Политики кибербезопасности предприятий связи

С. А. Петренко, В. А. Курбатов

Как правило, политика безопасности предприятия связи разрабатывается и утверждается руководством компании. В этой политике определяются принципы, порядок и правила обеспечения информационной безопасности, права и обязанности сотрудников компании, а также степень ответственности в случае нарушения правил безопасности. Также существует ряд других частных политик безопасности, в частности, политика допустимого использования, определяющая доступ к определенным сервисам. При приеме на работу каждый новый сотрудник должен подписать соглашение о том, что с политиками безопасности компании ознакомлен и обязуется их выполнять. Партнеры, поставщики и клиенты при получении доступа к конфиденциальной информации компании подписывают «Соглашение о неразглашении конфиденциальной информации». Политики безопасности компании регулярно пересматриваются не реже одного раза в год. Далее рассмотрены основные положения типовой политики и правил безопасности предприятия связи.

Характеристика инфраструктуры компании

Взаимодействие с партнерами, клиентами и поставщиками осуществляется с использованием сервисов Internet. Для этих целей разработан ряд веб-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. Этот уровень не имеет доступа из Internet. Страницы Active Server Pages на серверах уровня представления активируют COM+ компоненты и позволяют выполнить бизнес-логику. Компоненты запускаются под непривилегированной учетной записью с необходимым минимумом привилегий.

Уровень баз данных состоит из базы данных и защищенного хранилища данных. Microsoft SQL Server 2000 Service Pack 3 используется как сервер управления базой данных и выполняется на 2-х узловом кластере Microsoft Windows 2000 Advanced Server Service Pack 4 Cluster для обеспечения отказоустойчивости. Только сервера промежуточного уровня имеют доступ к этим серверам. Сервера расположены в изолированном сегменте сети, разделенном межсетевыми экранами.

Правила использования сервисов Internet

Согласно принятой в компании политики безопасности для сотрудников определены следующие правила использования сервисов Internet:

- Разрешается исходящий веб-трафик — HTTP, SSL и FTP для различных групп сотрудников. Доступ в Интернет контролируется и регистрируется, доступ к некоторым категориям веб-ресурсов блокируется в соответствии с Политикой использования ресурсов Интернет.
- Запрещается использовать 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 имен.

Разрешение на использование дополнительных сервисов осуществляется в соответствии с политикой использования ресурсов Internet.

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.
- Доступ администраторов организуется через VPN к сегменту управления, для удаленного администрирования серверов используется Microsoft Terminal Services.

Правила обеспечения физической безопасности

В организациях, где физической безопасности уделяется должное внимание, все оборудование находится в защищенных помещениях с резерв-

ными источниками питания, оборудованными 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, ведется запись всех действий сотрудников и приглашенных лиц компании.

Архитектура корпоративной системы защиты информации

Основной задачей при создании защищенной инфраструктуры компании является реализация надежного контроля доступа на уровне приложений и сети в целом. При этом логический контроль доступа на уровне сети осуществляется путем сегментации сетей и разграничении трафика с помощью межсетевых экранов. Созданы две раздельные подсети — одна для доступа извне к веб-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.

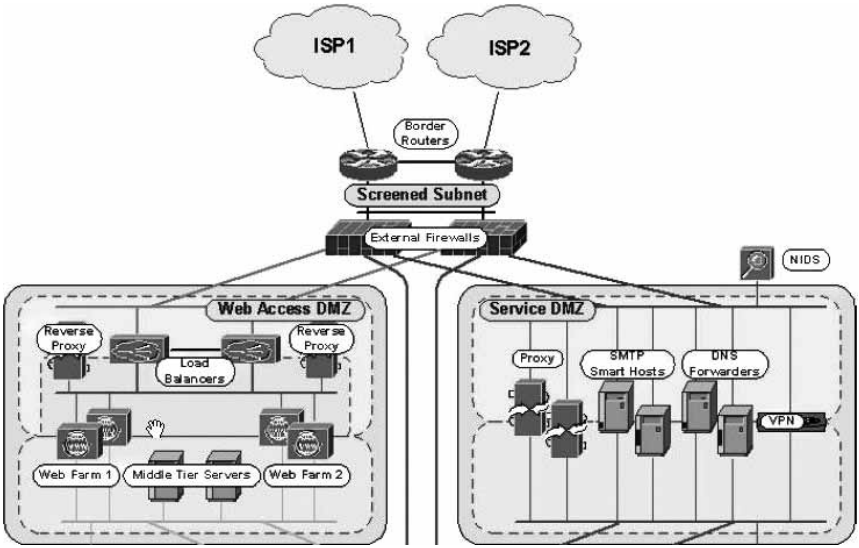

Рис. 1. Зоны выхода в Internet и доступа к веб-приложениям

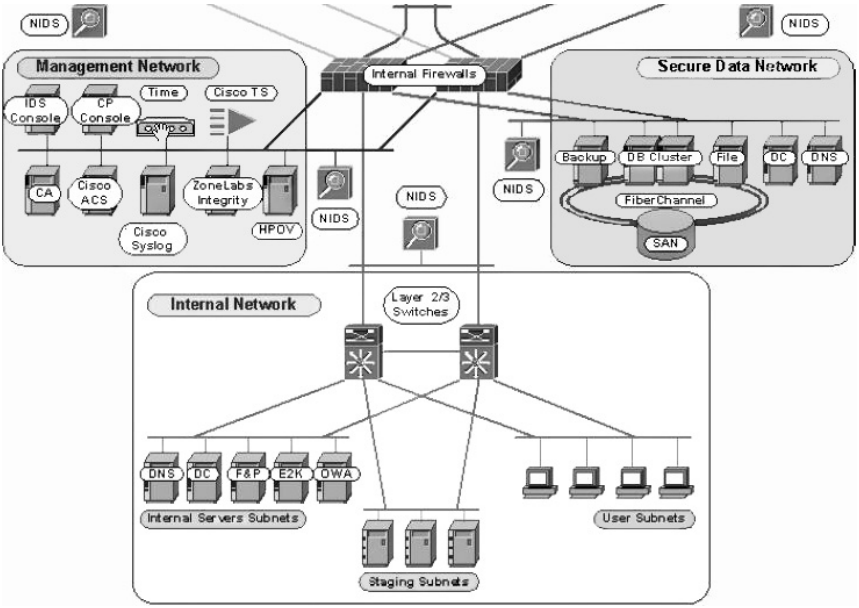

Рис. 2. Зоны управления ресурсами сети, защищаемых данных и внутренней сети

В компании было создано несколько зон безопасности:

- **Зона подключения к Internet.** 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 межсетевых экранов;
- **Зона доступа к веб-приложениям компании, Web Access DMZ**. В этой подсети находятся веб-приложения компании и разрешены только входящие через межсетевой экран запросы из Интернета. Доступ из внутренней сети запрещен;
- **Зона выхода в Internet, Service DMZ.** Эта зона представляет собой подсеть, с помощью которой предоставляется доступ сотрудникам компании в Интернет. Разрешен только исходящий через межсетевой экран трафик, за исключением доступа к электронной почте и доступ 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 веб-приложения, базы данных и базу данных пользователей (Active Directory);
- **Зона внутренней сети компании, Internal Network.** Зона содержит сервера, рабочие станции сотрудников и приложения Интранет.
- При этом компания использует следующие диапазоны IP адресов: 70.70.70.0/24 и 90.90.1.0/30 (реально 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. При этом используется 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 выглядит следующим образом:

Сеть	Подсеть
Соединение с ISP1	70.70.1.0/30
Соединение с ISP2	90.90.1.0/30
Подсеть между пограничными маршрутизаторами и внешними межсетевыми экранами	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 межсетевыми экранами	172.16.1.16/29
Внешние адреса веб-приложений	70.70.70.64/27
Внутренние адреса веб-приложений (NAT)	172.16.2.0/24
Внутренние адреса веб-приложений	172.16.3.0/24
Внешние адреса зоны ServiceDMZ	70.70.70.96/27
Внутренние адреса зоны ServiceDMZ	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

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

Зона подключения к Internet

Одно из главных бизнес-требований компании — обеспечение доступности Интернета 24 часа × 7 дней. Для обеспечения этого требования были выбраны два провайдера, ISP.

Для надлежащего распределения маршрутизации и избыточности был сконфигурирован BGP v. 4 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 маршрутизатора является поддержка Cisco Express Forwarding (CEF), что существенно увеличивает производительность маршрутизаторов.

Пограничные маршрутизаторы являются первой линией обороны. Так как они являются первой точкой входа в сеть, то на них настроены списки контроля доступа (ACL) для фильтрации нежелательного трафика, уменьшая, таким образом, нагрузку на остальную сетевую инфраструктуру. Реализована фильтрация как входящего, так и исходящего трафика. Для защиты от SYN flood атак используется возможность Cisco IOS TCP Intercept. Другая задача, которую решают пограничные маршрутизаторы — защита внешних межсетевых экранов от трафика направленного на IP адреса межсетевых экранов. 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. Для обеспечения горячего резервирования на внутренних интерфейсах маршрутизаторов сконфигурирован 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, Checkpoint FW-1 NG FP3. К основным факторам, повлиявшим на выбор данных устройств, относятся:

- высокая надежность, защищенность и производительность аппаратных платформ Nokia;
- развитая функциональность и технологическая зрелость межсетевого экрана Checkpoint FW-1 NG FP3;
- наличие подготовленных специалистов в компании.

Как было описано ранее, в компании существуют две DMZ зоны, одна для доступа к веб-приложениям и другая для выхода в Интернет, каждая из зон защищена межсетевыми экранами. Это было сделано для разделения

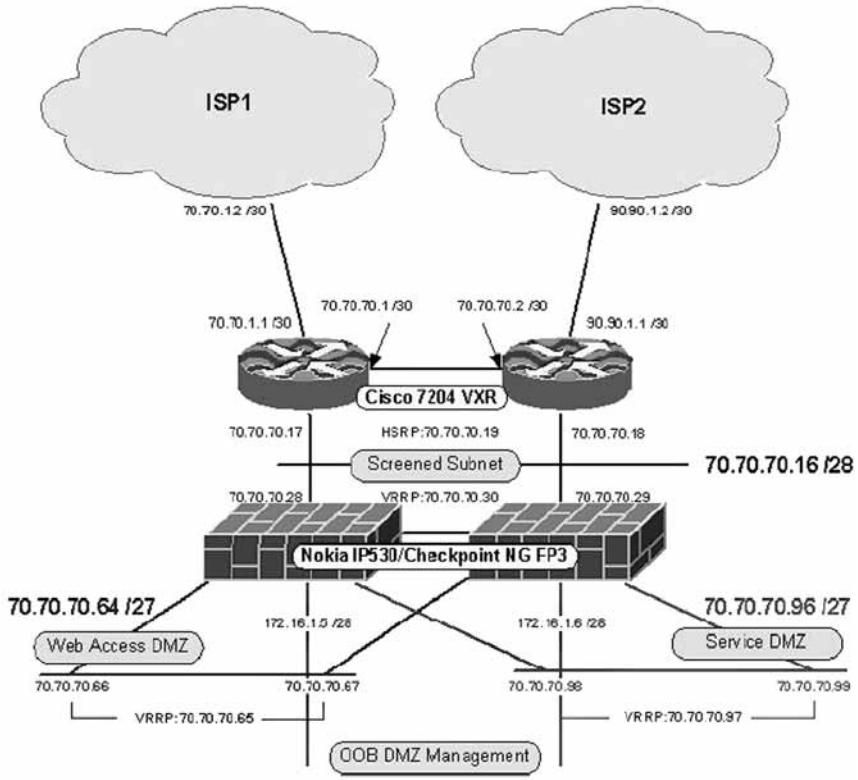

Рис. 3. Зона подключения к Internet

ресурсов, чтобы при проникновении злоумышленников в одну из зон, это не сказалось на работе другой зоны.

Каждый межсетевой экран имеет 5 интерфейсов, подключенных к разным зонам. Межсетевые экраны также имеют выделенный интерфейс для Out-of-band управления посредством сервера Checkpoint Management Console из зоны управления. Это повышает защищенность 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 путем использования Nokia IPSO VRRP и возможностью синхронизации соединений Firewall-1.Через межсетевые экраны разрешен ограниченный набор трафика согласно принятой в компании политики безопасности. На этом же уровне реализована и защита от SYN Flood атак.

Зона доступа к веб-приложениям компании, Web Access DMZ

Эта зона защищена на уровне представления, промежуточном уровне, а также на уровне баз данных компании. Сервера 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 веб-серверах выполняется Microsoft IIS 5.0. Сервера имеют по два сетевых интерфейса. Через один интерфейс поступают запросы из Интернета, через другой осуществляются запросы к базе данных. Таким образом, осуществляется изоляция веб-приложений от базы данных.

Зона выхода в Internet, Service DMZ

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 отключенной 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 используется для ограничения доступа к определенным веб-ресурсам, запрещенным Политикой использования Интернета, например к веб-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 отчеты по использованию ресурсов Интернета по конкретным сотрудникам. Для обнаружения вирусов в трафике HTTP, SMTP и FTP используется продукт Trend Micro InterScan VirusWall.

SMTP сервера

SMTP сервера работают на OpenBSD 3.2 с Sendmail v. 8.12.6. Это один из немногих случаев, когда используется продукт, не произведенный Microsoft. Этот выбор обусловлен тем, что Microsoft Exchange 2000 Server

имеет избыточное для компании количество функциональных возможностей, 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 защищенных операционных систем. OpenBSD и Sendmail бесплатны, что ведет 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 для затруднения получения злоумышленником информации о версии программного обеспечения внешнего SMTP сервера. Для предупреждения возможности просмотра списка почтовых ящиков и сервисов отключены команды VRFY и EXPN.

DNS

В качестве концепции построения DNS было выбрано решение по разделению на внутренний и внешний DNS. Внешний DNS сервер обслуживается провайдерами Интернета 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 сервера являются одним из самых слабо защищенных сервисов и постоянно являются мишенью для атак злоумышленников. Этот дизайн также обеспечивает избыточность и улучшает доступность сервисов, потому что достаточно мала вероятность, что DNS сервера обоих провайдеров одновременно подвергнутся атаке и не смогут обслуживать запросы.

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

VPN

Для обеспечения доступа к корпоративной сети работающих удаленно сотрудников и персонала, ответственного за управление сетевыми устройствами, используется концентратор Cisco VPN 3030. Доступ по коммутируемым соединениям запрещен. Так как сервис VPN не является критичным для обеспечения бизнес-процессов, то используется 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, должен подписать Политику использования VPN.
- Разрешен к использованию 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 использовании USB устройством, где доступ к сертификату защищен паролем. После создания ключи сертификатов не могут быть экспортированы из устройства.
- Каждый сотрудник имеет персональный идентификатор и пароль для использования этого сервиса. Аутентификация и управление идентификаторами осуществляется 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 Security 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.

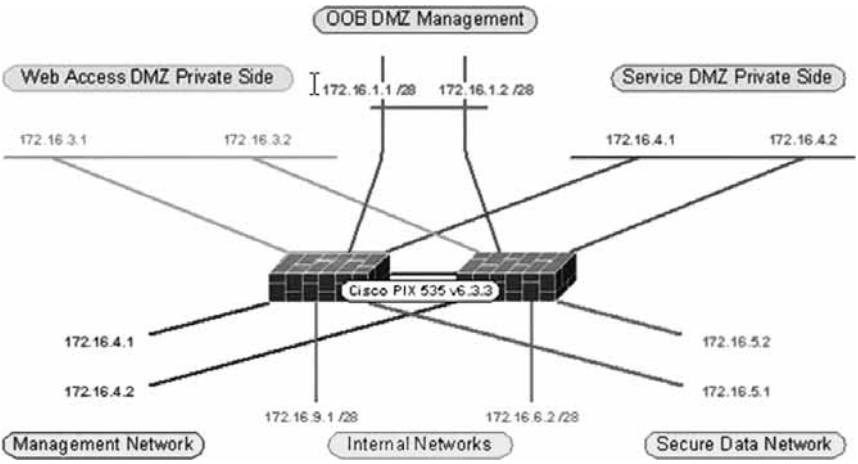

Рис. 4

Кроме того достигается изоляция сегмента управления от остальной сети, управление доступом через VPN, защита внутренней сети путем запрещения трафика из менее защищенных зон сети и пр. Каждый межсетевой экран имеет шесть интерфейсов, каждый из которых подключен к разным зонам, также существует выделенный интерфейс для поддержания режима горячего резервирования (на рис. 4 не показано).

Система построена на двух межсетевых экранах Cisco PIX 535, функционирующих в режиме горячего резервирования. Выбор продукта был обусловлен его высокой производительности, надежности и приемлемой для компании стоимостью решения. Кроме того, использование межсетевых экранов разных производителей увеличивает общую защищенность сети компании, так как при возникновении уязвимости в Checkpoint FW-1 эта уязвимость вряд ли может быть использована против Cisco PIX и наоборот.

Зона управления ресурсами сети компании, Management Network

Все сервера управления сетью и сервера мониторинга расположены на выделенной сети защищенной внутренними межсетевыми экранами:

1. Сервер времени — Datum TymServe TS2100 Firmware Code Release v. 2.1.
2. Сервер аутентификации — Compaq Proliant DL360 с Windows Server 2000 Service Pack 4 и Cisco Secure ACS v. 3.3 for Windows Server.

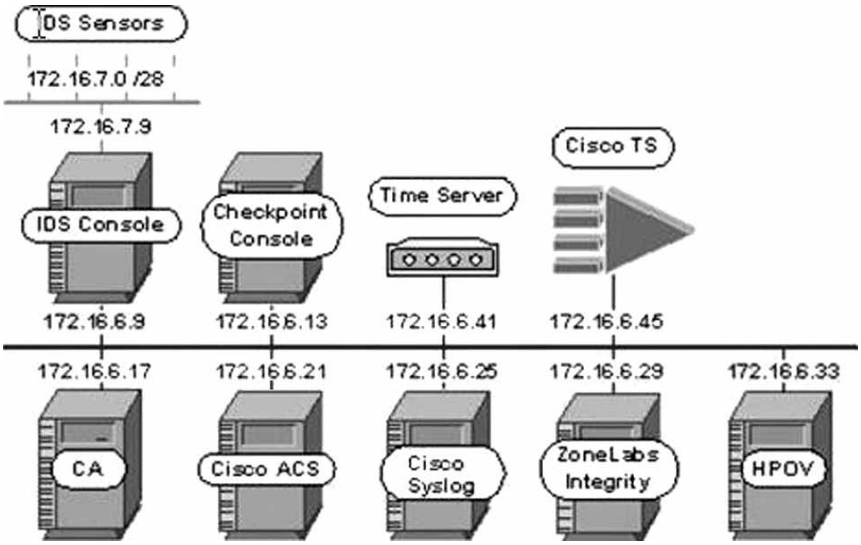

Рис. 5

3. Терминальный сервер — Cisco 2620 Access Router с Cisco IOS 12.2(12).
4. Сервер журналирования — Compaq Proliant DL580 с Windows Server 2000 Service Pack 4 и Cisco Security Information Management Solution v. 3.1.
5. Сервер Integrity — Compaq Proliant DL360 Windows Server 2000 Service Pack 4 с Zone Labs Integrity Server v. 1.6.
6. Сервер управления Checkpoint — Compaq Proliant DL360 с Windows Server 2000 Service Pack 4 и Checkpoint Firewall-1 NG FP3 Management.
7. Сервер мониторинга — HP OpenView Compaq Proliant DL360 с Windows Server 2000 Service Pack 4 и HP OpenView Network Node Manager v. 6.31.

В компании организован центр управления сетью для мониторинга и управления сетевыми устройствами. Центр находится в защищенном от проникновения посторонних лиц помещении. График работы персонала 16 часов × 5 дней в неделю. Поддержка в ночное время реализуется через VPN соединения. При этом 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. Также, доступ к любому сетевому оборудованию огра-

ничен списком IP адресов сети управления. Пограничные маршрутизаторы и все коммутаторы управляются через консоль с использованием маршрутизатора доступа Cisco 2620 и все остальные управляющие интерфейсы на устройствах отключены. Другие устройства — SMTP сервера, VPN концентратор — управляются с помощью SSH. Сервера с операционной системой Windows 2000 управляются с использованием Microsoft Terminal Services, который поднят на внутренних интерфейсах серверов и сконфигурирован для использования максимального уровня шифрования. Кроме этого, настроены фильтры IPSec таким образом, чтобы разрешать доступ к серверам с использованием Terminal Services (TCP 3389), если соединение инициируется из сети управления.

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.

В состав продукта входят следующие функциональные модули:

- CiscoWorks 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 также имеет средства мониторинга производительности и инвентаризации сети. Доступ к этому устройству из сети, отличной от сети управления, запрещен.

Сервер Checkpoint Management Console

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

Сервер времени

Синхронизация сетевого времени — очень важный аспект правильного функционирования сети и надлежащего журналирования. Если установлено разное время на нескольких устройствах, то при анализе журналов очень трудно будет разбираться, когда реально и в какой последовательности произошли события, кроме этого каждый из сертификатов имеет определенный срок жизни и при неправильно установленном времени его будет невозможно использовать. Злоумышленники нередко используют слабости в защите протокола NTP или неправильные настройки сетевых устройств для проведения атак с целью установки неверного времени и, таким образом, выводят из строя все устройства и соединения, которые используют сертификаты. Кроме этого, Microsoft Active Directory использует протокол Kerberos для аутентификации, который очень сильно зависит от точных настроек времени. Из-за важности обеспечения точного времени был приобретен аппаратный сервер времени Datum TymServe TS2100. Это устройство использует GPS антенну для синхронизации с сервером времени NIST (Национальный институт стандартов США). Это устройство служит мастер сервером для всех устройств в сети. К этому устройству разрешен 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 на получение точного времени. В случае возникновения такой ситуации будут сделаны соответствующие изменения в списках доступа на межсетевых экранах.

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, также, определенному списку инженеров подключающимся через VPN соединение. Разрешен 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 программного обеспечения (28 источников) с которых оно может принимать и обрабатывать сообщения. В компании используется часть из них:

- Checkpoint FireWall-1;
- Cisco IOS ACL, FW, IDS;
- Cisco Secure ACS;
- Cisco Secure IDS;
- Cisco Secure PIX;
- Cisco Secure PIX IDS;
- Cisco Security Agent;
- Концентратор Cisco VPN;
- Cisco Firewall Switch Module;
- Tripwire NIDS;
- Веб-сервера Microsoft IIS;
- Windows Events;
- UNIX OS Events.

Центр управления сертификатами

В сети широко используются сертификаты — для доступа посредством VPN, к веб-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 для выпуска сертификата для выпускающего центра управления сертификатами и после этого был немедленно переведен в режим offline. Секретный (private) ключ основного центра сертификации был перемещен на дискету, удален с жесткого диска, и эта дискета была помещена в сейф отдела информационной безопасности. Копия дискеты хранится за пределами офиса в защищенном помещении в сейфе.

Cisco Secure ACS Server

Для аутентификации используется Cisco Secure ACS Server v. 3.3 for Windows:

- Сотрудники, использующие VPN, аутентифицируются и получают IP адрес из ACS сервера с использованием протокола RADIUS.
- Доступ к сетевым устройствам для администрирования контролируется с использованием протокола TACACS+.

TACACS+ является протоколом последнего поколения из серии протоколов TACACS. TACACS — это простой протокол управления доступом, основанный на стандартах User Datagram Protocol (UDP) и разработанный компанией Bolt, Beranek, and Newman, Inc. (BBN) для военной сети Military Network (MILNET). Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась ее собственная версия TACACS, известная как TACACS+. TACACS+ пользуется транспортным протоколом TCP. Демон 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.

Протокол TACACS+ работает по технологии клиент/сервер, где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается «демон» (процесс, запускаемый на машине UNIX или NT). 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 передается по каналам связи. Обычно этот секрет вручную устанавли-

вается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом TACACS+ и демоном сервера TACACS+.

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

- ACS посылает START запрос на TACACS+ сервер для начала процесса аутентификации;
- сервер отсылает ACS пакет с запросом GETUSER, содержащий запрос пользователю на ввод имени;
- ACS отображает запрос пользователю и отсылает серверу TACACS+ введенное 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+;
- TACACS+ сервер 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 TACACS+ сервером 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.

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, допускать такого пользователя к запрашиваемым услугам или нет. Протокол TACACS+ допускает только положительную или отрицательную авторизацию, однако этот результат 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 использоваться для учета использованных услуг (например, для выставления счетов). Во-вторых, его можно использовать в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт» указывают, что услуга должна быть запущена. Записи «стоп» говорят о том, что услуга только что окончилась. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется.

Учетные 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 TACACS+ сервера выглядит следующим образом:

- ACS отсылает учетную запись TACACS+ серверу, основываясь на выбранных методах и событиях;
- TACACS+ сервер отсылает ответный пакет ACS серверу, подтверждая прием учетной записи.

Zone Labs Integrity Server

Zone Labs Integrity Server v. 1.6 используется для принудительного применения политики на компьютерах сотрудников, которые подключаются посредством VPN. В данном случае потребуется установка на каждом компьютере Integrity Agent для приема 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 удаленный компьютер может быть незащищен надлежащим образом и стать точкой входа во внутреннюю сеть вирусам и злоумышленникам. 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 24×7 для обеспечения высокой доступности сервисов. Из-за большой степени риска разрешено использовать SNMP только в режиме read-only. Правила на межсетевых экранах разрешают этот трафик

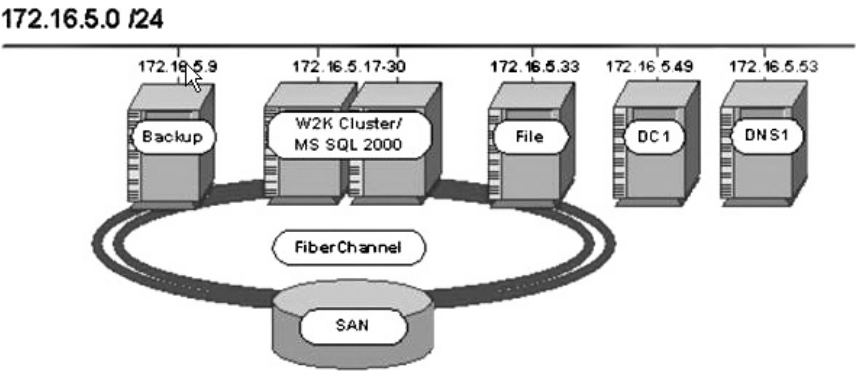

Рис. 6

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 запрещен любой другой доступ из-за пределов сети управления.

Зона защищаемых данных компании, Secure Data Network

Схема зона защищаемых данных компании, Secure Data Network представлена ниже.

В этой сети находятся все данные веб-приложений. Также здесь располагаются сервера Active Directory, контроллеры доменов веб-приложения и DNS сервера. Каждый из них является кластером, который состоит из двух компьютеров. На рис. 6 это не отображено для того чтобы сделать рисунок более читабельным.

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-сервера построены на Microsoft Windows 2000 Server Service Pack 4 и Microsoft File and Print Services. Для обеспечения избыточности и высокой доступности на файл-серверах развернута, интегрированная с Active Directory, служба Distributed File System. Только сервера промежуточного уровня имеют доступ к Microsoft SQL Server. При этом стандартный порт TCP 1433 изменен на нестандартный порт TCP 2000. Доступ из внутрен-

ней сети к базе данных ограничен только выполнением запросов к базе данных и только с определенного списка IP адресов.

Active Directory

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

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

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

Зона внутренней сети компании, Internal Network

Во внутренней сети находятся рабочие станции сотрудников и внутренние сервера. Сеть логически разделена на 2 части: подсеть серверов и подсеть сотрудников. В качестве ядра дизайна используются 2 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. Использование раздельных маршрутизирующих интерфейсов для каждого VLAN позволяет задействовать дополнительные списки контроля доступа для ограничения доступа из определенных подсетей или компьютеров. На рис. 7 изображен только один сервер каждого типа для улучшения читабельности.

Внутренняя сеть Windows 2000 использует изолированный «лес» Active Directory со своими собственными DNS серверами и контроллерами домена. Все сервера используют Windows 2000 Server Service Pack 4 и защищены в соответствии с перечисленными выше руководствами.

DNS сервера — Microsoft DNS Server с использованием Dynamic DNS в режиме «Allow Secure Updates Only». Эти сервера используются только для разрешения имен внутренних ресурсов и перенаправляют запросы на разрешение внешних имен в зону Интернет.

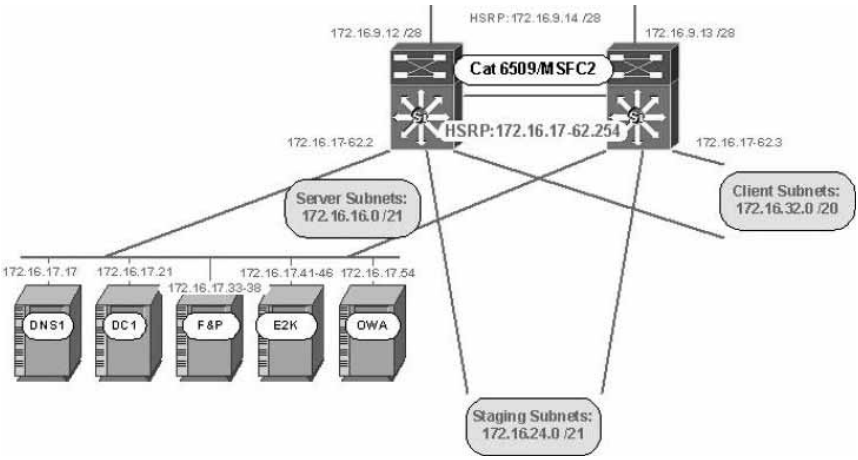

Рис. 7

В качестве внутреннего сервера обмена сообщениями и совместной работы используется Microsoft Exchange 2000 Service Pack 3. Он работает на 2-х узловом 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 используется Sybari Antigen v. 7.0 for Exchange с проверкой входящих и исходящих сообщений.

Для обеспечения возможности работы с почтой удаленным пользователям, установлен сервер Exchange 2000 Service Pack 3 Outlook Web Access, который доступен через VPN соединение поверх HTTPS. Выбор объясняется тем, что для подключения достаточно использование только одного порта (HTTPS). При использовании же обычного способа доступа к Exchange пришлось бы открывать целый набор портов, что существенно увеличивает риск взлома системы.

Файл-сервера реализованы с использованием Microsoft SharePoint Portal Server 2003. Доступ к файлам осуществляется через VPN поверх HTTP/HTTPS. Это делает ненужным настраивать межсетевой экран для трафика SMB/CISF, что упрощает конфигурацию межсетевого экрана и делает дизайн более защищенным.

Исходящий доступ разрешен только для HTTP/HTTPS из сети сотрудников через Proxy сервер. По причинам обеспечения безопасности не разрешен доступ из подсети серверов в Интернет. При необходимости установки драйверов или обновлений, они загружаются обслуживающим персоналом на свои рабочие места и далее переносят на сервера на CD дисках или дискетах.

Доступ к серверам баз данных предоставлен ограниченному списку администраторов баз данных с определенного списка IP адресов. Аналогично предоставлен доступ к серверам данных и для менеджеров, ответственных за наполнение веб-страниц приложения.

Сеть тестирования используется для тестирования приложений перед их перемещением в действующую сеть. Эта сеть полностью имитирует рабочие сервера и также используется для тестирования сервисных пакетов и обновлений перед их установкой на сервера и рабочие станции. Это позволяет уменьшить вероятность несовместимости приложений и увеличить надежность функционирования сети и приложений. Реализована процедура управления изменениями.

Литература

1. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. 416 с.
2. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. 400 с.
3. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.