УДК 004.047

О.В.Копейка

ПРОЕКТИРОВАНИЕ СЕРВИСОВ БЕЗОПАСНОСТИ В ДАТА-ЦЕНТРАХ

Рассматривается задача проектирования сервисов безопасности в Дата- центрах, которые определяются в соответствии с архитектурой системы безопасности ИТ-инфраструктуры. Эти сервисы обеспечивают необходимый уровень защиты ИТ-активов Корпорации путем описания подходов по организации и формированию требований к персоналу, процессам и технологиям. Изучаются сервисы безопасности, в состав которых входят службы защиты периметра и управления сертификатами (PKI).

Ключевые слова: Дата-центр, сервисы безопасности, службы защиты периметра и управления сертификатами.

Введение и постановка задачи

В Украине уже 85% предприятий малого и среднего бизнеса используют тот или иной «облачный сервис». И это количество будет расти, так как сегодня «облачные технологии» предлагают практически безлимитные ресурсы бизнесу любого размера при стоимости, которая несопоставима с капитальными инвестициями в собственную инфраструктуру.

При реализации концепции «облачных сервисов» возникает задача построения Дата-центров с современной архитектурой и наличием полного объема сервисов.

В современных Дата-центрах выделяют следующие сервисы: сетевые; управления данными; управления ИТ-инфраструктурой; инфраструктуры приложений; безопасности.

В данной статье рассматриваются сервисы безопасности, которые состоят из служб: защиты периметра и управления сертификатами (PKI).

Основная часть

Службы защиты периметров (МЭ периметра и внутренние, proxy/cache сервисы)

Служба защиты периметра (firewall) контролирует поток сетевого трафика между двумя сегментами сети. Служба обеспечивает:

1. Защиту внутренних серверов от сетевых атак.
2. Реализацию зонирования сети, политик доступа и использования сети.
3. Мониторинг трафика и обнаружение нарушений в работе.

Служба защиты периметров сети состоит из семи функциональных уровней.

1. Фильтры сетевых адаптеров устройств.
2. Статические фильтры пакетов.
3. NAT (не рекомендован к использованию).
4. Stateful inspection.
5. Circuit-level inspection.
6. Прокси.
7. Фильтрация уровня приложений.

В Корпорации будет развернуто три класса служб защиты периметра.

Таблица 1

Классы службы защиты периметра

	Класс 1: Персональный (Windows)	**Класс 2: Экран сетевых зон**	**Класс 3: Специализированный сервер**
Features supported	Статические фильтры пакетов, фильтры уровня сессий, фильтры уровня приложений	Статические фильтры пакетов	Статические фильтры пакетов, фильтры уровня сессий, фильтры уровня приложений
Configuration	Автоматическая	Ручная	Ручная (централизованная)
Block or allow IP addresses	Да	Да	Да
Block or allow protocol/port numbers	Да	Да	Да
Block or allow incoming ICMP messages	Да	Да	Да
Control outgoing access	Да	Да	Да
Application protection	Да	Да	Да
Audible/visible alerts	Да	Да	Да
Log file of attacks	Минимальное	Да	Да
Real-time alerts	Нет	Нет	Да
VPN support	Да	Нет	Да
Remote management	Нет	Да	Да
Manufacturer support	Да	Да	Да
High-availability option available	Нет	Дублирование	Кластеризация и создание множеств
Number of concurrent sessions	До 10	10 000	500,000
Modular upgradeability (hardware or software)	Нет	Нет	Да
Other		Cisco Router firewall options	
Price range	Входит в стоимость операционной системы		

Класс 1. Персональный брандмауэр обеспечивает защиту каждого рабочего места пользователя.

Класс 2. Экран сетевых зон. Для контроля и инспекции сетевого трафика между зонами сети с помощью возможностей сетевых устройств создается каркас защиты.

Класс 3. Специализированные серверы защиты обеспечивают дополнительные функции инспекции и защиты для корпоративных клиентов использующие публичные ресурсы и для внешних клиентов использующие службы Корпорации. Специализированные сервера располагаются в зоне периметра и обслуживают связь между зонами Периметр и граница сети. Специализированные серверы также отвечают за кэширование информации.

Для каждого класса системы будет создана таблица правил в соответствии с которой устройства будут настроены.

Логическая организация

Логическая архитектура службы представляет собой каркасную модель (рис. 1). Каждое клиентское устройство имеет компонент службы первого класса. Персональные Firewalls установлены на каждой рабочей станции и получают свою конфигурацию централизовано – посредством групповых политик Active Directory.

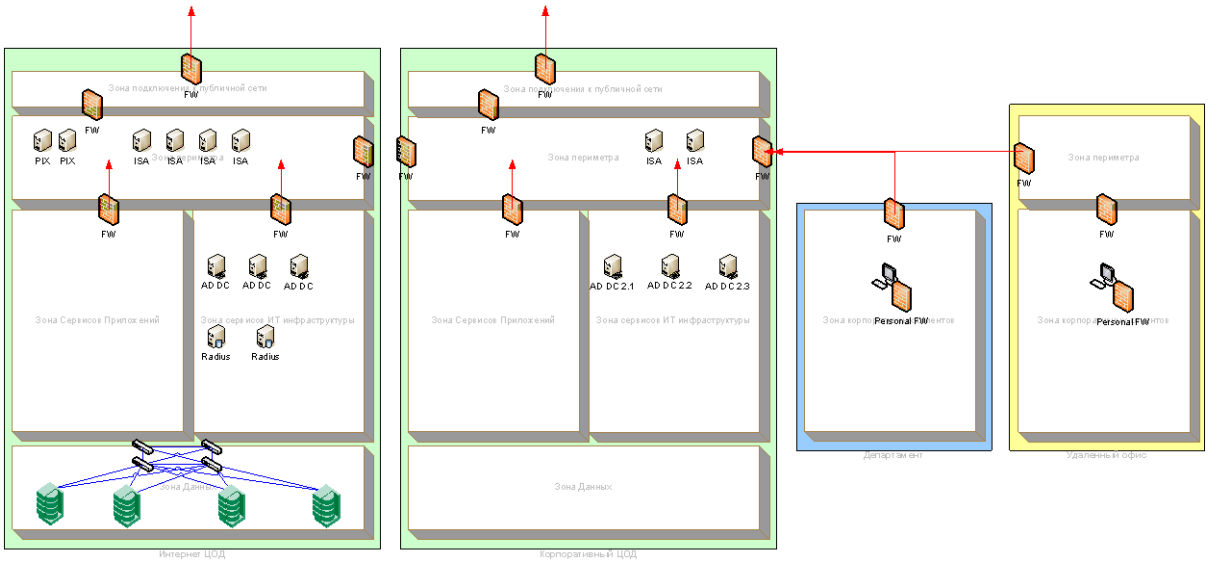

Рис. 1. Организация сервиса защиты периметра

Сетевые экраны развернуты на маршрутизаторах сети и формируют собой границы зон. Специализированные сервера защиты, Internet Security and Acceleration Server и Cisco PIX развернуты в зоне периметра на границе с Зоной подключения к публичной сети и на границе подключения к Зонам корпоративных клиентов и зонам периметра удаленных офисов.

Для контроля доступа и контроля доступной полосы пропускания на уровне пользователей ISA сервер использует Active Directory, в качестве службы каталога. PIX системы могут использовать службу каталогов Active Directory посредством интеграционных механизмов Internet Authentication Server или Microsoft Identity Integration Server. Принципиальным является существование одной службы каталогов, обслуживающих учетные записи пользователей. Дублирование каталогов для отдельных служб и устройств не допускается.

Серверное обеспечение

Четырнадцать серверов ISA 2003 по два в каждом ЦОД, объединенных в множество (array). Сервера четырех процессорные с 2 Гб памяти и 16 Гб дискового пространства. Два и более - серверов в каждом из двух Интернет Дата-центров, в зоне периметра.

Сервера четырехпроцессорные с 2Гб памяти и 16 Гб дискового пространства. Модель сервера уровня - HP DL380.

Сеть хранения данных

Используется для хранения базы данных серверов TACACS. Поэтому в зоне сервисов приложений работает кластер СУБД, который оборудован двумя HBA адаптерами для подключения к сети хранения данных.

Коммуникационная сеть

В ЦОД настраиваются:

1. Коммутатор Внутренней Интеграции – используются функции VLAN и Firewall.

2. Центральный Коммутатор ЦОД – используются функции VLAN и Firewall.
3. Коммутатор Периметра – используются функции VLAN и Firewall.
4. Оборудование Границы сети.

Доступность

Доступность обеспечивается с помощью NLB кластеризации, формированием множеств (array) ISA серверов и дублированием элементов сети хранения данных.

Безопасность

Качество продуктов службы защиты периметра подтверждается экспертной оценкой оргнанизации - International Computer Security Association.

Масштабируемость

Масштабируемость достигается горизонтальным наращиванием серверов. Использование NLB технологии позволяет исключить модернизацию ИТ инфраструктуры при выполнении масштабирования сервиса.

Управляемость

Для централизованного управления ISA сервера являются членами домена Active Directory – corp.ukrtelecom.net. Контролеры домена хранят конфигурационную информацию об множествах и позволяют управлять службой одной рабочей группе.

Консолидация и взаимодействие

Служба консолидирована с сетевыми устройствами. Специализированные сервера защиты консолидированы с системами кэширования содержания.

Службы управления сертификатами (PKI)

Служба управления сертификатами отвечает за управление жизненным циклом сертификатов безопасности, используемых в системах криптографической защиты информации и цифровой подписи (рис. 2).

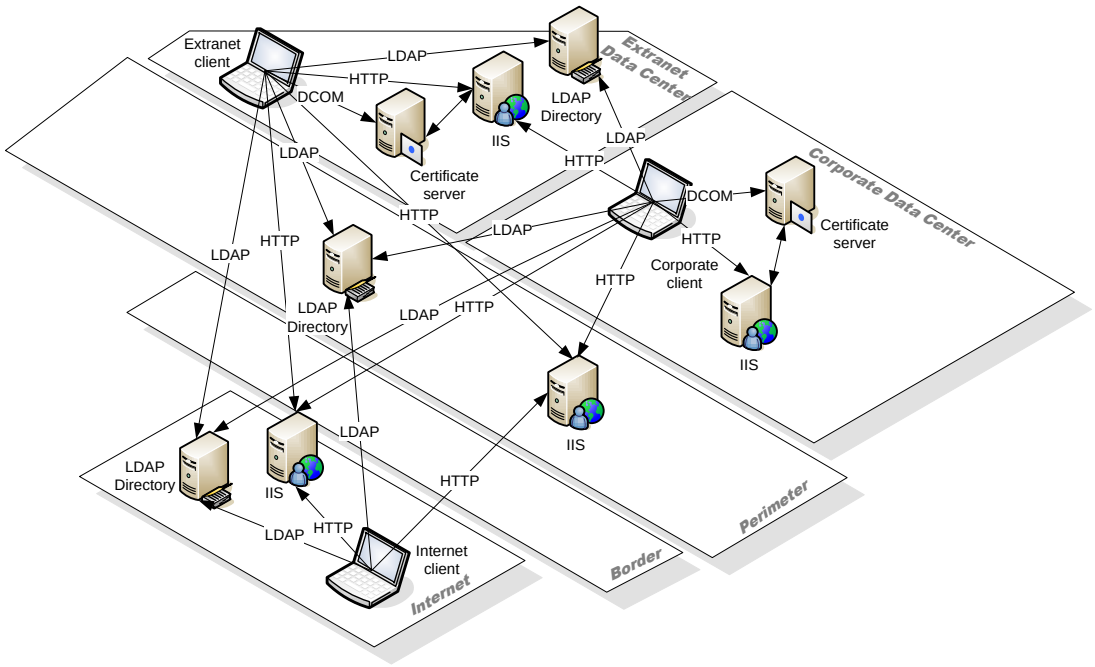

Рис. 2. Информационные потоки в службе сертификатов

Служба сертификатов в частности обеспечивает использование в Корпорации:

1. Цифровой подписи.
2. Смарт-карт для аутентификации пользователей.
3. Защищенной почты (S/MIME).
4. Авторизации ПО (Authenticode).

5. Использование протокола IPSec.
6. Использование протокола 802.1x.
7. Использование шифрованной файловой системы (EFS).
8. Использование протоколов SSL и TLS.

Логическая организация

Сертификаты для сотрудников Корпорации выдаются многоцелевые. Для служб и внешних клиентов – одноцелевые. Служба сертификатов реализована в режиме Enterprise (Корпоративная интегрированная).

Корень дерева службы сертификатов внешний. Служба сертификатов развернута в виде дерева с тремя уровнями иерархии и включает в себя шесть компонентов:

1. Промежуточный сервер первого уровня (отключен).
2. Серверы промежуточные второго уровня.
3. Серверы выдающие.
4. Документ «Политика Инфраструктуры Открытых ключей».
5. Документ «Регламент Инфраструктуры Открытых Ключей» на базе RFC 2525. OID регистрируется независимо.
6. Шаблоны сертификатов для пользователей выданные и опубликованные в Active Directory.

Служба Active Directory отвечает за автоматическую установку новых сертификатов на рабочие станции пользователей.

Физический дизайн (рис.3)

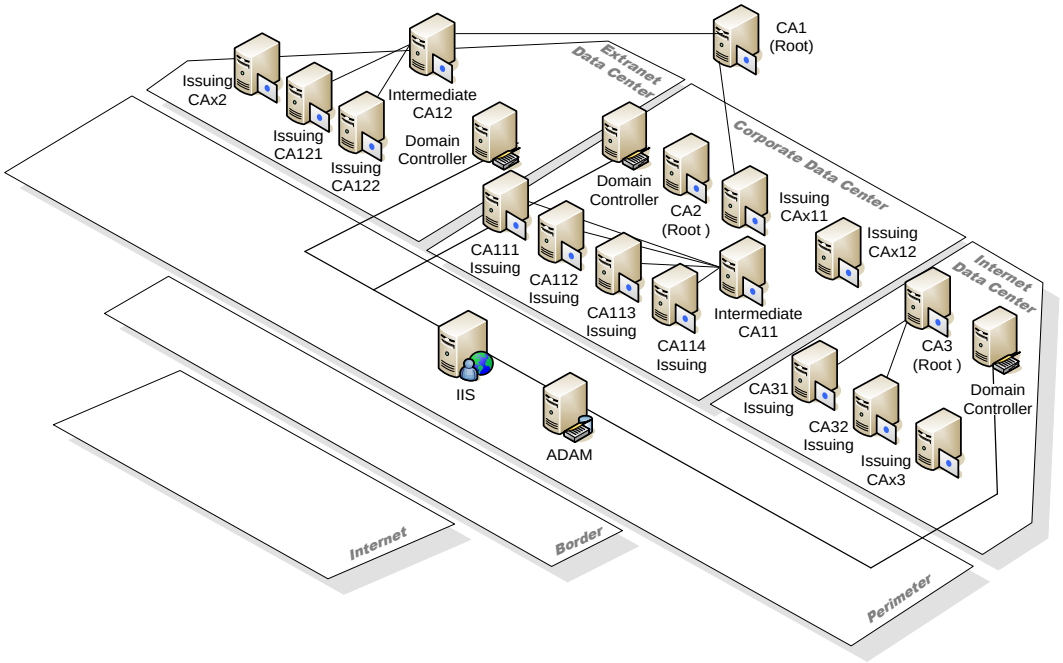

Рис. 3. Организация сервиса сертификатов

Выводы

Рассмотрена задача проектирования сервисов безопасности в Дата-центрах, которые определяются в соответствии с архитектурой системы безопасности ИТ-инфраструктуры. Эти сервисы обеспечивает необходимый уровень защиты ИТ-активов Корпорации путем описания подходов по организации и формированию требований к персоналу, процессам и технологиям. В состав сервисов безопасности входят службы защиты периметра и управления сертификатами (PKI).

При проектировании служб к ним предъявляются следующие требования:

Доступность.

Доступность обеспечивается с помощью NLB кластеризации, формированием множеств (array) ISA серверов и дублированием элементов сети хранения данных.

Безопасность.

Качество продуктов службы защиты периметра подтверждается экспертной оценкой оргнанизации - International Computer Security Association.

Масштабируемость.

Масштабируемость достигается горизонтальным наращиванием серверов. Использование NLB технологии позволяет исключить модернизацию ИТ инфраструктуры при выполнении масштабирования сервиса.

Управляемость.

Для централизованного управления ISA сервера являются членами домена Active Directory – corp.ukrtelecom.net. Контролеры домена хранят конфигурационную информацию об множествах и позволяют управлять службой одной рабочей группе.

Консолидация и взаимодействие.

Служба консолидирована с сетевыми устройствами. Специализированные сервера защиты консолидированы с системами кэширования содержания.

Література

1. Информационные технологии – практические правила управления информационной безопасностью //ISO/IEC 17799 МЕЖДУНАРОДНЫЙ СТАНДАРТ - Первое издание 2000-12-01-87 с.
2. Копейка О.В. Сетевые службы и службы сетевых устройств в Дата-центрах/О.В. Копейка//Системи управління, навігації та зв'язку: наукове періодичне видання. – 2013. – Випуск 4 (28). – С. 98-104
3. Копейка О.В. Архитектура системы управления ИТ-инфраструктурой в современных Дата-центрах/О.В.Копейка// Наукові записки Українськогонауково-дослідногоінститутузв'язку: науково-виробничийзбірник. – 2014. - №1 (29). – С. 29-37
4. Еталонніархітектури MSA. – К.: Майкрософт Україна; К.: Видавничагрупа BHN, 2005. – 352 с.
5. Засади регіональноїінформатизації/ Довгий С.О., Копійка О.В., Черепін Ю.Т.- К.:ВПЦ «ТИРАЖ», 2004.-304с.
6. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития/ С.А.Довгий, О.В.Копейка, С.П.Поленок. – К.:Укртелеком,2001.- 281 с.
7. O.Kopeika, I.Tarasenko, A.Kisselevskiy, A.Karichenskiy, T.ValiulinSoftline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom// TM Forum Case Study Handbook, Volume 3, May 2007 – S. 27
8. http://www.tiaonline.org/standards/
9. Jew, Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010- page 28.
10. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric – page 4.
11. Telecommunications Infrastructure Standard for Data Centers//TIA STANDARD TIA-942. TELECOMMUNICATIONS INDUSTRY ASSOCIATION - April 2005. - p. 135
12. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices// Committee Approval - January 2011 First Published: March 2011 - p. 367

Надійшла 15.05.2014 р. Рецензент: д.т.н., проф. Розорінов Г.М.