УДК 004.716.(043.2)

О.В. Дубчак,
І.А. Кравчук,
С.І. Ожерельєв,
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ РОЗШИРЕНИХ ACL ОБЛАДНАННЯ CISCO ДЛЯ УБЕЗПЕЧЕННЯ LAN ВІД ЗОВНІШНІХ ЗАГРОЗ

Новітні інформаційні технології, зокрема з підтримкою віддаленого доступу, активно впроваджуються в усі сфери життєдіяльності людини. Кібербезпека наразі має основоположне значення щодо розв'язання нагальних задач із забезпечення цілісності, конфіденційності і доступності ресурсів інформаційних систем і мереж. Враховуючи статистичні дані за 2020 р. щодо суми нанесених кіберзлочинцями збитків, яка становила понад 1% світового ВВП, що на 50% вище, ніж було у 2018 р., можна визначити несанкціонований доступ як одну з найпоширеніших загроз мережевим інфраструктурам [1].

Відповідно до RFC 4949 «InternetSecurityGlossary» [2] Access Control List (ACL) є механізмом реалізації контролю доступу до системних ресурсів. Цілі застосування ACL - обмеження мережевого трафіку для підвищення продуктивності LAN та налаштування відповідного рівня безпеки відносно доступу до різних мережевих пристроїв.

ACL слід налаштовувати на пристроях «брандмауера», які часто розташовані між внутрішньою мережею підприємства та зовнішньою мережею, наприклад, Інтернетом. Також використовуються ACL на роутері, локалізованому між двома частинами мережі, з метою контролювати трафік, що входить або виходить із локальної мережі. [3]

На прикордонних пристроях слід налаштувати ACL для кожного встановленого на інтерфейсах пристрою мережевого протоколу таким чином, що вхідний, вихідний або обидва види трафіка фільтруватимуться через інтерфейс.

Доступ до налаштування пристроїв Cisco, а саме маршрутизатору Cisco 1841 та комутатору Cisco Catalyst 2960 відбувається за допомогою кабелю Cisco Switch Router Console Cable RJ-45 to RS-232 через позасмуговий доступ (консольний порт). Можливості даного мережевого обладнання також

дозволяють використовувати протоколи Telnet та більш захищений його аналог Secure Shell (SSH).

Отже, політики безпеки реалізуються в повній мірі за допомогою вбудованих функцій мережевого обладнання Cisco у вигляді стандартних та розширених ACL. Для обмеження доступу іззовні в середину LAN, пропонується застосовувати розширені ACL. Обмеження такого трафіку можна створити у двох місцях: зі сторони LAN або зі сторони маршрутизатора провайдера (рис. 1.).

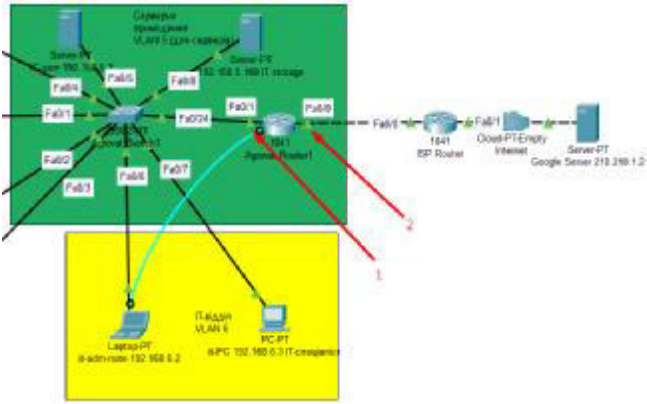

Рис. 1. Місця можливого розташування ACL: інтерфейс до LAN (1) та інтерфейс до провайдера (2)

У результаті ACL надали можливість фільтрувати будь-які Інтернет-з'єднання на 3-му (IP-адреси джерела та призначення), 4-му (TCP, UDP), та 7-му (HTTP, HTTPS, telnet) рівнях моделі OSI.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Кіберзлочини у 2020 р. Дослідження. URL:https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/55857766*
2. *Дубчак О.В. Списки контролю доступу обладнання Cisco як засіб мережевої безпеки / О.В.Дубчак, С.І.Ожерельєв// Materials of XVI Intenational Research And Practice Conference «Cutting-Edge Science – 2020», 30.04.20 – 07.05.20. – Sheffield (UK):"Science&Education Ltd". - V.8.- P.50-52.*
3. *Security Configuration Guide:Access Control Lists. Cisco IOS Release 15M&T. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration*