https://www.proconference.org/index.php/gec/article/view/gec35-00-021
DOI: 10.30890/2709-1783.2024-35-00-021

УДК 004.716(043.2)

CORPORATE SECURE LAN MODELING USING CISCO TOOLS
МОДЕЛЮВАННЯ КОРПОРАТИВНОЇ УБЕЗПЕЧЕНОЇ LAN ЗАСОБАМИ CISCO

Dubchak E.V. / Дубчак О.В.
ORCID: 000-0001-9739-3960
Gulak N.K. / Гулак Н.К.
c.t.s./ к.т.н.
ORCID: 0000-0001-8524-8635
National Aviation University, Kyiv, Guzara 1,03058
Національний авіаційний університет, м. Київ, Л. Гузара 1, 03058

***Анотація**. Розглянуто можливості емулятора Cisco Packet Tracer для моделювання захищеної корпоративної LAN; проаналізовано існуючі можливості захисту LAN за допомогою стандартних та розширених ACL; створено модель захищеної від несанкціонованого доступу корпоративної локальної мережі з підключенням до Інтернет; технічне рішення ґрунтується на використанні засобів Cisco,*

***Ключові слова:** моделювання мереж, мережева безпека, Cisco Packet Tracer, фільтрація трафіку, списки контролю доступу, адміністрування мереж*

***Abstract.** Cisco Packet Tracer emulator capabilities for secure corporate LAN simulating are reviewed; existing LAN protection possibilities using standard and extended ACLs are analyzed; a corporate local network model protected from unauthorized access with an Internet connection has been created; the technical solution using Cisco tools.*

***Key words**: network modeling, network security, Cisco Packet Tracer, traffic filtering, access control lists, network administration.*

Вступ

За даними Digital 2024: Global Overview Report, що опубліковано дослідницькою компанією DataReportal, наразі Інтернет використовують 5,35 млрд. осіб, що складає понад 66% світового населення. Кількість користувачів у поточному році перевищує минулорічні показники на 97 млн. або на 1,8%. *[1]*

Кількість Інтернет - користувачів в Україні, які щоденно використовують можливості міжмережевих комунікацій, за поточний рік зросла з 72% до 80%. *[2]*

Комунікаційні мережі зазнали широкого розповсюдження й у виробничому середовищі. Зворотною стороною такої їхньої популярності є відповідне збільшення кількості та складності кіберзагроз. Так, за даними SonicWall, у першому півріччі 2024 року спостерігалося зростання кіберзлочинності з використанням шкідливого програмного забезпечення, що

становить загрози для мереж як загального призначення, так і Інтернету речей, а також зашифрованої активності загроз. *[3]*

До корпоративних втрат через кіберзлочинність зазвичай відносять: пошкодження та знищення даних; викрадення коштів; втрату продуктивності; крадіжку інтелектуальної власності; крадіжку особистих і фінансових даних; шахрайство; порушення сталого ходу процесів бізнесу або неможливість їхнього поновлення після атак; нанесення репутаційної шкоди тощо.

Одним із основних завдань під час проєктування корпоративної локальної обчислювальної мережі (LAN, Local Area Network) є обрання моделі, оптимальної як з точки зору її складових, так і щодо питань убезпечення від можливих загроз, зокрема, небажаного трафіку.

Основний текст Моделювання комунікаційних мереж широко використовується не тільки для розробки нових архітектур, але й для моніторингу, управління та прогнозування їхнього функціонування. *[4]*

Метою роботи є створення моделі захищеної від несанкціонованого доступу корпоративної локальної мережі з підключенням до Інтернет. Технічне рішення ґрунтується на використанні засобів Cisco, зокрема емулятора Packet Tracer, для побудови моделі власно мережі та моделі її захисту від зловмисного втручання. Обрання саме цього програмного забезпечення обумовлено висновками експертів щодо доцільності використання емулятора *[4]* та власним досвідом, набутим в процесі викладання курсів «Network Essentials», «Introduction to Internet of Things», «Introduction to Packet Tracer», «Network Security». *[5]*

За допомогою Cisco Packet Tracer можна імітувати роботу багатьох мережевих пристроїв: маршрутизаторів, комутаторів, бездротових точок доступу, персональних комп’ютерів, мережевих принтерів, IP-телефонів тощо. Робота з інтерактивним емулятором дає відчуття створення реальної мережі, що складається з десятків або навіть сотень пристроїв, які можна налаштовувати, використовуючи команди Cisco IOS або графічний інтерфейс (рисунок1).

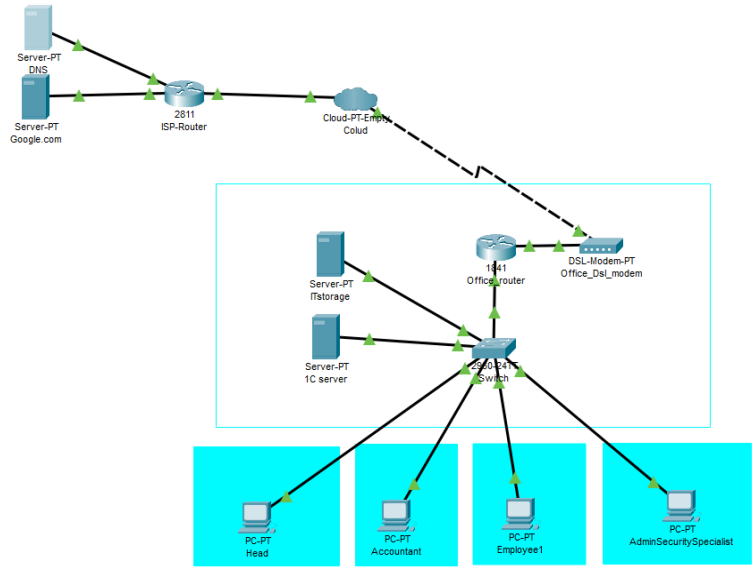

Рисунок 1- Приклад логічної топології корпоративної LAN, змодельованої засобами Cisco Packet Tracer *[5]*

Використовуючи режим графічного відображення Cisco Packet Tracer, можна відстежувати мережевий трафік, спостерігати за зміною параметрів IP-пакетів під час проходження даних мережевими пристроями, швидкість і шлях передачі IP-пакетів тощо. Аналіз подій, що відбуваються в змодельованій мережі, дозволяє поглибити розуміння взаємодії мережевих компонентів, виявити можливі недоліки та помилки й обрати засоби їхнього виправлення. Тестування в емуляторі впливає на правильність встановлення необхідних кінцевих точок і створення коректних налаштувань.

Ґрунтуючись на результатах проведеного аналізу існуючих засобів для організації захищеного від небажаного трафіку функціонування мережі, пропонується обрати один із інструментів Cisco - списки контролю доступу (ACL, Access Control Lists).

ACL широко використовуються в комп'ютерних мережах та в мережевій безпеці для пом'якшення мережевих атак та контролю мережевого трафіку. Мережеві інженери використовують ACL для визначення та керування класами трафіку на мережевих пристроях на основі різних параметрів, що належать до рівнів 2, 3, 4 та 7 моделі OSI (Open System Interconnection). Під час класифікації трафіку, найпоширеніші типи параметрів, що використовуються у пов'язаних із

безпекою списках ACL, включають адреси IPv4 та IPv6, а також номери портів TCP та UDP.

ACL являють собою набір умов дозволу та заборони, які забезпечують захист мережі шляхом блокування неавторизованих користувачів, дозволяючи користувачам авторизованим отримувати доступ до певних ресурсів. До можливостей ACL належать також: забезпечення контролю над потоком трафіку; обмеження вмісту оновлень маршрутизації; вказання типу трафіку, який потрібно переспрямовувати або блокувати. Мережеві ACL налаштовуються в маршрутизаторах або комутаторах, де вони діють як фільтри трафіку. Кожний мережевий ACL містить певні правила для контролю, яким пакетам чи оновленням маршрутизації дозволено чи заборонено доступ до мережі.

Стандартні ACL співставляють пакети, перевіряючи поле IP-адреси джерела в заголовку пакета. Ці ACL використовуються для фільтрації пакетів на основі виключно інформації про джерело рівня 3.

Розширені ACL відповідають пакетам на основі інформації про джерело та пункт призначення рівня 3 та рівня 4. Інформація рівня 4 може містити дані про порти TCP та UDP. Розширені ACL забезпечують більшу гнучкість та контроль доступу до мережі, ніж стандартні ACL. *[5]*

Отже, маршрутизатори Cisco з ACL працюють як пакетні фільтри, які дозволяють або забороняють надходження пакетів на основі критеріїв фільтрації. Як пристрій рівня 3 моделі OSI, маршрутизатор із фільтрацією пакетів використовує правила, щоб визначити, дозволити чи заборонити доступ трафіку.

Як стандартні, так і розширені ACL можуть використовуватися для опису пакетів, що входять або виходять з інтерфейсу. Список опрацьовується послідовно. Перший знайдений оператор зупиняє пошук у списку та визначає дію, яку необхідно зробити.

Після створення стандартного або розширеного списку ACL необхідно його застосувати до відповідного інтерфейсу.

Рішення приймається на основі вихідної та кінцевої IP-адрес, кінцевого порту та вихідного порту, а також офіційної процедури пакета. *[6]*

Слід зауважити, що від типу ACL залежить їхнє розміщення на мережевих пристроях: стандартні ACL розміщуються якомога ближче до місця призначення, оскільки фільтрують пакети лише на основі адреси джерела; їхнє розміщення надто близько до джерела може негативно вплинути на пакети, заборонивши весь трафік, включаючи дійсний; розширені ACL розміщуються на маршрутизаторах якомога ближче до джерела, яке фільтрується; їхнє розміщення занадто далеко від джерела - неефективне використання мережевих ресурсів.

Визначення того, використовувати стандартні або розширені ACL, базується на спільній меті всього ACL. Порівняно зі стандартними ACL розширені ACL забороняють або дозволяють певні типи трафіку.

У наведеній вище моделі LAN доречно застосувати ACL на інтерфейсі, звідки можна очікувати загрози, тобто щоб пакети були відхилені до потрапляння до маршрутизатора. Така практика дозволить зберегти обчислювальні ресурси маршрутизатора. В даному випадку пропонуються розширені ACL, оскільки ініціація будь-яких сесій (атака) може надходити із зовнішньої мережі, отже, в якості джерела буде виступати будь-яка IP-адреса, а як отримувачі - конкретні локальні підмережі (рисунок 2). Можливі місця розташування ACL: інтерфейс до LAN; інтерфейс ISP (Internet Service Provider)

```
office_router(config)#ip access-list extended outTraffic
office_router(config-ext-nacl)#deny tcp any host 10.10.10.10 eq telnet
office_router(config-ext-nacl)#permit ip any host 10.10.10.10
office_router(config-ext-nacl)#copy run startup
                              ^
% Invalid input detected at '^' marker.

office_router(config-ext-nacl)#do copy run startup
Destination filename [startup-config]?
Building configuration...
[OK]
office_router(config-ext-nacl)#exit
office_router(config)#int f0/0
office_router(config-if)#ip access-group outTraffic in
office_router(config-if)#exit
```

Рисунок 2 – Приклад розширеного ACL у моделі корпоративної LAN для захисту від зовнішніх загроз

Підсумки та висновки

Було розглянуто можливості емулятора Cisco Packet Tracer для моделювання захищеної корпоративної LAN; проаналізовано існуючі можливості захисту LAN за допомогою стандартних та розширених ACL.

З використанням технологій апаратного забезпечення Cisco розроблено модель, що дозволяє захистити мережу від несанкціонованого доступу за рахунок фільтрації трафіку засобами розширених ACL; імітовано реальне середовище та проведено тестування моделі.

У спроєктованій моделі корпоративної LAN, убезпеченій за допомогою ACL, зменшується потенційна кількість спроб доступу до конфіденційної інформації та даних. Модель може бути використано мережевими інженерами, які мають досвід моніторингу та управління корпоративними мережами.

Література:

1. DataReportal. Digital 2024: Global Overview Report [Електронний ресурс] - Режим доступу: https://datareportal.com/reports/digital-2024-global-overview-report

2. Мінфін. Опитування: 80% українців користуються інтернетом щодня [Електронний ресурс] - Режим доступу: https://minfin.com.ua/2024/01/28/120490102/

3. SonicWall. 2024 SonicWall Mid-Year Cyber Thread Report [Електронний ресурс] - Режим доступу: https://www.sonicwall.com/threat-report

4. Michel Bakni, Yudith Cardinale, Luis Manuel Moreno. An Approach to Evaluate Network Simulators: An Experience with Packet Tracer. 2018 [Електронний ресурс] - Режим доступу: https://hal.science/hal-02066550/document

5. Cisco Networking Academy. Network Security. [Електронний ресурс] - Режим доступу: https://www.cisco.com/

6. Imperva. Access Control Lists (ACL) [Електронний ресурс] - Режим доступу: https://www.imperva.com/learn/data-security/access-control-list-acl/