УДК 004.722

Є. Р. Сорока
Л. А. Савицька

МЕТОД АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ VPN-ТУНЕЛІВ SITE-TO-SITE НА ОСНОВІ КОНТЕЙНЕРИЗАЦІЇ

Вінницький національний технічний університет

Анотація

Запропоновано удосконалений метод автоматизованого розгортання site-to-site IPsec VPN-тунелів у контейнеризованому середовищі, який не порушує роботи наявних з'єднань. Метод поєднує підключення керованих конфігураційних фрагментів до наявного файлу ipsec.conf через директиву include з монотонним розподілом ідентифікаторів reqid, узгодженим з найбільшим значенням в основній конфігурації. На основі методу розроблено програмний комплекс із серверною частиною на Node.js, вебінтерфейсом на React і CLI-клієнтом. Експериментальна перевірка на тестовому стенді показала, що під час 10 послідовних операцій додавання нових тунелів унікальний ідентифікатор і SPI наявного тунелю не змінюються.

Ключові слова: VPN, site-to-site, IPsec, strongSwan, контейнеризація, Docker, автоматизація розгортання, reqid.

Abstract

An improved method for the automated deployment of site-to-site IPsec VPN tunnels in a containerized environment is proposed. The method does not disrupt existing connections. It combines attaching managed configuration fragments to an existing ipsec.conf file through the include directive with monotonic allocation of reqid identifiers, aligned with the largest value in the main configuration. Based on the method, a software suite has been developed with a Node.js server, a React web interface and a CLI client. An experiment on a test bench showed that the unique identifier and SPI of an existing tunnel remain unchanged during 10 consecutive operations of adding new tunnels.

Keywords: VPN, site-to-site, IPsec, strongSwan, containerization, Docker, deployment automation, reqid.

Вступ

Підприємства з розподіленою інфраструктурою з'єднують свої майданчики site-to-site VPN-тунелями на основі IPsec [1, 2]. Для зв'язку з обладнанням сторонніх організацій IPsec лишається практичним стандартом, бо дозволяє узгодити саме той набір криптографічних алгоритмів, який вимагає протилежна сторона. Ціна цього – складна конфігурація: сторони мають погодити десятки параметрів двох фаз IKE та ESP.

У реалізації strongSwan тунелі здебільшого описують у класичному файлі ipsec.conf [3]. Новий тунель додають ручним редагуванням цього файлу з перезапуском демона, і на час зміни розриваються всі активні з'єднання. Зі зростанням кількості тунелів частішають помилки в параметрах і колізії ідентифікаторів reqid у підсистемі ядра Linux XFRM [4]. Інтерфейс swanctl/vici дозволяє завантажувати окремі з'єднання програмно, але перехід на нього вимагає міграції всієї наявної конфігурації і перевстановлення всіх тунелів [5]. Тому потрібен метод автоматизації, який вбудовується в наявну конфігурацію і не перериває роботу вже встановлених з'єднань.

Результати дослідження

Метод ґрунтується на двох положеннях. Перше – неінвазивна інтеграція. У кінець наявного ipsec.conf один раз додається директива include /etc/ipsec.d/managed/*.conf, а в ipsec.secrets – аналогічна директива для каталогу ключів. Після цього програмний комплекс основні файли не редагує: створення, зміна чи видалення тунелю зводяться до запису або видалення окремого файлу в керованому каталозі та виконання команд ipsec rereadall і ipsec update, які застосовують зміни без перезапуску демона charon. Тунелі, описані безпосередньо в ipsec.conf, лишаються поза керуванням комплексу. Механізм інтеграції наведено на рисунку 1.

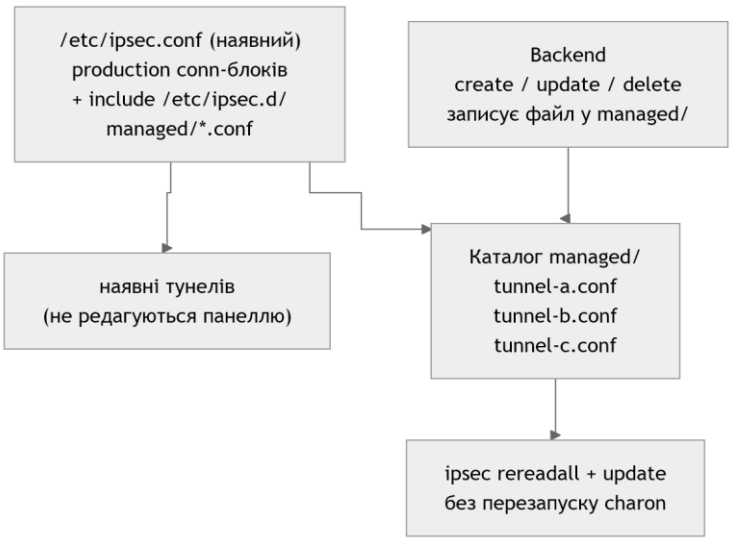


Рисунок 1 – Механізм неінвазивної інтеграції через директиву include

Друге положення – безконфліктний розподіл reqid. Цей параметр пов'язує політику безпеки із захищеною асоціацією в ядрі [4]. Якщо покладатися на автоматичне присвоєння або повторно використовувати значення видалених тунелів, залишкові стани ядра можуть посилатися на старе значення, і трафік різних тунелів змішується. Тому reqid нового тунелю видається за монотонним лічильником, який ніколи не зменшується. Перед кожною видачею значення лічильника порівнюється з найбільшим reqid серед з'єднань основного файлу ipsec.conf. Новий тунель отримує більше з цих двох значень, збільшене на одиницю.

Видача значення і збільшення лічильника виконуються в одній транзакції бази даних, тож два паралельні запити не отримають однаковий reqid. Значення керованих і некерованих тунелів не перетинаються, а звільнені після видалення тунелю значення в обіг не повертаються.

На основі методу розроблено програмний комплекс. strongSwan працює в окремому контейнері Docker у режимі network_mode: host, оскільки демону потрібен доступ до таблиці маршрутизації та підсистеми XFRM хоста [6]. Серверна частина на Node.js працює в іншому контейнері, зберігає дані в SQLite і керує strongSwan через docker exec. Вебінтерфейс на React і CLI-клієнт звертаються до неї через REST API. Крім того, комплекс виконує такі функції:

- зберігання ключів PSK у шифрованому вигляді з переглядом лише після повторного введення пароля;
- автоматичний перезапуск з'єднань, що завершилися у стані CONNECTING довше заданого часу;
- сповіщення оператора про відмову та відновлення тунелів;
- журнал аудиту всіх дій, що змінюють стан системи.

Архітектуру програмного комплексу наведено на рисунку 2.

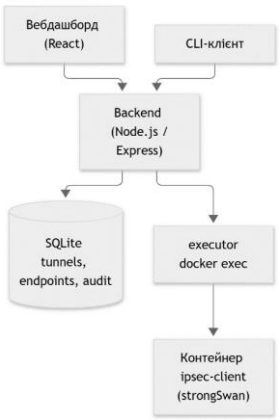


Рисунок 2 – Архітектура програмного комплексу

Метод перевірено на тестовому стенді з hub-вузлом і двома віртуальними машинами VirtualBox зі strongSwan 6.0.4 та 5.9.13. Один тунель встановлювався поза керуванням комплексу, після чого через REST API послідовно додавалися нові керовані тунелі. До і після кожної операції фіксувалися унікальний ідентифікатор з'єднання та пара IKEv2 SPI, які змінюються при будь-якому перевстановленні захищеної асоціації. Результати наведено в таблиці 1.

Таблиця 1 – Результати перевірки ізольованості наявного тунелю

Прогін	Спроби	Unique id (до - після)	SPI однакові	Результат
1	1–4	1 - 1	так	PASS
1	5–8	1 - 1	так	PASS
2	1–2	1 - 1	так	PASS

В усіх 10 спробах ідентифікатор і SPI наявного тунелю не змінилися, тобто додавання нового тунелю не перериває роботи вже встановлених з'єднань. Програмний комплекс покрито 175 автоматизованими тестами.

Висновки

Удосконалено метод автоматизованого розгортання site-to-site VPN-тунелів, який, на відміну від переходу на swanctl/vici або повної заміни конфігурації, підключає керовані фрагменти через директиву include і розподіляє reqid монотонно з урахуванням наявної конфігурації. Це дозволяє впроваджувати автоматизацію на інфраструктурі з робочими тунелями без їх перезапуску. Експеримент підтвердив, що захищені асоціації наявного тунелю під час додавання нових не змінюються.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kent S. Security Architecture for the Internet Protocol [Електронний ресурс] : RFC 4301 / S. Kent, K. Seo. – IETF, 2005. – Режим доступу: https://www.rfc-editor.org/rfc/rfc4301.
2. Internet Key Exchange Protocol Version 2 (IKEv2) [Електронний ресурс] : RFC 7296 / C. Kaufman, P. Hoffman, Y. Nir [et al.]. – IETF, 2014. – Режим доступу: https://www.rfc-editor.org/rfc/rfc7296.
3. strongSwan Documentation [Електронний ресурс] / strongSwan Project. – Режим доступу: https://docs.strongswan.org.
4. ip-xfrm – transform configuration [Електронний ресурс] // Linux man-pages project. – Режим доступу: https://man7.org/linux/man-pages/man8/ip-xfrm.8.html.
5. Versatile IKE Configuration Interface (VICI) [Електронний ресурс] / strongSwan Project. – Режим доступу: https://docs.strongswan.org/docs/latest/plugins/vici.html.
6. Merkel D. Docker: Lightweight Linux Containers for Consistent Development and Deployment / D. Merkel // Linux Journal. – 2014. – № 239. – Article 2.

Сорока Євгеній Русланович – студент групи 1КІ-25м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: esoroka732@gmail.com.

Савицька Людмила Анатоліївна – к.т.н., доцент кафедри обчислювальної техніки, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: savytska.liudmyla@vntu.edu.ua.

Soroka Yevhenii Ruslanovich – student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: esoroka732@gmail.com.

Savitska Lyudmila Anatoliivna – Ph.D., Associate Professor of the Department of Computer Engineering, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: savytska.liudmyla@vntu.edu.uau.ua.