Перша лінія захисту мережі організації - визначити користувачів і пристрої, які мають доступ до мережі, перевірити стан таких пристроїв і уточнити має рацію і привілеї, що дозволяють цим пристроям отримати доступ до ресурсів. Система довір'я і ідентифікації Cisco перешкоджає розкраданню інформації, надаючи доступ до корпоративної мережі тільки довіреним користувачам і пристроям, причому ці користувачі і пристрої не можуть отримати доступ до заборонених для них інформаційних ресурсів [2].

Перший крок до організації захищеного мережного середовища – це перевірка ідентичності і повноважень доступу користувачів. Система довір'я і ідентифікації Cisco забезпечує ідентифікацію користувачів за допомогою стандартних протоколів і технологій аутентифікації, таких як протокол 802.1X і технологія аутентифікації, авторизації і обліку (AAA), інтегрованого в комутатори Cisco Catalyst® і маршрутизатори Cisco. Після перевірки ідентичності користувача йому можна надати привілеї доступу. Сервер Cisco ACS (Cisco Secure Access Control Server) управляє настройкою політик і доступом в мережу. Сервер Cisco ACS дозволяє адміністраторам контролювати доступ користувачів до різних сегментів мережі, дозволяти використовування різних мережних служб окремим користувачам або групам користувачів і реєструвати всі дії користувачів в журналі.

Перед тим, як дозволити пристрою доступ в мережу, його необхідно перевірити на відповідність політиці безпеки для кінцевих вузлів. Система контролю доступу Cisco NAC (Cisco Network Admission Control) зіставляє дані про стан системи пристрою з діючою політикою безпеки. Взаємодіючи з галузевими партнерами, такими як Trend Micro і IBM, мережа, використовуючи інтелектуальні механізми Cisco NAC, визначає ступінь відповідності кінцевого вузла діючим політикам безпеки і на підставі отриманої інформації дозволяє або забороняє доступ.

ПОСИЛАННЯ

1.Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windiws Sockets. - Диалог - МИФИ, 1996.

2. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994.

3. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994.

УДК 004.738

V. Lakhno [1][0000-0001-9695-4543],
[1] Professor, National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
A. Blozva [2][0000-0002-4377-0916]
[2] National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
G. Zhilkishbayeva [3][0000-0001-9955-5994],
[3] Yessenov University, Aktau, Kazakhstan,
A. Asselkhan [4][0000-0001-7233-4104]
[4] Abai Kazakh National Pedagogical University, Almaty, Kazakhstan,

ЗАСТОСУВАННЯ ПІДХОДІВ ЗОНАЛЬНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗВО

Анотація У даній публікації розглянуто проблеми побудови компютерних мереж ЗВО, які загрози виникають та можливість забезпечити комплексну безпеку всіх користувачів.

Ключові слова: Zone Base Firewall, інспектування трафіку, ЗВО, демілітаризована зона.

Останнім часом заклади вищої освіти стикнулися із необхідністю більше широко застосувати дистанційне навчання у своїй роботі. Використання різноманітних платформ для дистанційного навчання (LMS Moodle, CANVAS та інші) стало застосовуватися більш широко. Також виникла необхідність проведення дистанційних лекцій та лабораторно-практичних занять. Все це потягнуло за собою необхідність вирішувати ряд проблем з IT інфраструктурою закладів вищої освіти.

Заклади вищої освіти в Україні завжди відчували деякі фінансові трудності і не завжди охоче виділяли кошти на оновлення чи навіть повну заміну певного обладнання. Тому вирішення проблеми надання доступу користувачам до навчального середовища та програмних продуктів університету з мінімальним капіталовкладеннями стоїть завжди гостро. Необхідно виокремити, що до IT інфраструктуру входять не тільки персональні комп'ютери, принтери та інша офісна техніка, а також і серверне обладнання так й мережеве (маршрутизатори, комутатори, фаєрволи та інше). Дане обладнання відноситься до критичної інфраструктури любого ЗВО. Та передбачає відповідне налаштування, обслуговування та підтримку.

Компонування комп'ютерної мережі ЗВО, як правило, завжди є стандартним. Так одне підключення до Internet Service Provider, далі ISP , який виділяє декілька білих IP адрес для доступу у мережу. Стоїть один маршрутизатор на периметрі мережі, до якого у свою чергу під'єднане комутаційне ядро. Рівень розподілення вже іде на кожен окремий корпус/клас. Враховувати треба різні обставини і розміри ЗВО, але принцип побудови та розгортання завжди залишається похожим. Серверний сегмент мережі, виділявся у окремий VLAN. До якого йшов виділений канал. Така схема побудови є досить простою і не потребує великих як матеріальних так і фізичних затрат на її розгортання та підтримку.

Головною проблемою у таких мережах є наявність петлі L2/L3 рівня, нестабільність каналу зв'язку, можливі атаки на серверний сегмент, як із ззовні так і з середини мережі. Найчастіше у цьому всьому страждала безпека. А враховуючи теперішні обставини, необхідно терміново приймати рішення щодо впровадження безпеки і IT інфраструктуру.

Можна виділити дві атаки та інфраструктуру: зовнішню та внутрішню. Якщо атаки із ззовні можливі і на них намагаються адекватно реагувати. То внутрішні є досить болючими для цілого ЗВО. Чому так виникає. Відповідь криється у загальнодоступності мережі. Будь то студенти чи викладач, кожен генерує трафік, який не відслідковується. Скачана програма із торрент трекерів, перегляд фішингових сайтів, пошта із руткітами та інші види загроз залишають на внутрішніх персональних комп'ютерах розміщених у корпусах. Якщо прослідкувати весь трафік по мережі, то можна побачити, що впливати якимось правилами на L2 трафік можливості немає. Звичайно можна налаштувтаи безпеку портів, і досить жорстко прив'язати ПК до портів комутатора. Налаштувати ACL для L3/IP. Та все ж відслідковувати трафік, а якщо точніше сказати, проводити інспекцію пакетів неможливо.

На пограничному маршрутизаторі є відповідні правила, що забезпечують фільтрацію IP пакетів. Включений режим Port address translation, що тоже є своєрідним захистом від атак із зовні. Але всі ці дії не захищають у повному обсязі. У чому саме полягає проблема. Перша у використанні NAT/PAT. Технологія яка дозволяє маскувати сірі IP адреси внутрішньої мережі, та «ховає» серверний сегмент, має своєрідну «дирку»; якщо взламати пристрій ISP, що надає лінк до маршрутизатора. Не відбувається перевірка ініціалізованого трафіку внутрішнього трафіку, та відкликів на ці запити.

Таких можливих прогалин е мережі є досить багато, деякі повязані із обмеженнями самого обладнаннями інші через людський фактор.

Одним із рішень є застосувати на пограничному маршрутизаторі підходу, що називається Zone Base Firawall. Це дає можливість інспектувати трафік на L4-L7 рівнях, зменшує кількість опису правил по трафіку та мережі. Важливим моментом є нагрузка на центральний процесор маршрутизатора, що веде до зменшення навантаження. Що вивільняє ресурси на обробку пакетів.

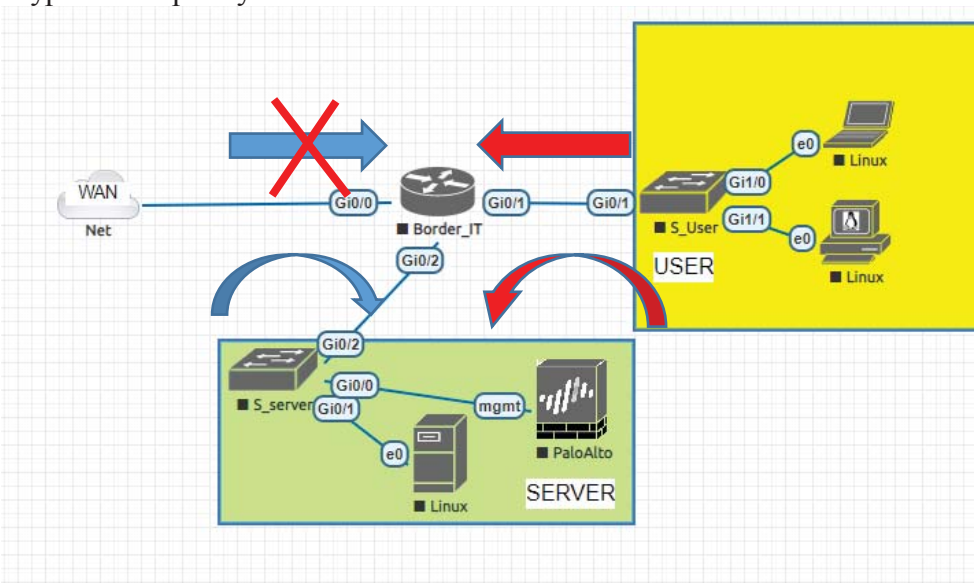

Рис. 1 Приклад застосування ZBF

На Рисунку 1 показано підхід до використання ZBF. У першу чергу, треба відмітити, що серверний сегмент треба виокремлювати у демілітаризовану зону, що є ще одним правилом у забезпеченні безпеки мережі. Для реалізації ZBF треба визначити зони, до яких відносяться відповідні інтерфейси. Лінки які направлені сторону ISP відносять до зовнішніх каналів і їх необхідно позначати як зовнішніми (WAN – позначка на рисунку). Порти з'єднанні із користувачами відносяться до користувацького сегменту – User. Також присутній сегмент серверного забезпечення. Трафік що ініціалізується з користувацького сегменту у мережу Інтернет, буде проходити через маршрутизатор, який у свою чергу запам'ятає сесію і провірить трафік що через нього проходить. Тобто, відповідь на ініціалізований запит буде проходити у середу до сегменту користувачів. Така ж сама ситуація, коли користувач заходить на серверний сегмент. Відповідь від навчальних порталів буде проходити через маршрутизатор. Перевага застосування саме такого підходу, полягає у тому, що сесія яка створюється пропускає у відповідь тільки відповідний трафік. Дані записуються у лог файл. Також дозволений трафік із зовні до серверного сегменту. Студенти будуть отримувати доступ до навчального порталу з дому. Відповідно такий трафік також буде відслідкований і в разі виявлення аномалій буде заблоковано мережу звідки проводяться незаконні дій. Щодо серверного сегменту, він не буде мати можливості виходити у будь яку із раніше описаних зон. Таким чином забезпечується безпека локальних користувачів від можливих загроз з боку серверного сегменту (якщо припустити злом серверів і зараження їх). Так і їх виходу в мережу Інтернет або атак на провайдера.

Використання даного підходу є більш ширшим і може бути розглянутим і подальших дослідженнях. Застосування комплексного підходу до забезпечення безпеки комп'ютерної мережі ЗВО, її користувачів та електронних порталів у даний час стає дуже важливим. Оскільки все частіше саме ЗВО стають під приціл атак хакерів. Можливість отримати цілі ферми серверів та їх слабка захищеність є лакомим шматком.