РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Защита информации от несанкционированного доступа

Тема 5. Разработка политики безопасности информационной системы

Вопросы:

1. *Общие положения разработки политики безопасности*
2. *Анализ отечественного рынка средств защиты информации*
3. *Процесс разработки политики безопасности*
4. *Реализация политик безопасности*

Литература

1. Щеглов А.Ю. Защита информации от несанкционированного доступа. – СПб.: Наука и техника. 2004. – 383 с

1. Общие положения разработки политики безопасности

Согласно RFC 2196 под политикой информационной безопасности компании понимается «формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе». При этом различают общую стратегическую политику безопасности компании, взаимоувязанную со стратегией развития бизнеса и ИТ-стратегией компании, а также частные тактические политики безопасности, детально описывающие правила безопасности при работе с соответствующими ИТ-системами и службами компании.

В соответствии с этим определением и рекомендациями ведущих международных стандартов в области планирования информационной безопасности (ИБ) и управления ею (BS 7799-2:2002, ISO/IEC 17799:2005, ISO/IEC TR 13335, ISO/IEC 10181-7:1996, ISO/IEC 15288:2002, ISO/IEC TR 15443, BSI, CobiT, ITIL, ГОСТ Р ИСО/МЭК 15408-2002) политики безопасности должны содержать следующее:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства компании в отношении выполнения политики безопасности и организации режима информационной безопасности компании в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности компании;
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

1. Общие положения разработки политики безопасности

Актуальность разработки политик безопасности для отечественных компаний и организаций объясняется необходимостью формирования основ планирования информационной безопасности и управления ею на современном этапе. В настоящее время большинством российских компаний определены следующие приоритетные задачи развития и совершенствования своей деятельности:

- минимизация рисков бизнеса путём защиты своих интересов в информационной сфере;
- обеспечение безопасного, доверенного и адекватного управления предприятием;
- планирование и поддержка непрерывности бизнеса;
- повышение качества деятельности по обеспечению информационной безопасности;
- снижение издержек и повышение эффективности инвестиций в информационную безопасность;
- повышение уровня доверия к компании со стороны акционеров, потенциальных инвесторов, деловых партнёров, профессиональных участников рынка ценных бумаг, уполномоченных государственных органов и других заинтересованных сторон.

1. Общие положения разработки политики безопасности

Успешное выполнение перечисленных задач в условиях воздействия внутренних и внешних факторов, а также действий конкурентов и злоумышленников проблематично.

Это связано с возрастающей необходимостью повышения уровня информационной безопасности и недостаточной проработанностью политик информационной безопасности в отечественных компаниях.

При разработке политик безопасности важно иметь в виду:

- в разрабатываемых политиках безопасности отечественных компаний необходимо учитывать в равной мере нормативные, экономические, технологические, технические и организационно-управленческие аспекты планирования информационной безопасности и управления ею. Только в этом случае можно достигнуть разумного баланса между стоимостью и эффективностью разрабатываемых правил политик безопасности;
- политики безопасности российских компаний не должны противоречить отечественной нормативной базе в области защиты информации в АС на территории РФ, в том числе нормативно-правовым документам (федеральным законам, указам Президента, постановлениям Правительства) и нормативно-техническим документам (государственным стандартам, руководящим документам Гостехкомиссии (ФСТЭК), Минобороны и ФСБ России);

1. Общие положения разработки политики безопасности

- при создании политик безопасности желательно учесть положения действующей Государственной системы стандартизации (ГСС) согласно Федеральному закону № 184-ФЗ «О техническом регулировании», рекомендации ГОСТ Р ИСО/МЭК 15408-2002, рекомендации функционального стандарта ГОСТ Р 51583-2000, описывающего этапность построения защищённых информационных систем, рекомендации функционального стандарта – документа ФСТЭК, под названием СТР-К, для выработки требований по технической защите конфиденциальной информации;
- при отражении в политиках безопасности нормативного аспекта рекомендуется следовать требованиям новой российской национальной системы стандартизации, основанной на системе технического регулирования в соответствии с рекомендациями Федерального закона № 184-ФЗ «О техническом регулировании». Это отвечает последним веяниям формирования в Российской Федерации технического законодательства, обеспечивающего выполнение Соглашений Всемирной торговой организации (ВТО) по техническим барьерам в торговле (ТБТ) и санитарным и фитосанитарным мерам (СФС) с учётом принципов нового подхода к технической регламентации в Европейском союзе (ЕС). Следование данным требованиям позволит устранить существующие технические барьеры для отечественных компаний в торговле и обеспечении конкурентоспособности продукции;

1. Общие положения разработки политики безопасности

- использование в политиках безопасности современных подходов и принципов обеспечения информационной безопасности, основанных на лучшем мировом и отечественном опыте (BS 7799-2:2002, ISO/IEC 17799:2005, ISO/IEC TR 13335, ISO/IEC 10181-7:1996, ISO/IEC 15288:2002, ISO/IEC TR 15443, BSI, CobiT, ITIL, ГОСТ Р ИСО/МЭК 15408-2002 и пр.), позволит выработать обоснованную парадигму планирования информационной безопасности и управления ею – концептуальную схему обеспечения информационной безопасности, а также требуемые модели постановки проблем в области управления информационной безопасностью и предложить разумно достаточные решения этих проблем. В частности, сформулировать основные принципы обеспечения информационной безопасности и доверия к ней, а также разработать требования по обеспечению информационной безопасности, адекватные целям и задачам развития бизнеса отечественных компаний;

1. Общие положения разработки политики безопасности

- при отражении в разрабатываемых политиках безопасности отечественных компаний экономического подхода к планированию информационной безопасности и управлению ею на основе концепции управления рисками рекомендуется обратить внимание на методы: прикладного информационного анализа (*Applied Information Economics*, AIE); расчёта потребительского индекса (*Customer Index*, CI); расчёта добавленной экономической стоимости (*Economic Value Added*, EVA); определения исходной экономической стоимости (*Economic Value Sourced*, EVS); управления портфелем активов (*Portfolio Management*, PM); оценки действительных возможностей (*Real Option Valuation*, ROV); поддержки жизненного цикла искусственных систем (*System Life Cycle Analysis*, SLCA); расчёта системы сбалансированных показателей (*Balanced Scorecard*, BSC); расчёта совокупной стоимости владения (*Total Cost of Ownership*, TCO); функционально-стоимостного анализа (*Activity Based Costing*, ABC). В частности, для расчёта расходной части на техническую архитектуру обеспечения информационной безопасности рекомендуется использовать метод совокупной стоимости владения (TCO), а для обоснования инвестиций в корпоративную систему защиты информации – методы ожидаемых потерь, оценки свойств системы безопасности, а также анализа дерева ошибок. При этом следует учитывать, что только метод ожидаемых потерь позволяет получить количественную оценку стоимости и выгод от контрмер безопасности;

1. Общие положения разработки политики безопасности

- при разработке детальных технических политик безопасности отечественных компаний целесообразно воспользоваться стандартами BSI IT *Protection Manual* (www.bsi.de), NIST США серии 800 (www.nist.gov) CIS (www.cisecurity.org) NSA (www.nsa.gov) Это позволит определить облик технической архитектуры корпоративных систем защиты конфиденциальной информации российских компаний, в частности:
  - определить цели создания технической архитектуры корпоративной системы защиты информации;
  - разработать эффективную систему обеспечения информационной безопасности на основе управления информационными рисками;
  - рассчитать совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям;
  - выбрать и использовать требуемый инструментарий обеспечения информационной безопасности и оценки её текущего состояния;
  - реализовать требуемые методики мониторинга и управления информационной безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности. Эти метрики и меры позволят объективно оценить защищённость информационных активов и управлять информационной безопасностью отечественных компаний;

1. Общие положения разработки политики безопасности

- политики безопасности должны представлять собой законченные нормативные документы, содержащие единые нормы и требования по обеспечению информационной безопасности, обязательные для утверждения и применения соответствующими органами управления, руководством служб безопасности, руководством служб информационно-технологического обеспечения отечественных компаний.

2. Анализ отечественного рынка средств защиты информации

Современный рынок средств защиты информации можно условно разделить на две группы:

- средства защиты для госструктур, позволяющие выполнить требования нормативно-правовых документов и нормативно-технических документов;
- средства защиты для коммерческих компаний и структур, позволяющие выполнить требования и рекомендации федеральных законов, указов Президента РФ, постановлений Правительства РФ, а также документа СТР-К Гостехкомиссии России, ГОСТ Р ИСО/МЭК 15408 и некоторых международных стандартов, главным образом ISO 17799:2005.

Например, к защите конфиденциальной информации в органах исполнительной власти могут предъявляться следующие требования:

1. Выбор конкретного способа подключения к сети Интернет, в совокупности обеспечивающего межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для сокрытия структуры внутренней сети, а также проведение анализа защищённости интернет-узла, использование средств антивирусной защиты и централизованное управление, должен производиться на основании рекомендаций документа Гостехкомиссии РФ СТР-К.

2. Анализ отечественного рынка средств защиты информации

2. АС организации должны обеспечивать защиту информации от несанкционированного доступа (НСД) по классу «1Г» в соответствии с Руководящим документом Гостехкомиссии РФ «РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации».
3. Средства вычислительной техники и программные средства АС должны удовлетворять требованиям четвёртого класса РД Гостехкомиссии России «РД. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации».
4. Программно-аппаратные средства межсетевого экранирования, применяемые для изоляции корпоративной сети от сетей общего пользования, должны удовлетворять требованиям «РД. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищённости от НСД к информации» по третьему классу защиты.
5. Информационные системы должны удовлетворять требованиям ГОСТ ИСО/МЭК 15408 по защищённости информационных систем в рамках заданных профилей защиты.
6. Программно-аппаратные средства криптографической защиты конфиденциальной информации, в том числе используемые для создания виртуальных защищённых сетей (Virtual Privat Network, VPN), должны быть легитимны.

2. Анализ отечественного рынка средств защиты информации

8. Для использования персональных цифровых сертификатов и поддержки инфраструктуры открытых ключей, средств ЭЦП и шифрования должен быть создан легитимный удостоверяющий центр (система удостоверяющих центров).
9. Политика информационной безопасности должна предусматривать обязательное включение в технические задания на создание коммуникационных и информационных систем требований информационной безопасности.
10. Должен быть регламентирован порядок ввода в эксплуатацию новых информационных систем, их аттестации по требованиям информационной безопасности.

Для выполнения перечисленных требований и надлежащей защиты конфиденциальной информации в госструктурах принято использовать сертифицированные средства, например средства защиты от несанкционированного доступа, межсетевые экраны и средства построения VPN, средства защиты информации от утечки за счёт ПЭМИН и пр. В частности, для защиты информации от несанкционированного доступа рекомендуется использовать аппаратно-программные средства семейства Secret Net («Информзащита»), семейства Dallas Lock («Конфидент»), семейства «Аккорд» (ОКБ САПР), электронные замки «Соболь» («Информзащита»), USB-токены (Aladdin) и пр.

2. Анализ отечественного рынка средств защиты информации

Для защиты информации, передаваемой по открытым каналам связи, рекомендованы аппаратно-программные межсетевые экраны с функциями организации VPN, например Firewall-1 (Check Point), «Застава» («Элвис+»), VipNet («Инфотекс»), «Континент» («Информзащита»), ФПСУ-IP (АМИКОН) и др.

Средства защиты информации для коммерческих структур более многообразны и включают в себя средства:

- управления обновлениями программных компонент,
- межсетевого экранирования,
- построения VPN,
- контроля доступа,
- обнаружения вторжений и аномалий,
- резервного копирования и архивирования,
- централизованного управления безопасностью,
- предотвращения вторжений на уровне серверов,
- аудита и мониторинга средств безопасности,
- контроля деятельности сотрудников в сети Интернет,
- анализа содержимого почтовых сообщений,
- анализа защищённости информационных систем,

2. Анализ отечественного рынка средств защиты информации

- защиты от спама,
- защиты от атак класса «отказ в обслуживании»,
- контроля целостности,
- инфраструктуры открытых ключей,
- усиленной аутентификации и пр.

3. Процесс разработки политики безопасности

3.1. Выбор уровня доверия

Прежде всего поговорим немного о проблеме доверия.

От правильного выбора уровня доверия к сотрудникам зависит успех или неудача реализации политики безопасности компании. При этом слишком большой уровень доверия может привести к возникновению проблем в области безопасности, а слишком малый – заметно затруднить работу сотрудника, вызвать у него недоверие и даже привести к увольнению. Насколько можно доверять сотрудникам компании?

Обычно используют следующие модели доверия:

- доверять всем и всегда – самая простая модель доверия, но, к сожалению, неприемлемая;
- не доверять никому и никогда – самая ограниченная модель доверия и также непрактичная;
- доверять избранным на время – модель доверия подразумевает определение разного уровня доверия на определённое время. При этом доступ к информационным ресурсам компании предоставляется по необходимости для выполнения служебных обязанностей, а средства контроля доступа используются для проверки уровня доверия к сотрудникам компании.

3. Процесс разработки политики безопасности

3.1. Выбор уровня доверия

Вряд ли существует компания, в которой следуют модели доверия «доверять всем и всегда». В сегодняшнем мире это нереально. То же самое относится и ко второй модели – «не доверять никому и никогда». Поэтому самая реалистичная модель доверия – «доверять некоторым из сотрудников компании на время».

3. Процесс разработки политики безопасности

3.2. Трудности внедрения политик безопасности

Опыт создания политик безопасности авторами показывает, что внедрение политики безопасности часто приводит к возникновению напряжённости во взаимоотношениях между сотрудниками компании. Это в основном связано с тем, что сотрудники часто стараются не следовать каким-либо правилам безопасности, так как не хотят себя ограничивать в своих действиях. Другая причина в том, что каждый сотрудник имеет своё представление (не обязательно солидарное с принятой в компании политикой безопасности) о необходимости и способах организации режима информационной безопасности в компании. Например, сотрудники отдела сбыта заинтересованы в оперативном исполнении своих обязанностей без каких-либо задержек, связанных с применением средств защиты информации. Персонал службы поддержки часто заинтересован только в простоте эксплуатации администрируемых ими информационных систем.

Топ-менеджмент компании заинтересован прежде всего в оптимизации затрат и уменьшении общей стоимости владения (TCO) корпоративной системы защиты информации. Получить одобрение всех положений политики безопасности у перечисленных групп сотрудников компании – трудная и практически неосуществимая задача. Поэтому лучше всего попробовать достигнуть некоторого компромисса.

3. Процесс разработки политики безопасности

3.3. Субъекты, заинтересованные в политиках безопасности

Политики безопасности затрагивают практически каждого сотрудника компании. Сотрудники службы поддержки будут осуществлять и поддерживать правила безопасности компании. Менеджеры заинтересованы в обеспечении безопасности информации для достижения своих целей. Юристы компании и аудиторы заинтересованы в поддержании репутации компании и предоставлении определённых гарантий безопасности клиентам и партнёрам компании. Рядовых сотрудников компании политики безопасности затрагивают больше всего, поскольку правила безопасности накладывают ряд ограничений на поведение сотрудников и затрудняют выполнение работы.

3. Процесс разработки политики безопасности

3.4. Состав группы по разработке политик безопасности

В общем случае рекомендуется следующий состав рабочей группы по разработке политик безопасности:

- член совета директоров;
- представитель руководства компании (финансовый директор, директор по развитию);
- директор по информационным технологиям;
- директор по информационной безопасности;
- аналитик службы безопасности;
- аналитик ИТ-службы;
- представитель юридического отдела;
- представитель от пользователей;
- технический писатель.

Численность группы по разработке политик безопасности будет зависеть от широты и глубины проработки политик безопасности. Например, разработка политик безопасности для офисной сети в 40…50 узлов может занять один человекомесяц.

3. Процесс разработки политики безопасности

3.4. Состав группы по разработке политик безопасности

Если это возможно, то о том, что разрабатывается новая политика информационной безопасности компании, необходимо уведомить сотрудников заранее. До начала внедрения новой политики безопасности желательно предоставить сотрудникам текст политики на одну-две недели для ознакомления и внесения поправок и комментариев. Также надо учитывать, что без прав нет обязанностей, то есть сотрудники, на которых распространяются правила безопасности, должны обладать всеми необходимыми полномочиями для того, чтобы выполнять эти правила.

3. Процесс разработки политики безопасности

3.5. Основные требования к политике безопасности

В идеале политика безопасности должна быть реалистичной и выполнимой, краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, чёткое описание области действия, а также указывать на ответственных и их обязанности.

Например, по мнению специалистов Cisco, желательно, чтобы описание политики безопасности занимало не более двух (максимум пяти) страниц текста. При этом важно учитывать, как политика безопасности будет влиять на уже существующие информационные системы компании. Как только политика утверждена, она должна быть представлена сотрудникам компании для ознакомления.

Наконец, политику безопасности необходимо пересматривать ежегодно, чтобы отражать текущие изменения в развитии бизнеса компании.

3. Процесс разработки политики безопасности

3.6. Уровень средств безопасности

Хорошо написанные политики безопасности компании должны позволять балансировать между достигаемым уровнем безопасности и получаемым уровнем производительности корпоративных информационных систем компании. Одна из основных целей политики безопасности состоит в том, чтобы обосновать и внедрить средства защиты информации, адекватные целям и задачам бизнеса.

Выбор необходимых средств защиты информации для определённой политики безопасности не всегда понятен и легко определяем. Здесь решающую роль играют необходимость организации режима информационной безопасности, а также бизнес-культура компании.

При этом если правила политики безопасности слишком ограничительны или слишком жёстки, для того чтобы их внедрять и соответствовать им в дальнейшем, то либо они будут игнорироваться, либо сотрудники компании найдут способ обойти средства безопасности.

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

В настоящее время ряд ведущих компаний в области безопасности выделяют следующие политики:

- допустимого шифрования,
- допустимого использования,
- аудита безопасности,
- оценки рисков,
- классификации данных,
- управления паролями,
- использования ноутбуков,
- построения демилитаризованной зоны (DMZ),
- построения экстранет,
- безопасности рабочих станций и серверов,
- антивирусной защиты,
- безопасности маршрутизаторов и коммутаторов,
- безопасности беспроводного доступа,
- организации удалённого доступа,
- построения виртуальных частных сетей (VPN) и пр.,
- безопасности периметра.

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Политика допустимого использования информационных ресурсов компании определяет права и ответственность сотрудников компании за надлежащую защиту конфиденциальной информации компании. В частности, политика допустимого использования определяет, могут ли сотрудники компании читать и копировать файлы, владельцами которых они не являются, но к которым имеют доступ. Также эта политика устанавливает правила допустимого использования корпоративной электронной почты, служб новостей и процедур доступа к сети компании.

Примерный текст из описания политики допустимого использования:

«*Сотрудники несут личную ответственность за безопасность любой информации, используемой и/или сохранённой с применением их учётных записей в компании. Используйте руководство пользователя для получения рекомендаций по защите вашей учётной записи и информации с использованием стандартных методов безопасности на уровне операционной системы или при помощи программного обеспечения для шифрования типа PGP. Конфиденциальная информация компании или сторонних организаций не должна храниться (или быть переданной) на компьютерах, не принадлежащих компании*».

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

«*Сотрудники не должны пытаться получить доступ к любым данным или программам, находящимся на рабочих станциях и серверах компании, если они не имеют соответствующего разрешения или явного согласия владельца этих информационных ресурсов*».

Политика организации удалённого доступа определяет допустимые способы удалённого соединения с корпоративной информационной системой.

Представляет собой основной документ безопасности в крупных транснациональных компаниях с географически разветвлённой сетью.

Должна описывать все доступные способы удалённого доступа к внутренним информационным ресурсам компании: доступ по коммутируемым сетям (SLIP, PPP), доступ с использованием ISDN/Frame Relay, Telnet/SSH-доступ через Интернет, выделенную линию/VPN/DSL и пр.

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Примерный текст из описания политики организации удалённого доступа:

«*1. Сотрудники, менеджеры по продажам и выездные специалисты компании, обладающие удалённым доступом к корпоративной сети компании, несут такую же ответственность, как и в случае локального подключения к сети компании.*

2. Для членов семьи сотрудника компании доступ к Интернету через сеть компании разрешается только в случае оплаты трафика самим сотрудником. При этом сотрудник компании несёт личную ответственность за то, чтобы член его семьи не нарушил правила политик безопасности компании, не выполнил противозаконные действия и не использовал удалённый доступ для собственных деловых интересов. Сотрудник компании также несёт ответственность за последствия неправильного использования удалённого доступа.

3. При осуществлении удалённого доступа к корпоративной сети, пожалуйста, ознакомьтесь со следующими политиками безопасности:

а) политика допустимого шифрования,

б) политика организации виртуальных частных сетей,

в) политика безопасности беспроводного доступа,

г) политика допустимого использования.

4. Для получения дополнительной информации относительно удалённого доступа, включения и отключения услуги, поиска неисправностей и т. д., обращайтесь на Web-сайт службы организации удалённого доступа к

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Политика удалённого доступа определяет, кто из сотрудников может иметь высокоскоростной удалённый доступ ISDN, Frame Relay. При этом определяются ограничения по организации удалённого доступа.

Пример требований политики удалённого доступа:
«*Защищённый удалённый доступ должен строго контролироваться. Требуемый уровень безопасности обеспечивается с помощью использования однократных (one-time) паролей или инфраструктуры открытых ключей устойчивыми к взлому ключевыми фразами (passphrase). (Для получения информации по созданию устойчивых ко взлому ключевых фраз, см. описание политики управления паролями.)*

Сотрудник никому не должен передавать или посылать по электронной почте свой пароль на вход в систему, включая даже членов семьи.

Сотрудники, имеющие привилегию удалённого доступа, должны гарантировать, что их компьютеры, которые удалённо подключены к сети, не подключены в то же самое время ни в какую другую сеть, за исключением домашних сетей, которые находятся под полным управлением сотрудника.

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Сотрудники, имеющие привилегию удалённого доступа к корпоративной сети, не должны использовать адреса электронной почты компании для ведения собственного бизнеса.

Маршрутизаторы для выделенных ISDN-линий, сконфигурированные для доступа к корпоративной сети, должны использовать для аутентификации, как минимум, CHAP«.

CHAP (англ. Challenge Handshake Authentication Protocol) – протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём. Аутентификация узла выполняется путём трёхэтапной процедуры согласования. Протокол CHAP широко используется различными поставщиками серверов и клиентов сетевого доступа

Политика безопасности периметра описывает порядок и правила получения привилегированного доступа к системам безопасности периметра корпоративной сети компании. Кроме того, описывает процедуру инициации и обработки запросов на изменение конфигурации систем безопасности периметра сети, а также порядок и периодичность проверки этих конфигураций.

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Примерный текст из политики безопасности периметра:
«*Доступ к информации о конфигурации систем безопасности периметра сети компании должен быть ограничен. Информация о конфигурации систем безопасности периметра никогда не должна храниться или передаваться по корпоративной сети и никогда не должна печататься и храниться в виде бумажной копии. Необходимо отслеживать все изменения конфигурации систем сетевой безопасности и периодически проводить аудит безопасности периметра сети*».

Политика управления паролями определяет правила и порядок создания и изменения паролей сотрудников компании.

Примерный текст из описания политики управления паролями:
«*Все пароли системного уровня (например, root, enable, administrator в системе Windows, пароли администраторов приложений и т.д.) должны изменяться, по крайней мере, раз в квартал. Все пароли системного уровня должны быть частью глобальной базы данных управления паролями отдела защиты информации. Все пароли пользовательского уровня (например, доступа к электронной почте, к сети, к настольному компьютеру и т.д.) должны изменяться, по крайней мере, раз в шесть месяцев. Рекомендованный интервал изменения – раз в четыре месяца.*

3. Процесс разработки политики безопасности

3.7. Примеры политик безопасности

Учётные записи сотрудников, которым предоставляется доступ к административным учётным записям на системах с помощью членства в группах или программ sudo, должны иметь пароль, отличный от всех других паролей данного сотрудника».

Это только несколько примеров политик, которые могут быть использованы вашей компанией.

С ними и другими политиками безопасности можно ознакомиться на Web-сайте американского института аудиторов и администраторов безопасности SANS (http://www.sans.org/newlook/resources/policies/policies.htm)

3. Процесс разработки политики безопасности

3.8. Процедуры безопасности

Процедуры безопасности так же важны, как и политики безопасности. Если политики безопасности определяют что должно быть защищено, то процедуры безопасности определяют как защитить информационные ресурсы компании. Приведём здесь примеры нескольких важных процедур безопасности.

Процедура управления конфигурацией обычно определяется на уровне отдела или на уровне компании. Но даже если есть процедура по управлению изменениями на уровне компании, индивидуальные группы могут иметь собственные процедуры. Процедура управления изменениями должна определять процесс документирования и запроса на изменения конфигурации всех масштабов (от простой инсталляции маршрутизатора до изменения списков контроля доступа на межсетевом экране).

Идеально, если служба защиты информации проводит анализ изменений и контролирует запросы на изменения. Процесс управления изменениями важен по нескольким ключевым причинам:

- документированные изменения обеспечивают возможность проведения аудита безопасности;
- в случае возможного простоя из-за изменения проблема будет быстро определена;
- обеспечивается способ координирования изменений таким образом, чтобы одно изменение не влияло на другое изменение.

3. Процесс разработки политики безопасности

3.8. Процедуры безопасности

Процедуры резервного копирования информации и хранения резервных копий вне офиса могут потребоваться из-за требований клиентов и партнёров по бизнесу. Число сотрудников компании, имеющих доступ к резервным копиям за пределами компании, должно быть сведено к минимуму. Вы должны тестировать возможность восстановления информации из резервных носителей на регулярной основе для проверки целостности резервных копий. Часть процедуры резервного копирования может быть выполнена в виде программы или сценария, который автоматизирует процесс создания резервных копий.

Процедура обработки инцидентов определяет порядок обработки и расследования инцидентов. Эта процедура должна осуществляться в любой компании. Невозможно определить порядок реагирования на все инциденты, но вы должны описать порядок реагирования на основные их типы.

Вот некоторые из них: сканирование портов, атаки типа «отказ в обслуживании», взлом компьютеров, взлом пароля учётной записи и несоответствующее использование информационных систем. Необходимо назначить одного сотрудника, отвечающего за взаимодействие с правоохранительными органами.

4. Реализация политик безопасности

4.1. Задание общих правил безопасности

Пусть объектом защиты является информационная система компании ЗАО «XXI век» (далее – «компания»). Название объекта защиты вымышленное, возможные совпадения случайны и носят непреднамеренный характер.

Состав и структура политик безопасности. Общая политика безопасности компании разработана и утверждена руководством организации. В этой политике определены принципы, порядок и правила предоставления доступа к информационным ресурсам компании, а также степень ответственности в случае нарушения правил безопасности.

Также существует ряд других политик безопасности, в частности политика допустимого использования, определяющая доступ к сервисам. При приёме на работу каждый новый сотрудник должен подписать соглашение о том, что с политиками безопасности компании ознакомлен и обязуется их выполнять. Партнёры, поставщики и клиенты банка при получении доступа к конфиденциальной информации компании подписывают Соглашение о неразглашении конфиденциальной информации. Политики безопасности компании регулярно пересматриваются (не реже одного раза в год).

4. Реализация политик безопасности

4.1. Задание общих правил безопасности

Характеристика инфраструктуры компании. Взаимодействие с партнёрами, клиентами и поставщиками осуществляется с использованием сервисов Интернета. Для этих целей разработан ряд Web-приложений. Архитектура приложений использует три уровня для реализации разделения ресурсов:

- *уровень представления* – выполняется на Microsoft IIS 5.0 на Microsoft Windows 2000 Server Service Pack 4 со всеми необходимыми обновлениями. Вся бизнес-логика выполняется на серверах второго уровня архитектуры;
- *промежуточный уровень* – содержит все бизнес-компоненты и также выполняется на Microsoft Windows 2000 Server Service Pack 4. К этому уровню нет доступа из Интернета. Страницы Active Server Pages на серверах уровня представления активируют компоненты COM+ и позволяют выполнить бизнес-логику. Компоненты запускаются под непривилегированной учётной записью с необходимым минимумом привилегий;
- *уровень баз данных* – состоит из базы данных и защищённого хранилища данных. Microsoft SQL Server 2000 Service Pack 3 используется как сервер управления базой данных и выполняется на двухузловом кластере Microsoft Windows 2000 Advanced Server Service Pack 4 Cluster для обеспечения отказоустойчивости. Только серверы промежуточного уровня имеют доступ к этим серверам. Серверы расположены в изолированном сегменте сети, разделённом межсетевыми экранами.

4. Реализация политик безопасности

4.1. Задание общих правил безопасности

Правила использования сервисов Интернета. Согласно принятой в компании политики безопасности для сотрудников определены следующие правила использования сервисов Интернета:

- разрешается исходящий Web-трафик – HTTP, SSL и FTP для различных групп сотрудников. Доступ в Интернет контролируется и регистрируется, доступ к некоторым категориям Web-ресурсов блокируется в соответствии с политикой использования ресурсов Интернета;
- запрещается применять средства обмена мгновенными сообщениями (например, ICQ) и одноранговые файлообменные системы (например, Napster). Также запрещено получать и отправлять электронную почту с использованием внешних почтовых серверов, не принадлежащих компании (например, www.mail.ru).
- разрешается использование внешних DNS-имён, разрешение на использование дополнительных сервисов зависит от политики использования ресурсов Интернета.

Правила доступа в сеть компании. Для сотрудников, работающих вне офиса компании, определяются следующие правила доступа в сеть компании:

- доступ к внутреннему почтовому серверу Outlook Web Access осуществляется через HTTPS. Обмен файлами реализуется с использованием Microsoft SharePoint Portal Server 2003 через HTTP/HTTPS. Это позволяет не настраивать межсетевой экран для трафика SMB/CISF, что упрощает конфигурацию межсетевого экрана;

4. Реализация политик безопасности

4.1. Задание общих правил безопасности

Правила обеспечения физической безопасности. Для должного обеспечения физической безопасности все оборудование компании расположено в защищённых помещениях с резервными источниками питания, оборудованных системами пожаротушения и кондиционерами.

Доступ в помещения осуществляется с использованием биометрической системы контроля доступа сотрудников. Действует правило обязательного сопровождения гостей компании во время деловых визитов.

Над каждым рядом стоек находится видеокамера с датчиком движения, ведётся запись всех действий сотрудников и приглашённых лиц компании.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Основной задачей при создании защищённой инфраструктуры компании (см. рис. 4.1) является реализация надёжного контроля доступа на уровне приложений и сети в целом.

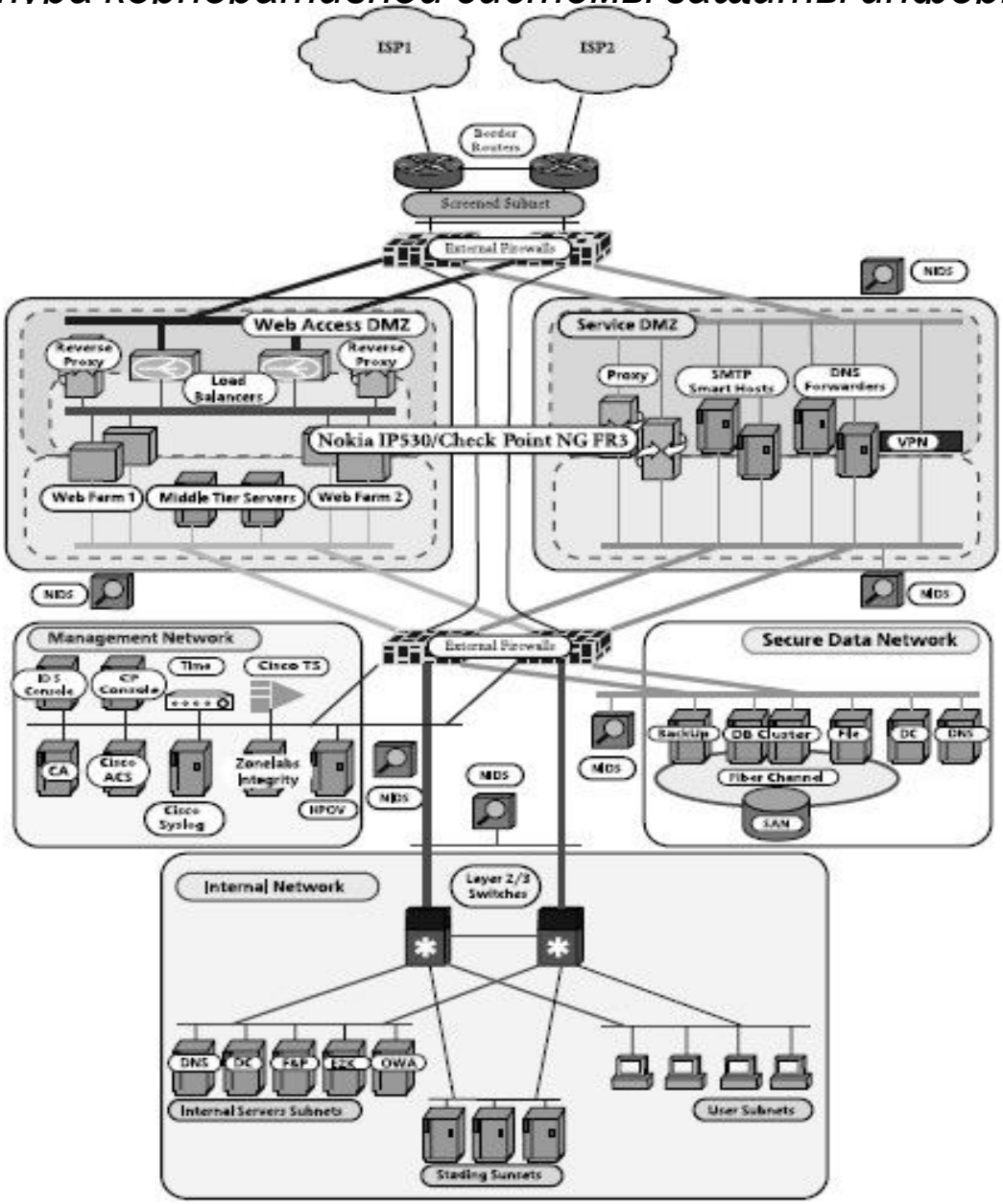
При этом логический контроль доступа на уровне сети осуществляется путём сегментации сетей и разграничения трафика с помощью межсетевых экранов.

Созданы две раздельные подсети – одна для доступа извне к Web-приложениям и вторая для доступа сотрудников в Интернет. Этим обеспечивается полное разделение входящего из Интернета и исходящего в Интернет трафика.

Многоуровневый подход с несколькими межсетевыми экранами обеспечивает фильтрацию всего нежелательного трафика.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

В компании было создано несколько зон безопасности:

- *зона подключения к Интернету* – эта зона представляет собой подсеть между пограничным маршрутизатором и внешними межсетевыми экранами. Пограничные маршрутизаторы используют списки контроля доступа (*ACL*), сконфигурированные для фильтрации входящего и исходящего трафика и защиты внешних МЭ;
- *зона доступа к Web-приложениям компании* (*Web Access DMZ*) – в этой подсети находятся Web-приложения компании и разрешены только входящие через межсетевой экран запросы из Интернета. Доступ из внутренней сети запрещён;
- *зона выхода в Интернет* (*Service DMZ*) – эта зона представляет собой подсеть, с помощью которой сотрудникам компании предоставляется доступ в Интернет.

Разрешён только исходящий через межсетевой экран трафик, за исключением доступа к электронной почте с помощью VPN;

- зона управления ресурсами сети компании (Management Network) – в этой зоне находятся приложения для мониторинга, аутентификации и журналирования событий в сети компании;
- зона защищаемых данных компании (*Secure Data Network*) – эта зона содержит все важные для компании Web-приложения, базы данных и базу данных пользователей (Active Directory);

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

При этом компания использует следующие диапазоны IP-адресов: 70.70.70.0/24 и 90.90.1.0/30 (в действительности сети 70.x.x.x и 90.90.1.0/30 зарезервированы IANA, но мы будем считать, что они реально существуют).

Сеть 70.70.70.0/24 разбита на подсети с использованием различных масок подсетей, задействована только первая часть – 70.70.70.0/25, все остальные адреса зарезервированы для последующего расширения сети.

Для внутренней сети используется подсеть 172.16.0.0/16. Общее распределение адресного пространства подсетей компании представлено в табл. 4.1

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Таблица 4.1. Распределение адресного пространства

Сеть	Подсеть
Соединение с ISP1	70.70.1.0/30
Соединение с ISP2	90.90.1.0/30
Подсеть между пограничными маршрутизаторами и внешними МЭ	70.70.70.16/28
Сеть между пограничными маршрутизаторами	70.70.1.0/30
Сеть управления устройствами в демилитаризованной зоне	172.16.1.0/28
Сеть между внешними МЭ	172.16.1.16/29
Внешние адреса Web-приложений	70.70.70.64/27
Внутренние адреса Web-приложений (NAT)	172.16.2.0/24
Внутренние адреса Web-приложений	172.16.3.0/24
Внешние адреса зоны Service DMZ	70.70.70.96/27
Внутренние адреса зоны Service DMZ	172.16.4.0/24
Сеть данных	172.16.5.0/24
Сеть управления	172.16.6.0/24
Внутренняя магистраль	172.16.9.0/28
Внутренние серверы	172.16.16.0/21
Внутренние серверы тестирования	172.16.24.0/21
Внутренние пользовательские компьютеры	172.16.32.0/20

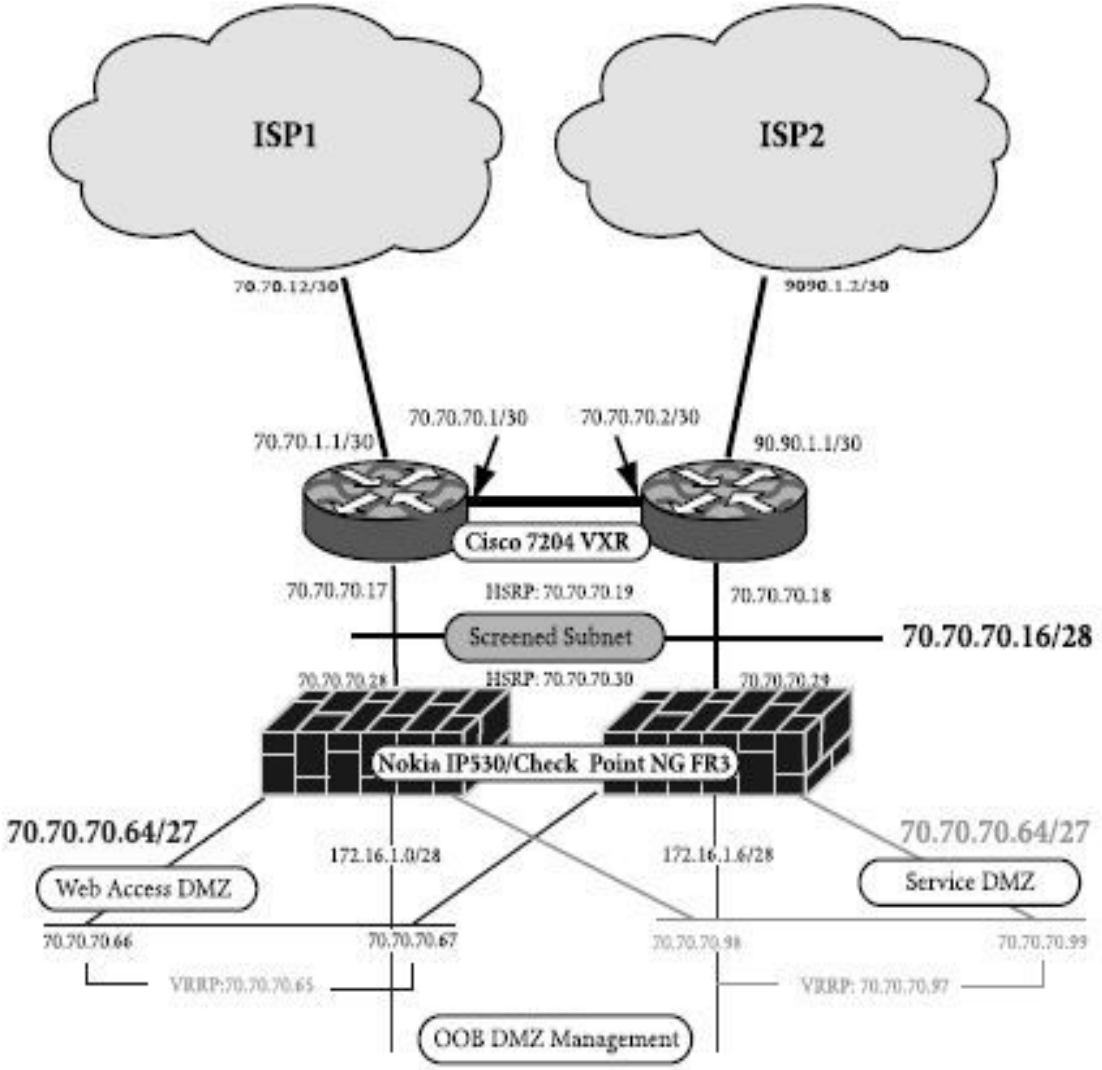
4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Теперь рассмотрим каждую из перечисленных зон безопасности компании подробно и определим правила безопасности.

Зона подключения к Интернету

Одно из главных бизнес-требований компании – обеспечение доступности Интернета 24 часа в сутки 7 дней в неделю. Для этого были выбраны два провайдера (ISP) (см. рис. 4.2).



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

С целью надлежащего распределения маршрутизации и избыточности был сконфигурирован динамический протокол маршрутизации BGP v.4 (*Border Gateway Protocol* – протокол граничного шлюза) между пограничными маршрутизаторами и маршрутизаторами провайдеров Интернета.

В качестве пограничных маршрутизаторов используется *Cisco* 7204 *VXR Router* с *Cisco IOS Release* 12.3. Преимуществом этой модели является поддержка *Cisco Express Forwarding* (*CEF*), что существенно увеличивает производительность маршрутизаторов.

Пограничные маршрутизаторы – это первая линия обороны. Так как они являются первой точкой входа в сеть, то на них настроены списки контроля доступа (ACL) для фильтрации нежелательного трафика, что уменьшает нагрузку на остальную сетевую инфраструктуру. Реализована фильтрация как входящего, так и исходящего трафика. Для защиты от атак *SYN Flood* используется возможность *Cisco IOS TCP Intercept*. Другая задача, которую решают пограничные маршрутизаторы, – защита внешних межсетевых экранов от трафика, направленного на IP-адреса межсетевых экранов.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Адресное пространство 70.70.70.16/28 используется для подсети между пограничными маршрутизаторами и внешними межсетевыми экранами. Подсети 70.70.70.4/30 и 70.70.70.8/29 зарезервированы для будущего решения с балансировкой нагрузки между межсетевыми экранами. «Горячее» резервирование на внутренних интерфейсах маршрутизаторов обеспечивает протокол *HSRP* (*Hot Standby Routing Protocol*). Для соединения устройств в DMZ используются коммутаторы *Cisco Catalyst* 3550. Коммутаторы не имеют IP-адресов и управляются посредством консольного доступа через *Cisco* 2620 *Terminal Server*.

Внешние межсетевые экраны. В качестве внешних межсетевых экранов используются *Nokia IPSO* v.3.6 *FCS4*, *Check Point FW*-1 *NG FP3*. К основным факторам, повлиявшим на выбор данных устройств, относятся:

- высокая надёжность, защищённость и производительность аппаратных платформ *Nokia*;
- развитая функциональность и технологическая зрелость межсетевого экрана *Check Point* FW-1 *NG FP3*;
- наличие в компании подготовленных специалистов.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Как было сказано выше, в компании существуют две DMZ-зоны, одна для доступа к Web-приложениям и другая для выхода в Интернет, каждая из зон защищена межсетевыми экранами. Это было сделано для разделения ресурсов, чтобы проникновение злоумышленников в одну из зон не сказалось на работе другой зоны.

Каждый межсетевой экран имеет 5 интерфейсов, подключённых к разным зонам. Межсетевые экраны также имеют выделенный интерфейс для управления *Out-of-band* посредством сервера *Check Point Management Console* из зоны управления. Это повышает защищённость управляющего трафика и делает недоступным изменение наблюдаемого трафика, так как он не проходит через общую сеть.

Система межсетевых экранов реализована в варианте с полной избыточностью и масштабируемостью. Это достигается путём использования *Nokia IPSO VRRP* и возможностью синхронизации соединений Firewall-1. Через межсетевые экраны разрешён ограниченный набор трафика согласно принятой в компании политики безопасности. На этом же уровне реализована и защита от атак *SYN Flood*.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Зона доступа к Web-приложениям компании

Эта зона защищена на уровне представления, промежуточном уровне, а также на уровне баз данных компании. Серверы названной зоны защищены в соответствии с рекомендациями руководств SANS (www.sans.org):

- *Level*-1 *Benchmark* for *Windows* 2000,
- *Level*-2 *Windows* 2000 *Professional Operating System Benchmark*,
- *Level*-2 *Windows* 2000 *Server Operating System Benchmark*,

а также в соответствии с официальными руководствами компании *Microsoft* (www.microsoft.com):

- *Security Operations Guide for Windows* 2000,
- *Hardening Guide for Windows* 2000.

Для централизованного управления обновлениями используется продукт *Microsoft SMS* 2003. На Web-серверах выполняется *Microsoft IIS* 5.0. Серверы имеют по два сетевых интерфейса. Через один интерфейс поступают запросы из Интернета, через другой осуществляются запросы к базе данных. Таким образом, реализуется изоляция Web-приложений от базы данных.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Зона выхода в Интернет

Эта зона безопасности обеспечивает доступ в Интернет из внутренней сети. Здесь также используется концепция разделения сети. Каждое устройство имеет два интерфейса – один для подключения к публичной зоне и другой для доступа к внутренней зоне с отключённой маршрутизацией пакетов между ними. Все оборудование дублируется для обеспечения высокой степени доступности. *DNS Forwarder* установлен на *Windows* 2000 *Service Pack* 4, *Microsoft DNS Service* на аппаратной платформе *Compaq Proliant DL360*. *SMTP Smart Host* установлен на *OpenBSD* 3.2 *with Sendmail* v.8.12.6 на аппаратной платформе *Compaq Proliant DL360*.

Для реализации политики использования Интернета развернут продукт *Websense*. Он предназначен для ограничения доступа к определённым *Web*-ресурсам, запрещённым политикой использования Интернета, например к *Web*-почте, чатам, сайтам с непристойным содержанием, блокирует службы мгновенного обмена сообщениями и одноранговые файлообменные сети. *Websense* также обеспечивает определение и удаление *ActiveX* и *Java applets*, позволяет создавать отчёты об использовании ресурсов Интернета конкретными сотрудниками. Для обнаружения вирусов в трафике *HTTP*, *SMTP* и *FTP* используется продукт *Trend Micro InterScan Virus* Wall.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

SMTP-серверы. SMTP-серверы работают на *OpenBSD* 3.2 с *Sendmail* v.8.12.6. Это один из немногих случаев, когда используется продукт, не произведённый *Microsoft*. Выбор обусловлен тем, что *Microsoft Exchange* 2000 *Server* обладает избыточными для компании функциональными возможностями, которые не нужно делать доступными из Интернета. Также, по сравнению с *Sendmail*, *Microsoft Exchange* характеризуется достаточно слабым уровнем защиты. По этим причинам и был сделан выбор в пользу *Sendmail* на платформе *OpenBSD*, которая является одной из самых защищённых операционных систем. *OpenBSD* и *Sendmail* бесплатны, что ведёт к уменьшению расходов на построение системы. *OpenBSD* и *Sendmail* были защищены в соответствии с рекомендациями производителей. Установлен минимально необходимый набор пакетов, включены только необходимые сервисы и установлены все существующие обновления и сервисные пакеты. На *SMTP*-сервере также установлено программное обеспечение для защиты от спама. Все входящие сообщения перенаправляются на внутренний сервер *Microsoft Exchange*, функционирующий в режиме кластера. Принимаются и направляются вне сети только сообщения, которые были получены от этого внутреннего сервера. Во всех исходящих сообщениях изменяется заголовок для удаления информации о внутренней маршрутизации и изменяется *SMTP*-приглашение, чтобы затруднить злоумышленникам получение информации о версии программного обеспечения внешнего *SMTP*-сервера. Для предупреждения возможности просмотра списка почтовых ящиков и сервисов отключены команды *VRFY* и *EXPN*.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

DNS. В качестве концепции построения *DNS* было выбрано решение по разделению на внутренний и внешний *DNS*. Внешний *DNS*-сервер обслуживается интернет-провайдерами и находится в их зоне ответственности. Эта опция обеспечивает дополнительную безопасность, связанную с проблемами администрирования, и уменьшает необходимость разрешения входящего DNS-трафика, так как исторически DNS-серверы являются одним из наиболее слабо защищённых сервисов и постоянной мишенью для атак злоумышленников. Этот дизайн также обеспечивает избыточность и улучшает доступность сервисов, потому что вероятность, того что *DNS*-серверы обоих провайдеров одновременно подвергнутся атаке и не смогут обслуживать запросы, достаточно мала.

DNS-сервер, расположенный в *DMZ*, работает с использованием службы *Microsoft DNS* и установлен на операционную платформу *Microsoft Windows* 2000 *Service Pack* 4. Серверы сконфигурированы как «только кэширующие», без установленных DNS-зон и перенаправляют все запросы на DNS-серверы провайдера. С провайдерами подписаны специальные соглашения по защите этого сервиса. Процесс разрешения имён, таким образом, становится более защищённым, так как используются строго определённые внешние серверы.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

VPN. Для обеспечения доступа к корпоративной сети работающим удалённо сотрудникам и персоналу, ответственному за управление сетевыми устройствами, используется концентратор *Cisco VPN* 3030. Доступ по коммутируемым соединениям запрещён. Так как сервис VPN не является критичным для обеспечения бизнес-процессов, то применяется только одно устройство. При изменении этих требований может быть установлено дополнительное устройство для обеспечения избыточности.

Доступ с использованием VPN построен на следующих принципах:

- каждый сотрудник, использующий этот сервис, подписывает политику использования VPN;
- разрешён к применению только протокол IPSec с шифрованием 3DES. PPTP и L2TP не поддерживаются;
- для аутентификации на этапе 1 (IKE) используются сертификаты;
- сертификаты выпускаются и распределяются внутренним Центром управления сертификатами;
- сертификаты хранятся на аппаратном токене *Aladdin Software eToken*. Выдаются каждому сотруднику компании, использующему этот сервис, отделом информационной безопасности. *eToken* является небольшим, простым в применении USB-устройством, где доступ к сертификату защищён паролём. После создания ключи сертификатов не могут быть экспортированы из устройства;

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

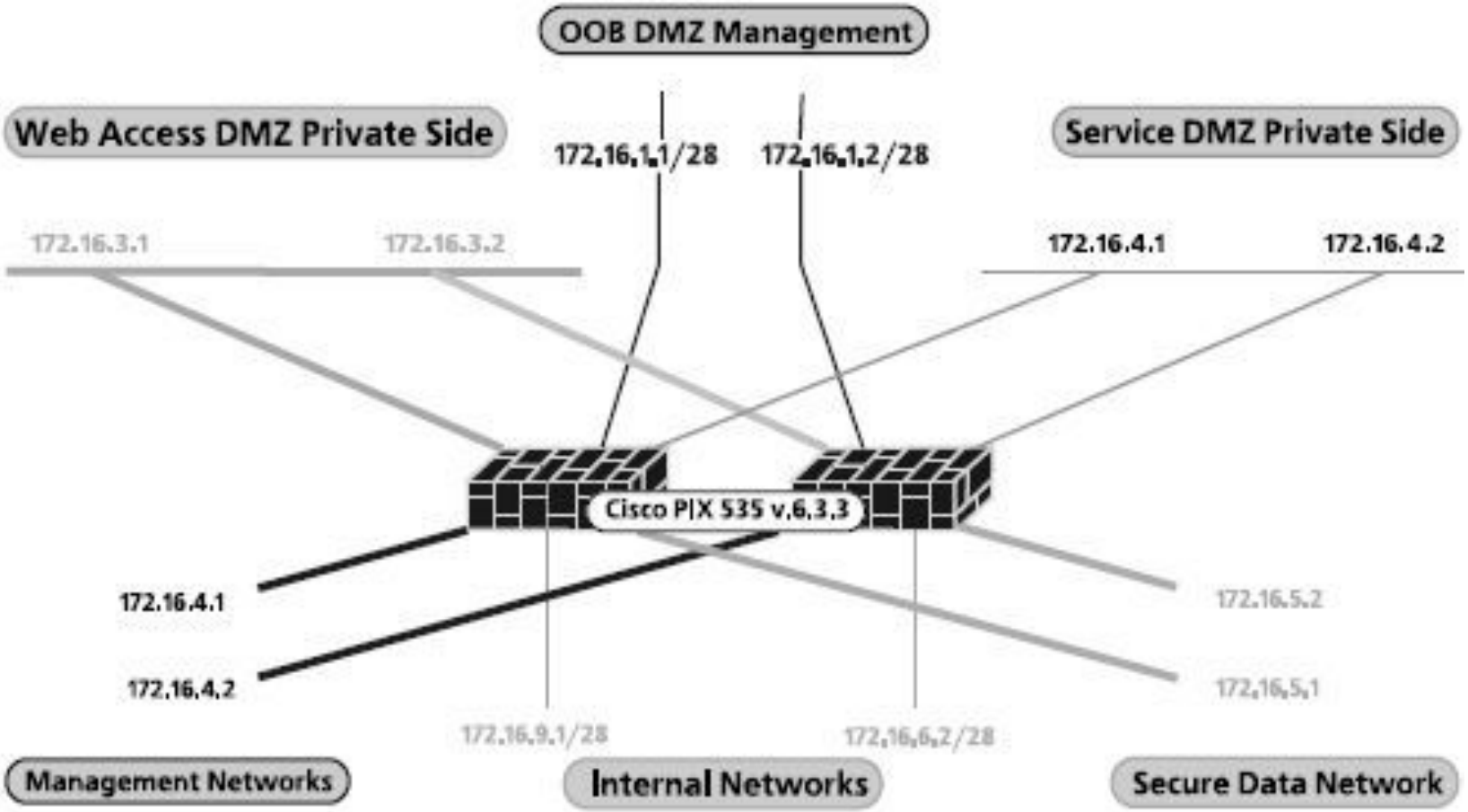
Аутентификация и управление идентификаторами осуществляются с использованием *Cisco ACS RADIUS*;

- *Cisco ACS RADIUS* также обеспечивает выдачу IP-адресов и применение списков контроля доступа для подключающихся сотрудников компании;
- *Zone Labs Integrity Server* применяет политику на персональном межсетевом экране и антивирусном программном обеспечении на каждом подключаемом через VPN компьютере. Эта политика определяется отделом информационной безопасности и принудительно применяется при подключении;
- журналирование VPN-сессий осуществляется на сервере *Cisco* Secu*r*ity *Information Management Solution* v.3.1.1 (*NetForensics*) с использованием *syslog*.

Внутренние межсетевые экраны. Наличие внутренних межсетевых экранов обеспечивает больший контроль и безопасность информационных потоков между внутренними сетями. Кроме того, достигается изоляция сегмента управления от остальной сети, управление доступом через VPN, защита внутренней сети путём запрещения трафика из менее защищённых зон сети и пр. Каждый межсетевой экран имеет шесть интерфейсов, подключённых к разным зонам (см. рис. 4.3), также существует выделенный интерфейс для поддержания режима «горячего» резервирования (на рис. не показано).

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Аутентификация и управление идентификаторами осуществляются с использованием *Cisco ACS* Система построена на двух межсетевых экранах *Cisco PIX 535*, функционирующих в режиме «горячего» резервирования.

Выбор продукта был обусловлен его высокой производительностью, надёжностью и приемлемой для компании стоимостью решения.

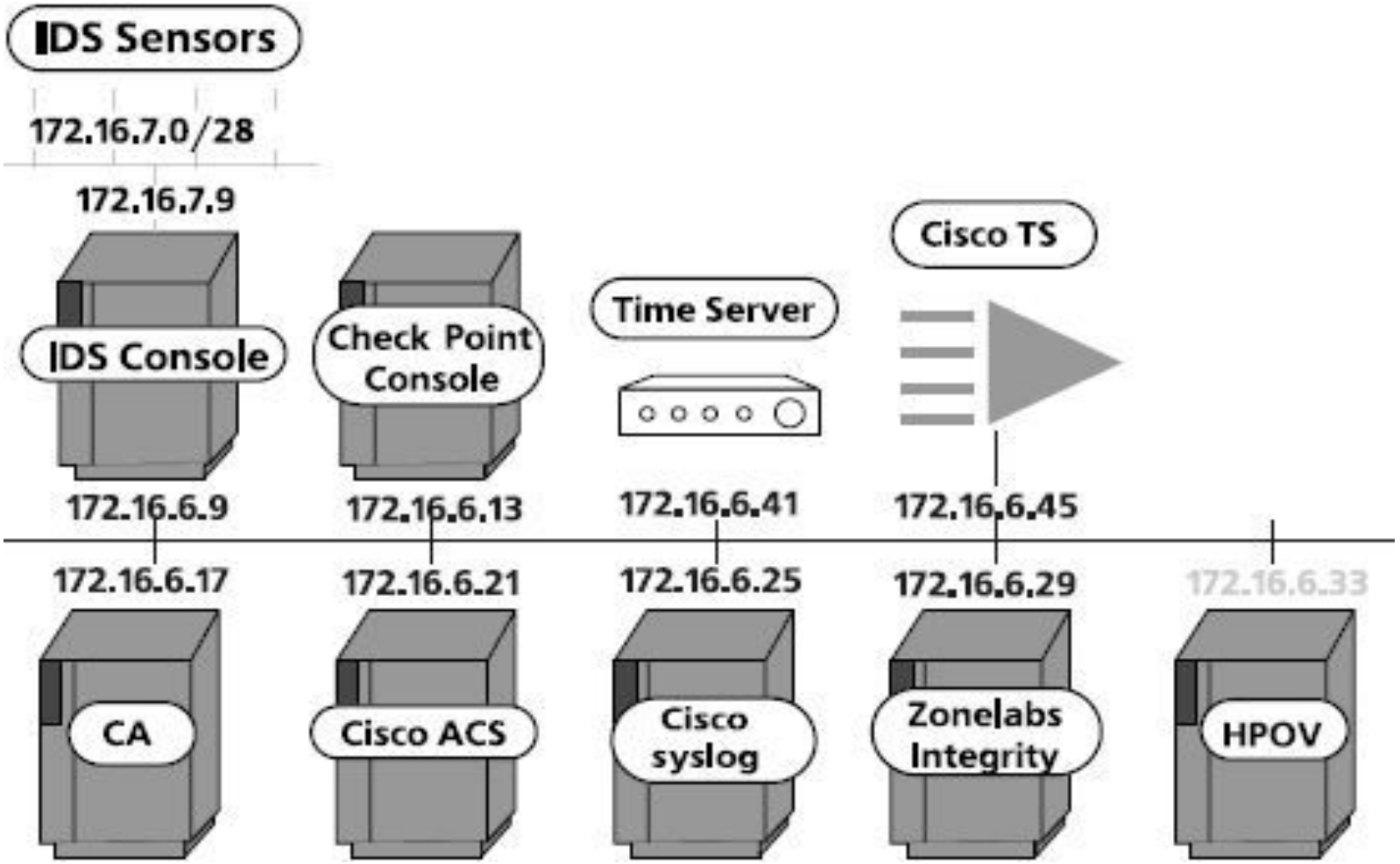
Кроме того, использование межсетевых экранов разных производителей увеличивает общую защищённость сети компании, так как, при возникновении уязвимости в *Check Point FW*-1, эта уязвимость вряд ли может быть использована против *Cisco PIX*, и наоборот.

Зона управления ресурсами сети компании

Все серверы управления сетью и серверы мониторинга расположены на выделенной сети, защищённой внутренними межсетевыми экранами (см. рис. 4.4).

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

В компании организован центр управления сетью для мониторинга и управления сетевыми устройствами. Центр находится в защищённом от проникновения посторонних лиц помещении. График работы персонала 16 часов в сутки 5 дней в неделю. Поддержка в ночное время реализуется через VPN-соединения. Сотрудник должен сначала зайти на один из компьютеров данной сети и только потом, с этого компьютера, он может получить доступ к сетевому оборудованию.

Это является дополнительным уровнем защиты. Кроме того, доступ к любому сетевому оборудованию ограничен списком IP-адресов сети управления. Пограничные маршрутизаторы и все коммутаторы управляются через консоль с использованием маршрутизатора доступа *Cisco* 2620, остальные управляющие интерфейсы на устройствах отключены.

Другие устройства – SMTP-серверы, VPN-концентратор – управляются с помощью SSH. Серверы с операционной системой *Windows* 2000 работают под управлением *Microsoft Terminal Services*, который поднят на внутренних интерфейсах серверов и сконфигурирован для использования максимального уровня шифрования. Помимо этого фильтры *IPSec* настроены таким образом, чтобы разрешать доступ к серверам с использованием *Terminal Services* (TCP 3389), если соединение инициируется из сети управления.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Консоль управления IDS. В качестве сетевой системы обнаружения вторжений используется *Cisco IDS* 4250, а на серверах установлены системы предупреждения вторжений *Cisco Security Agent* v.4.0 (продукция компании *Okena*, продаваемая под торговой маркой *Cisco*).

В системе *Cisco IDS* 4250 один интерфейс работает в режиме сниффера и не имеет IP-адреса, а другой используется для получения сообщений о найденных сигнатурах и для управления.

Передача сообщений осуществляется по протоколу SSL. В качестве устройства управления выбран *Cisco Works VPN/Security Management Solution* v.2.2. Данное программное обеспечение позволяет управлять конфигурациями следующих устройств:

- *Cisco PIX Firewall*,
- *Cisco VPN Router*,
- *Cisco IDS* 4200,
- *Cisco Security Agent*.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

В состав продукта входят следующие функциональные модули:

- *Cisco Works Common Services*,
- *Management Center for Firewalls*,
- *Management Center for IDS Sensors*,
- *Management Center for Cisco Security Agents*,
- *Management Center for VPN Routers*,
- *Monitoring Center for Security*,
- *Monitoring Center for Performance*,
- *Cisco View*,
- *Auto Update Server*,
- *Resource Manager Essentials*.

Monitoring Center for Security позволяет принимать и коррелировать сообщения со всех вышеперечисленных устройств, а кроме того, он оснащён средствами мониторинга производительности и инвентаризации сети. Доступ к этому устройству из сети, отличной от сети управления, запрещён.

Сервер Check Point Management Console. Сервер *Check Point Management Console* используется для управления модулями Check Point Firewall-1 и журналирования событий. Доступ к нему ограничен IP-адресами интерфейсов администрирования *Nokia Check Point FW*-1.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Сервер времени. Синхронизация сетевого времени – очень важный аспект правильного функционирования сети и надлежащего журналирования. Если на нескольких устройствах установлено разное время, то при анализе журналов очень трудно будет разбираться, когда реально и в какой последовательности произошли события, к тому же каждый из сертификатов имеет определённый срок жизни и, при неправильно установленном времени, его будет невозможно эксплуатировать. Нередко слабости в защите протокола NTP или неправильные настройки сетевых устройств дают злоумышленникам возможность проведения атак с целью установки неверного времени и, таким образом, выведения из строя всех устройств и соединений, использующих сертификаты. Кроме того, *Microsoft Active Directory* для аутентификации применяет протокол *Kerberos*, который очень сильно зависит от точных настроек времени. Из-за важности обеспечения точного времени был приобретён аппаратный сервер времени *Datum TymServe* TS2100 с GPS-антенной для синхронизации с сервером времени *NIST* (Национальный институт стандартов США). Это устройство служит мастер-сервером для всех устройств в сети. К нему разрешён только NTP-трафик и используется NTP-аутентификация везде, где это возможно. На случай отказа сервера компания заключила соглашение с владельцами одного из NTP-серверов в Интернете о получении точного времени. В случае возникновения такой ситуации будут внесены соответствующие изменения в списки доступа на межсетевых экранах.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Cisco Terminal Server. Для управления всеми сетевыми устройствами (маршрутизаторами, коммутаторами) с помощью консольного соединения используется Cisco Router 2620. На всех устройствах отключены все протоколы сетевого управления. Соединения к самому Cisco Router 2620 ограничены списком IP-адресов из сети управления и определённым списком инженеров, подключающихся через VPN-соединение. Разрешён доступ только по SSH, и все сотрудники должны быть аутентифицированы с использованием TACACS+. Уровень доступа регулируется членством в группах и настройками на сервере TACACS+.

Cisco Security Information Management Solution. Cisco Security Information Management Solution v.3.1 (продукт компании Netforensics) на аппаратной платформе Cisco 1160 используется для сбора, коррелирования, анализа и хранения журналов. Данное программное обеспечение позволяет производить мониторинг безопасности в режиме реального времени и поддерживает широкий перечень устройств и программных продуктов (28 источников), от которых оно может принимать и обрабатывать сообщения. В компании используется часть из них:

- Check Point Firewall-1,
- Cisco IOS ACL, FW, IDS,
- Cisco Secure ACS,
- Cisco Secure IDS,
- Cisco Secure PIX

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

- Cisco Secure PIX IDS,
- Cisco Security Agent,
- Концентратор Cisco VPN,
- Cisco Firewall Switch Module,
- Tripwire NIDS,
- Web-серверы Microsoft IIS,
- Windows Events,
- UNIX OS Events.

Центр управления сертификатами. В сети широко применяются сертификаты: для доступа посредством VPN, к Web-сайтам по SSL, для шифрования электронной почты. Сервер центра управления сертификатами является частью внутренней инфраструктуры открытых ключей и используется для выпуска или отзыва внутренних сертификатов и публикации списка отозванных сертификатов (Certificate Revocation List). Центр управления сертификатами развернут на неподключенном к сети Windows 2000 Server Service Pack 4. В качестве процедуры установки инфраструктуры открытых ключей основной (root) центр управления сертификатами был использован только однажды, с целью выпуска сертификата для выпускающего центра управления сертификатами, и после этого был немедленно переведён в офлайн-режим.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Секретный (private) ключ основного центра сертификации перемещён на флэш-карту, удалён с жёсткого диска, и эта флэш-карта была помещена в сейф отдела информационной безопасности. Копия флэш-карты хранится за пределами офиса в защищённом помещении в сейфе.

Cisco Secure ACS Server. С помощью Cisco Secure ACS Server v.3.3 for Windows осуществляется аутентификация:

- сотрудники, использующие VPN, аутентифицируются и получают IP-адрес из ACS-сервера на основе протокола RADIUS;
- доступ к сетевым устройствам для администрирования контролируется с использованием протокола TACACS+.

TACACS+ является протоколом последнего поколения из серии протоколов TACACS. Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась её собственная версия TACACS, известная как TACACS+. TACACS+ пользуется транспортным протоколом TCP. «Демон» (процесс, запускаемый на машине UNIX или NT) сервера «слушает» порт 49, который является портом протокола IP, выделенным для протокола TACACS. Этот порт зарезервирован для выделенных номеров RFC в протоколах UDP и TCP. Все текущие версии TACACS и расширенные варианты этого протокола используют порт 49.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Протокол TACACS+ работает по технологии «клиент-сервер», где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается «демон». Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и журналирования (AAA – Authentication, Authorization, Accounting).

Это позволяет обмениваться идентификационными сообщениями любой длины и содержания и, следовательно, использовать для клиентов TACACS+ любой механизм аутентификации, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos.

Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего ключа – «секрета», который никогда не передаётся по каналам связи. Обычно этот секрет вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передаётся между клиентом TACACS+ и «демоном» сервера TACACS+.

Процесс обмена информацией между ACS и сервером TACACS+ во время процесса аутентификации протекает по следующей схеме:

- ACS посылает START-запрос на сервер TACACS+ для начала процесса аутентификации;

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

- сервер отсылает ACS-пакет с запросом GETUSER, содержащий запрос пользователю на ввод имени;
- ACS отображает запрос пользователю и отсылает серверу TACACS+ введённое пользователем имя в пакете CONTINUE;
- сервер отсылает ACS-пакет с запросом GETPASS, содержащий запрос пользователю на ввод пароля;
- ACS высылает пакет CONTINUE, содержащий пароль, введенный пользователем серверу TACACS+;
- сервер TACACS+ выполняет проверку полученной пары «имя-пароль» и в зависимости от результата проверки отсылает ACS-пакет, содержащий результат (FAIL – в случае несовпадения, PASS – успешная аутентификация). На этом процесс аутентификации завершается.

Процесс обмена информацией между ACS и сервером TACACS+ во время процесса авторизации протекает по следующей схеме:

- ACS от отсылает пакет START AUTHORIZATION серверу TACACS+;
- сервер TACACS+ обрабатывает полученные данные и принимает решение, основываясь на политике безопасности, связанной с данным пользователем. Результат отсылается ACS-серверу в RESPONSE-пакете.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Здесь под авторизацией понимается процесс определения действий, которые позволены данному пользователю. Обычно идентификация предшествует авторизации, однако это не обязательно. В запросе на авторизацию можно указать, что идентификация пользователя не проведена (личность пользователя не доказана). В этом случае лицо, отвечающее за авторизацию, должно самостоятельно решить, предоставлять такому пользователю запрашиваемые услуги или нет. Протокол TACACS+ предусматривает только положительную или отрицательную авторизацию и допускает настройку на потребности конкретного заказчика.

Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс или когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях «демон» сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

Следом за идентификацией и авторизацией следует журналирование, которое представляет собой запись действий пользователя. В системе TACACS+ журналирование может выполнять две задачи. Во-первых, оно может применяться для учёта использованных услуг (например, для выставления счетов). Во-вторых, его можно применять в целях безопасности. Для этого TACACS+ поддерживает три типа учётных записей. Записи «старт» указывают, что

Записи «стоп» говорят о том, что предоставление услуги только что прекратилось.
Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется.

Учётные записи TACACS+ содержат всю информацию, которая используется в ходе авторизации, а также другие данные, такие, как время начала и окончания (если это необходимо), и данные об использовании ресурсов.

Механизм взаимодействия ACS и сервера TACACS+ выглядит следующим образом:

- ACS отсылает учётную запись серверу TACACS+, основываясь на выбранных методах и событиях;
- сервер TACACS+ отсылает ответный пакет ACS-серверу, подтверждая приём учётной записи.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Zone Labs Integrity Server. Zone Labs Integrity Server v. 1.6 используется для принудительного применения политики безопасности организации VPN на компьютерах сотрудников, которые подключаются посредством VPN. В данном случае потребуется установка на каждом компьютере Integrity Agent для приёма и применения политики во время установления VPN-соединения. Integrity Agent позволяет также производить мониторинг антивирусного программного обеспечения на клиенте и отключает VPN-соединение, если программное обеспечение не установлено или не имеет последних обновлений. Это очень важно, так как удалённый компьютер может быть не защищён надлежащим образом и стать точкой входа во внутреннюю сеть для вирусов и злоумышленников. Единственным устройством, которому разрешено устанавливать соединение с этим сервером, является VPN-концентратор.

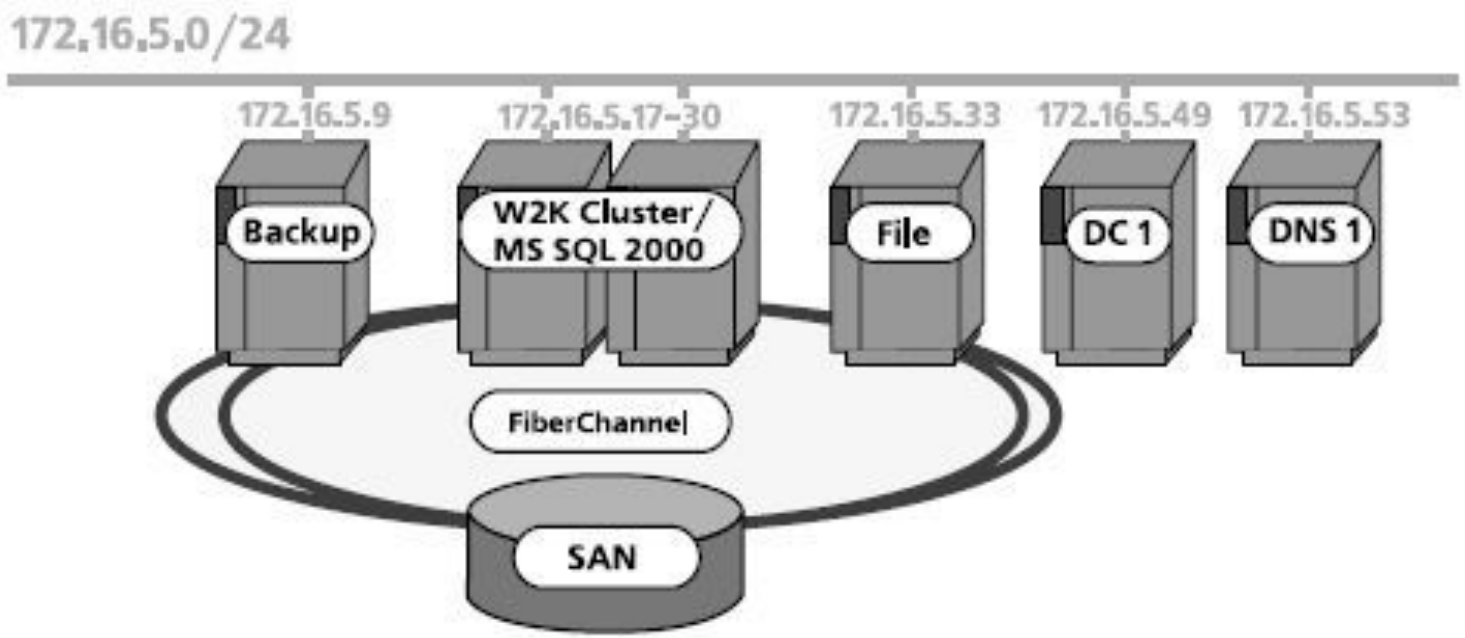
HP OpenView. Для мониторинга всех сетевых устройств и серверов используется HP OpenView Network Node Manager v.6.31. Компания осознает необходимость мониторинга в режиме 24 часа в сутки 7 дней в неделю для обеспечения высокой доступности сервисов. Из-за большой степени риска разрешено использовать SNMP только в режиме read-only. Правила на межсетевых экранах разрешают данный трафик только на станцию управления NNM. Этот сервер использует Windows 2000 Server Service Pack 4 и защищен в соответствии с перечисленными выше руководствами. Все устройства сконфигурированы для отправления SNMP traps на сервер NNM, и любой другой доступ из-за пределов сети управления запрещён.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Зона защищаемых данных компании

В этой сети (см. рис, 4.5) находятся все данные Web-приложений. Также здесь располагаются серверы Active Directory, контроллеры доменов Web-приложения и DNS-серверы. Каждый из них является кластером, который состоит из двух компьютеров. На рис. 4.5 это не отображено для того, чтобы сделать его более читабельным.



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Система управления базами данных и файл-серверы. В качестве сервера баз данных используется Microsoft Windows 2000 Advanced Server Service Pack 4 и Microsoft SQL Server 2000 Service Pack 3. Файл-серверы построены на Microsoft Windows 2000 Server Service Pack 4 и Microsoft File and Print Services. Для обеспечения избыточности и высокой доступности на файл-серверах развёрнута интегрированная с Active Directory служба Distributed File System. Только серверы промежуточного уровня имеют доступ к Microsoft SQL Server. При этом стандартный порт TCP 1433 изменён на нестандартный порт TCP 2000. Доступ из внутренней сети к базе данных ограничен только выполнением запросов к базе данных и только с определённого списка IP-адресов.

Active Directory. «Лес» Active Directory Web-приложений полностью отделен от внутреннего «леса». Серверы из Web-зоны подключаются к контроллеру домена с использованием IPSec в режиме Authentication Header (AH). Этот дизайн имеет следующие преимущества:

- разрешается использование IPSec-фильтрования на самих серверах;
- упрощается конфигурирование межсетевого экрана, так как требуется только два правила;
- нагрузка на процессор минимальная, так как используется не шифрование, а только аутентификация.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Active Directory DNS-серверы сконфигурированы для использования DNS-серверов Web-зоны как перенаправляющих для разрешения внешних адресов. Резервное копирование реализовано с помощью Fiber Channel, поэтому не требуется дополнительный сетевой сегмент. Серверы, которые осуществляют резервное копирование, не имеют сетевых подключений за пределами сегмента.

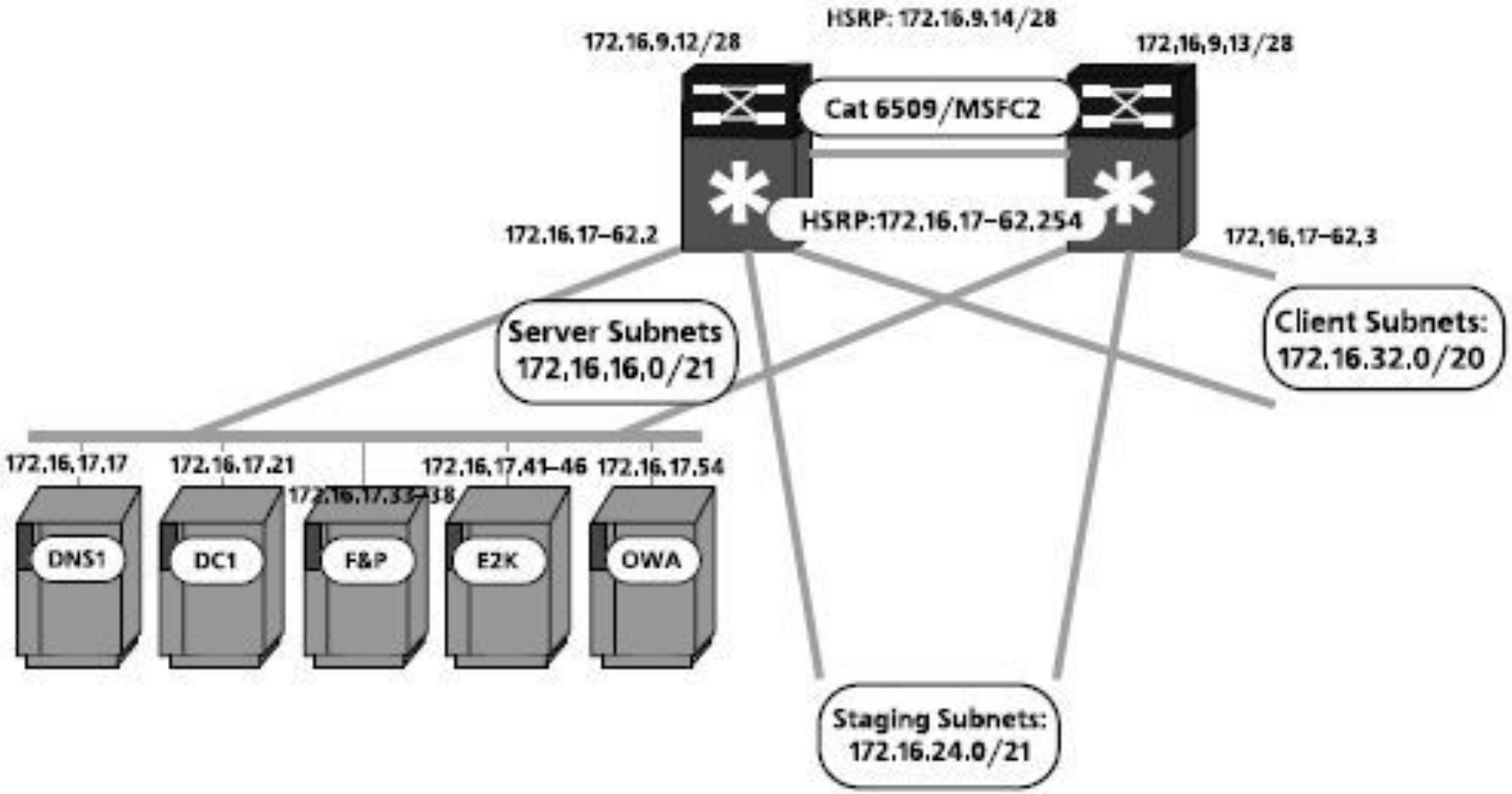
Зона внутренней сети компании

Во внутренней сети находятся рабочие станции сотрудников и внутренние серверы. Сеть логически разделена на две части: подсеть серверов и подсеть сотрудников. Ядром проекта являются два коммутатора Cisco Catalyst 6509 с модулями маршрутизации MSFC2. Коммутаторы используют trunk для избыточности. Для каждой внутренней подсети создан отдельный VLAN и сконфигурирован HSRP на каждом из VLAN-интерфейсов для «горячего» резервирования. Раздельные маршрутизирующие интерфейсы для каждого VLAN позволяют задействовать дополнительные списки контроля доступа для ограничения доступа из определённых подсетей или компьютеров. На рис. 4.6 изображён только один сервер каждого типа для читабельности.

Внутренняя сеть Windows 2000 использует изолированный "лес" Active Directory со своими собственными DNS-серверами и контроллерами домена. На всех серверах установлен Windows 2000 Server Service Pack 4, при этом они защищены в соответствии с перечисленными выше руководствами.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации



4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

В качестве внутреннего сервера обмена сообщениями и совместной работы используется Microsoft Exchange 2000 Service Pack 3. Он работает на двухузловом кластере Windows 2000 Advanced Server Service Pack 4 для обеспечения избыточности и балансировки нагрузки. Все исходящие сообщения перенаправляются к SMTP-серверам в интернет-зону. В качестве антивирусного программного обеспечения применяется Sybari Antigen v.7.0 for Exchange с проверкой входящих и исходящих сообщений.

Работа с почтой удалённых пользователей обеспечивается сервером Exchange 2000 Service Pack 3 Outlook Web Access, который доступен через VPN-соединение поверх HTTPS. Выбор объясняется тем, что для подключения достаточно только одного порта (HTTPS). При обычном же способе доступа к Exchange пришлось бы открывать целый набор портов, что существенно увеличивает риск взлома системы.

Файл-серверы реализованы с использованием Microsoft SharePoint Portal Server 2003. Доступ к файлам осуществляется через VPN поверх HTTP/HTTPS. Это делает ненужной настройку межсетевого экрана для трафика SMB/CISF, что упрощает конфигурацию межсетевого экрана и делает дизайн более защищённым.

4. Реализация политик безопасности

4.2. Архитектура корпоративной системы защиты информации

Исходящий доступ разрешён только для HTTP/HTTPS из сети сотрудников через ргоху-сервер. В целях обеспечения безопасности не разрешён доступ из подсети серверов в Интернет. При необходимости установки драйверов или обновлений они загружаются обслуживающим персоналом на свои рабочие места и далее переносятся на серверы на CD-дисках или дискетах.

Доступ к серверам баз данных предоставлен ограниченному списку администраторов баз данных из определённого списка IP-адресов. Таким же образом предоставляется доступ к серверам данных и для менеджеров, ответственных за наполнение Web-страниц приложения.

В сети тестирования тестируются приложения перед их перемещением в действующую сеть. Данная сеть полностью имитирует рабочие серверы и также используется для тестирования сервисных пакетов и обновлений перед их установкой на серверы и рабочие станции.

Это позволяет уменьшить вероятность несовместимости приложений и увеличить надёжность функционирования сети и приложений. Реализована процедура управления изменениями.

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Настройки пограничных маршрутизаторов

Пограничные маршрутизаторы являются первой линией защиты. Для создания технических настроек использовались руководства Агентства национальной безопасности США: NSA/SNAC Router Security Configuration Guide, NSA/SNAC Router Security Configuration Guide Executive Summary.

Пароли. Пароли на маршрутизаторах должны храниться в зашифрованном виде. Нельзя использовать enable-пароль, так как для его шифрования используется слабый алгоритм и злоумышленник легко вскроет его.

Необходимо применить следующие команды:

service password-encryption
enable secret Gh!U765H!!
no enable password

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Отключение неиспользуемых возможностей управления. Для управления используется консольный доступ, поэтому все остальные способы доступа должны быть отключены:

```
line vty 0 15
no login
transport input none
transport output none
line aux 0
no login
transport input none
transport output none
```

Отключение возможности маршрутизатора загружать конфигурацию из сети:

```
no boot network
no service config
```

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Настройка TACACS+. Необходимо защитить доступ для управления. Хотя этот доступ не разрешён по сети, нужно использовать TACACS+ для централизованного управления аутентификацией и авторизацией доступа с целью управления и журналирования изменений, произведённых на маршрутизаторах. TACACS+ был выбран вместо RADIUS по причине большей защищённости. Имя пользователя и пароль в TACACS+ шифруются, в то время как в RADIUS шифруется только пароль. При использовании Cisco ACS TACACS+ можно настроить детальные уровни доступа для различных пользователей и групп пользователей.

Определяем IP-адрес сервера TACACS+ и пароль для аутентификации:

tacacs-server 172.16.6.21
tacacs-server key F$!19Ty
tacacs-server attempts 3
ip tacacs source-interface Fa0/0

Далее настраивается аутентификация, авторизация и журналирование. TACACS+ будет использоваться в качестве главного средства аутентификации, а локальная база пользователей маршрутизатора будет использоваться в случае, если сервер TACACS+ станет недоступным. Для этого обязательно должны быть созданы локальные учётные записи на маршрутизаторе.

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Настройка использования TACACS+ для AAA:

aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs + local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+

Используемый метод аутентификации применяется для консольного доступа:

line console 0
login authentication default exec-timeout 5 0
logging synchronous

Предупреждающий баннер:

banner login "This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted".

"Ежедневное" сообщение, выводимое в первую очередь при попытке получения доступа к маршрутизатору:

banner motd "This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted".

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Сообщение, выводимое при входе в непривилегированный (EXEC) режим:

banner exec "Any unauthorized access will be vigorously prosecuted".

Маршрутизация «от источника». Отключение маршрутизации «от источника». Маршрутизация от источника даёт пакетам возможность переносить информацию о «верном» или более удобном маршруте и позволяет пренебречь правилами, которые предписаны в таблице маршрутизации для данного пакета, то есть модифицирует маршрут пакета. Это позволяет злоумышленнику управлять трафиком по своему желанию. Необходимо отключить маршрутизацию «от источника»:

no ip source-route

Сервисы маршрутизатора

Необходимо отключить все неиспользуемые и опасные сервисы на маршрутизаторе и сконфигурировать нужные сервисы для обеспечения безопасности. Некоторые из них уже отключены по умолчанию в версии IOS 12.3, поэтому здесь они приводятся для дополнительной проверки.

«Малые» сервисы. Отключение редко используемых UDP-и TCP-сервисов диагностики:

no service tcp-small-servers

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Чтобы уменьшить для злоумышленника возможности получения дополнительной информации о маршрутизации, надо отключить сервисы finger и identd. Также требуется отключить HTTP-, DNS-, DHCP-, bootp-сервисы:

no ip finger
no service finger
no ip identd
no ip http server
no ip bootp service
no ip domain-lookup
no service pad
no service dhcp
no call rsvp-sync

Определяется максимальное количество получателей для SMTP-соединений для встроенной в IOS функции поддержки факсов. Установка максимального количества, равного 0, означает отключение сервиса:

mta receive maximum-recipients 0

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Отключение протокола CDP (Cisco Discovery Protocol), который позволяет обмениваться информацией канального уровня с другими устройствами от компании Cisco:

no cdp running

Отключение функций proxy arp на маршрутизаторе. Proxy arp позволяет распространяться ARP-запросам по смежным сетям, что даёт злоумышленнику дополнительную возможность узнать о структуре сети:

no ip proxy-arp

Для того чтобы в сообщениях, отправляемых по syslog, присутствовала временная метка, необходимо выполнить команды:

service timestamps debug datetime msec localtime showtimezone
service timestamps log datetime msec localtime showtimezone

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Конфигурирование SNMP. Так как мониторинг сетевых устройств осуществляется из сети управления и является критичным аспектом обеспечения высокой доступности, решено использовать SNMP, несмотря на проблемы безопасности, связанные с ним.

Для минимизации риска предприняты следующие шаги:

- запрещён SNMP-трафик в Интернет и из Интернета;
- ограничено количество используемых счётчиков.

Используемые команды:

snmp-server view NNM-Only internet included
snmp-server view NNM-Only ipRouteTable excluded
snmp-server view NNM-Only ipNetToMediaTable excluded
snmp-server view NNM-Only at excluded

Списки контроля доступа сконфигурированы для ограничения доступа только с HP OpenView NNM:

access-list 5 permit host 172.16.6.33

и SNMP используется только для чтения:

snmp-server community ThaaMasdf view NNM-Only RO 5

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Маршрутизатор также сконфигурирован для отправки trap только к SNMP-серверу:

snmp-server host 172.16.6.33 Thaa!!asdf
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server trap-authentication
snmp-server trap-source Fa0/0

Конфигурирование протокола NTP Сконфигурирован список контроля доступа для ограничения получения времени через NTP только с сервера времени:

access-list 10 permit 172.16.6.41
access-list 10 deny any
ntp authentication-key 1 md5 Hn!hj
ntp authenticate
ntp trusted-key 1
ntp access-group peer 10
ntp update-calendar
ntp server 172.16.6.41 key 1
ntp source Fa0/0

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Журналирование событий маршрутизатора. Для журналирования событий используется протокол syslog. Журналы собираются на Cisco SIMS:

logging buffered 16000
no logging console
logging source-interface Fa0/0
logging trap informational
logging facility local7
logging 172.16.6.25

Настройки безопасности на уровне интерфейса. Для предупреждения использования интерфейса как усилителя при проведении атаки типа "отказ в обслуживании", например smurf, надо отключить маршрутизацию пакетов на broadcast-адреса. По умолчанию маршрутизатор не пропускает широковещательных сообщений с IP-адресом приёмника 255.255.255.255.

Для того чтобы ограничить негативное влияние направленных широковещательных сообщений на определённые сети, необходимо использовать эту команду:

no ip directed-broadcast

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Чтобы уменьшить для злоумышленника возможности получения информации о сети, надо выполнить следующие команды:

no ip unreachable
no ip mask-reply
no ip redirect

Для уменьшения проблем, вызываемых пакетами с неправильными или подменёнными IP-адресами, а также с исходными IP-адресами, которые не могут быть проверены, используется функция Unicast RPF:

ip cef
interface hssi2/0
ip verify unicast reverse-path

Конфигурирование функции TCP Intercept. Функция TCP Intercept помогает предупредить атаки типа SYN Flood путём прерывания и проверки TCP-соединений. В режиме Intercept программное обеспечение прерывает пакеты синхронизации TCP SYN от клиентов к серверам, совпадающие с расширенным списком контроля доступа. Осуществляются проверки, и попытки достичь сервер с несуществующих (неотвечающих) компьютеров пресекаются. Включение функции TCP Intercept:

access-list 110 permit tcp any 70.70.70.0 0.0.0.255
ip tcp intercept list 110

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Конфигурирование BGP. BGP v. 4 используется для обмена информацией о маршрутизации и политиках с маршрутизаторами интернет-провайдера. Так как уже существуют атаки, направленные против протокола BGP, то необходимо обеспечить надлежащий уровень защиты.

Для защиты используем возможность BGP аутентифицироваться с помощью MD5:

router bgp 5500 (здесь 5500 – номер автономной системы)
neighbor 70.70.1.2 password F!$asB!
ip as-path access-list 30 permit
router bgp 5500
neighbor 70.70.1.2 filter-list 30

Этот фильтр гарантирует, что маршрутизатор сможет принимать трафик только из определённой автономной системы. Также используется список контроля доступа на входящий трафик, разрешающий трафик по TCP 179 только от маршрутизаторов интернет-провайдера.

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Маршрут «чёрная дыра». Для увеличения производительности маршрутизатора при запрещении пакетов с недостижимыми адресами назначения используется статический маршрут в null. Кроме этого данная конфигурация позволит предупредить простейшие атаки типа «отказ в обслуживании». Такая конфигурация стала возможной благодаря тому, что для получения маршрутов используется BGP. Маршрут должен иметь наивысший вес, то есть маршрутизатор никогда не будет запрещать любой легитимный трафик.

Также необходимо отключить ICMP Unreachable на null-интерфейсе:

ip route 0.0.0.0 0.0.0.0 null 0 255
interface Null0
no icmp unreachables

Конфигурирование списков контроля доступа. На пограничных маршрутизаторах очень хорошо фильтровать ненужный входящий трафик, уменьшая, таким образом, нагрузку на внешние межсетевые экраны и уменьшая размеры журналов на внутренних устройствах. Пограничные маршрутизаторы также защищают внешние межсетевые экраны.

4. Реализация политик безопасности

4.3. Настройки основных компонент системы защиты компании

Для ограничения трафика используются расширенные списки контроля доступа. Используется новая возможность компилирования списков контроля доступа Turbo ACL, которая существенно увеличивает производительность обработки списков контроля доступа. К сожалению, эта функция не работает с рефлексивными списками контроля доступа и с CBAC (Context-Based Access Control). Для включения этой функциональности требуется всего одна команда:

access-list compiled

Сконфигурированы два списка контроля доступа – для входящего и исходящего трафика.

Список контроля доступа для входящего трафика. Блокируется трафик с недействительными адресами, без исходного адреса, направленный на «опасные» порты – NetBIOS, SNMP, TFTP, syslog, направленный в сеть между внешними маршрутизаторами и внешними межсетевыми экранами, направленный на диапазон адресов, используемых для multicast:

no ip extended Ingress
ip access-list extended Ingress
deny ip host any 255.255.255.255
deny ip host 0.0.0.0 any

Сети 70.0.0.0/8 и 90.0.0.0/8 также зарезервированы IANA, но не включены сюда из-за нашего первоначального предположения: