Построение централизованной системы информационной безопасности (ЦСИБ) для компании «Акрон», Великий Новгород

КРАТКОЕ ОПИСАНИЕ

Компания «Акрон»

Компания «Акрон» – один из крупнейших российских и мировых производителей минеральных удобрений с объемом годового производства свыше 4,1 млн тонн. Компания производит свыше 40 наименований химической продукции. «Акрон» обеспечивает полную прозрачность своей производственной и коммерческой деятельности. Финансовые результаты деятельности компании подтверждаются крупнейшей международной аудиторской компанией PricewaterhouseCoopers.

«Акрон» объединяет три производственных предприятия, два из которых находятся в России и одно – в КНР.

В городе Великий Новгород (Россия) расположено ОАО «Акрон», выпускающее более 30 наименований продукции, которая используется во многих отраслях промышленности и в сельском хозяйстве.

В городе Дорогобуж (Смоленская область, Россия) расположено ОАО «Дорогобуж», производящее аммиак и минеральные удобрения (аммиачную селитру и азофоску), а также продукты органической и неорганической химии. Принадлежащее ОАО «Дорогобуж» дочернее общество ЗАО «Катализатор» является крупнейшим производителем катализаторов для химической и нефтехимической промышленности России.

В городе Линьи (провинция Шаньдун, Китай) находится ОАО «Хунжи-Акрон». Предприятие производит высококонцентрированные комплексные удобрения, серную, фосфорную и соляную кислоты, синтетический аммиак и моноаммонийфосфат.

Сбытовая сеть компании «Акрон» – ЗАО «Агронова» – объединяет 10 региональных представительств и 16 специализированных агрохимических предприятий, расположенных в основных сельскохозяйственных центрах России.

В структуру компании с ноября 2003 г. входит дочернее транспортно-экспедиционное предприятие ЗАО «Акрон-Транс».

Предыстория проекта

Крупное химическое предприятие – компания «Акрон», г. Великий Новгород, – столкнулось с определенными сложностями при внедрении корпоративных политик безопасности и осуществлении полноценного контроля над их соблюдением.

К моменту начала разработки проекта локально-вычислительная сеть (ЛВС) предприятия насчитывала более 500 рабочих мест. Общая сетевая инфраструктура, обеспечивающая транспортный функционал, не позволяла в полном объеме обеспечить защиту и целостность данных, контроль использования каналов связи и их резервирования. Развитие компьютерных технологий и средств оперативного хранения данных (CD, DVD, USB-Flash) требовало повышенного внимания службы безопасности предприятия к порядку использования этих средств как внутри предприятия, так и при обмене данными с партнерами и поставщиками.

Цели проекта

Целью проектирования ЦСИБ ЛКС компании «Акрон» является построение системы информационной безопасности, отвечающей текущим стандартам на построение защищенных сетей корпоративного уровня.

Для полной реализации проекта надо решить ряд задач:

- обеспечение системы антивирусной защиты серверов и рабочих станций как извне, так и изнутри сети;
- обеспечение системы защиты от несанкционированного доступа к ресурсам локальной компьютерной сети как извне, так и изнутри сети;
- обеспечение комплексной системы мониторинга и управления средствами защиты.

Описание проекта

Над реализацией данного проекта работала группа технических специалистов компании «СТЭП ЛОДЖИК». В качестве «нулевого»

этапа разработки системы был проведен детальный аудит всех сетевых систем предприятия. В результате были получены объективные данные, характеризующие:

• текущую топологию сети,

• параметры коммутации и маршрутизации трафика,

• назначение зон и компонентов сети,

• текущие настройки и версии программно-аппаратных частей,

• правила аутентификации и авторизации пользователей,

• правила трансляции адресов при выходе в публичные сети,

• параметры маршрутизации почтовых сообщений,

• версии ПО пользовательских систем,

• версии ПО серверных платформ и систем хранения данных,

• нагрузку в сети.

После анализа результатов аудита было сформулировано назначение будущей системы. Централизованная система информационной безопасности (ЦСИБ) локальной компьютерной сети «Акрон» предназначена для обеспечения надежной защиты локально-компьютерной сети (ЛКС) от проникновения компьютерных вирусов по каналам внешней связи, а также от несанкционированного доступа к ресурсам ЛКС. Данные классы атак включают в себя модификацию, уничтожение или компрометацию внутренних данных, проведение атак класса «отказ в обслуживании», произвольное выполнение кода на компьютерах и серверах заказчика и т. д., что в конечном счете может привести к финансовым и технологическим потерям.

В основе решения заказчику была предложена модульная концепция защищенного предприятия Cisco SAFE. Узлы и компоненты сети были классифицированы и разделены на группы согласно рекомендациям концепции. Такой подход нацелен не на механическую установку межсетевого экрана и системы обнаружения атак, а на анализ ожидаемых угроз и разработку методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности.

«Архитектура SAFE – это не догма, а набор рекомендаций, так называемых Best Practices, составленных специалистами компании Cisco в результате работы с десятками тысяч заказчиков по всему миру. Учитывая международный характер деятельности ''Акрон'' и большой процент оборудования Cisco, вполне закономерно, что для защиты своей корпоративной сети эта компания выбрала архитектуру SAFE, максимально учитывающую инвестиции, сделанные в сетевую инфраструктуру».

Алексей Лукацкий, бизнес-консультант по безопасности

Основные достоинства Cisco SAFE

• Обеспечение основы для построения безопасных, доступных, интегрированных сетей.

• Открытая модульная структура.

• Возможность упростить процесс разработки, внедрения и управления сетевой безопасностью.

• Обеспечение масштабируемости решений.

• Возможность эффективного поэтапного внедрения.

Корневым блоком (Core) сети был назначен кластер коммутаторов Cisco Catalyst 4500, которые уже успешно использовались заказчиком. Данный блок определяет общие для всей сети параметры маршрутизации трафика и условия сегментации сети на виртуальные подсети (VLAN).

Распределительный блок (Distribution) был сформирован из части имеющихся коммутаторов Cisco Catalyst 2950 и дополнен новыми коммутаторами Catalyst 3550. В задачу распределительного блока входила сквозная поддержка протокола 802.1q.

Блок доступа (Access) был сформирован из имеющегося оборудования заказчика. В основном в состав блока вошли ранее использовавшиеся в распределительном блоке неуправляемые коммутаторы 3Com и оборудование иных производителей. Блок доступа обеспечивал непосредственное подключение рабочих групп пользователей к ЛКС.

Серверный модуль был коммутирован непосредственно в корневой блок. Там, где это было технологически целесообразно, VLAN серверного модуля коммутировался с определенным устройством распределительного блока. Это позволило

избежать обязательного перемещения всех серверов в центральную серверную комнату. Везде, где позволяло оборудование и ПО, были задействованы схемы резервирования подключений.

В центре интернет-модуля был внедрен межсетевой экран Cisco PIX Firewall 515 Active-Standby Failover с шестью физическими интерфейсами и отказоустойчивой конфигурацией. Два канала от разных провайдеров связи терминировались на выделенные маршрутизаторы Cisco 2800.

В модуль ДМЗ (демилитизированной зоны) были включены все ресурсы, имеющие отношение к обмену данными через публичные сети. Данный модуль был реализован на отдельном физическом интерфейсе отказоустойчивого Cisco PIX Firewall 515 Active-Standby Failover.

Это позволило полностью контролировать прохождение трафика в данных модуль вплоть до уровня приложений (Layer 7 Inspection).

В модуле управления были смонтированы Cisco ACS 4.0 Solution Engine для обеспечения сквозной аутентификации доступа к управлению оборудованием, а также для будущей реализации защиты пользовательских портов на основе протокола 802.1x. Для управления системой обнаружения вторжений на локальных серверах (Cisco Secure Agent) был развернут сервер с Cisco VMS 2.3 с консолью управления агентами. Дополнительно был размещен сервер для запуска системы Adaptive Security Device Manager, предназначенной для управления межсетевым экраном Cisco Pix Firewall 515E.

В основе резервирования внешних каналов связи использован протокол OSPF совместно с технологией Cisco IOS EOT (Enhanced Object Tracking).

Отказоустойчивость в локальном сегменте контролируется протоколом 802.1s (Rapid Spanning Tree).

«Компания “СТЭП ЛОДЖИК” начала сотрудничать с объединением “Акрон” в Великом Новгороде несколько лет назад. За эти годы для “Акрона” нашими специалистами были разработаны и внедрены несколько проектов по модернизации и развитию сети. Проекты были разработаны на основе современного оборудования Cisco Systems, дизайн каждого проекта также разрабатывался по стандартам, принятым корпорацией Cisco. Компания “Акрон” – наш давний, постоянный клиент. Учитывая тот объем работ, который был сделан нашими специалистами для данного предприятия, можно сказать, что “Акрон” является нашим почетным клиентом. Мы рады, что компания “Акрон” выбрала “СТЭП ЛОДЖИК” для сотрудничества, и готовы работать с этой компанией в дальнейшем».

Инженерная группа компании «СТЭП ЛОДЖИК»

Результаты внедрения

Централизованное управление виртуальными подсетями VLAN существенно снизило нагрузку на корневые коммутаторы. Одновременно система была подготовлена для внедрения технологий 802.1x и Cisco Network Admission Control.

Обеспечен бесперебойный доступ пользователей ко всем серверным ресурсам, при этом сами серверы защищены персональными системами обнаружения вторжений на основе Cisco Security Agent. Инфраструктура подготовлена для внедрения CSA агентов и на пользовательские рабочие станции.

Оптимизирована утилизация внешних подключений. Наиболее критичный трафик имеет три маршрута доставки, определяемых автоматически технологией Cisco IOS EOT. Пользовательский доступ в Интернет защищен отказоустойчивым межсетевым экраном Cisco PIX 515E.

Модуль управления позволяет ответственному оператору контролировать работу всех компонентов системы, а администратор сети имеет возможность разграничивать доступ к управлению оборудованием согласно должностным обязанностям при помощи Cisco ACS 4.0. Дополнительно задействована служба протоколирования активности.

Результатами осуществления проекта стало построение защищенной мультисервисной сети предприятия. Несколько лет назад в компании «Акрон», Великий Новгород, была построена сеть на оборудовании 3Com. В дальнейшем инженерами «СТЭП ЛОДЖИК» были разработаны проект по модернизации ЛВС и проект по созданию системы информационной безопасности (ЦСИБ) на оборудовании Cisco Systems. Постепенно был осуществлен полный переход на оборудование Cisco Systems.

В конце 2006 года между компаниями «Акрон» и «СТЭП ЛОДЖИК» подписан контракт на постоянное сервисное обслуживание.

О компании «СТЭП ЛОДЖИК»

Российская компания «СТЭП ЛОДЖИК» (www.step.ru) предоставляет услуги сетевой и системной интеграции. У компании два офиса: головной офис в Москве и филиал в Санкт-Петербурге. Компания имеет многолетний опыт применения высокотехнологичного оборудования в проектах любого уровня сложности. Интеллектуальную основу компании составляют свыше 100 инженеров и системных архитекторов, сертифицированных ведущими мировыми производителями. В состав компании входит многопрофильный сервисный центр. Системная интеграция является для «СТЭП ЛОДЖИК» генеральным направлением деятельности.

Основные направления деятельности

- Услуги по созданию инфраструктуры здания, включая кабельную разводку для связи компьютерных и телефонных систем (СКС), коммуникации охранных и пожарных систем, а также электрическую проводку.
- Создание локальных вычислительных и телефонных сетей, построенных на современном оборудовании от лидирующих производителей.
- Построение территориально распределенных мультисервисных сетей и сетей операторского класса.
- Построение сетей сотовой радиотелефонной связи, радиорелейных и оптоволоконных линий связи.
- Проведение аудита информационной безопасности, надежности и эффективности.
- Интеграция приложений на базе уже существующих или вновь создаваемых информационных сетей в области применения OSS-, BSS- и CRM-систем.
- Пакет услуг по внедрению и технической поддержке аппаратно-программных комплексов.
- Поставка оборудования и ПО напрямую от производителя или разработчика.
- Оказание информационно-консультационных услуг в области сетевых технологий и менеджмента.

Отдельные направления деятельности

- Проведение технических мероприятий по защите информации в ведомственных сетях силовых структур РФ (Минобороны, МВД РФ и др.), а также органов федеральной власти.
- Создание систем на базе web-технологий: корпоративные интернет-порталы и интранет-ресурсы со сложной функциональностью, web-представительства, торговые площадки.
- Услуги повышения квалификации IT-специалистов на базе собственного учебного центра.

Информация о компании Cisco

Cisco Systems, Inc. (NASDAQ: CSCO) – мировой лидер в области сетевых технологий и оборудования для Интернет. В 2004 году компания отметила 20-летие своей деятельности, неотъемлемыми атрибутами которой являются техническое новаторство, передовые позиции в отрасли и социальная ответственность. Информацию о решениях, технологиях и деятельности компании Вы можете найти на *www.cisco.com* и *www.cisco.ru*. Новости Cisco публикуются на сайте *http://www.cisco.com/global/RU/news/* и *http://newsroom.cisco*.

Cisco Systems
Россия, 115054, Москва
бизнес центр
«Риверсайд Тауерс»
Космодамианская наб., 52
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186,
Санкт-Петербург,
бизнес центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099
Алматы
бизнес центр «Самал 2»
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр
«Горайзон Тауерс»
Ул. Шовковична, 42-44,
этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)