ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Кафедра управління інформаційною безпекою

Освітня компонента “Інструменти кібербезпеки”

Л Е К Ц І Я

Класифікація firewall-ів

План лекції:

1. Технології firewall-ів: пакетні фільтри, пограничні роутери, stateful inspection firewall-и, Host-based firewall-и, персональні firewall-и, проксі прикладного рівня, гібридні технології firewall-у.
2. Сервіс NAT. Статична, динамічна та прихована трансляція адресів.

Інформаційні джерела

Основні

1. Курс дисципліни у віртуальному університеті

Додаткові

1. Chris Sanders. PRACTICAL PACKET ANALYSIS. 3-RD EDITION. Usng Wireshark to Solve Real-World Problems.San Francisco. 2017. 450 p.
2. James D. Miller Implementing Splunk 7. Third Edition. Effective operational intelligence to transform machine-generated data into valuable business insightr. Packt Publishing. 2018. 490 p.
3. Левин М. Библия хакера 2. Книга 1. - М.: Майор, 2003. - 640 с. 4. Левин М. Библия хакера 2. Книга 2. - М.: Майор, 2003. - 688 с.
4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ.: BHV, 2009. – 607 с.

Міжмережевий екран (МЕ) — це спеціалізований комплекс міжмережевого захисту, що називається також брандмауером або системою firewall. МЕ дозволяє розділити загальну мережу на дві частини (чи більше) і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальною) мережею підприємства і глобальною мережею Internet.

Зазвичай МЕ захищають внутрішню мережу підприємства від «вторгнень» з глобальної мережі Internet, хоча вони можуть використовуватися і для захисту від «нападів» з корпоративної інтрамережі, до якої підключена локальна мережа підприємства. Технологія МЕ одна з найперших технологій захисту корпоративних мереж від зовнішніх загроз.

Для більшості організацій установка МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі.

1. Функції МЕ

Для протидії несанкціонованому міжмережевому доступу МЕ повинен розташовуватися між мережею організації, внутрішньої, що являється, що захищається, і потенційно ворожою зовнішньою мережею (Рис. 1). При цьому усі взаємодії між цими мережами повинні здійснюватися тільки через МЕ. Організаційно МЕ входить до складу мережі, що захищається.

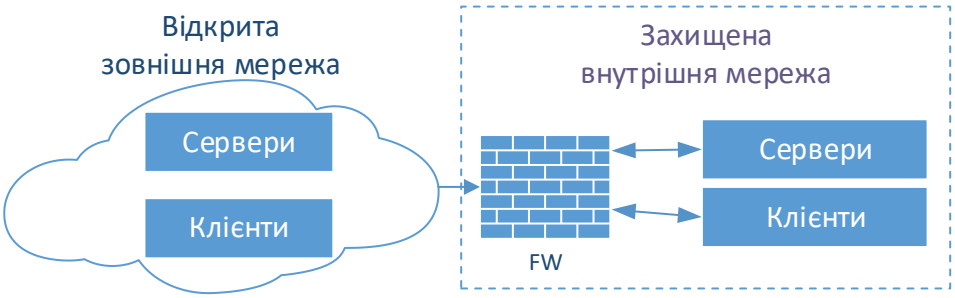

Рис. 1. Схема підключення міжмережевого екрану МЕ

МЕ, що захищає відразу безліч вузлів внутрішньої мережі, покликаний вирішити:

- завдання обмеження доступу зовнішніх (по відношенню до мережі, що захищається) користувачів до внутрішніх ресурсів корпоративній мережі. До таких користувачів можуть бути віднесені партнери, видалені користувачі, хакери і навіть співробітники самої компанії, що намагаються отримати доступ до серверів баз даних, МЕ, що захищаються;
- завдання розмежування доступу користувачів мережі, що захищається, до зовнішніх ресурсів. Рішення цієї задачі дозволяє, наприклад, регулювати доступ до серверів, що не вимагаються для виконання службових обов'язків.

Досі не існує єдиної загальновизнаної класифікації МЕ. Їх можна класифікувати, наприклад, за наступними основними ознаками [32].

По функціонуванню на рівнях моделі OSI:

- пакетний фільтр (екрануючий маршрутизатор — screening router);
- шлюз сеансового рівня (екрануючий транспорт);
- прикладний шлюз (application gateway);
- шлюз експертного рівня (stateful inspection firewall).

За використовуваною технологією:

- контроль стану протоколу (stateful inspection);
- на основі модулів посередників (proxy).

По виконанню:

- апаратно програмний;
- програмний.

За схемою підключення:

- схема єдиного захисту мережі;
- схема із закритим, що захищається, і відкритим, що не захищається, сегментами мережі;
- схема з роздільним захистом закритого і відкритого сегментів мережі.

1.1. Фільтрація трафіку

Фільтрація інформаційних потоків полягає в їх вибірковому пропусканні через екран, можливо, з виконанням деяких перетворень [9, 32]. Фільтрація здійснюється на основі набору заздалегідь завантажених в МЕ правил, таких, що відповідають прийнятій політиці безпеки. Тому МЕ зручно представляти як послідовність фільтрів, оброблювальних інформаційний потік (Рис. 2).

Рис. 2. Структура міжмережевого екрану

Кожен з фільтрів призначений для інтерпретації окремих правил фільтрації шляхом:

1) аналізу інформації за заданими в правилах, що інтерпретуються, критеріями, наприклад по адресах одержувача і відправника або за типом додатка, для якого ця інформація призначена;

2) прийняття на основі правил одного з наступних рішень, що інтерпритуються:

- не пропустити дані;
- обробити дані від імені одержувача і повернути результат відправнику;
- передати дані на наступний фільтр для продовження аналізу;
- пропустити дані, ігноруючи наступні фільтри.

Правила фільтрації можуть задавати і додаткові дії, які відносяться до функцій посередництва, напри заходів перетворення даних, реєстрація подій та ін. Відповідно правила фільтрації визначають перелік умов, по яких здійснюється:

- дозвіл або заборона подальшої передачі даних;
- виконання додаткових захисних функцій.

Як критерії аналізу інформаційного потоку можуть використовуватися наступні параметри:

- службові поля пакетів повідомлень, що містять мережеві адреси, ідентифікатори, адреси інтерфейсів, номери портів і інші значимі дані;
- безпосередній вміст пакетів повідомлень, що перевіряється, наприклад, на наявність комп'ютерних вірусів;
- зовнішні характеристики потоку інформації, наприклад, тимчасові, частотні характеристики, об'єм даних і т. д.

Використовувані критерії аналізу залежать від рівнів моделі OSI, на яких здійснюється фільтрація. У загальному випадку, чим вище рівень моделі OSI, на якому МЕ фільтрує пакети, тим вище і забезпечуваний ним рівень захисту.

1.2. Виконання функцій посередництва

Функції посередництва МЕ виконує за допомогою спеціальних програм, що називаються екрануючими агентами або програмами посередники. Ці програми є резидентними і забороняють безпосередню передачу пакетів повідомлень між зовнішньою і внутрішньою мережею.

При необхідності доступу з внутрішньої мережі в зовнішню мережу або навпаки спочатку має бути встановлене логічне з'єднання з програмою посередником, що функціонує на комп'ютері МЕ. Програма посередник перевіряє допустимість запрошеної міжмережевої взаємодії і при його дозволі сама встановлює окреме з'єднання з необхідним комп'ютером. Далі обмін інформацією між комп'ютерами внутрішньої і зовнішньої мережі здійснюється через програмного посередника, який може виконувати фільтрацію потоку повідомлень, а також здійснювати інші захисні функції.

Слід мати на увазі, що МЕ може виконувати функції фільтрації без застосування програм посередників, забезпечуючи прозору взаємодію між внутрішньою і зовнішньою мережею. В той же час програмні посередники можуть і не здійснювати фільтрацію потоку повідомлень.

У загальному випадку програми посередники, блокуючи прозору передачу потоку повідомлень, можуть виконувати наступні функції:

- перевірку достовірності передаваних даних;
- фільтрацію і перетворення потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;
- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- кешування даних, що просяться із зовнішньої мережі;
- ідентифікацію і аутентифікацію користувачів;
- трансляцію внутрішніх мережевих адрес для витікаючих пакетів повідомлень;

- реєстрацію подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і генерацію звітів [9, 32].

Програми посередники можуть здійснювати перевірку достовірності отримуваних і передаваних даних. Це актуально не лише для аутентифікації електронних повідомлень, але і мігруючих програм (Java, ActiveX Controls), по відношенню до яких може бути виконана підробка. Перевірка достовірності повідомлень і програм полягає в контролі їх цифрових підписів.

Програми посередники можуть виконувати розмежування доступу до ресурсів внутрішньої або зовнішньої мережі, використовуючи результати ідентифікації і аутентифікації користувачів при їх зверненні до МЕ.

Способи розмежування доступу до ресурсів внутрішньої мережі практично не відрізняються від способів розмежування, підтримуваних на рівні операційної системи.

При розмежуванні доступу до ресурсів зовнішньої мережі найчастіше використовується один з наступних підходів:

- дозвіл доступу тільки по заданих адресах в зовнішній мережі;
- фільтрація запитів на основі оновлюваних списків неприпустимих адрес і блокування пошуку інформаційних ресурсів за небажаними ключовими словами;
- накопичення і оновлення адміністратором санкціонованих інформаційних ресурсів зовнішньої мережі в дискової пам'яті МЕ і повна заборона доступу в зовнішню мережу.

За допомогою спеціальних посередників підтримується також кешування даних, що просяться із зовнішньої мережі. При доступі користувачів внутрішньої мережі до інформаційних ресурсів зовнішньої мережі уся інформація накопичується на просторі жорсткого диска МЕ, що називається в цьому випадку proxy сервером. Тому якщо при черговому запиті потрібна інформація виявиться на proxy сервер, то посередник надає її без звернення до зовнішньої мережі, що істотно прискорює доступ. Адміністраторові слід потурбуватися тільки про періодичне оновлення вмісту proxy сервера.

Функція кешування успішно може використовуватися для обмеження доступу до інформаційних ресурсів зовнішньої мережі. В цьому випадку усі санкціоновані інформаційні ресурси зовнішньої мережі накопичуються і оновлюються адміністратором на proxy сервері. Користувачам внутрішньої мережі дозволяється доступ тільки до інформаційних ресурсів proxy сервера, а безпосередній доступ до ресурсів зовнішньої мережі забороняється.

Фільтрація і перетворення потоку повідомлень виконується посередником на основі заданого набору правил. Тут слід розрізняти два види програм посередників:

- екрануючі агенти, орієнтовані на аналіз потоку повідомлень для певних видів сервісу, наприклад FTP, HTTP, Telnet;
- універсальні екрануючі агенти, оброблювальні увесь потік повідомлень, наприклад агенти, орієнтовані на пошук і знешкодження комп'ютерних вірусів, або прозоре шифрування даних.

Програмний посередник аналізує пакети даних, що поступають до нього, і, якщо будь-якої об'єкт не відповідає заданим критеріям, то або блокує його подальше просування, або виконує відповідні перетворення, наприклад

знешкоджує виявлені комп'ютерні віруси. При аналізі вмісту пакетів важливо, щоб екрануючий агент міг автоматично розпаковувати файлові архіви.

МЕ з посередниками дозволяють також організовувати захищені віртуальні мережі VPN (Virtual Private Network), наприклад безпечно об'єднувати декілька локальних мереж, підключених до Internet, в одну віртуальну мережу.

1.3. Додаткові можливості МЕ

Окрім виконання фільтрації трафіку і функцій посередництва деякі МЕ дозволяють реалізовувати інші, не менш важливі функції, без яких забезпечення захисту периметра внутрішньої мережі було б неповним .

Ідентифікація і аутентифікація користувачів. Окрім дозволу або заборони допуску різних застосувань в мережу, МЕ можуть також виконувати аналогічні дії і для користувачів, які бажають отримати доступ до зовнішніх або внутрішніх ресурсів, МЕ, що розділяється.

Перш ніж користувачеві буде надано право використання будь-якого сервісу, необхідно переконатися, що він дійсно той, за кого себе видає. Ідентифікація і аутентифікація користувачів є важливими компонентами концепції МЕ. Авторизація користувача зазвичай розглядається в контексті аутентифікації — як тільки користувач аутентифікований, для нього визначаються дозволені йому сервіси.

Ідентифікація і аутентифікація користувача іноді здійснюються при пред'явленні звичайного ідентифікатора (імені) і пароля. Проте ця схема уразлива з точки зору безпеки — пароль може бути перехоплений і використаний іншою особою. Багато інцидентів в мережі Internet сталися частково через уразливості традиційних багаторазових паролів. Зловмисники можуть спостерігати за каналами в мережі Internet і перехоплювати ті, що передаються в них відкритим текстом паролі, тому така схема аутентифікації вважається неефективною. Пароль слід передавати через загальнодоступні комунікації в зашифрованому виді (Рис. 3). Це дозволяє запобігти діставанню несанкціонованого доступу шляхом перехоплення мережевих пакетів.

Надійнішим методом аутентифікації є використання одноразових паролів. Широке поширення отримала технологія аутентифікації на основі одноразових паролів SecurID (див. л. 7 і 13).

Зручно і надійно також застосування цифрових сертифікатів, що видаються довіреними органами, наприклад центром розподілу ключів. Більшість програм посередників розробляються так, щоб користувач аутентифікувався тільки на початку сеансу роботи з МЕ. Після цього від нього не потрібно додаткової аутентифікації впродовж часу, визначуваного адміністратором.

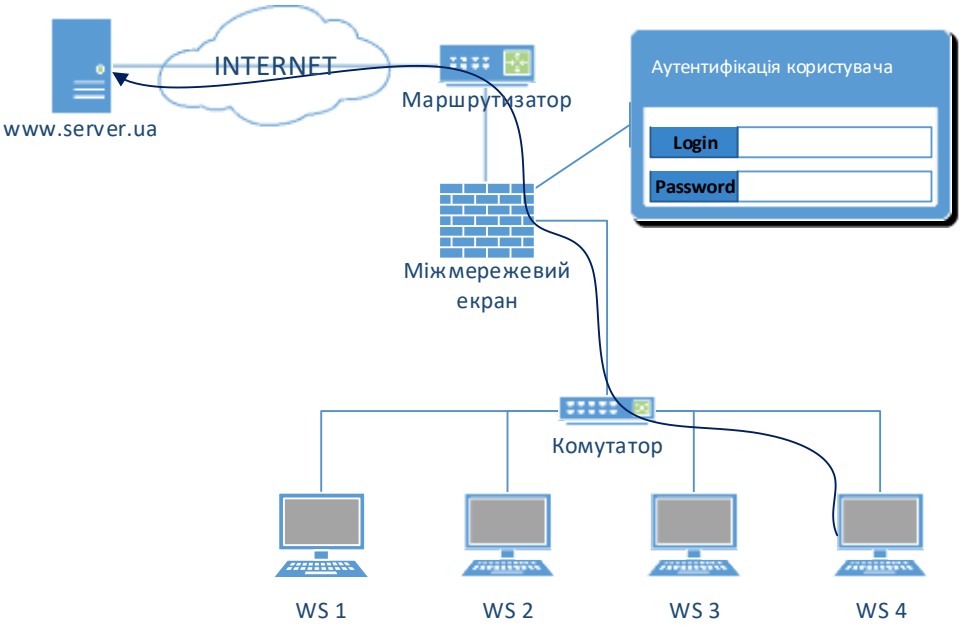

Рис. 3. Схема аутентифікації користувача по паролю

Оскільки МЕ можуть централізувати управління доступом в мережі, вони є відповідним місцем для установки програм або облаштувань посиленої аутентифікації. Хоча засоби посиленої аутентифікації можуть використовуватися на кожному хості, більше практичне їх розміщення на МЕ. За відсутності МЕ, що використовує заходи посиленої аутентифікації, неаутентифікований трафік таких застосувань, як Telnet або FTP, може безпосередньо проходити до внутрішніх систем в мережі.

Ряд МЕ підтримують Kerberos — один з поширених методів аутентифікації. Як правило, більшість комерційних МЕ підтримують декілька різних схем аутентифікації, дозволяючи адміністраторові мережевої безпеки зробити вибір найбільш прийнятної схеми для своїх умов.

Трансляція мережевих адрес. Для реалізації багатьох атак зловмисникові необхідно знати адресу своєї жертви. Щоб приховати ці адреси, а також топологію усієї мережі, МЕ виконують дуже важливу функцію — трансляцію внутрішніх мережевих адрес (Рис. 4).

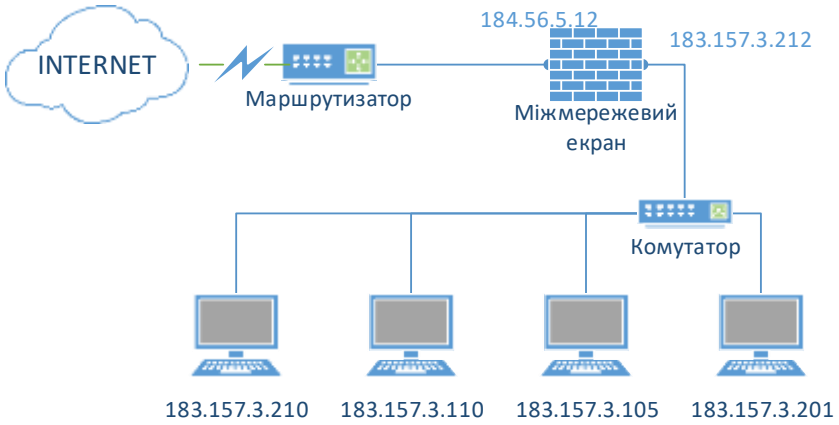

Рис. 4. Трансляція мережевих адрес

Ця функція реалізується по відношенню до усіх пакетів, що виходять з внутрішньої мережі в зовнішню. Для цих пакетів виконується автоматичне перетворення IP-адрес комп'ютерів відправників в один «надійний» IP-адрес.

Трансляція внутрішніх мережевих адрес може здійснюватися двома способами — динамічно і статично. У першому випадку адреса виділяється вузлу у момент звернення до МЕ. Після завершення з'єднання адреса звільняється і може бути використаний будь-яким іншим вузлом корпоративної мережі. У другому випадку адреса вузла завжди прив'язується до однієї адреси МЕ, з якої передаються усі вихідні пакети. IPадрес МЕ стає єдиним активним IP-адресом, який потрапляє в зовнішню мережу. В результаті усі пакети, що виходять з внутрішньої мережі, виявляються відправленими МЕ, що виключає прямий контакт між авторизованою внутрішньою мережею і що є потенційно небезпечною зовнішньою мережею.

При такому підході топологія внутрішньої мережі прихована від зовнішніх користувачів, що ускладнює завдання несанкціонованого доступу. Окрім підвищення безпеки трансляція адрес дозволяє мати усередині мережі власну систему адресації, не погоджену з адресацією в зовнішній мережі, наприклад в мережі Internet. Це ефективно вирішує проблему розширення адресного простору внутрішньої мережі і дефіциту адрес зовнішньої мережі.

Адміністрування, реєстрація подій і генерація звітів.

Простота і зручність адміністрування є одним з ключових аспектів в створенні ефективної і надійної системи захисту. Помилки при визначенні правил доступу можуть утворити діру, через яку можливий злом системи. Тому у більшості МЕ реалізовані сервісні утиліти, що полегшують введення, видалення, перегляд набору правил. Наявність цих утиліт дозволяє також робити перевірки на синтаксичні або логічні помилки при введенні або редагування правил. Як правило, утиліти дозволяють переглядати інформацію, згруповану за будь-яким критеріями, наприклад все, що відноситься до конкретного користувача або сервісу.

Важливими функціями МЕ є реєстрація подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і складання звітів. МЕ, будучи критичним елементом системи захисту корпоративної мережі, має можливість реєстрації усіх дій, їм що фіксуються. До таких дій відносяться не лише пропуск або блокування мережевих пакетів, але і зміна правил розмежування доступу адміністратором безпеки і інші дії. Така реєстрація дозволяє звертатися до створюваних журналів в міру необхідності (у разі виникнення інциденту безпеки або збору доказів для надання їх в судові інстанції або для внутрішнього розслідування).

При правильно налагодженій системі фіксації сигналів про підозрілі події (alarm) МЕ може дати детальну інформацію про те, чи були МЕ або мережа атаковані або зондовані. Збирати статистику використання мережі і доказу її зондування важливо з кількох причин. Передусім треба знати напевно, що МЕ стійкий до зондування і атак, і визначити, чи адекватні заходи захисту МЕ. Крім того, статистика використання мережі важлива в якості початкових даних при проведенні досліджень і аналізі ризику для формулювання вимог до мережевого устаткування і програм.

Багато МЕ містять потужну систему реєстрації, збору і аналізу статистики. Облік може вестися по адресах клієнта і сервера, ідентифікаторах користувачів, часу сеансів, часу з'єднань, кількості переданих/прийнятих даних, діях

адміністратора і користувачів. Системи обліку позволяют зробити аналіз статистики і надають адміністраторам детальні звіти. За рахунок використання спеціальних протоколів МЕ можуть виконати видалене сповіщення про певні події в режимі реального часу.

В якості обов'язкової реакції на виявлення спроб виконання несанкціонованих дій має бути визначене повідомлення адміністратора, т. е. видача попереджувальних сигналів. Будь-який МЕ, який не здатний посилати попереджувальні сигнали при виявленні нападу, не можна вважати ефективним засобом міжмережевого захисту.

2. Особливості функціонування МЕ на різних рівнях моделі OSI

МЕ підтримують безпеку міжмережевої взаємодії на різних рівнях моделі OSI. При цьому функції захисту, що виконуються на різних рівнях еталонної моделі, істотно відрізняються один від одного. Тому комплексний МЕ зручно представити у вигляді сукупності неділимих екранів, кожен з яких орієнтований на окремий рівень моделі OSI.

Найчастіше комплексний екран функціонує на мережевому, сеансовому і прикладному рівнях еталонної моделі. Відповідно розрізняють такі неділимі МЕ (Рис. 5), як:

- екрануючий маршрутизатор;
- шлюз сеансового рівня (екрануючий транспорт);
- шлюз прикладного рівня (екрануючий шлюз) [9, 32].

Використовувані в мережах протоколи (TCP/IP, SPX/IPX) не повністю відповідають еталонній моделі OSI, тому екрани перерахованих типів при виконанні своїх функцій можуть охоплювати і сусідні рівні еталонної моделі. Наприклад, прикладний екран може здійснювати автоматичне зашифровування повідомлень при їх передачі в зовнішню мережу, а також автоматичну розшифровку криптографічний закритих даних, що приймаються. В цьому випадку такий екран функціонує не лише на прикладному рівні моделі OSI, але і на рівні представлення.

Шлюз сеансового рівня при своєму функціонуванні охоплює транспортний і мережевий рівні моделі OS1. Екрануючий маршрутизатор при аналізі пакетів повідомлень перевіряє їх заголовки не лише мережевого, але і транспортного рівня.

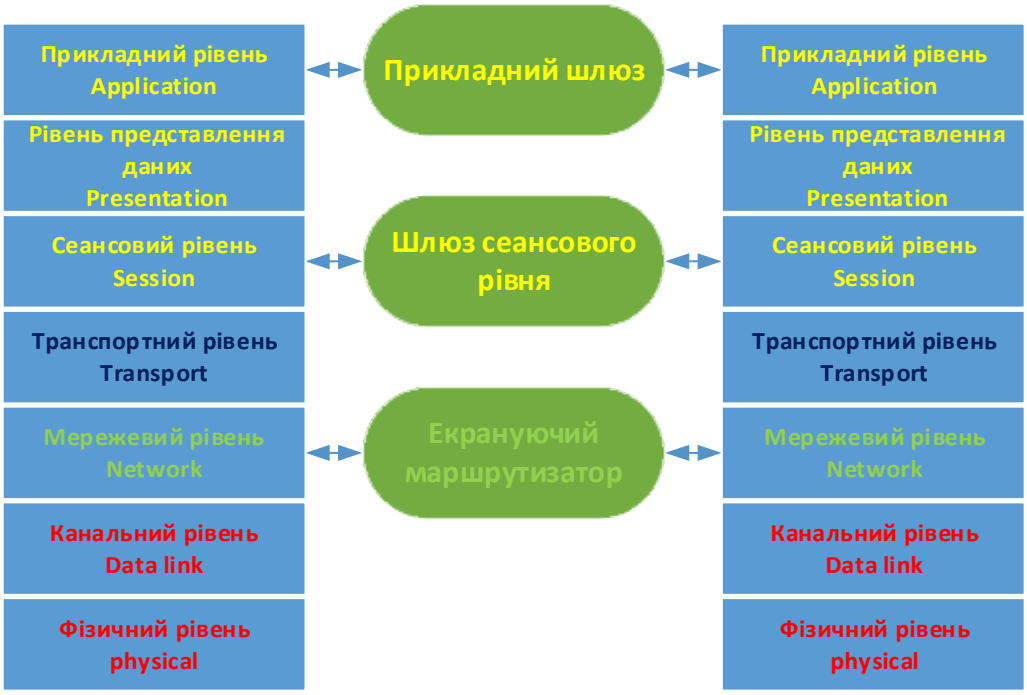

Рис. 5. Типи міжмережевих екранів, що функціонують на окремих рівнях моделі OSI

МЕ вказаних типів мають свої Переваги і недоліки. Багато хто з використовуваних МЕ є або прикладними шлюзами, або екрануючими маршрутизаторами, не забезпечуючи повну безпеку міжмережевої взаємодії. Надійний захист забезпечують тільки комплексні міжмережеві екрани, кожен з яких об'єднує екрануючий маршрутизатор, шлюз сеансового рівня, а також прикладний шлюз.

Розглянемо функціонування прикладного шлюзу.

9.2.1. Прикладний шлюз

Прикладний шлюз, що називається також екрануючим шлюзом, функціонує на прикладному рівні моделі OSI, охоплюючи також рівень представлення, і забезпечує найбільш надійний захист міжмережевих взаємодій [9, 32]. Захисні функції прикладного шлюзу, як і шлюзу сеансового рівня, відносяться до функцій посередництва. Проте прикладний шлюз, на відміну від шлюзу сеансового рівня, може виконувати істотно більшу кількість функцій захисту, до яких відносяться наступні:

- ідентифікація і аутентифікація користувачів при спробі встановлення з'єднань через МЕ;
- перевірка достовірності інформації, що передається через шлюз;
- розмежування доступу до ресурсів внутрішньої і зовнішньої мереж;
- фільтрація і перетворення потоку повідомлень, наприклад динамічний пошук вірусів і прозоре шифрування інформації;
- реєстрація подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і генерація звітів;
- кешування даних, що просяться із зовнішньої мережі.

Оскільки функції прикладного шлюзу відносяться до функцій посередництва, цей шлюз є універсальним комп'ютером, на якому функціонують

програмні посередники (екрануючі агенти), — по одному для кожного обслуговуваного прикладного протоколу (HTTP, FTP, SMTP, NNTP та ін.). Програмний посередник (application proxy) кожної служби TCP/IP орієнтований на обробку повідомлень і виконання функцій захисту, що відносяться саме до цієї служби.

Прикладний шлюз перехоплює за допомогою відповідних екрануючих агентів пакети, що входять та виходять, копіює і перенаправляє інформацію, т. е. функціонує в якості сервера посередника, виключаючи прямі з'єднання між внутрішньою і зовнішньою мережею (Рис. 6).

Посередники, використовувані прикладним шлюзом, мають важливі відмінності від канальних посередників шлюзів сеансового рівня

Рис. 6. Схема функціонування прикладного шлюзу

Поперше, посередники прикладного шлюзу пов'язані з конкретними застосуваннями (програмними серверами), подруге, вони можуть фільтрувати потік повідомлень на прикладному рівні моделі OSI.

Прикладні шлюзи використовують як посередників спеціально розроблені для цієї мети програмні сервери конкретних служб TCP/IP — сервери HTTP, FTP, SMTP, NNTP та ін. Ці програмні сервери функціонують на МЕ в резидентному режимі і реалізують функції захисту, що відносяться до відповідних служб TCP/IP.

Шлюз прикладного рівня має наступні переваги:

- забезпечує високий рівень захисту локальної мережі завдяки можливості виконання більшості функцій посередництва;
- захист на рівні додатків дозволяє здійснювати велике число додаткових перевірок, зменшуючи тим самим вірогідність проведення успішних атак, можливих через недоліки програмного забезпечення;
- при порушенні його працездатності блокується наскрізне проходження пакетів між мережами, що розділяються, внаслідок чого безпека мережі, що захищається, не знижується через виникнення відмов.

До недоліків прикладного шлюзу відносяться:

- високі вимоги до продуктивності і ресурсоємності комп'ютерної платформи;
- відсутність «прозорості» для користувачів і зниження пропускної спроможності при реалізації міжмережевих взаємодій.

2.2. Варіанти виконання МЕ

Існує два основні варіанти виконання МЕ — програмний і програмно апаратний. У свою чергу програмно апаратний варіант має два різновиди — у вигляді спеціалізованого пристрою і у вигляді модуля в маршрутизаторі або комутаторі.

Нині частіше використовується програмне рішення, яке на перший погляд виглядає привабливішим. Це пов'язано з тим, що для його застосування досить, тільки придбати програмне забезпечення (ПЗ) МЕ і встановити на будь-який комп'ютер, наявний в організації. Проте на практиці далеко не завжди в організації знаходиться вільний комп'ютер, що задовольняє досить високим вимогам по системних ресурсах. Тому одночасно з придбанням ПЗ отримується і комп'ютер для його установки. Потім слідує процес установки на комп'ютер операційної системи (ОС) і її налаштування, що також вимагає часу і оплати роботи установників. І тільки після цього встановлюється і настроюється ПЗ системи виявлення атак. Неважко помітити, що використання звичайного персонального комп'ютера далеке не так просто, як здається на перший погляд.

Тому останніми роками значно зріс інтерес до програмно апаратним рішень [9, 32], які поступово витісняють «чисто» програмні системи. Широкого поширення стали набувати спеціалізовані програмно апаратні рішення, що називаються security appliance. Програмно апаратний комплекс міжмережевого екранування зазвичай складається з комп'ютера, а також ОС, що функціонують на нім, і спеціального ПЗ. Слід зазначити, що це спеціальне ПЗ часто називають firewall. Використовуваний комп'ютер має бути досить потужним і фізично захищеним, наприклад знаходитися в спеціально відведеному приміщенні, що охороняється. Крім того, він повинен мати засоби захисту від завантаження ОС з несанкціонованого носія. Програмноапаратні комплекси використовують спеціалізовані або звичайні ПЗ (як правило, на базі FreeBSD, Linux або Microsoft Windows, «урізані» для виконання заданих функцій і задовольняючі ряду вимог:

- мати засоби розмежування доступу до ресурсів системи;
- блокувати доступ до комп'ютерних ресурсів в обхід програмного інтерфейсу, що надається;
- забороняти привілейований доступ до своїх ресурсів з локальної мережі;
- містити засоби моніторингу/аудиту будь-яких адміністративних дій.

Переваги спеціалізованих програмно-апаратних рішень:

- простота впровадження в технологію обробки інформації. Такі засоби поставляються із заздалегідь встановленою і налагодженою ОС і захисними механізмами, тому необхідно тільки підключити їх до мережі, що виконується впродовж декількох хвилин;
- простота управління. Ці засоби можуть управлятися з будь-якої робочої станції Windows 9x, NT, 2000 або Unix. Взаємодія консолі управління з пристроєм здійснюється або по стандартних протоколах, наприклад Telnet або SNMP, або за допомогою спеціалізованих або захищених протоколів, наприклад SSH або SSL;
- відмовостійкість і висока доступність. Виконання МЕ у вигляді спеціалізованого програмноапаратного комплексу дозволяє реалізувати механізми

забезпечення не лише програмної, але і апаратної відмовостійкості і високої доступності;

- висока продуктивність і надійність. За рахунок виключення з ОС усіх «непотрібних» сервісів і підсистем, програмноапаратний комплекс працює ефективніше з точки зору продуктивності і надійності;
- спеціалізація на захисті. Рішення тільки завдань забезпечення мережевої безпеки не призводить до витрат ресурсів на виконання інших функцій, наприклад маршрутизації і т. п.

3. Схеми мережевого захисту на базі МЕ

При підключенні корпоративної або локальної мережі до глобальних мереж потрібні:

- захист корпоративної або локальної мережі від віддаленого НСД з боку глобальної мережі;
- приховання інформації про структуру мережі і її компонентів від користувачів глобальної мережі;
- розмежування доступу в мережу, що захищається, з глобальної мережі і з мережі, що захищається, в глобальну мережу.

Для ефективного захисту міжмережевої взаємодії система МЕ має бути правильно встановлена і конфігурована. Цей процес полягає:

- з формування політики міжмережевої взаємодії;
- вибору схеми підключення і налаштування параметрів функціонування МЕ.

3.1. Формування політики міжмережевої взаємодії

Політика міжмережевої взаємодії є складовою частиною загальної політики безпеки в організації. Вона визначає вимоги до безпеки інформаційного обміну організації із зовнішнім світом і повинна відбивати два аспекти [9, 32]:

- політику доступу до мережевих сервісів;
- політикові роботи МЕ.

Політика доступу до мережевих сервісів визначає правила надання і використання усіх можливих сервісів комп'ютерної мережі, що захищається. У рамках цієї політики мають бути задані усі сервіси, що надаються через МЕ, і допустимі адреси клієнтів для кожного сервісу. Крім того, для користувачів мають бути вказані правила, що описують, коли, хто, яким сервісом і на якому комп'ютері може скористатися. Задаються також обмеження на методи доступу, наприклад на використання протоколів SLIP (Serial Line Internet Protocol) і PPP (PointtoPoint Protocol). Обмеження методів доступу потрібне для того, щоб користувачі не могли звертатися до «заборонених» сервісів Internet обхідними шляхами. Правила аутентифікації користувачів і комп'ютерів, а також умови роботи користувачів поза локальною мережею організації мають бути визначені окремо.

Для того, щоб МЕ успішно захищав ресурси організації, політика доступу користувачів до мережевих сервісів має бути реалістичною. Реалістичною вважається така політика, при якій знайдений баланс між захистом мережі організації від відомих ризиків і необхідним доступом користувачів до мережевих сервісів.

Політика роботи МЕ задає базовий принцип управління міжмережевою взаємодією, покладений в основу функціонування МЕ. Може бути вибраний один з двох принципів:

1) заборонено все, що явно не дозволене;
2) дозволено все, що явно не заборонене.

Фактично вибір принципу встановлює, наскільки «підозрілою» або «довірчою» має бути система захисту. Залежно від вибору, рішення може бути прийняте як на користь безпеки і на шкоду зручності використання мережевих сервісів, так і навпаки.

При виборі принципу 1 МЕ настроюється так, щоб блокувати будь-які явно не дозволені міжмережеві взаємодії. Цей принцип відповідає класичній моделі доступу, використовуваної в усіх областях інформаційної безпеки. Такий підхід дозволяє адекватно реалізувати принцип мінімізації привілеїв, тому з точки зору безпеки він є кращим. Адміністратор безпеки повинен на кожен тип дозволеної взаємодії задавати правила доступу (одне і більше). Адміністратор не зможе по забудькуватості залишити дозволеними будьякі повноваження, оскільки за умовчанням вони будуть заборонені. Доступні зайві сервіси можуть бути використані на шкоду безпеці, що особливо характерно для закритого і складного ПЗ, в якому можуть бути різні помилки і некоректності. Принцип 1, по суті, є визнанням факту, що незнання може завдати шкоди. Слід зазначити, що правила доступу, сформульовані відповідно до цього принципу, можуть доставляти користувачам певні незручності.

При виборі принципу 2 МЕ настроюється так, щоб блокувати тільки явно заборонені міжмережеві взаємодії. В цьому випадку підвищується зручність використання мережевих сервісів з боку користувачів, але знижується безпека міжмережевої взаємодії. Користувачі мають більше можливостей обійти МЕ, наприклад, можуть отримати доступ до нових сервісів, що не забороняються політикою (або навіть не вказаним в політиці), або запустити заборонені сервіси на нестандартних портах TCP/UDP, які не заборонені політикою. Адміністратор може врахувати не усі дії, які заборонені користувачам. Йому доводиться працювати в режимі реагування, передбачаючи і забороняючи ті міжмережеві взаємодії, які негативно впливають на безпеку мережі. При реалізації принципу 2 внутрішня мережа виявляється менш захищеною від нападів хакерів, тому виробники МЕ зазвичай відмовляються від його використання.

МЕ є симетричним. Для нього окремо задаються правила, що обмежують доступ з внутрішньої мережі в зовнішню мережу, і навпаки. У загальному випадку його робота заснована на динамічному виконанні двох функцій:

- фільтрації інформаційних потоків, що проходять через нього;
- посередництва при реалізації міжмережевих взаємодій.

Залежно від типу екрану ці функції можуть виконуватися з різною повнотою. Прості МЕ орієнтовані на виконання тільки одній з них. Комплексні МЕ забезпечують спільне виконання вказаних функцій захисту. Власна захищеність МЕ досягається за допомогою тих же засобів, що і захищеність універсальних систем [9].

Щоб ефективно забезпечувати безпеку мережі, комплексний МЕ зобов'язаний управляти усім потоком, що проходить через нього, і відстежувати свій стан. Для ухвалення рішень, що управляють, по використовуваних сервісах

МЕ повинен отримувати, запам'ятовувати, вибирати і обробляти інформацію, отриману від усіх комунікаційних рівнів і від інших застосувань.

Недостатньо просто перевіряти пакети окремо. Інформація про стан з'єднання, отримана з інспекції з'єднань у минулому і інших застосувань — головний чинник в ухваленні рішення, що управляє, при встановленні нового з'єднання. При ухваленні рішення враховуються як стан з'єднання (отримане з минулого потоку даних), так і стан додатка (отримане з інших застосувань). Повнота і правильність управління вимагають, щоб комплексний МЕ мав можливість аналізу і використання наступних елементів:

- інформації про з'єднання — інформацію від усіх семи рівнів в пакеті;
- історії з'єднань — інформація, отримана від попередніх з'єднань;
- стану рівня додатка — інформація про стан, отриманого з інших застосувань. Наприклад, аутентифікованому користувачеві можна надати доступ через МЕ тільки для авторизованих видів сервісу;
- агрегуючих елементів — обчислення різноманітних виразів, заснованих на усіх вищеперелічених чинниках.

3.2. Основні схеми підключення МЕ

При підключенні корпоративної мережі до глобальних мереж необхідно розмежувати доступ в мережу, що захищається, з глобальної мережі і з мережі, що захищається, в глобальну мережу, а також забезпечить захист мережі, що підключається, від видаленого НСД з боку глобальної мережі. При цьому організація зацікавлена в прихованні інформації про структуру своєї мережі і її компонентів від користувачів глобальної мережі. Робота з видаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається.

Часто виникає потреба мати у складі корпоративної мережі декілька сегментів з різними рівнями захищеності:

- вільно доступні сегменти (наприклад, рекламний WWW сервер);
- сегмент з обмеженим доступом (наприклад, для доступу співробітникам організації з видалених вузлів);
- закриті сегменти (наприклад, фінансова локальна підмережа організації).

Для підключення МЕ можуть використовуватися різні схеми, які залежать від умов функціонування мережі, що захищається, а також від кількості мережевих інтерфейсів і інших характеристик, використовуваних МЕ. Широке поширення отримали схеми:

- захисту мережі з використанням екрануючого маршрутизатора;
- єдиного захисту локальної мережі;
- із закритою, що захищається, і відкритою, що не захищається, підмережами;
- з роздільним захистом закритої і відкритої підмереж [9, 32].

Розглянемо детальніше схему із закритою, що захищається, і не відкритою, що захищається, підмережами. Якщо у складі локальної мережі є загальнодоступні відкриті сервери, то їх доцільно винести як відкриту підмережу

до МЕ (Рис. 7). Цей спосіб має високу захищеність закритої частини локальної мережі, але забезпечує знижену безпеку відкритих серверів, розташованих до МЕ.

Рис. 7. Схема із закритою, що захищається, і відкритою, що не захищається, під мережами

Деякі МЕ дозволяють розмістити ці сервери на собі. Проте таке рішення не є кращим з точки зору безпеки самого МЕ і завантаження комп'ютера. Схему підключення МЕ із закритою підмережею, що захищається, і відкритою підмережею, що не захищається, доцільно використати лише при невисоких вимогах по безпеці до відкритої підмережі.

Якщо ж до безпеки відкритих серверів пред'являються підвищені вимоги, тоді необхідно використати схему з роздільною зашитою закритою і відкритою підмереж.

3.3. Персональні і розподілені мережеві екрани

За останні декілька років в структурі корпоративних мереж сталися певні зміни. Якщо раніше межі таких мереж можна було чітко обкреслити, то зараз це практично неможливо. Ще нещодавно така межа проходила через усі маршрутизатори або інші пристрої (наприклад, модеми), через які здійснювався вихід в зовнішні мережі. У видалених офісах організації ситуація була схожа. Проте зараз повноправним користувачем МЕ мережі, що захищається, є співробітник, що знаходиться за межами периметра, що захищається. До таких співробітників відносяться користувачі, працюючі вдома або що знаходяться у відрядженні. Поза сумнівом їм також потрібно захист. Але все традиційні МЕ побудовані так, що користувачі, що захищаються, і ресурси повинні знаходитися під їх зашитою з внутрішньої сторони корпоративної або локальної мережі, що є неможливим для мобільних користувачів.

Для вирішення цієї проблеми були запропоновані наступні підходи:

- застосування розподілених МЕ (distributed firewall);
- використання можливостей віртуальних приватних мереж VPN (л. 10).

Розподілений міжмережевий екран (distributed firewall) — централізована керована сукупність мережевих мініекранів, що захищають окремі комп'ютери мережі.

Для індивідуальних користувачів представляє інтерес технологія персонального мережевого екранування. В цьому випадку мережевий екран встановлюється на персональний комп'ютер, що захищається. Такий екран, що

називається персональним екраном комп'ютера (personal firewall) або системою мережевого екранування, контролює увесь вихідний трафік, що входить, незалежно від усіх інших системних захисних засобів. При екрануванні окремого комп'ютера підтримується доступність мережевих сервісів, але зменшується навантаження, що створюється зовнішньою активністю. В результаті знижується уразливість внутрішніх сервісів комп'ютера, що захищається таким чином, оскільки спочатку сторонній зловмисник повинен здолати екран, де захисні засоби конфігуровані особливо ретельно і жорстко.

Ці засоби не лише захищають від зовнішніх атак комп'ютери, на яких вони встановлені, але і забезпечують захист трафіку, що передається за межі цього вузла (т. е. організовують захищені канали VPN). Саме таке рішення дозволило забезпечити захист мереж з нечітко обкресленими межами.

Наявність функції централізованого управління у розподіленого МЕ — його головна відмінність від персонального екрану. Якщо персональні мережеві екрани управляються тільки з комп'ютера, на якому вони встановлені, і ідеально підходять для домашнього застосування, то розподілені МЕ можуть управлятися централізований, з єдиної консолі управління, встановленої в головному офісі організації. Це дозволило деяким виробникам випускати МЕ в двох версіях:

- персональною (для індивідуальних користувачів);
- розподіленою (для корпоративних користувачів).

У сучасних умовах більше 50 % різних атак і спроб доступу до інформації здійснюється зсередини локальних мереж, тому класичний «периметровий» підхід до створення системи захисту корпоративної мережі стає недостатньо ефективним. Корпоративну мережу можна вважати дійсно захищеною від НСД тільки за наявності в ній засобів захисту точок входу з боку Internet і рішень, що забезпечують безпеку окремих комп'ютерів, корпоративних серверів і фрагментів локальної мережі підприємства. Рішення на основі розподілених або персональних МЕ най

кращим чином забезпечують безпеку окремих комп'ютерів, корпоративних серверів і фрагментів локальної мережі підприємства [64].

3.4. Проблеми безпеки МЕ

МЕ не вирішує усі проблеми безпеки корпоративної мережі. Окрім описаних вище достоїнств МЕ, існують обмеження в їх використанні і загрози безпеки, від яких МЕ не можуть захистити. Відмітимо найбільш суттєві з цих обмежень [9, 43]:

- можливе обмеження пропускної спроможності. Традиційні МЕ є потенційно вузьким місцем мережі, оскільки усі з'єднання повинні проходити через МЕ і в деяких випадках вивчатися МЕ;
- відсутність вбудованих механізмів захисту від вірусів. Традиційні МЕ не можуть захистити від користувачів, що завантажують заражені вірусами програми для ПЕВМ з інтернетівських архівів або при передачі таких програм в якості додатків до листа, оскільки ці програми можуть бути зашифровані або стислі великим числом способів;
- відсутність ефективного захисту від отримуваного з Internet небезпечного вмісту (аплети Java, елементи ActiveX, що управляють, сценарії

JavaScript і т. д.). Специфіка мобільного коду така, що він може бути використаний як засіб для проведення атак. Мобільний код може бути реалізований у виді:

— вірусу, який вторгається в ІС і знищує дані на локальних дисках, постійно модифікуючи свій код і утрудняючи тим самим своє виявлення і видалення;

— агента, що перехоплює паролі, номери кредитних карт і т. д.;

— програми, що копіює конфіденційні файли, що містять ділову і фінансову інформацію і ін.;

• МЕ не може захистити від помилок і некомпетентності адміністраторів і користувачів;

• традиційні МЕ є по суті засобами, тільки блокуючими атаки. У більшості випадків вони захищають від атак, які вже знаходяться в процесі створення. Ефективнішим було б не лише блокування, але і попередження атак, т. е. усунення передумов реалізації вторгнень. Для організації попередження атак необхідно використати засоби виявлення атак і пошуку вразливості, які своєчасно виявлятимуть і рекомендуватимуть заходи по усуненню «слабких місць» в системі захисту. Технології виявлення атак і аналізу захищеності мереж розглядаються в л. 14.

Для захисту інформаційних ресурсів розподілених корпоративних систем потрібне застосування комплексної системи інформаційної безпеки, яка дозволить ефективно використати Переваги МЕ і компенсувати їх недоліки за допомогою інших засобів безпеки.