РОБОТА ТА МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ В УМОВАХ ВОЄННОГО СТАНУ

Автори: *Трибулькевич С.Л., ст. викладач; Трибулькевич В.В., аспірантка, Національній університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Більшість сучасних бізнес та технологічних процесів оцифровані та пов'язані з роботою IT-систем, таких як ERP, CRM, SCADA, тощо. Тому будь-які збої в IT-інфраструктурі спричиняють фінансові та репутаційні втрати для бізнесу. Робота підприємства в умовах воєнного стану пов’язана з деякими труднощами у функціонуванні IT підсистем, якими можуть являться відсутність електроживлення, труднощі у системах зв’язку, руйнування мережевої інфраструктури через обстріли.

Для безперебійного функціонування мережевого та серверного обладнання у складних умовах необхідно виконання таких заходів:

– резервування живлення за рахунок використання генераторів та оснащення критичного обладнання джерелами безперебійного живлення;

– резервування каналів виходу у мережу Інтернет шляхом використання різних провайдерів, а також мобільних або супутникових технології;

– надання працівникам, що евакуювалися у інші міста України та світу, захищених каналів доступу до внутрішньої мережі підприємства;

– резервування каналів зв’язку у внутрішній мережі шляхом прокладки кабелів різними маршрутами та використанням бездротових технологій;

– своєчасне копіювання даних у локальні та хмарні сховища резервних копій;

– постійний моніторинг мережі та серверного обладнання, сповіщення про виникнення аварійних ситуацій.

Моніторинг роботи мережевого устаткування та ключового ПО – це одна з найважливіших задач системного адміністрування. Сучасні комп’ютерні системи побудовані на мережі Internet, або об’єднані в локальну мережу з подальшим виходом до Internet. Ураховуючи сучасний стан інформаційних і комунікаційних технологій для концентрації інформації щодо комп’ютерних мереж постає проблема моніторингу. Доцільним є створення програм мережевого моніторингу для

забезпечення доступу до інформації, стосовно мережевого контенту, топології, обладнання як спеціалістів так і користувачів.[1]

Zabbix – це повномасштабний інструмент для мережного й системного моніторингу мережі, який поєднує кілька функцій в одній веб-консолі. Він може бути сконфігурован для моніторингу й збору даних із самих різних серверів і мережних пристроїв, забезпечуючи обслуговування й моніторинг продуктивності кожного об'єкта. Zabbix дозволяє робити моніторинг серверів і мереж за допомогою широкого набору інструментів, включаючи моніторинг гіпервізорів віртуалізації й стеков веб-додатків.

В основному, Zabbix працює із програмними агентами, запущеними на контрольованих системах. Але цей розв'язок також може працювати й без агентів, використовуючи протокол SNMP або інші можливості для здійснення моніторингу. Zabbix підтримує VMWare і інші гіпервізори віртуалізації, надаючи докладні дані про продуктивність гіпервізор і його активності. Особлива увага також приділяється моніторингу серверів додатків Java, веб-сервісів і баз даних.

Zabbix дозволяє набудовувати панелі моніторингу й веб-інтерфейс, щоб сфокусувати увагу на найбільш важливих компонентах мережі. Повідомлення й ескалації проблем можуть ґрунтуватися на діях, що настроюються, які застосовуються до хостів або груп хостів. Дії можуть навіть настроюватися для запуску віддалених команд, тому якийсь ваш сценарій може запускатися на контрольованому хості, якщо спостерігаються певні критерії подій.

Програма відображає у вигляді графіків дані про продуктивність, такі як пропускна здатність мережі й завантаження процесора, а також збирає їх для систем, відображення, що настроюються. Крім того, Zabbix підтримує карти, що настроюються, екрани й навіть слайд-шоу, що відображають поточний статус контрольованих пристроїв.

Zabbix може бути складним для реалізації на початковому етапі, але розумне використання автоматичного виявлення й різних шаблонів може частково полегшити труднощі з інтеграцією. На додаток до встановлюваного пакета, Zabbix доступний як віртуальний пристрій для декількох популярних гіпервізорів.

Дуже зручно переглядати працездатність пристроїв на мапі (рис. 1). Також з вікна мапи можна викликати вікна Dashboard пристроїв для перегляду детальної інформації або запуску простих тестів.

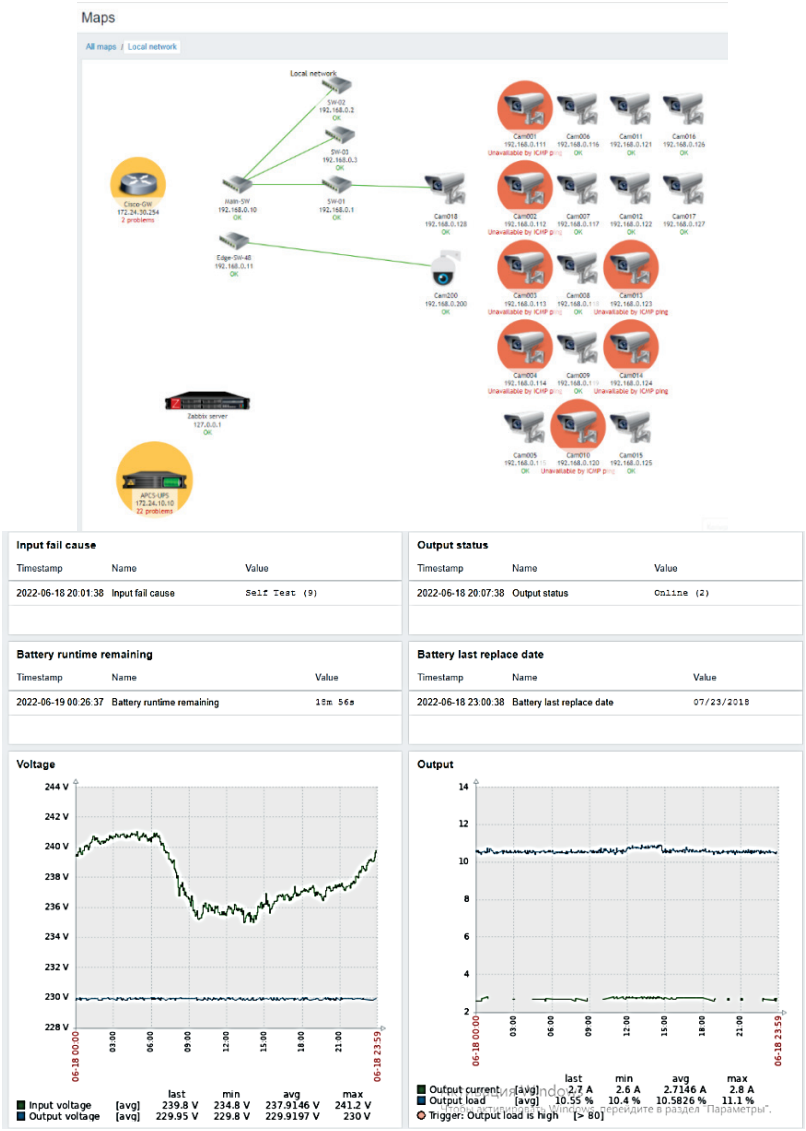

Рисунок 1 – Система моніторингу

Якщо потрібно включити в систему обладнання, що не має мережених інтерфейсів, то можна використати перетворювачі інтерфейсів Ethernet – RS232. У даному випадку інформаційний обмін може бути реалізовано шляхом використання спеціалізованих драйверів віртуальних послідовних портів. Шляхом тестування подібного програмного забезпечення визначено, що найбільш функціональним є Null-modem emulator [2] це драйвер віртуального послідовного порту Windows, який працює в режимі ядра (kernel-mode driver), з відкритим вихідним кодом, доступний під захистом ліцензії GPL. Null-modem emulator дозволяє створювати необмежену кількість пар віртуальних COM-портів. Кожна пара COM-портів складається з двох COM-портів, віртуально з'єднаних один з одним каналом даних. Вихід одного COM-порту пари з'єднується з входом іншого COM-порту пари, і навпаки. Отже, можна використовувати будь-яку пару для з'єднання будь-якої однієї програми, розрахованої на роботу з COM-портом, з іншим додатком, що також працює з COM-портом, і вони будуть передавати дані один одному. Єдиним знайденим недоліком даного програмного забезпечення є відсутність цифрового підпису драйверів, що ускладнює встановлення у сучасних операційний системах.

На стороні ПК за зв'язок відповідають 3 пари послідовних портів, об'єднаних одним концентратором (рис. 2):

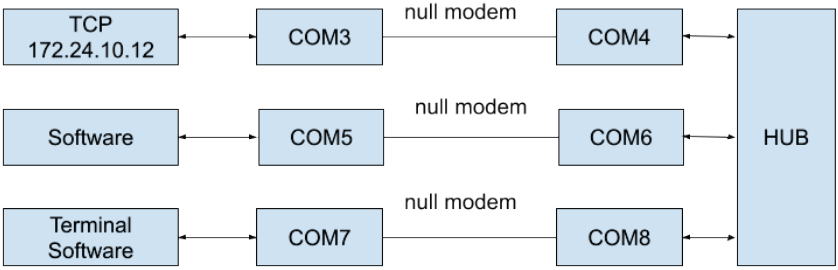

Рисунок 2 – Схема послідовних портів

– Пара COM3-TCP відповідає за зв'язок з обладнанням. 172.24.10.12 – IP адреса перетворювача Ethernet – RS232;

– Пара COM5-Software призначена для опитування та видачі параметрів за допомогою існуючого програмного забезпечення;

– Пара COM7-Terminal Software призначене для діагностики за будь-якого термінального ПЗ, наприклад, Putty.

Дана схема використовується для моніторингу роботи джерел безперебійного живлення APC Smart SMC1500I-2U не оснащених UPS Network management card. Дане рішення дозволяє перекласти роль моніторингу та керування завершенням роботи фізичних серверів на віртуальну машину, подібна ситуація наступає у разі складнощів при розгортанні оригінального програмного забезпечення від виробника джерела безперебійного живлення напряму у операційній системі Server Core гіпервізору. Експлуатація даного обладнання показала роботоспроможність даної схеми, стабільність виводу параметрів у стандартне програмне забезпечення для ПК, широкі можливості по маршрутизації потоків даних між віртуальними послідовними портами та можливість перехвату потоку даних, його аналізу та передачі у інше програмне забезпечення, відмінне від стандартного.

Для віддаленого доступу користувачів використовуються різноманітні протоколи VPN. Протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol) – це протокол, винайдений Microsoft для організації VPN через мережі комутованого доступу. PPTP є стандартним протоколом для побудови VPN вже багато років. Хоча PPTP зазвичай і використовується зі 128-бітовим шифруванням, у наступні кілька років після включення цього протоколу до складу Windows 95 OSR2 у 1999 році було знайдено низку вразливостей. Найбільш серйозною з яких стала вразливість протоколу аутентифікації MS-CHAP v.2. Використовуючи цю вразливість, PPTP було зламано протягом 2 днів. І хоча компанією Microsoft було виправлено цю помилку (за рахунок використання протоколу аутентифікації PEAP, а не MS-CHAP v.2), вона сама рекомендувала до використання як VPN проколів L2TP або SSTP.

Протокол тунелювання 2 рівня (Layer 2 Tunnel Protocol) – це протокол VPN, який сам по собі не забезпечує шифрування та конфіденційність трафіку, що проходить через нього. З цієї причини зазвичай використовується протокол шифрування IPsec для забезпечення безпеки та

конфіденційності. L2TP/IPsec вбудований у всі сучасні операційні системи та VPN-сумісні пристрої, і так само легко може бути налаштований як і PPTP (зазвичай використовується той самий клієнт). Проблеми можуть виникнути в тому, що L2TP використовує UDP-порт 500, який може бути заблокований файрволом, якщо ви за NAT. Тому може знадобитися додаткове налаштування роутера (переадресація портів).

Протокол IPsec на даний момент не має жодних серйозних уразливостей і вважається дуже безпечним під час використання таких алгоритмів шифрування, як AES. Однак, оскільки він інкапсулює дані двічі, це не так ефективно, як рішення SSL (наприклад, OpenVPN або SSTP), і тому працює трохи повільніше.

Протокол безпечного тунелювання сокетів (Secure Socket Tunneling Protocol) – був представлений Microsoft у Windows Vista SP1, і хоча він тепер доступний на Linux, RouterOS та та ін., він, як і раніше, використовується значною мірою лише Windows-системами. SSTP використовує SSL v.3 і, отже, пропонує аналогічні переваги, що і OpenVPN (наприклад, можливість використовувати TCP-порт 443 для обходу NAT).

OpenVPN є програмним додатком з відкритим вихідним кодом, який використовує можливості віртуальної приватної мережі (VPN) для створення захищених з'єднань точка-точка або сайт-сайт на всьому маршруті інформації, а також при використанні містків конфігурацій дистанційно. Всередині OpenVPN використовуються протоколи безпеки SSL (Secure Socket Layer – рівень захищених сокетів) або TLS (Transport Layer Security – безпека транспортного рівня), за допомогою яких користувачі можуть обмінюватися ключами.

OpenVPN є досить новою технологією з відкритим кодом, яка використовує бібліотеку OpenSSL та протоколи SSLv3/TLSv1, поряд з багатьма іншими технологіями для забезпечення надійного VPN-рішення. Однією з його головних переваг є те, що OpenVPN дуже гнучкий у налаштуваннях. Цей протокол може бути налаштований на роботу на будь-якому порту, у тому числі на 443 TCP-порту, що дозволяє маскувати трафік усередині OpenVPN під звичайний HTTPS (який використовує, наприклад, Gmail) і тому його важко заблокувати.

Отже OpenVPN має найбільш високу захищеність, можливість використання у будь-яких операційних системах таких, як Windows,

Linux, Android, Mac OS та iOS, можливість використовувати 443 TCP порт для маскування трафіку та обходу блокування провайдерами GRE трафіку. Саме тому даний протокол було використано для віддаленого доступу користувачів через канали зв'язку з невизначеними блокуваннями та з будь-яких персональних пристроїв.

OpenVPN сервер легко реалізувати на будь-якій операційній системі Linux та налаштувати одним із готових скриптів. Також можлива реалізація серверу у RouterOS, але щоб повноцінно використовувати OpenVPN-сервер на Mikrotik, потрібно оновити версію прошивки до версії 7.1 і вище, крім того, у Mikrotik OpenVPN трохи урізаний: немає підтримки UDP (додали до стабільної версії RouterOS 7.1), немає LZO-компресії. Тому при готовому середовище віртуалізації роль сервера віддаленого доступу віддано віртуальній машині Debian (рис. 3).

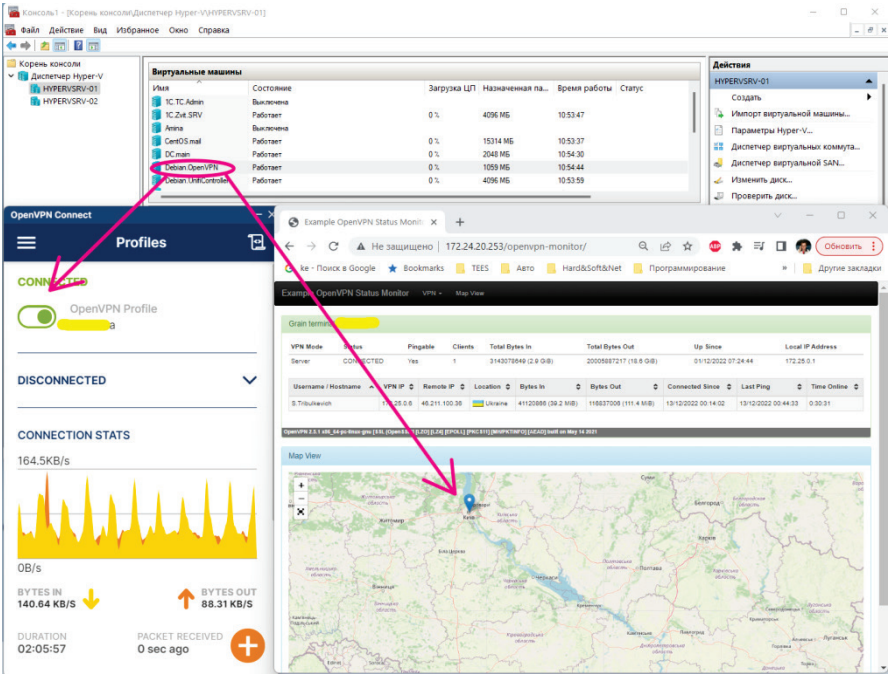

Рисунок 3 – Сервер та клієнт OpenVPN

При використанні стаціонарних провайдерів зв'язку зовнішня «біла» IP адреса може бути визначена за рахунок служб DNS та динамічного оновлення А записів при переключенні між основним та резервними каналами зв'язку. При переході на доступ в інтернет через мережі стільникового зв'язку або тимчасовому переміщенні серверного обладнання у безпечні місця, отримання «білої» IP адреси може бути не можливим, тоді найбільш простим способом побудови роботи мережі VPN є сервер у хмарі, у даному випадку системні вимого до серверу невисокі та можливе використання не дорогих VPS.

Однією із найбільш ефективних систем резервного копіювання є Veam Backup and Replication (рис. 4), яка забезпечує бізнес-стійкість, захист даних від зловмисників, запобігання втратам даних і вимушеним простоям. Надійне перенесення даних у хмару та відсутність прив'язки до постачальника завдяки мобільності хмарних рішень. Доступні варіанти інтеграції з більш ніж 100 системами зберігання даних та хмарними інфраструктурами. Це означає максимальну гнучкість та оптимальну сукупну вартість володіння.

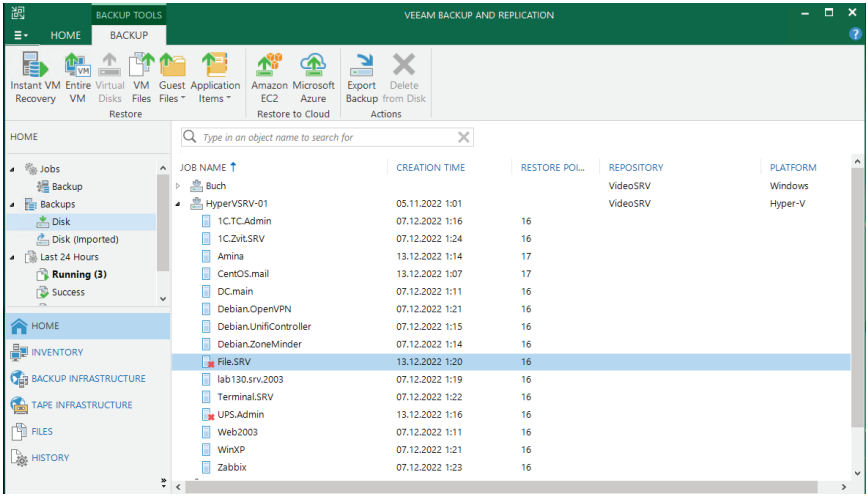

Рисунок 4 – Veam Backup and Replication

Veeam надає гнучке комплексне рішення, яке захищає дані чотирма різними способами та гарантує дотримання вимог до RPO та RTO.

Для захисту невеликої кількості фізичних та віртуальних машин є безкоштовні редакції.

Висновок: Надано загальні рекомендації по роботі IT інфраструктури підприємства малого та середнього бізнесу. Дані рекомендації справедливі незалежно від умов воєнного чи мирного часу, але в умовах саме воєнного часу себе проявляють найбільш тонкі місця IT інфраструктури. Своєчасне реагування на сповіщення систем моніторингу дозволяють забезпечити стабільну та безперебійну роботу наскільки це можливо в даних умовах.

Список літератури:

1. Гузій, М. М., Станіславова, О. В., Кадет, М. В. Аналіз технологій моніторингу комп'ютерних мереж. Наукоємні технології, № 1, 2009. Відновлено з https://jrnl.nau.edu.ua/index.php/SBT/article/view/5091
2. Null-modem emulator (com0com). Відновлено з http://com0com.sourceforge.net/

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РЕЖИМНО-СЕКРЕТНОГО ВІДДІЛУ МОРСЬКОГО ПОРТУ

Автор: *Харченко М.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Баронова О.А., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Морський транспортний комплекс є багатофункціональною структурою, що задовольняє потреби національної економіки у транспортному забезпеченні. Від ефективності функціонування морських портів, рівня їх технологічного та технічного оснащення, відповідності системи управління та розвитку інфраструктури сучасним міжнародним вимогам залежить конкурентоспроможність вітчизняного транспортного комплексу на світовому ринку.

Після вторгнення РФ портова галузь України була паралізована. Чотири морські порти – Херсонський, Скадовський, Бердянський та