Инженерный вестник Дона, №10 (2023)
ivdon.ru/ru/magazine/archive/n10y2023/8724

Принципы создания архитектуры сервера для стабильной работы iTOP CMDB и обеспечения защиты сервера от хакерских атак

М.В. Радченко, А.М. Кумратова, К.А. Тарасенко, А.И. Василенко

Кубанский государственный аграрный университет, Краснодар

Аннотация: В развитии облачных провайдеров значительную роль играют не только виды услуг, которые они предоставляют, но и отказоустойчивость к сбоям работы сервисов. Провайдеру облачных услуг важно подготовить и настроить сервер и сервис к отказоустойчивой работе, чтобы заказчик работал с высокой степенью готовности и надежности в выделенной ему системе. Для подготовки такого сервера очень важно грамотно продумать архитектуру виртуальной машины, на которой будут установлены все необходимые средства обмена и интеграции данных для работы сервиса, а также настроена защита от сетевых угроз, которые могут нарушить работоспособность сервера. Целью работы является создание архитектуры виртуальной машины, защищенной от сетевых угроз, которая предоставляет заказчикам доступ к iTOP CMDB - системе. При том, что заказчиков может быть любое количество, iTOP CMDB - система должна предоставлять каждому заказчику свою версию, которую он может администрировать. Заходить в систему пользователь может с помощью интернет-браузера, введя имя своей организации в качестве домена. Авторами представлена демонстрация работы iTOP CMDB - системы, которая расположена на виртуальной машине, защищенной от сетевых угроз.

Ключевые слова: виртуальная машина, архитектура, межсетевой экран, iTOP CMDB - система, сервер, сетевая угроза, сетевая атака, IP-адрес, межсетевой экран, запрос.

В настоящее время в России в условиях импортозамещения и импортоопережения, растет спрос на системы с открытым исходным кодом и свободным доступом, а также на приложения отечественного производства.

Вопросам архитектуры сервера для бесперебойной работы и обеспечения защиты сервера от хакерских атак посвящены работы отечественных и зарубежных ученых [4–1]. В работах [4, 5] особое внимание уделено вопросам ускорения работы межсетевых экранов, а также точности обнаружения различных угроз в корпоративных компьютерных сетях.

В связи с этим, в статье будет разработана архитектура для внедрения iTOP CMDB - системы – программное обеспечение (ПО) с открытым исходным кодом для виртуальной машины (ВМ), защищенной от сетевых атак [4, 7].

Грамотная разработка архитектуры необходима для того, чтобы виртуальная машина смогла работать стабильно, без прерываний работы сервисов. Архитектура сервера является одним из ключевых факторов, которые обеспечивают защиту от хакерских атак. Хакеры могут использовать различные методы для взлома сервера, включая атаки на уязвимости в программном обеспечении, перехват данных, атаки на сетевые протоколы и многое другое. Но, с помощью правильной архитектуры сервера, можно значительно снизить риск взлома и обеспечить безопасность данных [4, 7].

Существуют два вида архитектуры взаимодействия клиент-сервер:

- двухзвенная архитектура клиент-серверного взаимодействия;
- многоуровневая архитектура взаимодействия.

Принцип работы двухуровневой архитектуры взаимодействия клиент-сервер заключается в том, что обработка запроса происходит на одной машине без использования сторонних ресурсов. Двухзвенная архитектура предъявляет жесткие требования к производительности сервера, но в то же время является очень надежной. Как многоуровневую архитектуру взаимодействия клиент-сервер, в качестве примера можно привести любую современную СУБД. Суть многоуровневой архитектуры заключается в том, что запрос клиента обрабатывается сразу несколькими серверами. Такой подход позволяет значительно снизить нагрузку на сервер из-за того, что происходит распределение операций, но в то же самое время данный подход не такой надежный, как двухзвенная архитектура [4–7].

Важным аспектом архитектуры сервера является выбор базы данных. Существует множество типов баз данных: реляционные, NoSQL, графовые, временные ряды и другие. Каждый из этих типов баз данных имеет свои особенности и подходит для разного типа приложений. Реляционные базы данных, например, хорошо подходят для приложений, в которых данные должны быть связаны между собой. NoSQL - базы данных хороши для

приложений с большими объемами данных и требований к масштабируемости.

Правильно подобранная архитектура сервера позволяет уменьшить нагрузку на сервер и ускорить работу приложения [8–10]. Она также делает приложение более надежным и устойчивым к сбоям. Например, если есть несколько серверов, работающих в кластере, и один из них выходит из строя, остальные серверы могут продолжать работу без проблем, взяв на себя нагрузку не работающего сервера. Другим важным аспектом архитектуры сервера является безопасность. Хакеры постоянно ищут уязвимости в веб-приложениях, поэтому безопасность должна быть на первом месте при разработке архитектуры сервера. Для защиты сервера необходимо придерживаться следующих принципов:

1. Разделение на слои. С этим методом функциональность сервера разделяется на отдельные слои, каждый из которых решает свою определенную задачу. Например, один слой отвечает за баннер в веб-приложении, а другой - за базу данных. Каждый слой может быть защищен отдельно с помощью шифрования данных, авторизации доступа, фильтрации входных данных, проверок входящего трафика и других способов.

2. Использование защищенных протоколов. Они являются очень важным принципом для архитектуры сервера. Эти протоколы пишутся, как SSL\TLS, они обеспечивают шифрование данных и подтверждение личности при обмене данными между клиентом и сервером.

3. Регулярные обновления. Они позволяют серверу оставаться защищенным от появляющихся новых угроз, т. к. обновления могут содержать исправления уязвимостей в программном обеспечении, которые помогают защитить сервер.

4. Мониторинг. Это инструмент, который обнаруживает проблемы сервера и сообщает о них оповещением на почту. С помощью него можно

отслеживать активность на сервере и предотвращать атаки, до того, как с сервером что-нибудь случится.

5. Логирование. Оно позволяет вести записи всей работы сервера, включая попытки неудачного входа, ошибки и другие события. Это дает возможность администраторам отслеживать проблемы и решать их.

6. Резервное копирование данных. Оно обеспечивает защиту сервера от потери данных, в случае поломки накопителя данных, взлома сервера, или при человеческой ошибке. И позволяет сохранить копии данных на других серверах, облачных хранилищах или на другом накопителе данных, что обеспечит восстановление потерянных данных в случае проблем на основном сервере.

На рисунке 1 представлена смоделированная архитектура сервера, для разворачивания приложения iTOP CMDB.

На этой модели архитектуры есть 2 взаимодействующих объекта, это пользователь из сети Интернет под своим ip-адресом и new Itop instance под выделенным для него белым ip-адресом.

Запрос от пользователя из сети интернет по запросу такого типа, как DOMANE_NAME.domain.ru, записанный в поисковой строке браузера, попадает на ВМ и обращается по 443 порту на прокси-сервер nginx, и определяет по имени сервера – DOMANE_NAME, к чьей именно ITOP CMDB-системе обращается пользователь и таким образом определяет, с каким портом необходимо отправить запрос для ITOP CMDB-системы, чтобы подключиться именно к нужной системе.

После подключения сама ITOP CMDB - система уже знает, как подключаться и какой конкретно БД находится в СУБД mariadb-server. Также, для полноценной и безопасной работы ВМ, необходимо настроить мониторинг и установить антивирус, для этого будет использоваться порт 10050 через приложение zabbix agent, а также Kaspersky client и Kaspersky

agent.

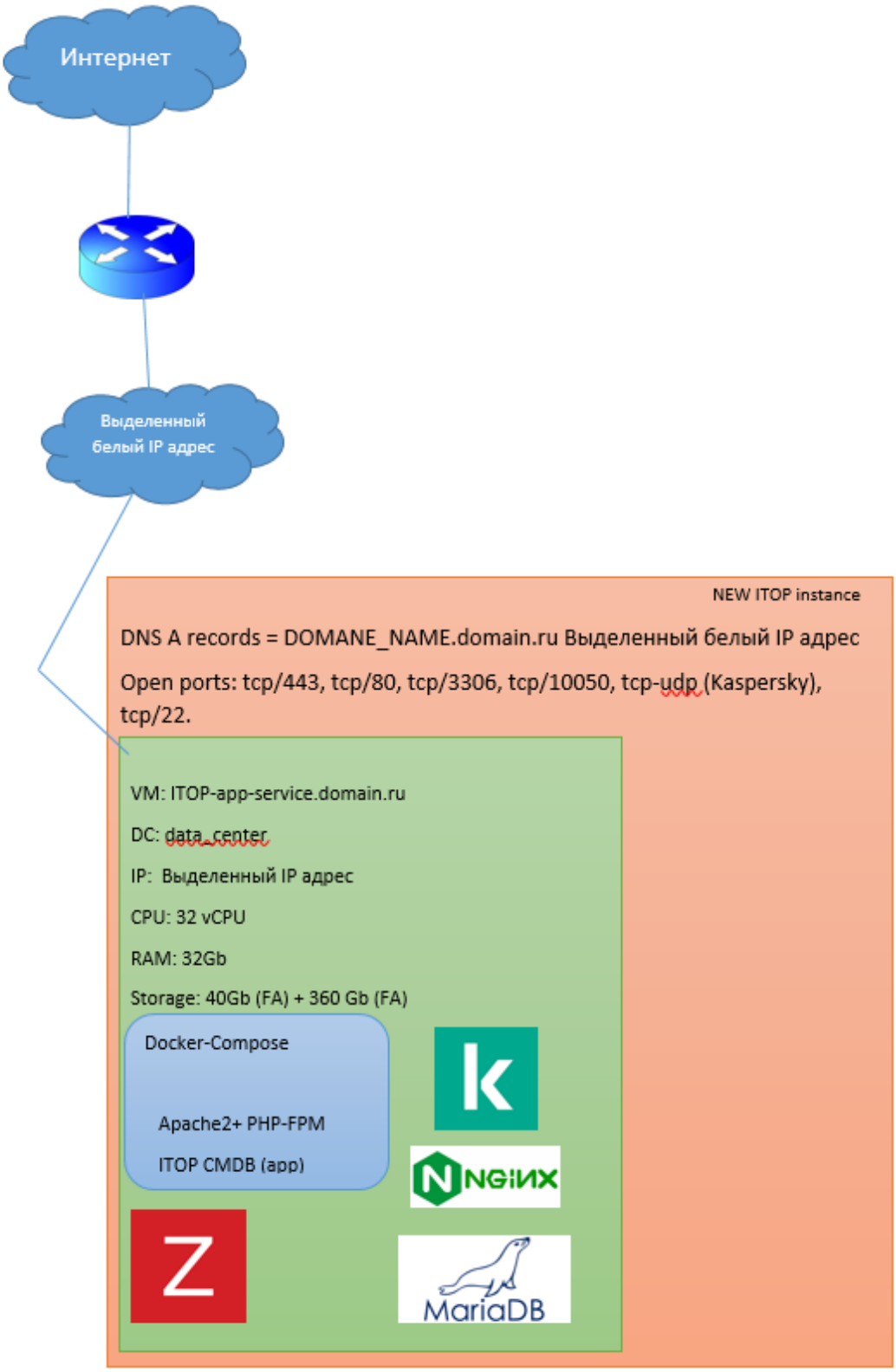

Рис. 1. – Архитектура ВМ, для работы ITOP CMDB – системы.

Поле того, как была составлена архитектура ВМ для работы сервиса,

необходимо составить архитектуру межсетевого экрана, чтобы обеспечить защиту виртуальной машины от сетевых угроз.

На рисунке 2 представлена схема работы межсетевого экрана для системы ITOP CMDB. Запрос, приходящий на ВМ по сети, должен прийти в цепочку «Prerouting», далее определяется, относится запрос к данной ВМ или нет, в запросе «route?». В случае, если запрос не относится к данной ВМ, он передается в цепочку «Forward», где будет отброшен. Если запрос относится к данной ВМ, то он передается в цепочку «INPUT», в данной цепочке должны быть прописаны правила для определения адресов, с которых приходят запросы на ВМ, если адреса прописаны, как разрешенные, то они проходят дальше, если же адреса не прописаны, то запросы, исходящие от них должны быть отброшены, что обеспечит защиту ВМ от DDOS атак и несанкционированного доступа. После проверки фильтром в цепочке «INPUT», запрос обрабатывается в цепочке «local process», внутри которой проверяется порт, является ли он tcp/443 или запрос идет по другому порту. Если запрос идет по tcp/443 порту, то его слушает nginx, который далее перенаправляет запрос на docker-compose по определенному порту, который он определяет по доменному имени, прописанному в запросе. Если же запрос не идет по порту tcp/443, то он будет обработан приложением, прослушиваемым портом, по которому и идет запрос, например, запрос в БД по tcp/3306.

Далее после обработки запрос попадает в цепочку «output», а затем - в цепочку «postrouting», в которых в принципе не требуется никаких дополнительных правил, так как если ВМ обработала запрос, то это значит, что он уже прошёл через цепочку с правилами, которые должны были его проверить.

После настройки ВМ по разработанной архитектуре и настройке её межсетевого экрана, можно заходить на сам сервис, введя в поиск доменное

имя компании, для которой настраивалась система. Вход на iTOP CMDB - систему показан на рисунке 3.

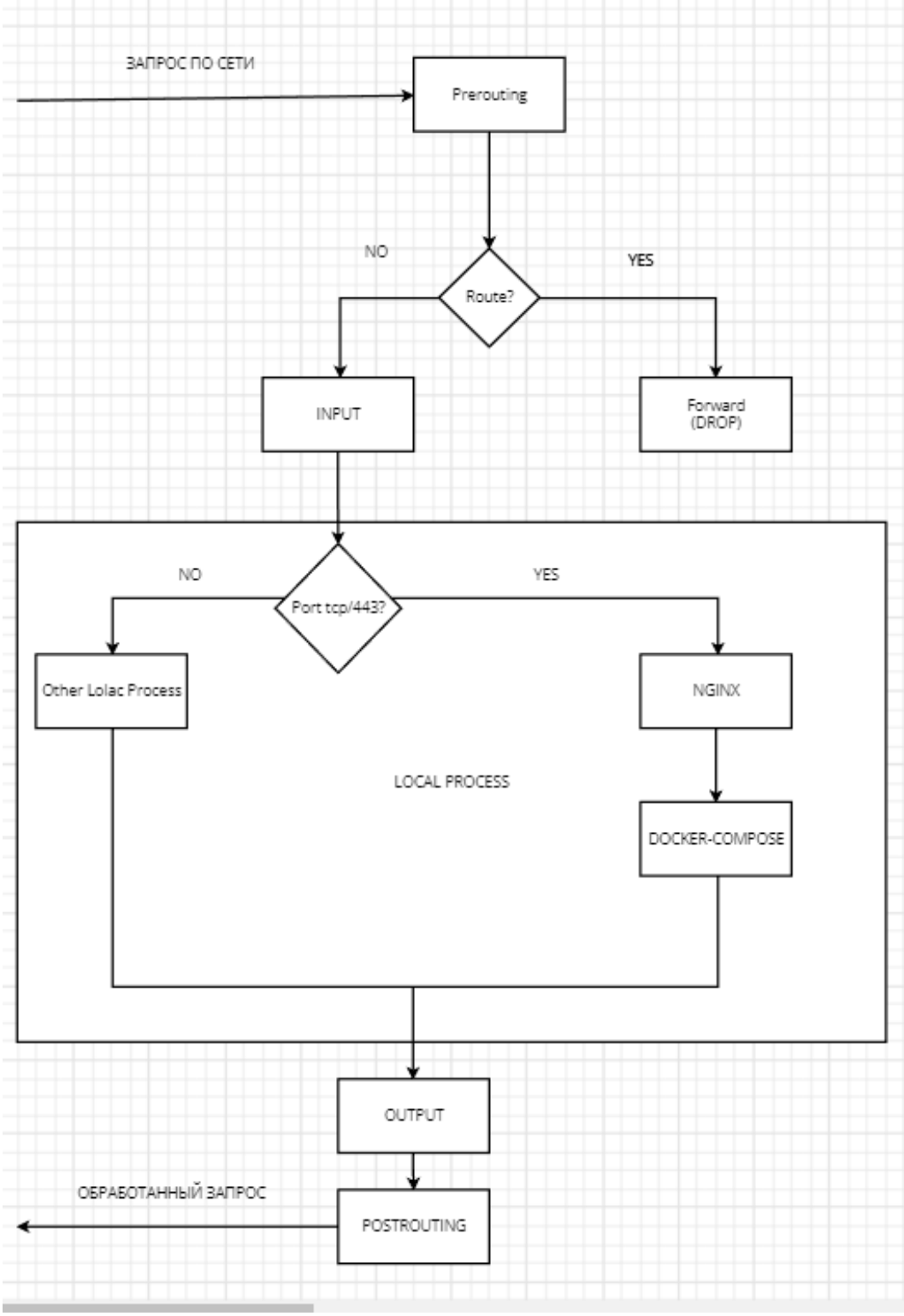

Рис. 2. – Схема работы межсетевого экрана iptables

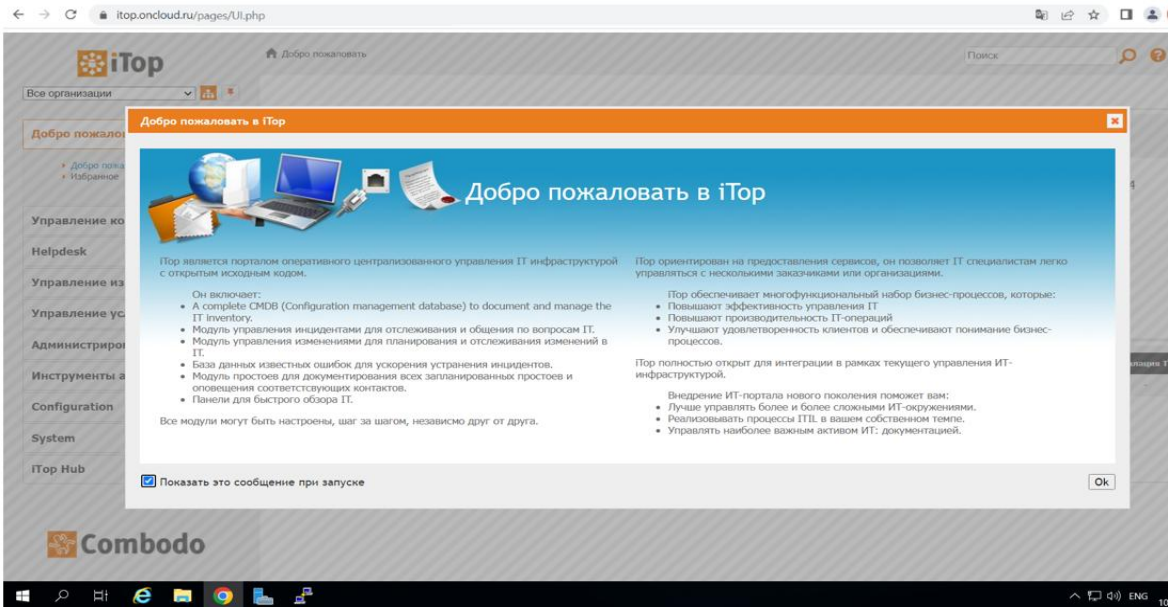

Рис. 3. – Приветственное сообщение при входе в iTOP CMDB - систему

При входе в приложение, пользователя встречает главное меню с приветственным сообщением, что означает, что приложение полностью работоспособно, и имеет подключение к базе данных. Также можно увидеть, что приложение имеет свой ip-адрес, который скрыт под доменным именем. Для каждого заказчика настраивается собственный домен, с сертификатом, что гарантирует безопасное соединение с сервером.

На рисунке 4 показан интерфейс главного меню.

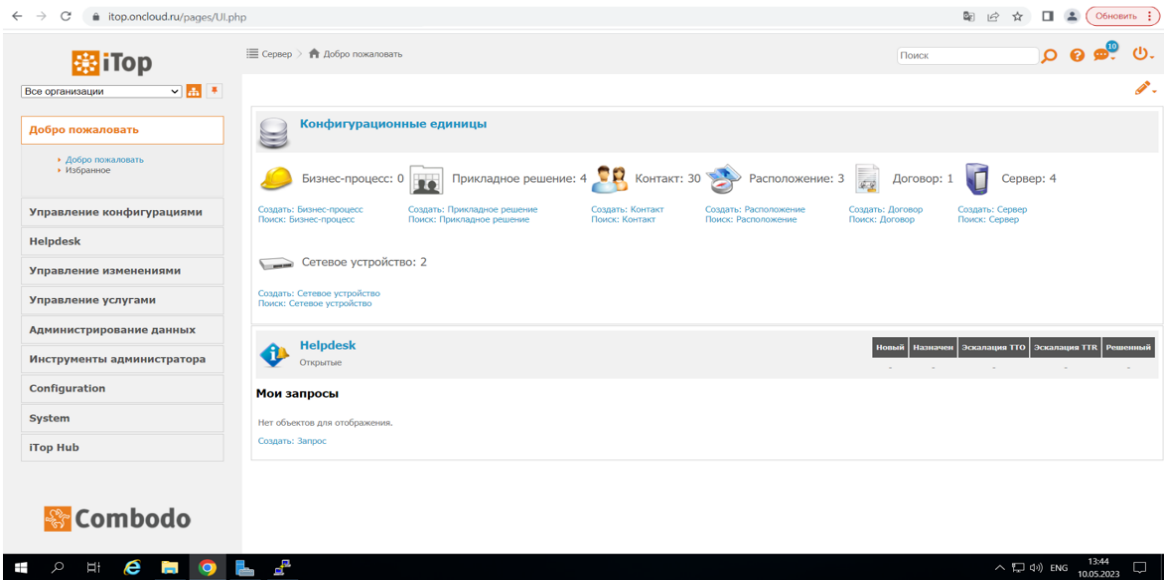

Рис. 4. – Главное меню iTOP CMDB - системы

В самом приложении пользователь может создавать пользователей, выдавать им права, настраивать права для каждого отдельного пользователя. Также в нем можно создавать карту сетей, обращения, базу принадлежностей конфигурационных единиц и многое другое, что может помочь любой компании работать более эффективно.

С данной архитектурой можно создавать на одной машине несколько контейнеров iTOP CMDB, которые будут работать с собственными базами данных и изолированно друг от друга, что позволяет создать для разных групп пользователей различных компаний собственные инстансы.

В результате реализации создана архитектура виртуальной машины для внедрения iTOP CMDB - системы, защищенной от сетевых атак. Также были рассмотрены способы обезопасить архитектуру сервера.

Для автоматизации создания отдельных инстансов можно разработать модуль, который будет разворачивать конфигурацию сервера под новый инстанс, а также добавлять запись в докер-композ и запускающий контейнер.

Разворачивания iTOP CMDB - системы позволят компаниям внедрять методологию ITIL, что приведет к сокращению издержек компаний, и позволит ввести историю перераспределения конфигурационных единиц. Также сама система очень гибкая и позволит пользователям настроить её, исходя из своих потребностей.

Литература

1. Xiong J., Wu J. Construction of information network vulnerability threat assessment model for CPS risk assessment // Computer Communications. – 2020. – Vol. 155. – pp. 197-204.

2. Lipatnikov V., Tikhonov V., Shevchenko A., Saharov D., Polyanicheva A. Security management in large-scale heterogeneous network systems based on intelligent information security services // ACM International

Conference Proceeding Series: 5, The Premier Conference on Smart Next Generation Networking Technologies, Virtual, Online, 15–16 декабря 2021 года. – Virtual, Online, 2021. – pp. 562–567.

3. Chen Z., Zuo X., Dong N., Hou B. Application of network security penetration technology in power internet of things security vulnerability detection // Transactions on Emerging Telecommunications Technologies. – 2019. – P. e3859.

4. Федоров В. А., Щипцов Д. И. Анализ релевантных решений оптимизации межсетевых экранов для их применения в корпоративных компьютерных сетях // Инновации. Наука. Образование. – 2021. – № 33. – С. 1071–1076.

5. Безродных О. А. Использование различных межсетевых экранов нового поколения для защиты корпоративной сети от сетевых атак // Инновации. Наука. Образование. – 2022. – № 50. – С. 1693–1702.

6. Гребешков А. Ю. Стандарты и технологии управления сетями связи. – Москва: «Эко-Трендз», 2003. – 288 с.

7. Громов Ю. Ю., Карасев П. И., Коршунов Д. С., Паршенкова Ю. А. Межсетевые экраны АСУ и принцип их работы // Промышленные АСУ и контроллеры. – 2023. – № 3. – С. 24–29.

8. Ибрагимова З. М., Батчаева З. Б. Ткаченко А. Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона. – 2022. – № 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

9. Кацупеев А. А., Щербакова Е. А., Воробьев С. П. Постановка и формализация задачи формирования информационной защиты распределённых систем // Инженерный вестник Дона. – 2015. – № 1, ч.2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2868.

10. Куликова О. В., Пиневич Е. В., Волохов А. С., Домбаян Г.С., Егоров Н.В. Оценка защищенности информации при передаче данных между субъектами доступа в клиент-серверной архитектуре // Инженерный вестник Дона. – 2021. – № 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6900.

11. Менциев А.У., Джангаров А.И. VoIP security threats // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636/.

References

1. Xiong J., Wu J. Computer Communications. 2020. Vol. 155. Pp. 197-204.

2. Lipatnikov V., Tikhonov V., Shevchenko A., Saharov D., Polyanicheva A. ACM International Conference Proceeding Series: 5, The Premier Conference on Smart Next Generation Networking Technologies, Virtual, Online, Virtual, Online, 2021. Pp. 562–567.

3. Chen Z., Zuo X., Dong N., Hou B. Transactions on Emerging Telecommunications Technologies. 2019. P. e3859.

4. Fedorov V. A., Shhipczov D. I. Innovacii. Nauka. Obrazovanie. 2021. № 33. Pp. 1071–1076.

5. Bezrodny`x O. A. Innovacii. Nauka. Obrazovanie. 2022. № 50. Pp. 1693–1702.

6. Grebeshkov A. Yu. Standarty` i texnologii upravleniya setyami svyazi [Communication network management standards and technologies]. Moskva: «E`ko-Trendz», 2003. 288 p.

7. Gromov Yu. Yu, Karasev P. I., Korshunov D. S., Parshenkova Yu. A. Promy`shlenny`e ASU i kontrollery`[Industrial automated control systems and controllers]. 2023. № 3. Pp. 24–29.

8. Ibragimova Z. M., Batchaeva Z. B. Tkachenko A. L. Inzhenernyj vestnik Dona. 2022. № 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

9. Kaczupeev A. A., Shherbakova E. A., Vorob`ev S. P. Inzhenernyj vestnik Dona. 2015. № 1, ch.2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/286810.

10. Kulikova O. V., Pinevich E. V., Voloxov A. S., Dombayan G.S., Egorov N.V. Inzhenernyj vestnik Dona. 2021. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6900.

11. Mentsiev A.U., Dzhangarov A.I. Inzhenernyj vestnik Dona, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636/.