УДК 681.12

Т. І. Коробейнікова
С. В. Шостак

МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ КОМПАНІЇ CISCO

Вінницький національний технічний університет

Анотація

Розглядаються методи та засоби створення захищеної корпоративної мережі на базі обладнання компанії Cisco, висновки обгрунтовано на основі проведеного дослідження засобів захисту інформації в корпоративних мережах.

Ключові слова: Cisco, захист, ACL, мережеві екрани, AAA ,VPN.

Abstract

The methods and means of creating a protected corporate network based on equipment of the Cisco company are considered, the conclusions are based on the conducted research of information protection means in corporate networks.

Keywords: Cisco, protection, ACL, firewall, AAA, VPN.

Вступ

Основою для надійного функціонування бізнес-процесів підприємства є надійна мережева інфраструктура, незалежно від масштабу та роду діяльності. Захищеність та надійність функціонування корпоративної мережі – основа діяльності підприємства, а збої в роботі мережі призводять до прямих матеріальних втрат підприємства. Корпоративна мережа може складатися з багатьох взаємопов'язаних підсистем, які виконують кожна свою функцію та роль у забезпеченні діяльності підприємства.

Чільним напрямком є надання всіх необхідних засобів захисту відділенням компанії для уникнення несанкціонованого доступу з зовні до інформації компанії, зменшення ризику виникнення атак на мережу та безпечної передачі даних в самій мережі [1, 2].

Результати дослідження

Сучасною тенденцією розвитку корпоративних мереж в цілому та інформаційних систем є централізація обчислювальних ресурсів [3,4], з можливістю доступу до них з будь-якої територіально віддаленої точки, тому розробка захищеної корпоративної мережі є актуальною прикладною задачею.

Залежно від поставленого завдання і цілі, засоби створення локальної мережі підприємства (корпоративної мережі) можуть бути різними. Найчастіше саме комбінація різних технологічних рішень дозволяє досягти оптимального рішення [5, 6]. До таких рішень можна віднести:

– LAN;
– VPN;
– WI-FI.

За результатами досліджень Forrester Research Inc. і Infonetics Research, витрати на використання та обслуговування VPN майже в три рази нижче, ніж логістичних структур, побудованих за технологією LAN.

Для забезпечення належного захисту корпоративної мережі, повинні бути реалізовані актуальні на даний час засоби захисту інформації в корпоративних мережах. До них відносяться:

– використання пристроїв, що вбудовуються безпосередньо в апаратуру, або пристроїв, які сполучаються з апаратурою локальних мереж по стандартному інтерфейсу (схеми контролю інформації по парності, схеми захисту полів пам'яті по ключу, спеціальні регістри);

– застосування засобів, що здійснюють злиття декількох файлів і навіть каталогів в єдиний файл – архів, одночасно зі скороченням загального обсягу вихідних файлів шляхом усунення надмірності, але без втрат інформації, тобто з можливістю точного відновлення вихідних файлів;

– використання програм, що розроблені для захисту інформації від вірусів;

– застосування способів забезпечення конфіденційності інформації, в тому числі за допомогою шифрування і автентифікації;

– застосування засобів ідентифікації і автентифікації користувачів. Автентифікація полягає в перевірці: чи є суб'єкт, що підключається, тим, за кого він себе видає. А ідентифікація забезпечує виконання функцій встановлення автентичності та визначення повноважень суб'єкта при його допуску в систему, контролювання встановлених повноважень в процесі сеансу роботи, реєстрації дій і ін.

– використання засобів управління доступом;

– протоколювання і аудит. Використання протоколювання забезпечує накопичення та збереження інформації про події, що відбуваються в інформаційній системі. Метою комп'ютерного аудиту є контроль відповідності системи або мережі необхідним правилам безпеки, принципам або індустріальним стандартам. Аудит забезпечує аналіз всього, що може відноситися до проблем безпеки, або все, що може привести до проблем захисту.

– використання брандмауерів, що дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищений різновид методу – це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою;

– використання proxy-серверів.

Висновки

Для надійного функціонування бізнес-процесів підприємства мають бути застосовані актуальні методи та засоби розробки захищеної корпоративної мережі. Актуальність методів та засобів визначається аналізом всіх існуючих методів та засобів і вибором найкращих варіантів. Також для релізації захисту даних в корпоративній мережі мають використовуватить всі доступні засоби захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. //Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
2. Трояновська Т. І. Аспекти побудови корпоративних мереж підприємства / Т. І. Трояновська, М. О. Максюта // Матеріали XLV Науково-технічної конференції ВНТУ, Вінниця, 23-24 березня 2016 р.
3. Troianovska T. I. Method of cyclic ADC calibration by the conversion characteristics analysis / S. M. Zakharchenko, T. I. Troianovska // ADVANCED INFORMATION AND COMMUNICATION TECHNOLOGIES-2017 : 2-nd International conference, 4-7 July 2017. – Lviv, Ukraine, 2017. – P. 120–123. (Scopus).
4. Трояновська Т. І. Побудова швидкісних мультисервісних мереж / Трояновська Т. І., Савицька Л. А., Максюта М. О., Поліщук Д. М. // Міжнародна науково-технічна конференція «Smart and Young». – Київ, 2016. – №8, с. 72–78.
5. Коробейнікова Т. І. Методи та засоби захисту інформації в IPv6 за допомогою протоколу IPSEC / Коробейнікова Т. І., Рильський І. А. Зимові наукові підсумки 2018 року: XII Міжнародна науково-практична інтернет-конференція: тези доповідей, Дніпро, 25 грудня 2018 р. – Ч. 1. – Дніпро: НБК, 2018, с. 85-93.
6. Коробейнікова Т. І. Комплексний метод організації IP-телефонії в структурі захищеної корпоративної мережі підприємства / Коробейнікова Т. І., Ткачук В. Ю. Зимові наукові підсумки 2018 року: XII Міжнародна науково-практична інтернет-конференція: тези доповідей, Дніпро, 25 грудня 2018 р. – Ч. 1. – Дніпро: НБК, 2018, с. 105-111.

Шостак Сергій Володимирович — студент групи 2КІ-18м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: sergey.shostak7@gmail.com.

Науковий керівник: ***Коробейнікова Тетяна Іванівна*** — к.т.н., доц. каф. ОТ, Вінницький національний технічний університет, м. Вінниця.

Shostak Serhii V. —student, 2KI-18m, Faculty of Information Technologies and Computer Engeneering, Vinnytsia National Technical University, Vinnytsia, email: sergey.shostak7@gmail.com.

Supervisor: ***Korobeinikova Tetiana I***. — PhD, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.