Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 17, брой 3, 2019 г.
Научно списание **http://www.mtc-aj.com** **статия № 1888**

МОДЕЛ ЗА CLOUD-БАЗИРАНО УПРАВЛЕНИЕ НА ИНТЕРНЕТ ТРАФИКА, СИГУРНОСТ И ЗАЩИТА НА ДАННИТЕ В АКАДЕМИЧНА КОМПЮТЪРНА МРЕЖА

Димитър Димитров, Антони Грънчаров
ddimitrov@vtu.bg, root@vtu.bg

ВТУ "Тодор Каблешков", ул. Гео Милев 158, гр. София
БЪЛГАРИЯ

Ключови думи: *информационна сигурност, информационни системи, интернет, компютърни системи и мрежи, системи за детектиране на интрузия.*

Резюме: *Управлението и защитата на информационните системи във всяка организация, както и данните в тях е задача с много висок приоритет. Информационните системи в академичните организации по принцип са по-ниско бюджетни, но въпреки това са свързани с редица изисквания по отношение защита на личните данни, осигуряване на надеждни финансови операции, както и предоставяне на редица информационни услуги касаещи тяхната цялостна дейност. Това прави задачата по осигуряване на защитата и управлението на академичните информационни системи истинско предизвикателство.*

В настоящия доклад се представя подхода използван във ВТУ "Тодор Каблешков", за осигуряване и управление на трафика и сигурността на информационните системи и данните в тях. Този подход се базира на дългогодишното еволюционно развитие на тези технологии, като се използват съвременните Cloud-базирани решения за виртуализация и управление на информационни системи.

ВЪВЕДЕНИЕ

Осигуряването на ефективността на съвременните информационни системи е задача, свързана с изграждането на сложна хардуерна и софтуерна архитектура. Това е свързано с интеграция и синхронизация на множество информационни операционни системи и паралелно работещи приложения споделящи общи хардуерни ресурси, процеси, бази данни и др. Напоследък това се комбинира с виртуализация на операционните информационни системи в така наречените Cloud-базирани решения. Много са предимствата на този тип решения, но най-главното е че Cloud-подхода позволява бързото архивиране, клониране, паралелна работа, мобилност и машинна независимост, нещо което е особено необходимо за съвременния информационен свят в който основно изискване е да има непрекъсваемост, надеждност и сигурност на предлаганите информационни услуги.

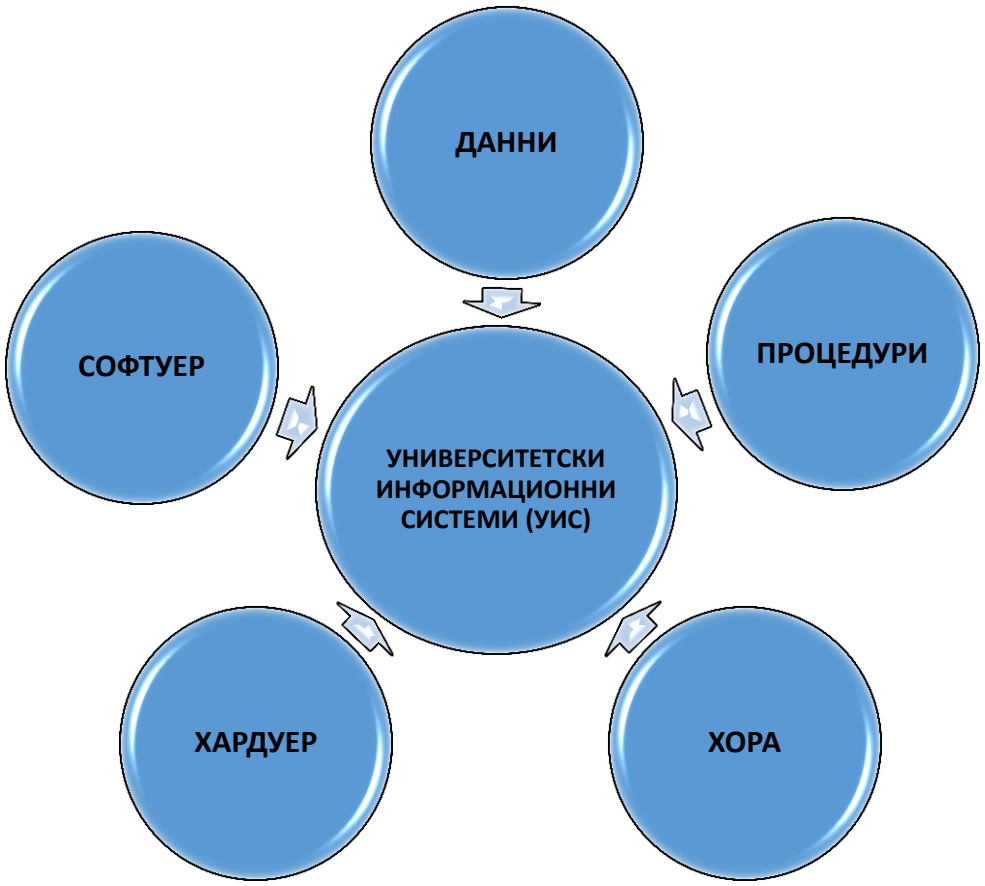
Що се отнася до управлението на университетските дейности, това е особено предизвикателство, предвид спецификата и изискванията, особено когато става дума за

нискобюджетен проект и където е необходимо най-доброто използване, както на комерсиални, така и на решения с отворен код.

В настоящия доклад се представя съвременен приложен мрежов модел за управление на информационни системи в академична мрежа. Използваният подход се основава на Cloud-базирани системи и инструменти, които изискват висока степен на автоматизация и стабилност на работното място. Показани са концепцията и основните елементи на интегрираната система за информационно обслужване на университетската мрежа на ВТУ „Тодор Каблешков“, която е изграждана и модернизирана във времето на базата на използването на добрите световни IT практики. Съществен момент е и системата за осигуряване на информационната сигурност и ефективното функциониране на университетската мрежа.

ИЗИСКВАНИЯ КЪМ УНИВЕРСИТЕТСКИТЕ ИНФОРМАЦИОННИ СИСТЕМИ

Управлението на всяка университетска организация е сложна, динамична и много параметрична задача, изискваща обобщено и подробно планиране, организация и изпълнение на процесите, свързани с провеждане на качествен учебен процес, развитие на научна и приложна дейност, както и пълноценна приложна дейност, свързана с управлението на материалните и човешките ресурси. На фиг. 1 се представят основните съставни компоненти на университетските информационни системи [1]. Те са обект на планиране и търсене на ефективност, което в крайна сметка влияе на тяхното проектиране, изграждане и използване на всяка информационна система и тя има своя жизнен цикъл, средства и ефект.



Фиг. 1. Основни компоненти на университетските информационни системи

Хардуерът включва компютрите, устройствата и IT инфраструктурата. *Софтуерът* е операционните системи, програмите и по специално реализацията на

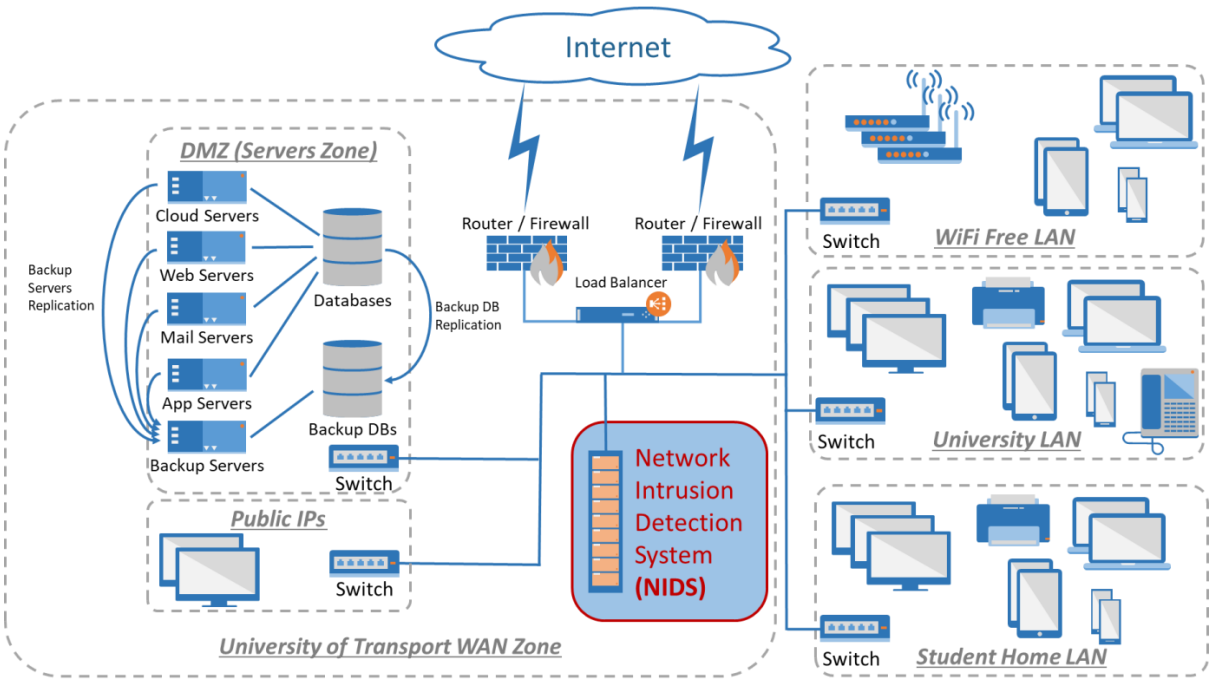
информационните системи. *Данните* и *процедурите* характеризират бизнес процесите и бизнес логиката, а *хората* се оказват най-важният компонент от цялостната система, тъй като от тях зависи ефективността на *университетските информационни системи*.

Всъщност информационната система се превръща в основно комуникационно средство между хората. В този смисъл внедряването и експлоатацията на университетските информационни системи е сложна задача, която трябва да удовлетворява на следните изисквания:

- дефиниране на бизнес логиката на процесите, подлежащи на автоматизация;
- програмиране на нови или внедряване на готови информационни системи;
- адаптиране, тестване и валидиране на внедрените информационните системи;
- поддържане, модернизация и усъвършенстване на информационните системи;
- мониторинг, превенция и отстраняване на нежеланите събития и инцидентите затрудняващи или дискредитиращи работата внедрените информационни системи;
- документиране на процедурите, обучение и контрол действията на потребителите на системите.

МОДЕЛ ЗА CLOUD-БАЗИРАНО УПРАВЛЕНИЕ НА ИНТЕРНЕТ ТРАФИКА

Изградената университетската компютърна мрежа е в резултат от многогодишно развитие [2, 3, 4, 5, 6] и е с Cloud-базирана виртуализация на основните сървъри, системи и услуги, включително и осигуряване на двуканална динамична връзка към интернет и академичната мрежата. На фиг. 2 се представя структурата на университетска компютърна мрежа, както и връзката с Интернет. Основните четири сегмента на мрежата включват: демилитаризиран сегмент на опорните сървъри и услуги; университетска LAN; студентски кампус LAN; WiFi Free LAN зона, както и сегмент от сървъри и компютърни клиенти с публични IP адреси.

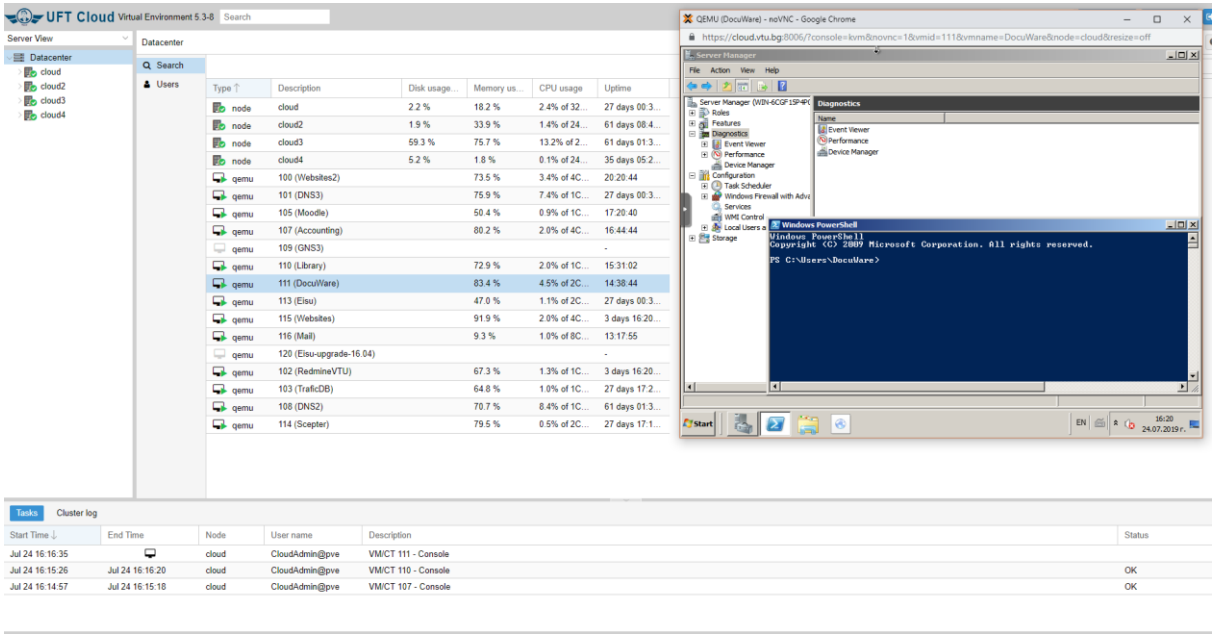


Фигура 2. Структура на изградената университетска компютърна мрежа.

Съществен елемент на системата се явява системата за детектиране на интрузия (NIDS), чрез която се следи за генерирания вътрешен и външен трафик от проникнал зловреден софтуер, вируси, спам и др., който е представен по-долу. Самата мрежа е сегментирана на по-малки виртуални мрежи, което допълнително улеснява

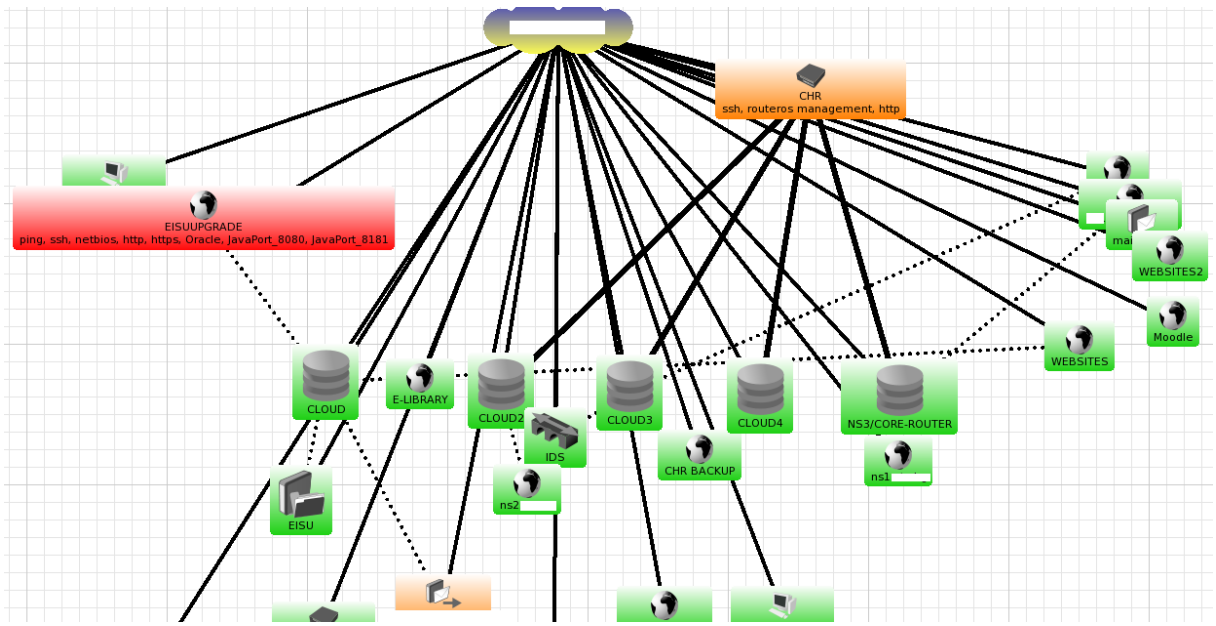
управлението и контрола на трафика и сигурността на системите. Основните сървъри и системи са позиционирани в самостоятелен демилитаризиран сегмент, което повишава степента на сигурност на информационните системи и бази данни.

На фиг. 3 се представя общ изглед от внедрената и адаптирана система за виртуализация на сървърните системи. Това се базира на Proxmox VE отворена платформа за виртуализация [7]. С вградения уеб интерфейс управлението виртуалните машини и контейнери е бързо, високопродуктивно и лесно.



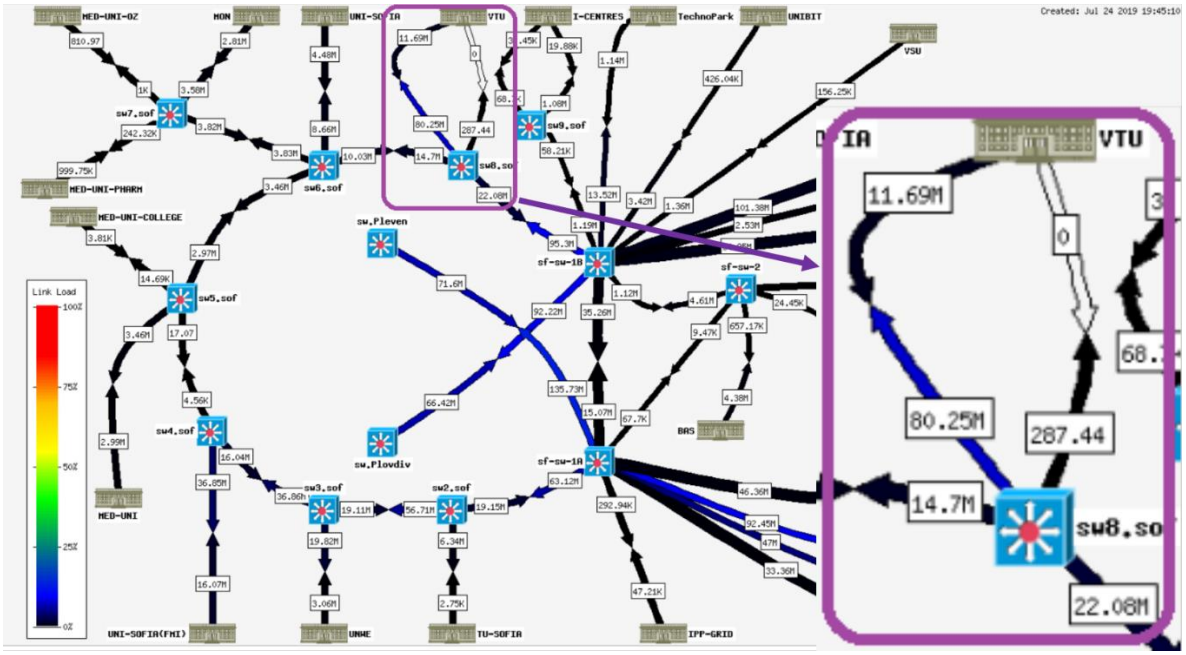
Фигура 3. Общ изглед на внедрената система за Cloud-базирана виртуализация.

На фиг. 4 се представя фрагмент от визуализиращия компонент за диагностика и следене работоспособността на мрежовите устройства и сървъри [8].



Фигура 4. Система за визуализация за диагностика и мониторинг на мрежовите устройства, сървъри и информационни системи.

На фиг. 5 се представя свързаността на университета с интернет, като част от общата академична мрежа [10].



Фигура 5. Графично представяне на структурата на университетската свързаност с интернет, като част от общата академична мрежа.

Основните web, mail услуги и др. се базират главно на Open Source операционни системи и специализирани информационни услуги [11, 12].

ОСИГУРЯВАНЕ НА СИГУРНОСТ И ЗАЩИТА НА СИСТЕМИТЕ И ДАННИТЕ

Използвания модел за внедряване и експлоатация на изградените информационни системи се основава на теоретични и приложни формулировки за осигуряване на защита и сигурност при работа на сървърите и системите, включително осигуряване на енергийна независимост от два градски електро източника и местни UPS панелни блока.

Практическата реализация се основава на адаптираните световни добри практики и приложни инструменти. Изградената система включва системи и ключове за криптиране на информацията и комуникациите в мрежата, системи за следене и детектиране на интрузия и действия на зловреден софтуер и потребители, както и система за предотвратяване и блокиране на нежелани действия и информационни събития дискредитиращи информационните системи и бази данни.

Архитектурата на NIDS работи с пренасочен трафик от рутерите / защитните стени и включва следните елементи:

-модул за предварителна обработка;

-модул за статистически анализ;

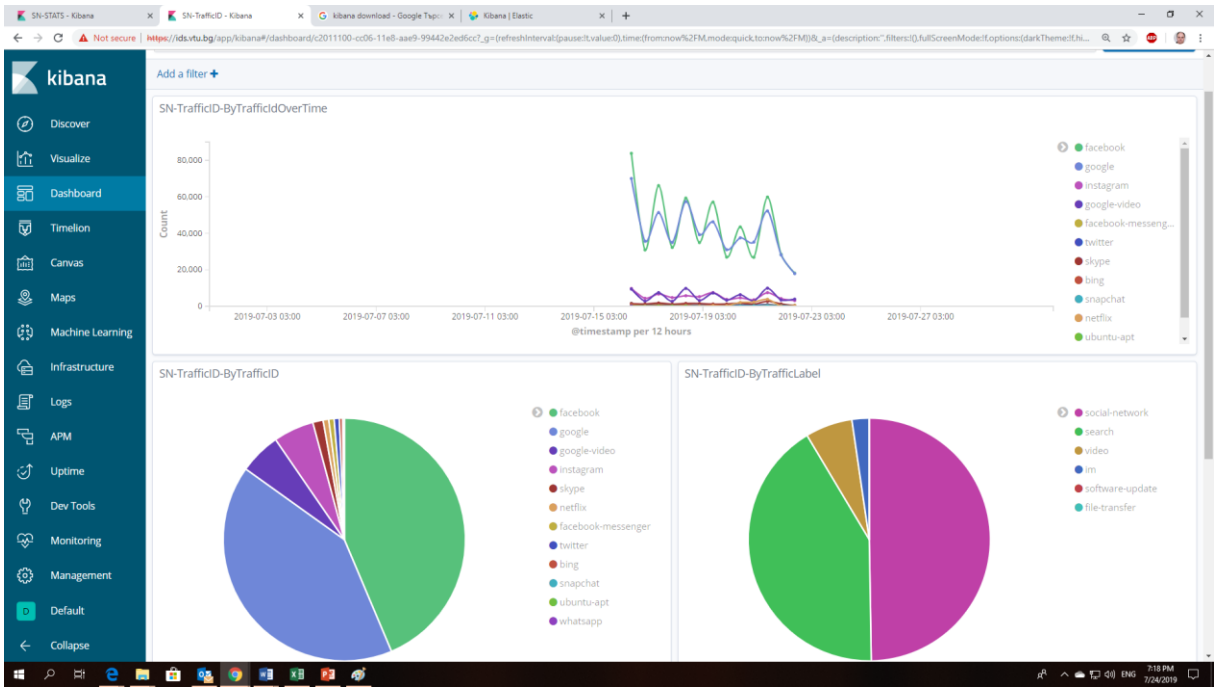
-модул за анализ на сигнатурата;

-база данни с предварително дефинирани подписи;

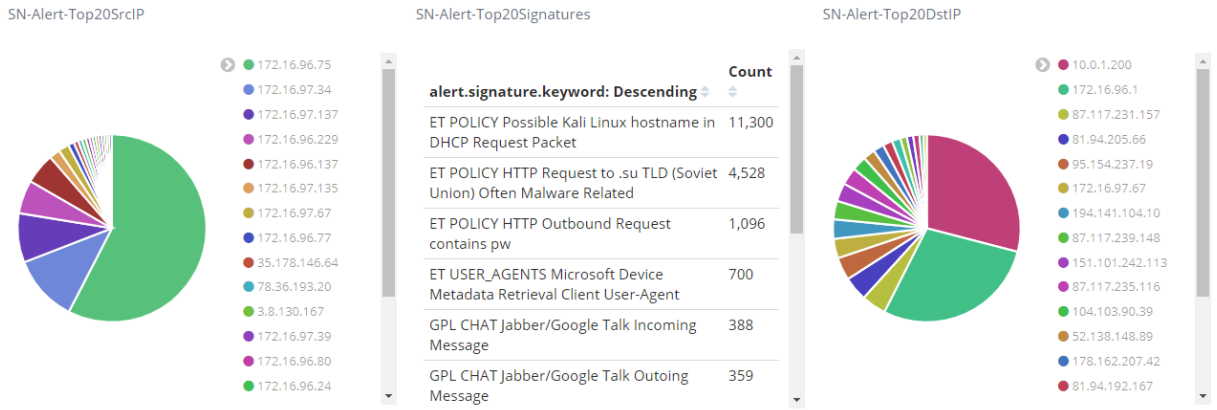
-база данни за открити аномалии;

-разумна логика, решаваща дали пакетът или източникът е интрудер или не.

На следващите фигури се представят резултатите от работата на внедрената в университетската мрежа система анализ на трафика. Входящият трафик по основните сегменти на мрежата се анализира и филтрира от NIDS, а визуализацията на резултатите се базира на графичния инструмент Kibana [9].



Фиг. 6. Общ изглед на основния визуализиращ екран на внедрената система NIDS.



Фиг. 7. Графики, показващи резултати от интрузионната активност в мрежата по протоколи на работа, сигнатури, адреси източници и адреси дестинации.

Внедрената NIDS система, част от която е показана на фигури 6 и 7, има много добър инструментариум за визуализация на интрузионните проблеми в мрежата. Възможностите за сечения и детайлизация на справките позволява на администраторите на мрежата да направят бърза и ефективна диагностика на проблемните сегменти точки. Това подпомага прилагането на ефективни мерки по филтриране на трафика и решаване на проблема с интрузията в мрежата.

ЗАКЛЮЧЕНИЕ

Настоящият доклад представи обобщен модел за Cloud-базирано управление на интернет трафика, сигурност и защита на данните в академична компютърна мрежа. Изграждането и усъвършенстване на тази система се превърна в целенасочена задача за откриване и ползване на така наречените „добри практики“ за планиране, внедряване и изграждане на подобни информационни системи, като са отчетени специфичните особености при внедряване на основните информационни и комуникационни модули.

Подходът и част от конкретните решения могат да се ползват и в друга академична институция или университет. Тази системата е в успешна експлоатация повече от десетилетие и постоянно се усъвършенства и модернизира, което свидетелства за нейната ефективност и полезност. Въпреки относително стабилната работа и малкото случаи на откази и дискредитиране, нейното развиване и поддържане става все по-актуално и все по-необходимо с оглед сложността на самите системи и потенциалните опасности от възникване на нежелани информационни инциденти. Въпросът е особено значим, тъй като те могат да бъдат използвани за неправомерни действия, а контролът и управлението на тези мрежи в повечето случаи е ниско бюджетно. Това прави въпроса комплексен, а търсенето на решение на проблема изисква висока степен на автоматизация и работна стабилност.

ЛИТЕРАТУРА:

[1] Димитров Д., Модел за изграждане на интегрирани информационни системи за управление на университети, , Издателство на ВТУ „Тодор Каблешков“, ISBN 978-954-12-0248-7, https://ddimitrov.vtu.bg/miiisuu.pdf, София, 2018г.

[2] Dimitrov D., Implementation of Contemporary Technologies in Virtualization and Construction of an Information Cloud of Systems for University Needs in the Field of Transport Education, , Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education – ICAICTSEE-2014, UNWE, Sofia, 2014.

[3] Dimitrov D., System for monitoring of the university computer network performance, , Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education – ICAICTSEE-2012, UNWE, Sofia, 2012.

[4] Димитров Д., Логическо развитие на мрежата в университетски кампус, , Сборник доклади на международна научна конференция "Приложение на информационните и комуникационни технологии в икономиката и образованието", ICAICTEE-2011, УНСС, София, 2011 г.

[5] Димитров Д., Проектиране и изграждане на автономна система за комплексно разпространение на интернет услуги в университетски кампус, , Научно списание „Механика Транспорт Комуникации”, ISSN 1312-3823, брой 3, 2011 г., статия № 0641, 2011 г.

[6] Grancharov A., Application model for developing and applying of university information systems, Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education – ICAICTSEE-2017, UNWE, Sofia

[7] https://www.proxmox.com/

[8] https://mikrotik.com/thedude

[9] https://www.elastic.co/products/kibana

[10] http://netmon.acad.bg/

[11] https://www.ubuntu.com/

[12] https://www.ispconfig.org/

CLOUD-BASED INTERNET TRAFFIC MANAGEMENT, DATA SECURITY AND DATA PROTECTION MODEL IN AN ACADEMIC COMPUTER NETWORK

Dimitar Dimitrov, Antony Grancharov
ddimitrov@vtu.bg, root@vtu.bg

Todor Kableshkov University of Transport,
158 Geo Milev Str., Sofia,
BULGARIA

Key words: *information security, information systems, internet, computer systems and networks, intrusion detection systems.*

Abstract: *The management and protection of the information systems in each organization, as well as the data in them, is a very high priority. Information systems in academic organizations are generally lower in budgetary terms, but they are nevertheless linked to a number of requirements regarding the protection of personal data, the provision of reliable financial operations and the provision of a range of information services related to their overall activity. This makes the task of providing the protection and management of academic information systems a real challenge.*

This report presents the approach used in the Todor Kableshkov University of Transport for providing and managing the traffic and the security of the information systems and the data in them. This approach is based on the long-term evolution of these technologies, using today's Cloud-based virtualization and information systems management solutions.