DOI 10.31891/2307-5732-2025-347-20
УДК 004.45

КРЕМІНЬ ІГОР
Луцький національний технічний університет
e-mail: igor.kremin@gmail.com
КРЕМІНЬ СЕРГІЙ
Луцький національний технічний університет
e-mail: sergiy.kremin@gmail.com
МІНДЗЯ ОЛЕКСАНДР
Луцький національний технічний університет
e-mail: olexandr.mindzia@gmail.com

DDOS АТАКА НА ПЕРЕПОВНЕННЯ ТАБЛИЦІ CONNTRACK

У статті розглянуто проблему DDoS-атак, які становлять одну з найсерйозніших загроз для стабільної роботи мережевих сервісів. Особливу увагу приділено атакам на переповнення таблиці Conntrack, ключового компонента ядра Linux, відповідального за відстеження стану мережевих з'єднань. Переповнення таблиці Conntrack може викликати відмову в обслуговуванні, блокуючи легітимний трафік.

Основна мета дослідження — аналіз механізмів роботи Conntrack та пошук ефективних підходів до захисту від атак. У статті досліджуються методи обмеження швидкості з'єднань, збільшення розміру таблиці Conntrack і використання SYN cookies. Обмеження швидкості сприяє зниженню навантаження, збільшення розміру таблиці дозволяє обробляти більше підключень, а SYN cookies мінімізують вплив незавершених з'єднань.

У статті також розглядається схема TCP-з'єднань та особливості їх відстеження за допомогою Conntrack. Проаналізовано динаміку атак SYN Flood, TCP RST/FIN Flood, які спрямовані на перевантаження таблиці Conntrack фальшивими або короткостроковими з'єднаннями. Наведено приклади конфігурацій із використанням nftables для ефективного запобігання атакам.

Практичні рекомендації статті спрямовані на оптимізацію системних параметрів для зменшення вразливості до атак. Вказано, як правильно налаштувати розмір таблиці Conntrack через параметри ядра та як активувати механізм SYN cookies. Зазначено також про можливість вимкнення відстеження HTTP/HTTPS-з'єднань у таблиці Conntrack для покращення продуктивності.

Висновки підкреслюють важливість комплексного підходу до захисту, що включає обмеження на швидкість з'єднань, фільтрацію пакетів, збільшення системних ресурсів і застосування адаптивних стратегій. Запропоновано напрямки подальших досліджень, зокрема впровадження машинного навчання для автоматизованого аналізу трафіку та адаптивної фільтрації.

Таким чином, стаття є корисним ресурсом для фахівців у галузі мережевої безпеки, які працюють над вирішенням проблеми DDoS-атак на рівні Conntrack. Висновки та рекомендації, представлені в статті, сприяють підвищенню стійкості систем і забезпеченню стабільної роботи мережевих сервісів навіть за умов високих навантажень.

Ключові слова: DDoS-атака, таблиця Conntrack, відмова в обслуговуванні, фільтрація пакетів, NAT, TCP-з'єднання, безпека мережі, Linux, обмеження швидкості, SYN cookies.

KREMIN IGOR
KREMIN SERHII
MINDZIA OLEKSANDR
Lutsk National Technical University

DDOS ATTACK ON CONNTRACK TABLE OVERFLOW

The article addresses the issue of DDoS attacks, which represent one of the most severe threats to the stable operation of network services. Particular attention is given to attacks on the Conntrack table overflow, a key component of the Linux kernel responsible for tracking the state of network connections. The overflow of the Conntrack table can result in a denial of service, blocking legitimate traffic.

The primary goal of the study is to analyze the mechanisms of Conntrack operation and identify effective approaches to protection against attacks. The article examines methods such as rate limiting, increasing the size of the Conntrack table, and using SYN cookies. Rate limiting helps reduce the load on the system, increasing the table size allows for handling more connections, and SYN cookies minimize the impact of incomplete connections.

The article also explores the TCP connection scheme and the specifics of their tracking using Conntrack. The dynamics of SYN Flood and TCP RST/FIN Flood attacks, which target Conntrack table overload with fake or short-lived connections, are analyzed. Examples of configurations using nftables for effective attack prevention are provided.

The practical recommendations in the article focus on optimizing system parameters to reduce vulnerability to attacks. It details how to properly configure the size of the Conntrack table via kernel parameters and how to enable the SYN cookies mechanism. It also highlights the possibility of disabling Conntrack table tracking for HTTP/HTTPS connections to improve performance.

The conclusions emphasize the importance of a comprehensive approach to protection, including rate limiting, packet filtering, increasing system resources, and applying adaptive strategies. Directions for further research are proposed, including the implementation of machine learning for automated traffic analysis and adaptive filtering.

Thus, the article serves as a valuable resource for network security specialists working to address the issue of DDoS attacks at the Conntrack level. The conclusions and recommendations presented in the article contribute to enhancing system resilience and ensuring the stable operation of network services, even under high load conditions.

Keywords: DDoS attack, Conntrack table, denial of service, packet filtering, NAT, TCP connections, network security, Linux, rate limiting, SYN cookies.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Розподілені атаки відмови в обслуговуванні DDoS становлять серйозну загрозу для мережевих систем, так як можуть повністю паралізувати роботу серверів, що обслуговують критично важливі послуги. Одною з поширених типів атак є перевантаження таблиці Conntrack, яка відповідає за відстеження стану з'єднання у Linux системах. У разі переповнення таблиці нові підключення до системи не можуть оброблятися, що призводить до відмови в обслуговуванні легітимних користувачів. Актуальність цієї проблеми зростає з поширенням DDoS, які використовують підроблені з'єднання для створення навантаження на систему. Отже, постає питання розробки ефективних методів захисту для запобігання переповнення таблиці Conntrack і забезпечення стабільної роботи мережевих сервісів.

Аналіз досліджень та публікацій

У роботі «Виявлення та ідентифікація DDoS-атак» досліджуються різні типи DDoS-атак, включаючи ті, що спрямовані на переповнення таблиці Conntrack. Автори пропонують методи виявлення та ідентифікації таких атак, підкреслюючи важливість моніторингу мережевого трафіку та аналізу аномалій для своєчасного виявлення загроз [9]. У статті «Cybersecurity: Research on Methods for Detecting DDoS Attacks» розглядаються сучасні підходи до виявлення DDoS-атак, серед них методи машинного навчання, такі як штучні нейронні мережі та дерева прийняття рішень. Автори підкреслюють ефективність цих методів у контексті захисту від атак, спрямованих на переповнення таблиці Conntrack [10].

У дослідженні «Механізми здійснення кібератак та їх аналітичного виявлення» аналізуються різні механізми проведення DDoS-атак та методи їх виявлення. Особлива увага приділяється атакам, що спрямовані на переповнення таблиці Conntrack, та методам їхнього виявлення за допомогою аналізу мережевого трафіку [10.a]. Ці дослідження зосередженні на виявленні та захисту від DDoS атак, спрямованих на переповнення таблиці Conntrack.

Формулювання цілей статті

Метою дослідження є: аналіз механізмів роботи таблиці Conntrack та визначення ефективних методів захисту від DDoS атак, спрямованих на її переповнення. Завданнями дослідження є: вивчення принципів роботи таблиці Conntrack у Linux-системах, аналіз видів атак, які призводять до її перевантаження, а також розробка практичних рекомендацій щодо налаштувань та методів захисту, які мінімізують ризик відмови в обслуговуванні.

Виклад основного матеріалу

У сучасних дослідженнях значна увага приділяється методам виявлення та запобігання DDoS-атак, зокрема переповненню таблиці Conntrack у Linux-системах. Однак існує низка невирішених аспектів цієї проблеми, які потребують подальшого вивчення. Перш за все, незважаючи на успіхи в розробці алгоритмів аналізу трафіку і фільтрації пакетів, відсутні достатньо ефективні механізми, які б враховували швидкість і обсяг сучасних DDoS-атак, здатних швидко заповнити таблицю Conntrack. Крім того, постає потреба у вдосконаленні методів оптимізації розміру таблиці Conntrack та її налаштувань, що дозволило б підвищити стійкість мережі без надмірного використання ресурсів системи. Окремим питанням залишається розробка адаптивних фільтраційних стратегій, що можуть самостійно підлаштовуватися під тип атаки в режимі реального часу. Необхідно також дослідити можливість інтеграції цих методів із сучасними технологіями машинного навчання для підвищення ефективності виявлення і блокування атак, спрямованих на перевантаження таблиці Conntrack.

Таблиця Conntrack (connection tracking table) є частиною підсистеми Netfilter [1] в ядрах Linux, і використовується для відстеження стану мережевих з'єднань. Система **ct** реалізована у модулі ядра **nft_ct**, який завантажується на вимогу. Кілька компонентів ядра потребують відстеження з'єднань як основи для роботи та можуть ініціювати завантаження системи **ct**. Одним із них є модуль ядра **nft_ct**, який є модулем фільтрації пакетів nftables із збереженням стану.

Таблиця Conntrack зберігає інформацію про кожне активне з'єднання. Вона включає такі параметри, як IP-адреси джерела і призначення, порти, стан з'єднання і лічильники пакетів. Ця інформація дозволяє ядру правильно обробляти пакети, що належать до існуючих з'єднань, і застосовувати політики фільтрації. Модуль **nft_ct** забезпечує contract expression [2, с 89] ці вирази починаються зі слова ***ct***.

Схема TCP (SYN, SYN-ACK, ACK) рукостискання [3] зображена на (рис. 1)

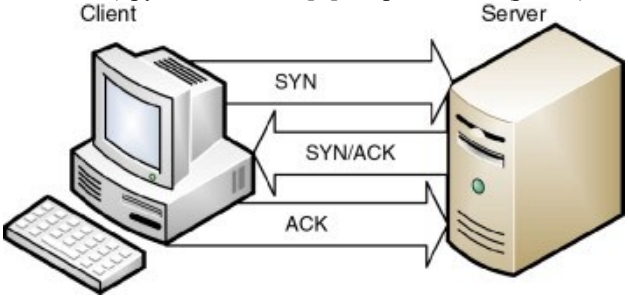

Рис. 1. Рукостискання SYN, SYN-ACK, ACK

Розглянемо заповнення таблиці Conntrack на прикладі http з'єднання.
Процес обробки HTTP-з'єднання

1. Перший пакет (ініціація з'єднання):
   - Перший TCP-пакет (SYN) від клієнта надходить на сервер.
   - Пакет проходить через ланцюг input, де ми будемо відстежувати з'єднання.
2. Запис у таблицю Conntrack [4]:
   - У таблицю Conntrack додається запис з інформацією про з'єднання:
     - IP-адреса джерела (клієнта)
     - IP-адреса призначення (сервера)
     - Порт джерела
     - Порт призначення
     - Стан з'єднання (NEW)
     - Порядковий номер TCP (SEQ)
   - Стан з'єднання змінюється з NEW на ESTABLISHED після завершення (SYN, SYN-ACK, ACK).
3. Наступні пакети (передача даних):
   - Наступні TCP-пакети, що відносяться до цього з'єднання, відслідковуються таблицею Conntrack.
   - Пакети обробляються відповідно до правил фільтрації і стану з'єднання.

```
table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;
        # Приймаємо пакети для існуючих з'єднань
        ct state established,related accept
        # Приймаємо нові HTTP-з'єднання
        tcp dport 80 ct state new accept
        # Приймаємо ICMP пакети
        ip protocol icmp accept
        # Приймаємо пакети з lo інтерфейсу
        iif lo accept
    }
}
```

Рис. 2. Приклад конфігурації для nftables

Наведемо приклад (рис. 2) для http з'єднання з <client-ip> до <sever-ip> схематично, використаємо hook input [6] (рис. 3).

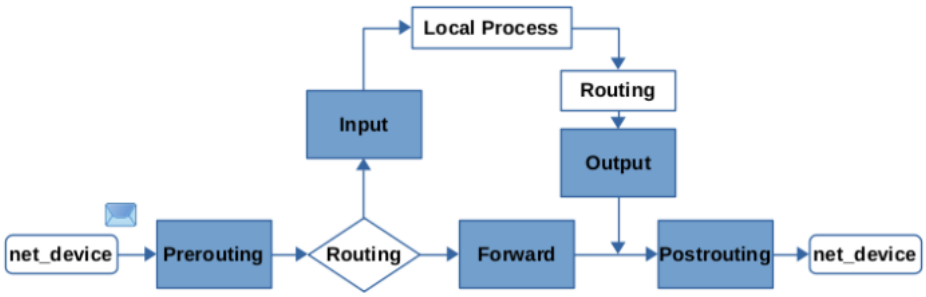

Рис. 3. Netfilter hook – проста блок діаграма

Перший пакет має state NEW після проходження рукостискання state змінюється на ESTABLISHED.

1. Перший пакет (початок з'єднання):
   - Клієнт -> Сервер:
     - IP-адреса джерела: <client-ip>
     - IP-адреса призначення: <sever-ip>
     - Порт джерела: 12345
     - Порт призначення: 80
     - TCP SEQ: X
   - Запис у Conntrack:
     - IP source: <client-ip>
     - IP destination: <sever-ip>
     - Source port: 12345

- Destination port: 80
- State: NEW
- TCP SEQ: X

2. Тристороннє рукостискання (SYN, SYN-ACK, ACK):
   - Сервер -> Клієнт:
     - SYN-ACK
   - Клієнт -> Сервер:
     - ACK
   - Стан у Conntrack:
     - State: ESTABLISHED
3. Передача даних:
   - Клієнт -> Сервер:
     - HTTP-запит
   - Сервер -> Клієнт:
     - HTTP-відповідь
   - Далі всі пакети обробляються як established.

Атака на переповнення таблиці Conntrack

DDoS атаки на переповнення таблиці Conntrack використовують велику кількість підроблених або короткочасних TCP з'єднань для заповнення таблиці до максимального розміру. Коли таблиця Conntrack переповнена, нові з'єднання не можуть бути оброблені, що призводить до відмови в обслуговуванні реальних користувачів. Деякі з основних типів атак[7]:

- Flood TCP SYN – надсилання великої кількості SYN пакетів без завершення тристороннього рукостискання.
- Flood TCP RST/FIN – надсилання великої кількості RST або FIN пакетів, що змушують сервер створювати нові записи у таблиці Conntrack.
- Flood TCP ACK – надсилання великої кількості ACK пакетів, що змушують сервер оновлювати існуючі записи у таблиці Conntrack.

Поточну кількість записів у таблиці Conntrack можна отримати за допомогою
cat /proc/sys/net/netfilter/nf_conntrack_count
а самі записи використовуючи пакет conntrack-tools [8].

Методи захисту та пом`якшення ефекту DDoS атаки.

1. Обмеження швидкості (Rate Limiting).
   Встановлення обмежень на кількість нових з'єднань з одного джерела за певний проміжок часу допомагає зменшити ймовірність переповнення таблиці Conntrack. Це може бути реалізовано за допомогою nftable [11] (рис. 4).

```
table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;
        # Відхилити нові з'єднання, якщо кількість з'єднань перевищує 20
        tcp flags syn ct state new limit rate over 10/second burst 20 packets drop
        # Прийняти нові з'єднання з обмеженням швидкості 10 з'єднань за секунду,
        # з можливістю одночасного пікового навантаження до 20 з'єднань
        tcp flags syn ct state new limit rate 10/second burst 20 packets accept
        # Приймати встановлені та пов'язані з'єднання
        ct state established,related accept
        # Приймати пакети локального інтерфейсу
        iif lo accept
        # Приймати ICMP пакети
        ip protocol icmp accept
    }
}
```

Рис. 4. Конфігурація nftables з обмеженням на нові з'єднання

2. Збільшення розміру таблиці Conntrack.
   Дозволяє обробляти більше з'єднань одночасно. Це може бути корисно для систем з високою навантаженістю. Налаштування можна змінити вказавши значення параметру ядра [12]:
   sysctl -w net.netfilter.nf_conntrack_max=262144
3. Використання фільтрації SYN пакета.

Використання SYN кукі (SYN cookies) дозволяє запобігти створенню нових записів у таблиці Conntrack до завершення тристороннього рукостискання:

sysctl -w net.ipv4.tcp_syncookies=1

вмикає захист від SYN-флуд атак для IPv4, що також захищає TCP-з'єднання IPv6 завдяки загальному механізму SYN cookie в TCP-стеку. Але це несе за собою деякі недоліки, а саме половина функцій tcp, включаючи керування великими вікнами, буде вимкнено, що може знизити продуктивність [13].

Якщо сервер надає лише HTTP/HTTPS сервіс існує можливість вимкнути використання таблиці Conntrack для http та https з'єднань. Це зменшує навантаження на систему відстеження з'єднань для цих специфічних типів трафіку, конфігурація наведена на (рис. 5) з використанням hook prerouting.

```
table inet filter {

    chain prerouting {
        type filter hook prerouting priority -100; policy accept;
        tcp dport { 80, 443 } notrack
    }

    chain output {
        type filter hook output priority -100; policy accept;
        tcp sport { 80, 443 } notrack
    }
}
```

Рис. 5. Конфігурація nftables з вимкненням Conntrack таблиці для http(s)

Обробка пакетів на ранньому етапі дозволяє швидко відфільтровувати певні типи трафіку, зменшуючи навантаження на систему і підвищуючи швидкість обробки даних. У нашому випадку, HTTP/HTTPS трафік може бути направлений до наступного рівня аналізу без додаткової перевірки на рівні з'єднань. Такий підхід зменшить використання пам'яті та обчислювальні ресурси, необхідні для аналізу трафіку, і дасть змогу дослідити інші параметри пакетів, що в результаті прискорить загальний процес обробки мережевого трафіку.

Висновки та перспективи подальшого дослідження

Захист від DDoS атак, спрямованих на переповнення таблиці Conntrack, вимагає комплексного підходу, що включає налаштування обмежень, збільшення ресурсів системи, використання спеціальних механізмів фільтрації та постійний моніторинг стану мережі. Поєднання цих методів дозволить значно знизити ризик відмови в обслуговуванні і забезпечити стабільну роботу мережевих сервісів.

Література

1. Ayuso, P. N. (2006). Netfilter`s connection tracking system. [Електронний ресурс]: [веб-сайт]. – Режим доступу : http://people.netfilter.org/pablo/docs/login.pdf (Дата звернення: 10.03.2024).
2. Suehring Steve (2015) Linux Firewals Fourth Edition [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://el.newoutlook.it/download/book/Linux-Firewalls-Enhancing-Security-with-nftables-and-Beyond.pdf – (Дата звернення: 10.03.2024).
3. Three-Way Handshake [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://www.sciencedirect.com/topics/computer-science/three-way-handshake – (Дата звернення: 10.03.2024).
4. Andreasson, O. (2006). Iptables tutorial 1.2.2: Chapter 7. The state machine.
5. [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html – (Дата звернення: 10.03.2024).
6. Nftables - Packet flow and Netfilter hooks in detail [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://thermalcircle.de/doku.php?id=blog:linux:nftables_packet_flow_netfilter_hooks_detail – (Дата звернення: 16.03.2024).
7. DDoS Attack Types [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://ddos-guard.net/en/terms/ddos-attack-types (дата звернення: 28.03.2024). – Назва з екрана.
8. Ayuso, P. N. (2012). The conntrack-tools user manual. [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://conntrack-tools.netfilter.org/manual.html – (Дата звернення: 28.03.2024). –
9. Войтович О. П. , Фесенко А. І. Виявлення та ідентифікація DDoS-атак. [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14516/zbirnyk-2015-Voyt1opt.pdf – (Дата звернення: 28.03.2024).
10. M. Chornobuk, V. Dibrovin, L. Deineha Cybersecurity: Research on Methods for Detecting DDoS Attacks [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://csitjournal.khmnu.edu.ua/index.php/csit/article/view/273/164 DOI: https://doi.org/10.31891/csit-2023-4-1
a. Vavilenkova, O. Skitsko, A. Piven, Механізми здійснення кібератак та їх аналітичного виявлення.
[Електронний ресурс] : [веб-сайт]. – Режим доступу : https://isg-journal.com/isjea/article/download/558/310/565
DOI: 10.46299/j.isjea.20230206.04

11. wiki.nftables.org. Quick reference - Ct. [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes#Ct. – (Дата звернення: 28.03.2024). – Назва з екрана.

12. I/O timeout error caused by error «nf_conntrack: table full». [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://support.hashicorp.com/hc/en-us/articles/15157216278931-I-O-timeout-error-caused-by-error-nf-conntrack-table-full. – (Дата звернення: 28.03.2024).

13. Kelly Chris (2007) Disadvantages of TCP SYN cookies. [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://ckdake.com/content/2007/disadvantages-of-tcp-syn-cookies.html – (Дата звернення: 28.03.2024).

References

1. Ayuso, P. N. (2006). Netfilter`s connection tracking system. ». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : http://people.netfilter.org/pablo/docs/login.pdf. (Data zvernennia: 10.03.2024).

2. Suehring Steve (2015) Linux Firewals Fourth Edition. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://el.newoutlook.it/download/book/Linux-Firewalls-Enhancing-Security-with-nftables-and-Beyond.pdf. (Data zvernennia: 10.03.2024).

3. Three-Way Handshake. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.sciencedirect.com/topics/computer-science/three-way-handshake. (Data zvernennia: 10.03.2024).

4. Andreasson, O. (2006). Iptables tutorial 1.2.2: Chapter 7. The state machine.

[Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html. (Data zvernennia: 10.03.2024).

5. Nftables - Packet flow and Netfilter hooks in detail. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://thermalcircle.de/doku.php?id=blog:linux:nftables_packet_flow_netfilter_hooks_detail. (Data zvernennia: 16.03.2024).

6. DDoS Attack Types [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://ddos-guard.net/en/terms/ddos-attack-types (Data zvernennia: 28.03.2024).

7. Ayuso, P. N. (2012). The conntrack-tools user manual. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://conntrack-tools.netfilter.org/manual.html. (Data zvernennia: 28.03.2024).

8. Voitovych O. P.Fesenko A.I. Detection and Identification of DDoS Attacks [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14516/zbirnyk-2015-Voyt1opt.pdf (Data zvernennia: 28.03.2024).

9. M. Chornobuk, V. Dibrovin, L. Deineha Research on Methods for Detecting DDoS Attacks. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://csitjournal.khmnu.edu.ua/index.php/csit/article/view/273/164

DOI: https://doi.org/10.31891/csit-2023-4-1

10. A. Vavilenkova, O. Skitsko, A. Piven, Mechanisms of Cyberattack Execution and Analytical Detection. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://isg-journal.com/isjea/article/download/558/310/565 DOI: 10.46299/j.isjea.20230206.04

11. wiki.nftables.org. Quick reference - Ct. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes#Ct. (Data zvernennia: 28.03.2024).

12. I/O timeout error caused by error «nf_conntrack: table full». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://support.hashicorp.com/hc/en-us/articles/15157216278931-I-O-timeout-error-caused-by-error-nf-conntrack-table-full. (Data zvernennia: 28.03.2024).

13. Kelly Chris (2007) Disadvantages of TCP SYN cookies. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://ckdake.com/content/2007/disadvantages-of-tcp-syn-cookies.html (Data zvernennia: 28.03.2024).