (при необходимости, администратор может самостоятельно определять правила активации того или иного канала связи, переводя их из «активного» в режим «резервирования»). При этом задействуются наиболее эффективно: в зависимости от текущей загрузки используется тот или иной узел или тот или иной канал связи. Все это снижает общую стоимость владения решением, включая снижение стоимости резервирования оборудования, снижения административных затрат на взаимодействие с провайдерами услуг Интернет и поддержку сложных протоколов маршрутизации типа BGP, OSPF.

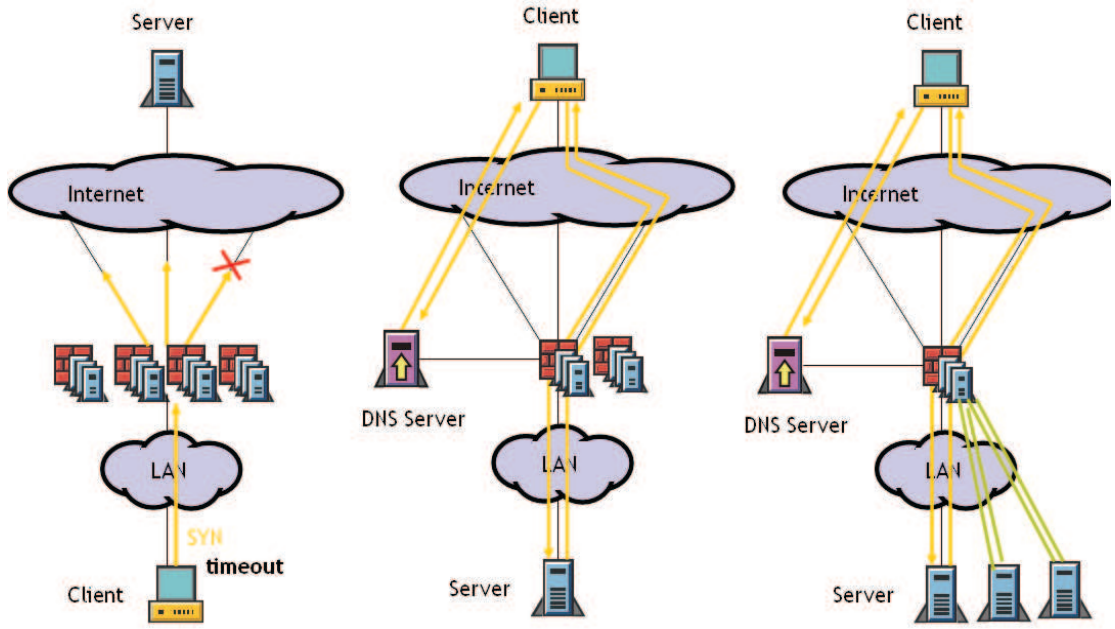


Рис. 11. Балансировка исходящего и входящего трафика

Аналогично, с использованием технологии MultiLink можно реализовать балансировку не исходящего (Outbound), а входящего (Inbound) трафика по пулу серверов, предоставляющих публичный сервис для Интернет-пользователей или интранет ресурс для сотрудников организации. Это позволяет отказаться от установки дополнительных аппаратных или программных платформ – балансировщиков нагрузки, которые не только стоят немалых денег, но и требуют дополнительного администрирования.

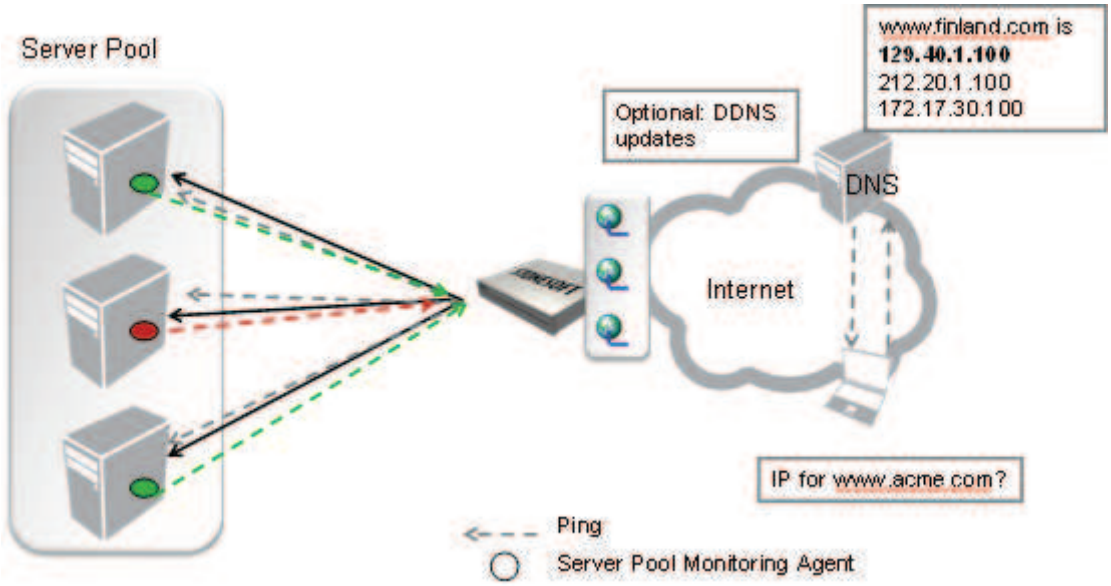


Рис. 12. Работа технологии Inbound MultiLink

Межсетевой экран самостоятельно контролирует доступность серверов, предоставляющих сервис для пользователей, степень их загрузки или другие существенные параметры, задаваемые администратором. По факту отклонения параметров от допустимых значений сервер исключается из алгоритма балансировки. Когда параметры обратно возвращаются в установленные пределы, межсетевой экран снова начинает передавать трафик на обработку серверу.

Кроме того, StoneGate MultiLink также интегрируется с технологиями построения защищенных VPN и позволяет настраивать отказоустойчивые защищенные соединение между офисами через нескольких провайдеров с автоматической балансировкой соединений между ними. Используемая при этом технология MultiLink VPN позволяет прозрачно переключаться с одного канала на другой без потери соединения с удаленным узлом. Таким образом для прикладной программы сбои канала или моменты переключения попросту незаметны (время переключения составляет порядка нескольких секунд).

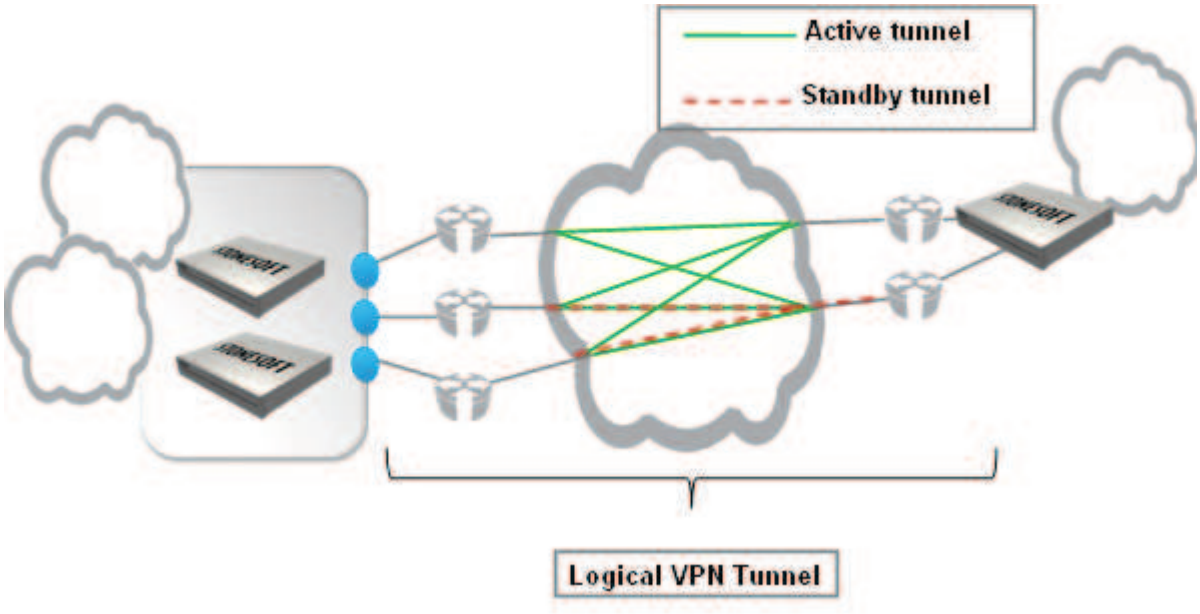


Рис. 13. Возможности технологии MultiLink VPN

Администратор может самостоятельно задавать режимы работы туннелей. Так, часть из них может быть активными, а остальные находится в резерве, активируясь только в моменты, когда рабочие соединения рвутся или испытывают проблемы связности. Нагрузка автоматически распределяется между активными каналами, а также между устройствами в кластере. Таким образом можно эффективно распределять соединения между узлами и плавно наращивать производительность решения, обеспечивая равномерную загрузку. С учетом того, что в кластер можно объединять устройства разной производительности, сеть организации может быть по-настоящему «живой», эволюционировать по мере роста нагрузки, тогда как с точки зрения администратора, вне зависимости от числа используемых шлюзов, технологии и правила доступа будут неизменными. Все это значительно упрощает сопровождение решения и его обслуживание, а также планирование и проектирование.

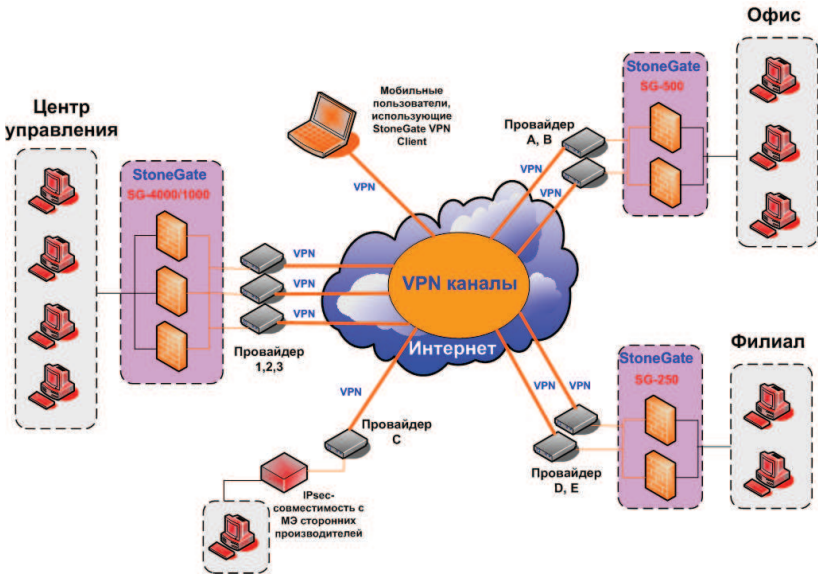


Рис. 14. Построение отказоустойчивой VPN сети

Традиционно построение отказоустойчивой системы требует резервирования линий связи и сетевой инфраструктуры, что существенно увеличивает ее стоимость. Применение StoneGate позволяет получить не только полностью отказоустойчивое, но и более экономичное решение. Работающие соединения пользователей будут активны до тех пор, пока остается «живым» хотя бы один узел кластера: поддерживается прозрачное переключение (failover) как для «обычных», так и VPN-соединений. Облегчению труда администраторов и исполнению корпоративной политики безопасности способствует также функция верификации настроек безопасности рабочей станции пользователя, удаленно подключающегося к VPN-шлюзу организации.

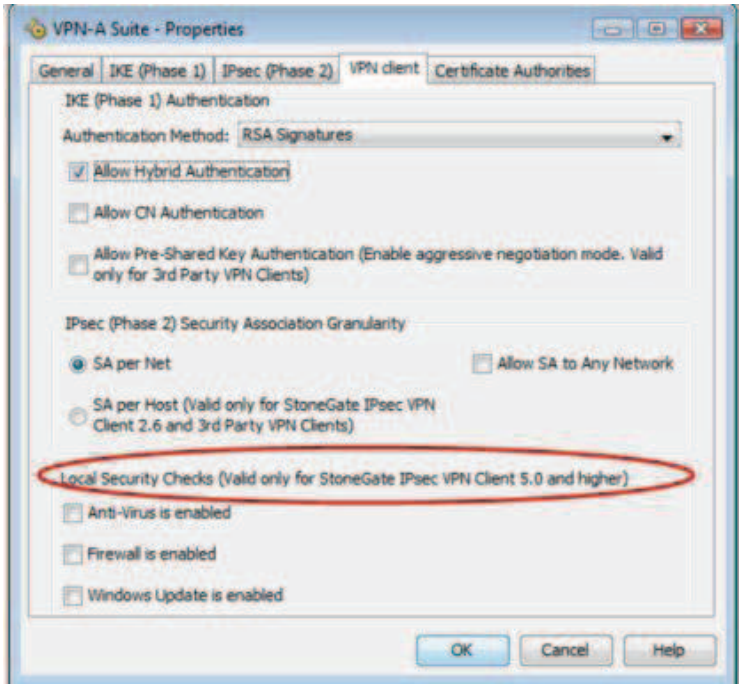


Рис. 15. Функции проверки безопасности для IPSec VPN клиента

Таким образом, необязательно для базовых проверок использовать сложные и ресурсоемкие технологии наподобие SSL VPN – в решение StoneGate VPN эти проверки поддерживаются штатно и задаются администратором централизованно (без участия пользователей, которым вообще ничего менять не нужно).

При построении защищенных VPN StoneGate FW поддерживает не только стандартные зарубежные криптоалгоритмы, такие как (3)DES, AES, но и «экзотические» варианты Blowfish, Twofish, CAST-128. Более того, в нем также поддерживается модуль шифрования с Российским криптопровайдером и, как следствие, StoneGate FW позволяет создавать VPN на базе алгоритма ГОСТ 28147-89. Кроме этого, встроенный центр сертификации (CA) позволяет развернуть для аутентификации пользователей и устройств в рамках VPN инфраструктуру PKI. Это позволяет не тратиться на дополнительные лицензии или установку программных средств, когда сертификаты нужны только для аутентификации в рамках VPN. Если же в организации уже используется инфраструктура PKI, то за счет встроенной поддержки внешних служб решение StoneGate FW/VPN можно легко интегрировать и с ней.

Что касается поддержки сторонних систем и совместимости с ними посредством технологии IPSec VPN, то StoneGate является признанным лидером в этой области. Так, его совместимость с другими продуктами и корректность реализации спецификации IPSec подтверждена такими уважаемыми Западными организациями, как VPN Consortium (сертификат VPNC Interoperability). Помимо этого, наличие сертификатов Common Criteria с высоким уровнем доверия EAL4+ (основные конкуренты имеют в лучшем случае EAL4) и ICSA Labs Firewall позволяет говорить о высоком качестве решения в целом. Что касается Российских сертификатов, то можно отметить наличие сертификатов ФСТЭК на МЭ 3-го класса и по ТУ (равно как и сертификат ФСБ на используемый криптопровайдер).

Кроме перечисленного межсетевой экран StoneGate FW/VPN поддерживает возможность инспекции ряда прикладных протоколов на предмет выявления аномалий, подозрительной активности, имеет возможность удаления из потока вирусов, сетевых червей. А именно, для HTTP(S) и SIP поддерживается полноценная система обнаружения и предотвращения вторжений (аналогичная той, которая доступна в виде отдельного устройства StoneGate IPS) и МЭ по полному набору правил может инспектировать поток, осуществляя, помимо всего прочего, контентную или URL-фильтрацию. Для почтовых протоколов поддерживается дополнительно антивирусная инспекция. Все эти правила легко настраиваются и централизованно распространяются по всем устройствам организации.

Более того, аналогичные методы проверок доступны не только для «открытого» протокола HTTP, но и для сервисов, работающих через HTTPS. Межсетевой экран может терминировать на себе SSL туннель, распаковывать его, проверять содержимое и дальше проключать до целевого сервера.

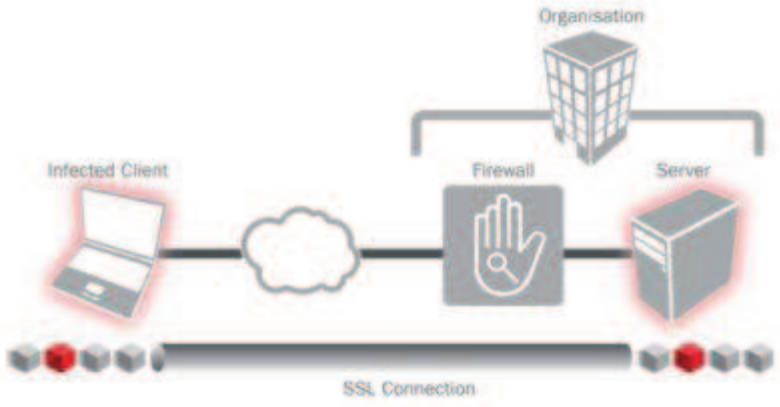


Рис. 16. SSL инспекция в межсетевом экране

Это позволяет реализовать несколько сценариев работы:

- защиту внутренних серверов, работающих через SSL, от злоумышленников, пытающихся злоупотребить их ресурсами в расчете на то, что система защиты неспособна выявить эксплоит в зашифрованном потоке (уникальная функция – работает также для StoneGate IPS);
- контроль работы внутренних пользователей с внешними сервисами посредством протокола SSL (HTTPS), который обычно не контролируется (уникальная функция – работает также для StoneGate IPS). Это позволяет, в том

числе, через сервис контентной инспекции следить и за утечкой конфиденциальной информации из компании (отслеживать ключевые слова, номера кредитных карт и т.п., передаваемые внешним сервисам).

Если перечисленных средств контентной инспекции недостаточно, то межсетевой экран StoneGate FW/VPN может передавать информацию серверу инспекции контента посредством перенаправления сетевого потока.

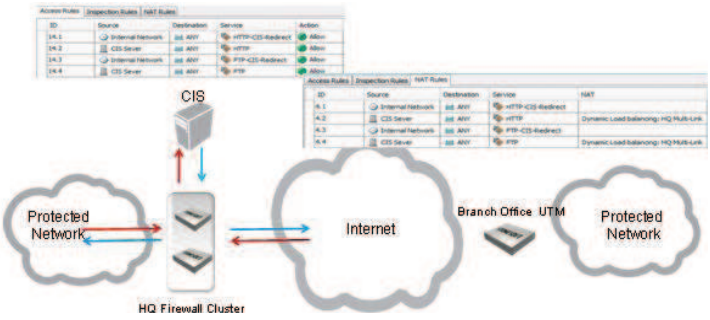


Рис. 17. Сервис перенаправления потока для инспекции

Для более эффективного управления потоками трафика внутри МЭ и на окружающем сетевом оборудовании StoneGate FW/VPN поддерживает механизмы QoS и управления полосой пропускания. Так, администратор имеет возможность задать определенные гарантии для трафика в виде минимально доступной полосы пропускания или ограничить сетевой поток (например, загрузку данных по FTP) какой-то величиной. Также можно описать приоритеты для потоков на случай перегрузки (congestion) выходных интерфейсов, равно как и установить определенные значения DSCP меток с целью последующей реализации QoS на окружающей сетевом оборудовании.

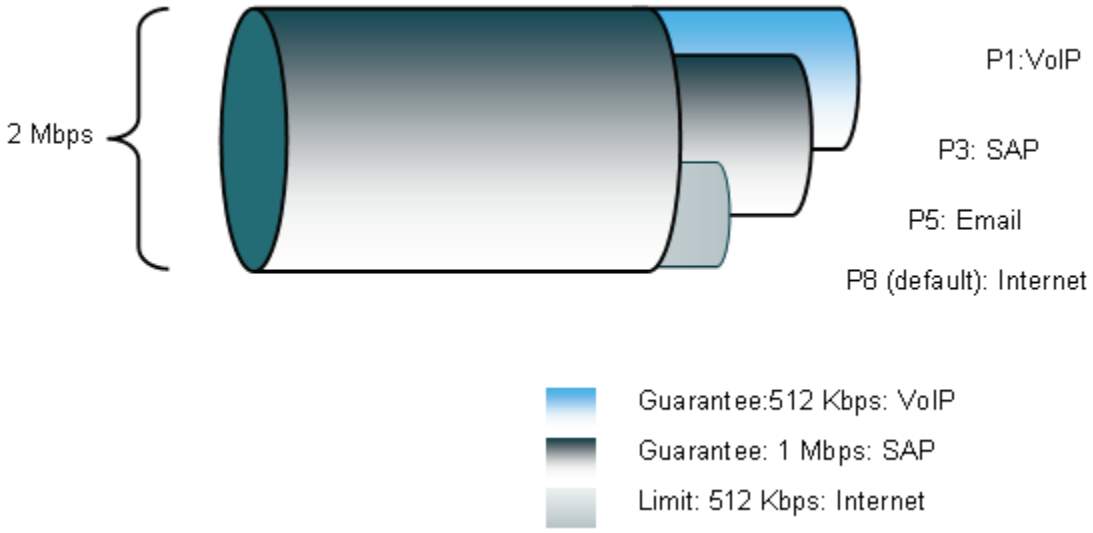


Рис. 18. Управление QoS политиками сетевых потоков

Одной из особенностей работы StoneGate FW/VPN также является поддержка технологий борьбы с (D)DoS-атаками. Специальные механизмы борьбы с SYN-flood, позволяют либо ограничить количество соединений, которые могут находиться в определенном состоянии, либо, используя специального «агента» (TCP proxy) не пропустить соединение до целевого сервера до тех пор, пока клиент не ответит на свой собственный

запрос подтверждающим сообщением в рамках стандартного алгоритма работы протокола TCP (т.е. позволяет сделать flood-атаку со спуфингом адресов незаметной для атакуемого сервера). Кстати, активированный механизм антиспуфинга по умолчанию (конфигурация которого составляется системой автоматически) также является особенностью решения StoneGate на фоне конкурентов.

2. StoneSoft SMC

Система централизованного управления StoneGate Management Center (SMC) предоставляет унифицированный интерфейс управления и мониторинга для StoneGate FW/VPN, IPS, SSL устройств. Устройства могут быть реальными (физический сервер или appliance) или виртуальными (специально подготовленная версия ПО для работы в виртуальной среде) – с точки зрения администратора нет никакой разницы. Он со своего рабочего места получает возможность, используя тонкий клиент на базе браузера, получить доступ к графическому интерфейсу системы (Java-апплет), в который стекается статистика реального времени со всех подключенных устройств. Так, можно в виде диаграмм, таблиц или графиков наблюдать загрузку ЦП или интерфейсов отдельного или группы межсетевых экранов, смотреть за распределением трафика по каналам связи, а также распределение пропущенного или отфильтрованного трафика.

Рис. 19. Система централизованного управления и мониторинга

Архитектура системы позволяет масштабировать её до неограниченных размеров. В зависимости от структуры сети и расположения сетевых элементов администратору доступны

возможности распределения компонент для оптимизации сетевых потоков между ними. При этом чтобы исключить вероятность возникновения слабых звеньев в системе, каждый из её компонентов может дополнительно резервироваться. Именно из-за этих функций высокой доступности и отказоустойчивости, как отмечалось в начале, «зоной комфорта» для решений StoneGate являются организации, для которых отсутствие простоев и высокая надежность являются повседневной реальностью.

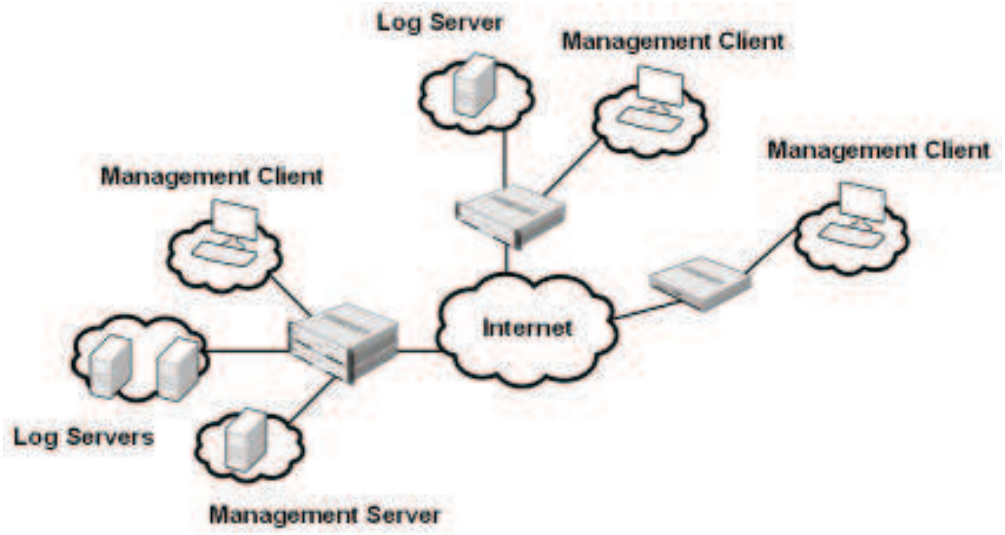
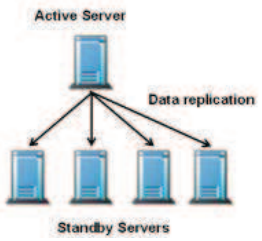


Рис. 20. Распределенная система управления

Так, возможности кластерного резервирования доступные для StoneGate FW/VPN, позволяет создавать отказоустойчивые конфигурации, недоступные в других системах. Однако, более того, в решении компании StoneSoft, в отличие от других вендоров, возможно использовать технологию кластеризации не самих межсетевых экранов, а систем управления – в этом случае даже если по какой-то причине сервер, который используется для мониторинга и хранения конфигураций вдруг откажет, его функции перехватит на себя один из оставшихся (их может быть до 5 в одном «кластере») – на нем уже будет готова полностью реплицированная копия данных. Тем самым обеспечивается нулевое время простоя, что снижает издержки на эксплуатацию решения.



Простое и эффективное управление StoneGate FW/VPN/IPS/SSL – центр управления SMC, обеспечивает единый интерфейс управления для всего многообразия решений компании StoneSoft, вне зависимости от количества и физического расположения сенсоров, анализаторов, FW/VPN или системы управления. Такой подход позволяет значительно уменьшить стоимость владения системой, ввиду полной интеграции решений в единое целое, а также значительно упростить саму процедуру управления. Кроме того, предусмотрена возможность интеграции с антивирусными системами, системами защиты от спама и др. А удобный графический интерфейс позволяет быстро и эффективно управлять событиями.

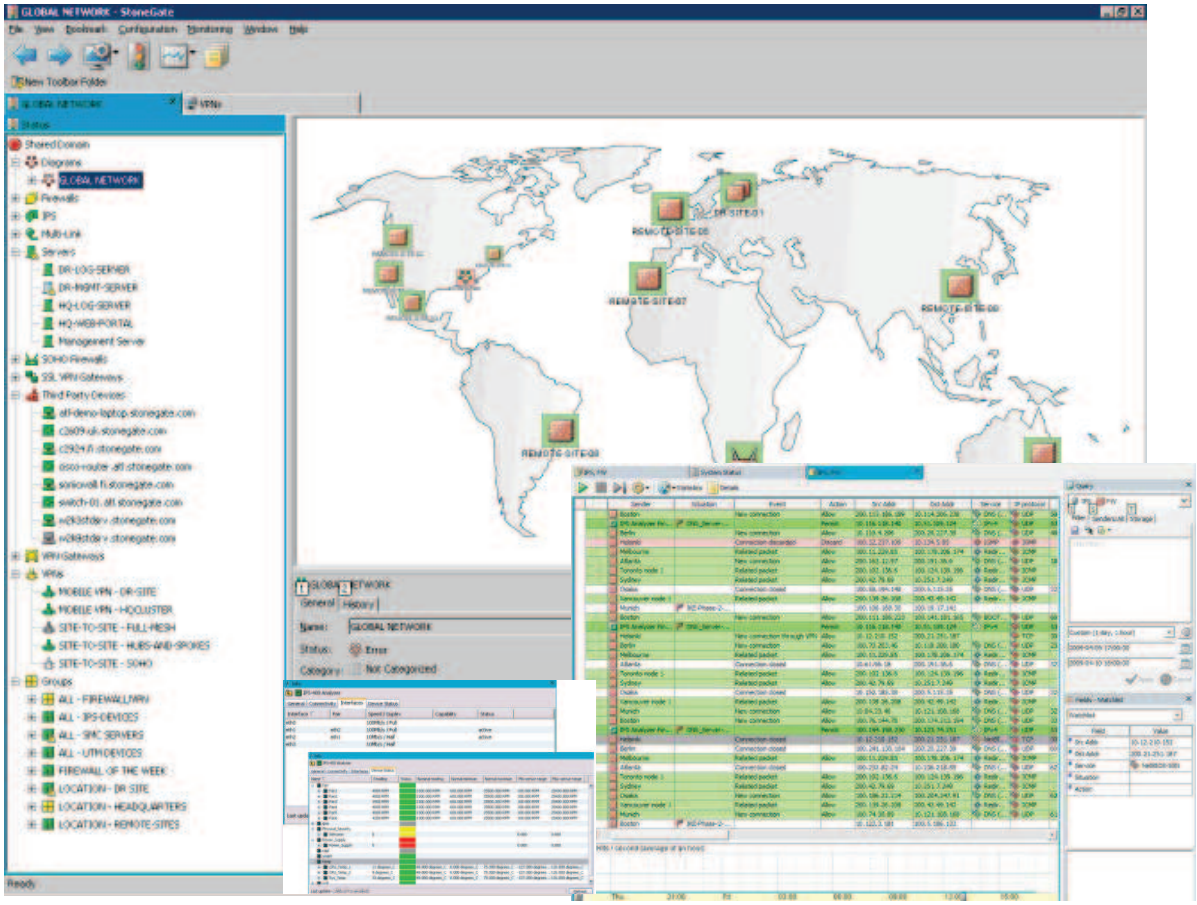


Рис. 21. Единый интерактивный интерфейс управления

Как уже отмечалось, для ряда протоколов уровня приложений в рамках межсетевого экрана без дополнительного лицензирования или установки специальных компонент (как в решениях других вендоров) доступна полноценная система обнаружения и предотвращения вторжений с полной БД аномалий и сигнатур. Таким образом можно превратить пограничное устройство фильтрации и терминирования защищенных VPN соединений в многофункциональный шлюз, помимо всего прочего, собирающий статистику о работе пользователей, осуществляющий URL-фильтрацию, контентную фильтрацию, перенаправляющий трафик для инспектирования в системы антиспам и антивирусной фильтрации (в случае необходимости), а также аутентифицирующий пользователей при доступе к ресурсам (из внутренней или внешней БД). При этом отчеты доступны как в режиме реального времени в виде статистики или файлов журналов с гибкой подсистемой фильтрации, а также в виде графиков, таблиц и других элементов одного из встроенных отчетов, либо одного из собственных, наполняемых с помощью более сотни различных счетчиков, записываемых в БД сервера хранения событий. Получается не межсетевой экран, а целый «комбайн», способный работать без потери производительности на гигабитных скоростях.

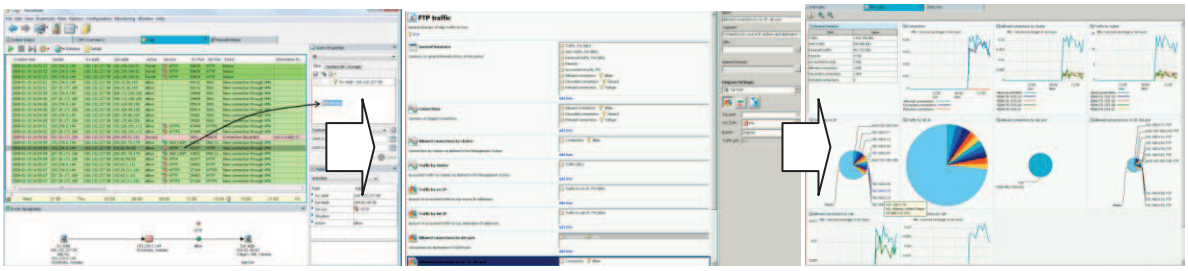


Рис. 22. Обработка событий

Для прозрачной аутентификации пользователей при доступе к ресурсам можно использовать встроенную БД или интегрировать последнюю с внешним хранилищем. В качестве внешнего поддерживаются RADIUS, TACACS+ серверы или LDAP(S) каталог. В структуре элементов каталога в полном объеме поддерживаются русские символы. Проблем с отображением и использованием киррилицы у продуктов StoneSoft, в отличие от альтернативных решений, нет.

Более того, администратор может в полуавтоматическом режиме составить диаграмму связности или карту сети, на которой в режиме реального времени будет изменяться статус подчиненных элементов, что делает возможным мгновенное диагностирование проблемы и выявление точки отказа. Карты могут быть вложенными, что особенно актуально для крупных сетей и большого числа подключений.

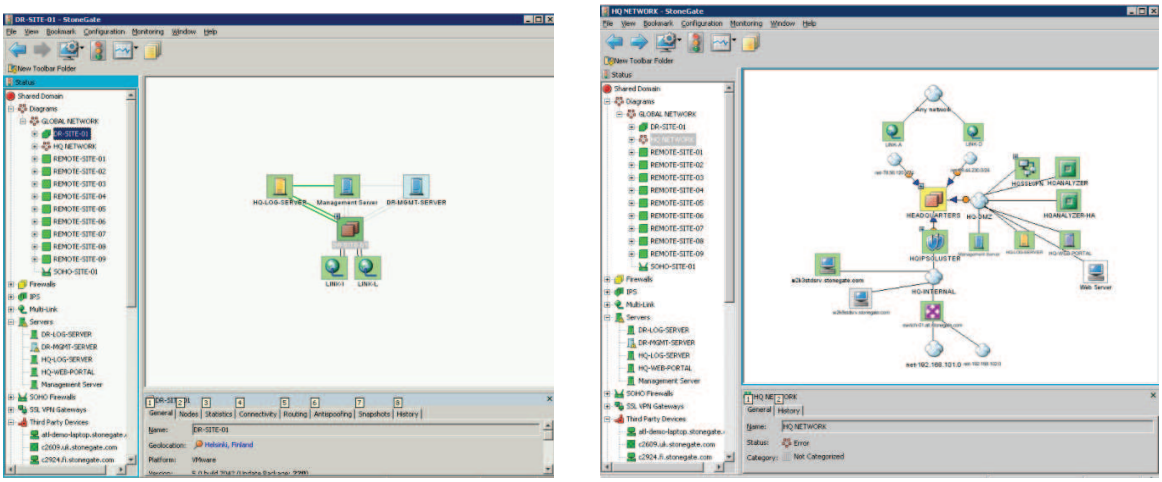


Рис. 23. Диаграмма связности и интерактивная карта сети

Более того, помимо управляемых элементов (StoneGate FW/VPN, IPS, VPN, компонентов SMC), как можно увидеть на примере карты сети справа, для мониторинга доступны также сторонние устройства (3-d party devices). SMC может осуществлять мониторинг сторонних устройств и контролировать их доступность, используя различные инструменты, например, ICMP, SNMP. В результате система централизованного редактирования политик безопасности (называемая по какой-то причине в рекламных материалах конкурентов «системой централизованного управления») превращается даже не в центр управления безопасностью, а в систему сетевого мониторинга и управления. Ведь в журнал событий можно собирать (и составлять потом по ним интерактивные отчеты) также события с других устройств. Например, можно подключить для мониторинга и сбора событий

все сетевые устройства безопасности и управления сетевыми потоками (маршрутизаторы, коммутаторы). Администратор получает возможность определения индивидуального формата представления журнала для каждого конкретного устройства, а также специальное «административное меню» для запуска специфичных утилит управления.

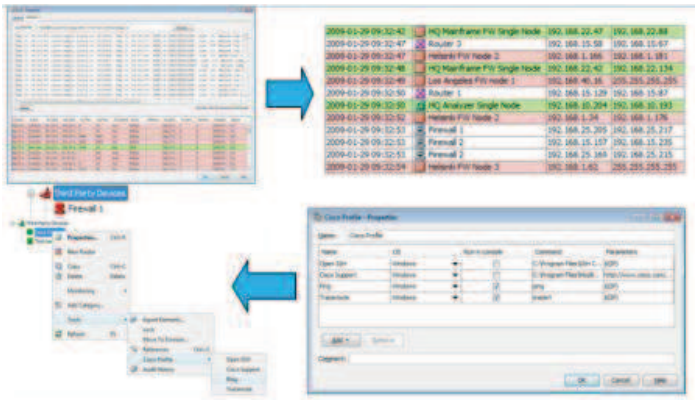


Рис. 24. Управление "сторонними" устройствами

В системе StoneGate есть 2 варианта для исследования происходящих событий:

- система «инцидентов безопасности»;
- подсистема журналирования и составления отчетов.

Система инцидентов создана специально для того, чтобы нескольким администраторам можно было обмениться информацией и совместно обрабатывать происходящие события. Она также позволяет хранить в специальном хранилище не только данные самой системы (например, информацию из журнала событий), но и внешние файлы (текстовые, графические и др.), вести журнал операций для отслеживания статуса инцидента и предоставлять для просмотра всю историю работы с заявкой.

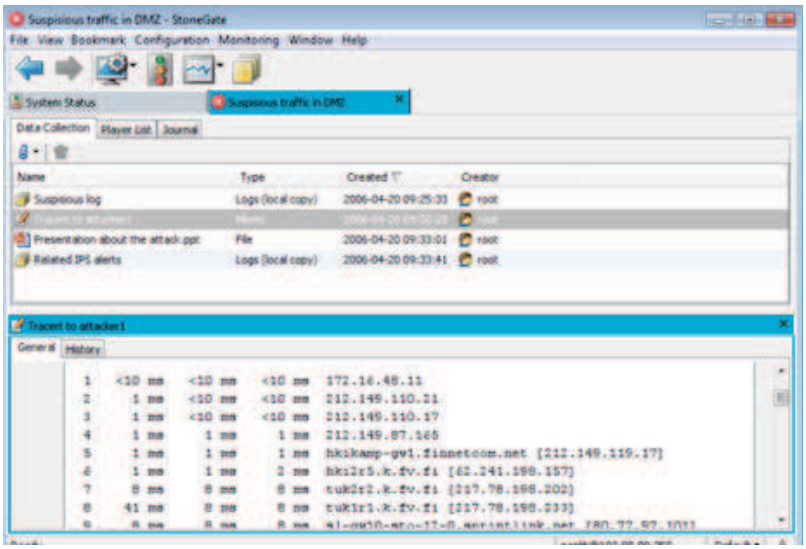


Рис. 25. Работа с инцидентами

Подсистема журналирования нужна для просмотра истории событий и предупрежденний о возникновении инцидентов. В зависимости от степени детализации, которая необходима, можно либо просматривать отдельные события со всеми релевантными полями, вплоть до заголовков пакетов или даже их содержимого, либо подняться до уровня отчета с агрегированными данными. Более того, переход из режима просмотра журналов в режим отображения статистики и обратно полностью прозрачен для администратора – он выбирает одним щелчком мыши тот объем данных, которые в данный момент хотел бы просмотреть и в том виде, который ему необходим. Встроенные шаблоны отчетов для быстрой инвентаризации устройств или задаваемые администратором для создания форм в соответствии с требованиями местных руководящих документов и определяющих соответствие стандартам отчетности позволяют с уверенность отвечать на вопрос о том, что именно случилось в сети, вне зависимости от происходящих или произошедших инцидентов.

Рис. 26. Отчеты и журналы событий

Администратор имеет полную свободу выбора варианта представления журналов, вплоть до визуализации на карте мира с БД геолокации (автоматически обновляется) и последующей привязкой к Google Maps.

Любые варианты реагирования или просмотра событий являются неполными и реактивными, позволяющими реализовать замедленное реагирование на происходящие инциденты, если они не поддерживаются мощными и гибкими возможностями оповещения администраторов. В решении StoneSoft есть возможность создания настоящих иерархических политик для распространения уведомлений о наступлении событий безопасности.

Среди вариантов оповещение может быть «банальное» - уведомление на консоль администратора, или более сложные:

- отправка письма по электронной почте;

- уведомление на систему сетевого управления через SNMP-trap;
- запуск внешней программы;
- даже отправка SMS-уведомления на мобильный телефон.

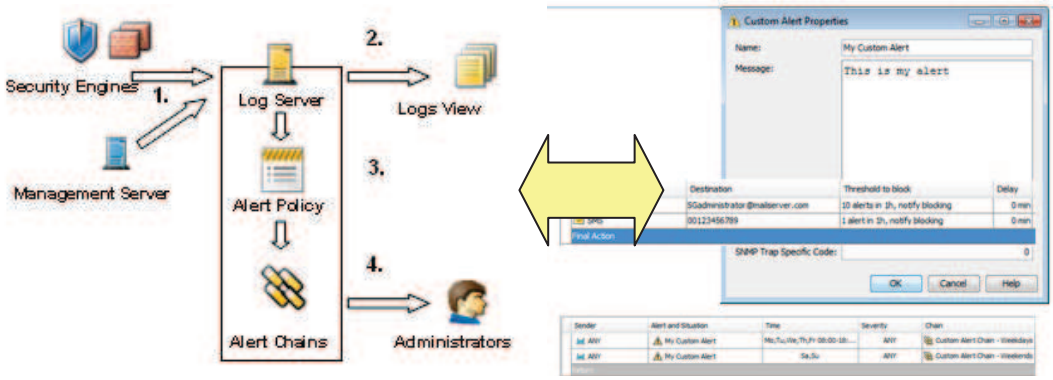


Рис. 27. Эскалация оповещений

Ролевое разделение администраторов позволяет гибко назначать права на те части системы, которые оператор может изменять. При этом можно задавать полномочия на доступ не только к объектам мониторинга (сенсор, МЭ, сервер, система SSL), а отдельным элементам – политикам доступа. Журнал аудита в каждый момент времени покажет, какие объекты и кем изменялись, а также кто входил в систему перед этим.

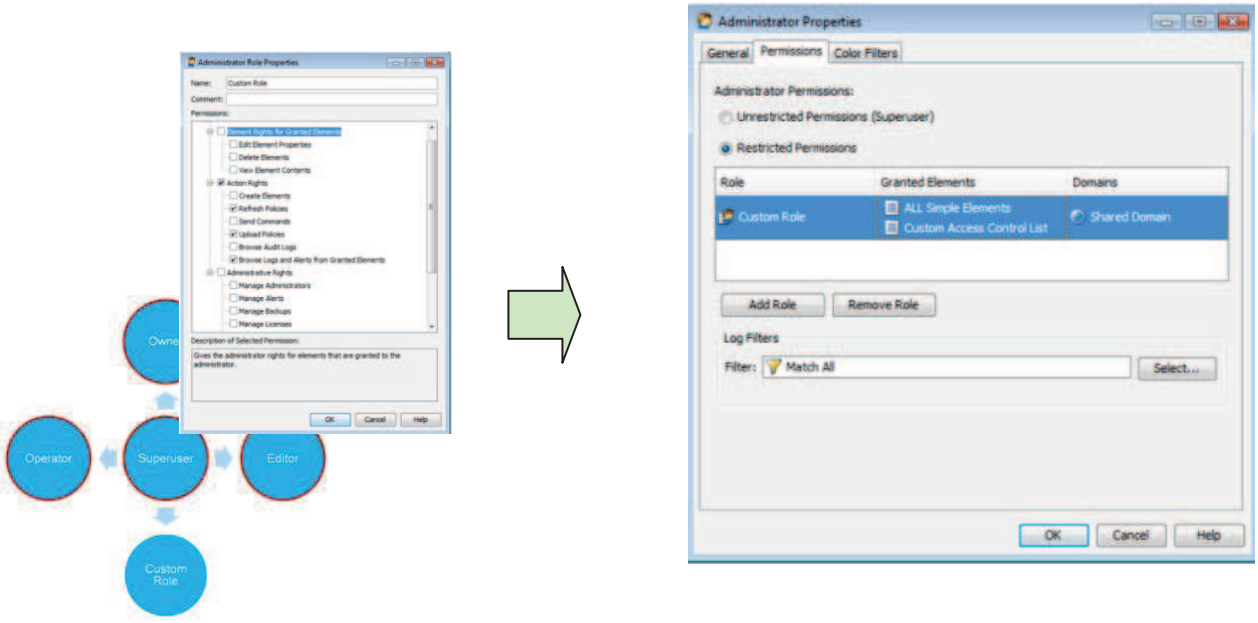


Рис. 28. Управления ролями администраторов

Кроме того, все эти задаваемые полномочия действуют в рамках «домена администрирования». Это особенно удобно для операторов, предоставляющих сервисы безопасности для клиентов или крупных распределенных организаций, сталкивающихся с подобными проблемами. А именно, к примеру, администратору небольшой филиала нужно дать возможность управления своим межсетевым экраном, без возможности влияния на другие созданные конфигурационные элементы, а также просмотра структуры сети или

конфигурации (созданных элементов управления). При этом администратор центрального офиса хочет сохранить за собой способность контроля за работой своего коллеги в филиале и возможность вмешательства в случае необходимости. В рамках доменов администрирования эту концепцию очень легко реализовать: можно создать несколько доменов управления (в рамках одного сервера), в каждом из которых завести соответствующее количество устройств. Это позволит и лучше структурировать имеющуюся конфигурацию, а также упростить её сопровождение.

Рис. 29. Независимые домены управления

Так, в рамках процедуры администрирования системы защиты стандартом является выделение нескольких администраторов с разными правами: одного, который имеет полный доступ к компонентам системы и обладает полномочиями на внесения корректирующих изменений в политики, и другого, который просматривает отчеты, журналы событий и, возможно, политики в режиме «для чтения». SMC позволяет реализовать эту концепцию в полной мере, а также сделать еще один «шаг вперед» в части разделения полномочий и доступа к компонентам системы. Более того, администратор, находясь в командировке или в дороге и не имея под рукой полноценной рабочей станции с поддержкой Java, легко может получить доступ к системе с любого мобильного устройства, где есть HTTP-браузер, чтобы разобраться с инцидентом, который пришел к нему в виде уведомления на тот же самый мобильный телефон.

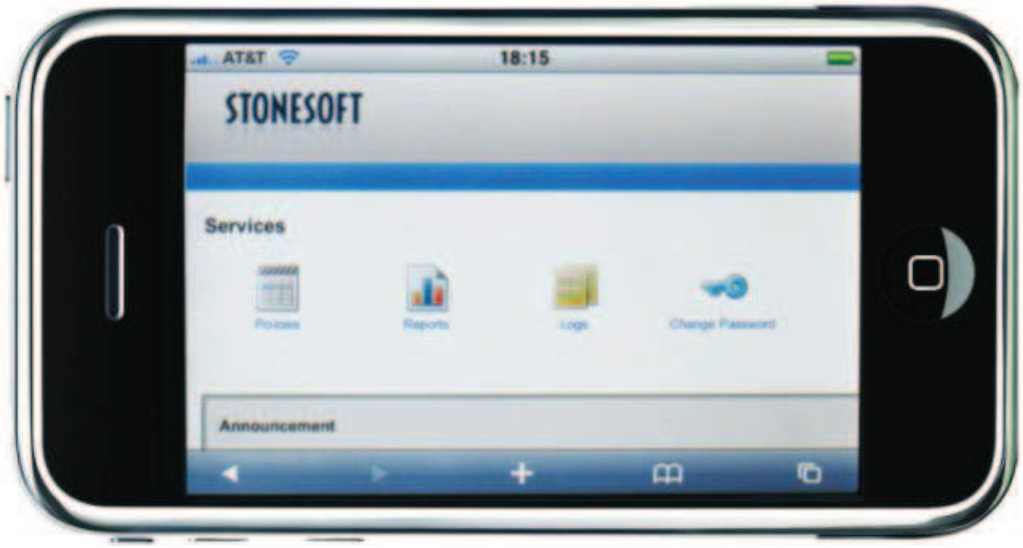


Рис. 30. Web-портал для удаленного доступа администраторов/клиентов

В рамках «интерфейса мониторинга» (Web-портала) у него есть возможность не только просмотра журналов или составления отчетов, но и верификации конфигураций устройств. Внешнее оформление портала может меняться в зависимости от «домена управления», в который попадает администратор.

Наконец, полностью конфигурируемая система напоминаний и заданий позволяет забыть о рутинных операциях и больше не заботиться о таких вопросах, как регулярное создание архива или резервирование конфигураций: достаточно один раз определить те действия, которые требуют внимания, и после этого можно только контролировать их выполнение через журналы оповещений. Более того, часть рутинных системных операций уже изначально автоматизировано.

Система безопасных обновлений позволяет централизованно управлять обновлениями ПО, и в случае неудачного обновления вернуться к предыдущей успешно работавшей версии. При этом новые версии сигнатур и правил выявления аномалий, а также версии ОС могут загружаться с сайта производителя и активироваться на межсетевом экране в автоматическом режиме. Администратор при этом будет «спать спокойно» и получать своевременно уведомления о том, что доступны новые версии ПО, которые были успешно установлены. В случае ошибок с активацией, как уже было сказано, межсетевой экран сам откатывается на предыдущую версию, чтобы не потерять работоспособность. Все это позволяет существенно снизить затраты на администрирование, которые, по оценкам множества инсталляций, позволяют окупить решение по сравнению с конкурентами уже в течение первого года.

3. Электронный идентификатор USB «eToken».

Электронный идентификатор - это компактное устройство в виде USB-брелка, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

Основу электронного идентификатора составляет микроконтроллер, который выполняет криптографическое преобразование данных, и память, в которой хранятся данные пользователя (пароли, сертификаты, ключи шифрования и т. д.).

Электронные идентификаторы используются в комплексе с соответствующими программными средствами «eToken Netwotk Logon».

4. ПО строгой аутентификации «eToken Netwotk Logon».

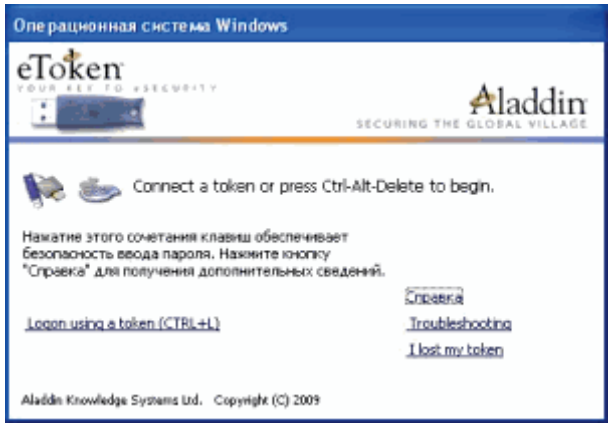
«eToken Network Logon» предназначен для кардинального решения проблемы "слабых" паролей при работе на компьютерах под управлением Microsoft Windows. Сразу после установки продукта для входа на компьютер или в сеть можно начать использовать надёжные и стойкие к перебору пароли, либо цифровые сертификаты.

«eToken Network Logon» сгенерирует сложный пароль, установит его в системе и сохранит в памяти «eToken». Пользователю не нужно запоминать новый пароль – достаточно при входе на компьютер подключить «eToken» и ввести пароль пользователя для «eToken» – хранящийся в памяти пароль будет передан в систему. Таким образом, пароль не надо запоминать и вводить с клавиатуры – это исключает возможность его подсматривания или перехвата злоумышленником.

«eToken Network Logon» значительно снижает влияние "человеческого фактора" на уровень безопасности Windows. Внедрение и правильное использование продукта позволят исключить возможность обращения злоумышленников к ресурсам системы от имени легальных пользователей.

«eToken Network Logon» обеспечивает:

- двухфакторную аутентификацию пользователей на компьютере и в сети Windows с помощью USB-ключей или смарт-карт «eToken»;
- использование регистрационных имён и паролей для локального входа в систему или для входа в домен;
- использование цифровых сертификатов X.509, сертификатов пользователя со смарт-картой и закрытых ключей для входа в домен;
- генерирование и последующее применение случайных паролей, неизвестных пользователю.



«eToken Network Logon» может быть установлен на компьютеры и ноутбуки под управлением ОС Microsoft Windows,

объединённые в рабочую группу или домен Windows.

После установки «eToken Network Logon» стандартное приглашение для входа в Microsoft Windows заменяется новым, которое расширяет возможности по входу пользователя в систему:

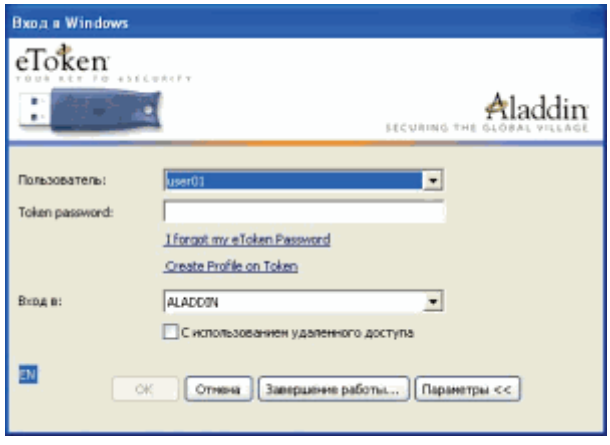
- можно подключить смарт-карту («eToken») с закрытым ключом и сертификатом пользователя, ввести пароль пользователя для «eToken» и войти в систему;
- можно нажать CTRL+ALT+DELETE, ввести имя пользователя, пароль и (при необходимости) имя домена, нажать OK и войти в систему.

Для каждого из этих двух способов аутентификации в «eToken Network Logon» предусмотрены усовершенствования:

- Вместо того чтобы каждый раз вводить имя пользователя и сложный пароль, пользователь один раз сохраняет их в памяти «eToken», а впоследствии лишь подключает «eToken» и вводит для него пароль пользователя.
- Для того чтобы войти в систему, предъявив сертификат пользователя со смарт-картой, надо подключить «eToken» и ввести для него пароль пользователя. Если «eToken» уже подключен, не нужно вынимать его и повторно подключать, достаточно лишь нажать CTRL+L, а затем ввести пароль пользователя для «eToken».

Главная возможность «eToken Network Logon» – это решение проблемы "слабых" паролей. После установки продукта можно:

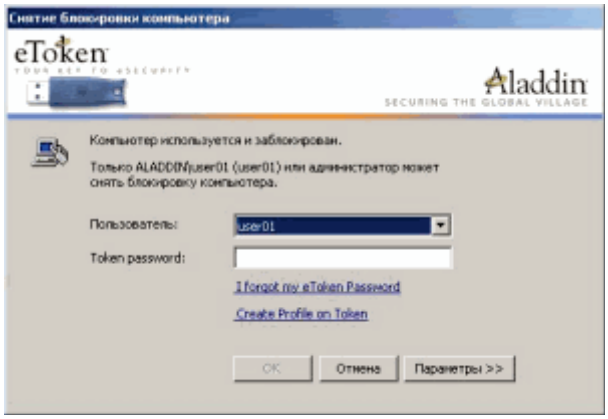
- полностью отказаться от использования паролей при входе на компьютер и в сеть, перейдя к использованию цифровых сертификатов, либо
- использовать хранимые в памяти «eToken» сложные пароли (заданные вручную с учётом действующих в организации требований к их сложности, либо автоматически сгенерированные).



В любом случае пароль перестаёт быть "слабым" (исключается риск его подбора злоумышленником), при возможной смене пароля пользователем исключается риск

задания им нового пароля, являющегося "слабым", пароль не вводится с клавиатуры (исключаются риски подсматривания пароля или его перехвата шпионским ПО), пользователь не должен помнить пароль (исключаются случаи его забывания и записывания на бумаге).

- Усиление безопасности при использовании паролей. Даже если для входа на компьютер и в сеть Windows используются пароли, то с помощью «eToken Network Logon» можно значительно усилить защищённость существующей системы. Имена и пароли пользователей можно сохранить в памяти «eToken» (что исключит риск их подсматривания злоумышленником). Дополнительно можно использовать встроенный в «eToken Network Logon» генератор паролей для генерации сложных паролей (это исключит риск их подбора злоумышленником). Сгенерированный пароль записывается в память «eToken» и сохраняется в ней. Количество наборов "имя пользователя – пароль", хранящихся в памяти «eToken», неограниченно.
- Простой переход к аутентификации с использованием цифровых сертификатов. При развёртывании инфраструктуры PKI появляется возможность использовать цифровые сертификаты для входа в сеть Windows и на локальный компьютер. Если в памяти «eToken» имеется сертификат пользователя со смарт-картой и соответствующий закрытый ключ, их можно использовать для входа в домен Windows вместо имени пользователя и пароля. Таким образом, обеспечивается плавность перехода от парольной аутентификации к строгой аутентификации с использованием цифровых сертификатов.



- Автоматическая блокировка рабочей станции. При отсоединении «eToken» от порта USB происходит автоматическая блокировка компьютера. Для разблокирования компьютера необходимо подсоединить «eToken» и ввести пароль пользователя для «eToken».
- Настройка продукта в соответствии с требованиями политики безопасности организации. Администратор может запретить или разрешить пользователю ввод пароля вручную.

- Настройка методов аутентификации. Администратор может управлять методами аутентификации:

  - какие методы разрешены на данном компьютере — использование профилей, применение сертификатов;
  - какой метод аутентификации используется по умолчанию и может ли пользователь самостоятельно выбирать метод при наличии в памяти «eToken» как профилей, так и сертификата.

Преимущества продукта:

- Отказ от ввода паролей вручную. Какой бы метод регистрации ни применялся, — использование хранимых в памяти «eToken» сертификатов или паролей, — при входе в систему пользователь никогда не вводит пароль. Это исключает риски подсматривания пароля или его перехвата при вводе с клавиатуры.
- Возможность применения длинных и сложных паролей. Поскольку пользователь не должен вводить пароль вручную, сам пароль может быть длиннее и сложнее, чем пользователь может запомнить.
- Использование сгенерированных случайных паролей, неизвестных пользователю. «eToken Network Logon» позволяет генерировать пароли заданной длины, сохранять их в памяти «eToken» и подставлять в хранилище учётных данных таким образом, что пользователь даже не знает своего пароля, а потому не может записать и тем самым скомпрометировать его.
- Аппаратная аутентификация пользователей. Для входа в систему пользователю надо иметь «eToken». Это надёжнее, чем ввод паролей с клавиатуры.
- Двухфакторная аутентификация. «eToken Network Logon» позволяет не просто сохранить реквизиты пользователя в памяти «eToken», но и защитить их паролем пользователя «eToken». При использовании этой возможности потеря или кража «eToken» не приведёт к компрометации пароля.
- Интеграция в инфраструктуру открытых ключей. «eToken Network Logon» поддерживает не только системы, в которых для аутентификации пользователей применяются пароли, но и более надёжный и современный метод регистрации с использованием смарт-карт.
- Простота и удобство для пользователей. Способы аутентификации, применяемые в «eToken Network Logon», удобнее для пользователей, чем стандартные способы. Требования к сложности паролей пользователя «eToken» не столь высоки, как требования к сложности паролей Windows. Поэтому при двухфакторной

аутентификации вводить простой пароль пользователя «eToken» проще, чем без таковой вводить сложный и длинный пароль.

- Улучшенный интерфейс при регистрации с использованием смарт-карт. Если «eToken» пользователя подключен к компьютеру, необязательно отключать его и подключать вновь. «eToken Network Logon» позволяет в таком случае нажать CTRL+L, ввести пароль пользователя «eToken» и войти в систему, не прикасаясь к eToken.

«eToken Network Logon» может интегрироваться с «eToken TMS» (Token Management System), системой управления жизненным циклом USB-ключей и смарт-карт. Это позволит управлять сертификатами и профилями централизованно.

Доступна сертифицированная версия «eToken Network Logon», которая может использоваться в ИСПДн до 1 класса включительно и для создания автоматизированных систем до класса защищенности 1Г включительно.

5. «eToken TMS».

Система «eToken TMS» предназначена для централизованного управления жизненным циклом устройств «eToken» и обеспечения целостности связей между учетными записями пользователей, средствами аутентификации и приложениями безопасности согласно установленным в организации политикам.

«eToken TMS» имеет сертификат соответствия ФСТЭК России №1700 от 16 октября 2008 года.

Сертифицированная версия «eToken TMS» может использоваться для создания автоматизированных информационных систем до класса защищенности 1Г.

Система TMS призвана полностью решить наиболее важную проблему корпоративной безопасности: обеспечение связи между пользователями, их средствами идентификации и организационными политиками с приложениями безопасности. Все эти компоненты объединены в виде автоматизированной и настраиваемой структуры, которая легко адаптируется в масштабах любого предприятия (в особенности в рамках инфраструктуры открытых ключей PKI).

Система TMS предоставляет широкий выбор необходимых средств для управления всеми аспектами жизненного цикла устройств «eToken». В частности, TMS позволяет выпускать и отзывать ключи, сбрасывать значение пароля и самостоятельно оформлять заявки на выпуск «eToken», автоматически копировать и восстанавливать идентификационные данные пользователя, решать проблемы, связанные с неисправными или утраченными ключами «eToken». Система обладает широкими возможностями ведения статистики и

отчетности в соответствии с отраслевыми стандартами, в том числе Sarbanes Oxley, HIPAA, Basel II и пр.

Концепция системы основана на использовании службы каталогов Microsoft Active Directory.

Рис. 31. Общая архитектура применения «eToken TMS»

Концепция «eToken TMS» предусматривает также использование дополнительных модулей (коннекторов), которые позволяют работать с внешними приложениями безопасности: для доступа к локальной сети, виртуальным частным сетям, аутентификации по одноразовым паролям, безопасного шифрования данных и электронной почты.

Система «eToken TMS»:

- обеспечивает полномасштабное развертывание в рамках компании и управление на всех стадиях жизненного цикла устройствами «eToken» и их связью с пользователями и совместимыми приложениями;
- обеспечивает упрощенную процедуру установки с помощью программы-мастера;
- обеспечивает работу пользователя, службы поддержки и администратора через Web-интерфейс (без необходимости установки дополнительного программного обеспечения);
- имеет модульную архитектуру на основе открытых стандартов, обеспечивает поддержку приложений, использующих настраиваемые коннекторы, которые позволяют расширять базовую функциональность системы;
- предоставляет комплект SDK для интеграции приложений сторонних разработчиков;

- предоставляет решение для пользователей «eToken», потерявших или забывших устройство, находясь вне офиса;
- обеспечивает безопасное резервное копирование и восстановление данных пользователей, сохраненных в памяти устройств «eToken»;
- предоставляет полный набор средств для аудита и создания отчетов;
- обеспечивает гибкую настройку разграничения полномочий доступа к различным функциям системы;
- обеспечивает встроенное шифрование данных с применением разных ключей для разных доменов.

Приложение 4: Перечень действующих лицензий в области защиты информации ЗАО «Энвижн Груп»

№ п.п	Название лицензии	№ лицензии	Кем выдана	Срок действия
ЗАО «Энвижн Груп»				
1.	На осуществление работ, связанных с использованием сведений, составляющих государственную тайну	ГТ № 0020237	ФСБ России	до 25.12.2012
2.	На осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	ЛЗ № 0016501 Рег. № 6793П	ФСБ России	до 10.08.2012
3.	На осуществление технического обслуживания шифровальных (криптографических) средств	ЛЗ № 0016502 Рег. № 6794Х	ФСБ России	до 10.08.2012
4.	На осуществление распространения шифровальных (криптографических) средств	ЛЗ № 0016503 Рег. № 6795Р	ФСБ России	до 10.08.2012
5.	На деятельность по технической защите конфиденциальной информации	серия КИ 0054 № 002655 Рег. № 0648	ФСТЭК	до 01.02.2013
6.	На деятельность по разработке и (или) производству средств защиты конфиденциальной информации	серия КИ 0054 № 002656 Рег. № 0378	ФСТЭК	до 01.02.2013
7.	Аттестат аккредитации в качестве органа по аттестации объектов информатизации, обрабатывающих сведения, составляющие государственную тайну	на стадии получения		
8.	На осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны (в части, касающейся технической защиты информации)	на стадии получения		

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного документа и дата	Подпись	Дата
	изменённых	замененных	новых	изъятых					

Подпись и дата | Инв. № дубл. | Взамен инв. № | Подпись и дата | Инв. № подл.