Захист інформації під час роботи в комп'ютерних мережах

Більшість реалізацій стека TCP/IP успадковують функції стека, розробленого більше 40 років тому, коли вимоги безпеки практично були відсутні і їм спочатку притаманна вразливість. Стек TCP/IP - базовий стек для Інтернет, як і більшість програмних засобів (включно з операційними системами FreeBSD, Linux) є відкритими і існує можливість використання хакерами "дір", які з'являються в тому чи іншому продукті і висвітлюються в Інтернет.

Класифікація мережевих атак та засоби їх попередження

Мережева розвідка - збір інформації про мережу за допомогою загальнодоступних даних та програм, наприклад, використання ping для виявлення адрес мережі, сканування портів, запити до DNS для дозволу адрес в імена хостів і навпаки.

Сканування портів - це процес зондування комп'ютера, сервера або іншого мережного пристрою для виявлення відкритих портів. В мережах кожному застосунку, запущеному на пристрої, призначається ідентифікатор, який називається номером порту. Саме завдяки використанню цього номера на обох кінцях сеансу зв'язку необхідні дані передаються до потрібного застосунку. Сканування портів може використовуватися зі зловмисною метою як розвідувальний інструмент для ідентифікації операційної системи та служб, що працюють на комп'ютері або іншому пристрої. А також цей підхід застосовується мережним адміністратором для перевірки політик безпеки в мережі.

Для захисту від атак цього типу можна рекомендувати:

- використання систем виявлення атак – Intrusion Detection System (IDS);
- заборона проходження пакетів ICMP.

Система виявлення вторгнень (Intrusion Detection System, IDS) може бути окремим мережним пристроєм або одним з кількох інструментів на сервері чи міжмережному екрані, який сканує трафік відповідно до бази даних правил або сигнатур у пошуках шкідливих атак. При виявленні відповідності правилам або сигнатурам IDS реєструє виявлення атаки та створює попередження для мережного адміністратора. Система виявлення вторгнень не запобігає атакам, оскільки не вживає ніяких дій при виявлення інциденту. Завдання IDS - виключно виявлення, реєстрація та створення попередження.

Сканування, яке виконує IDS, уповільнює роботу мережі (відоме як латентність). Щоб запобігти затримці у мережі , IDS зазвичай розміщують офлайн (в автономному режимі), окремо від звичайного мережного трафіку. Дані копіюються або віддзеркалюються комутатором, а потім пересилаються до IDS для проведення аналізу в режимі офлайн. Існують також інструменти IDS, які можна встановлювати поверх операційної системи комп'ютера, наприклад Linux або Windows.

Система запобігання вторгненням (Intrusion Prevention System, IPS) має можливість блокувати або відхиляти трафік на основі спрацювання правила або відповідної сигнатури. Однією з найбільш відомих систем IPS/IDS є Snort. Комерційна версія Snort - це Cisco’s Sourcefire. Sourcefire має можливість у реальному часі виконувати аналіз трафіку і портів, ведення журналів, пошук і зіставлення контенту, а також виявлення спроб зондування, атак і сканування портів. Це рішення також інтегрується з іншими сторонніми інструментами для створення звітності, аналізу лог-файлів та продуктивності.

Парольні атаки – виконуються з метою виявлення паролів користувачів на доступ до системи. Найпростіший варіант - перехоплення мережевих пакетів з даними

реєстрації telnet-сервера, FTP-сервера або POP3-сервера, складніші - копіювання файлів, що зберігають бази з ідентифікаторами користувачів та паролями (Sam для Windows, masterpasswd для UNIX-систем) та їх зламування методами перебору за словником або повним перебором (brute-force).

Загроза парольних атак може бути знижена такими способами:

- використанням складних паролів, що включають малі та великі символи, цифри, службові символи та мають достатню довжину (не менше 8 символів).
- використанням "сильної" аутентифікації - наприклад, з використанням біометричних засобів або одноразових паролів. Застосування методів автентифікації, які не надсилають відкритий пароль по мережі.
- розробкою та впровадженням політики безпеки - "формальних правил, яким повинні підкорятися люди, які отримують доступ до корпоративної технології та інформації" - (RFC 2196).

Сніфери пакетів - програми, що використовують мережну карту, яка працює в "нерозбірливому режимі" (promiscuous mode), і що копіюють у свій буфер всі пакети сегмента мережі (домена колізій - для Ethernet). Ці програми призначені для діагностики несправностей та аналізу трафіку і навіть включаються до операційних систем (Мережевий Монітор Windows, tcpdump UNIX). У той же час ці засоби можуть бути використані для перехоплення конфіденційних даних (насамперед мережевих ідентифікаторів та паролів користувачів), які в класичних реалізаціях мережевих сервісів (Telnet, FTP, SMTP, POP3) передаються у пакетах у відкритому вигляді.

Пом'якшити загрозу сніфінгу пакетів можна за допомогою:

- використання комутованої інфраструктури - при використанні комутаторів сніффер може захопити трафік тільки порту комутатора, до якого він підключений.
- шифрування сеансу передачі - наприклад з використанням VPN і протоколів IPSec, SSH, SSL та інших.
- антисніферів - апаратних або програмних засобів, що вимірюють час реагування хостів на тестовий пакет і визначають хости, що обробляють більше, ніж зазвичай, кількість пакетів в одиницю часу (наприклад, AntiSniff) .
- "сильна" аутентифікація - наприклад, з використанням біометричних засобів або одноразових паролів.

Спуффінг мережевих адрес - підстановка в пакетах хакером мережного адреси комп'ютера користувача мережі (можна змінювати як адресу мережного, і адресу канального рівня) замість свого. Часто спуфінгом вважають також вставку хибної інформації або шкідливих команд у звичайний потік даних, наприклад, широкомовне розсилання хибного DHCP сервера, що автоматично призначає мережеві адреси, необхідні зловмиснику (далі комп'ютер зловмисника, наприклад, може імітувати мережеві сервіси та отримувати ідентифікацію їх реєстрації на "хибних серверах").

Пом'якшити загрозу спуфінгу пакетів можна за допомогою:

- фільтрів мережевих екранів, що відсікають будь-який трафік, що надходить із зовнішньої мережі з вихідною адресою, що має розташовуватися всередині мережі;
- фільтрації, що рекомендується RFC 2827 - відкидає вихідний трафік з IP адрес, що не належать організації. використанням діапазону адрес для локальних мереж і технології трансляції мережевих адрес, коли шлюз замінює мережеву адресу відправника в пакетах, що відправляються з локальної мережі, на адресу свого вихідного інтерфейсу.

Відмова в обслуговуванні (Denial of Service - DoS) - один із найпоширеніших типів атак, відносно простий і в той же час завдає величезної шкоди мережам і серверам. Атака DoS робить мережу або мережеві послуги недоступними для звичайного використання за рахунок перевищення допустимих меж навантаження на мережу, операційну систему або додаток серверів.

Розрізняють два основні типи DoS-атак:

- надмірна кількість даних (Overwhelming Quantity of Traffic) - це коли до мережі, хоста або програми надсилається величезна кількість даних з такою швидкістю, що вони не спроможні їх обробити. Це спричиняє затримку передачі чи відгуку, або відмову пристрою, аварійне завершення роботи сервісу.
- пакети зловмисного формату (Maliciously Formatted Packets) - це коли пакет зловмисного формату надсилається до хоста або програми і одержувач не здатен його обробити. Наприклад, зловмисник пересилає пакети, що містять помилки, які не можуть бути ідентифіковані програмою, або передає неправильно відформатовані пакети. Це може викликати сповільнення роботи або відмову пристрою-отримувача.

DoS атаки вважаються серйозною загрозою, оскільки вони можуть легко переривати зв'язок та викликати значну втрату часу та грошей. Ці атаки відносно прості для виконання навіть некваліфікованим нападником.

Розподілена DoS атака (Distributed DoS Attack, DDoS) подібна до атаки DoS, але вона походить від декількох скоординованих джерел. Наприклад, атака DDoS може відбуватися наступним чином:

1. Нападник створює мережу заражених хостів, яка називається ботнетом. Заражені хости називаються "зомбі". Їх контролюють системи керування.
2. Зомбі-комп'ютери постійно сканують і заражають нові хости, збільшуючи кількість "зомбі". У призначений час, хакер наказує центрам керування розпочати DDoS-атаку за участі зомбі-ботнету.

Прикладами DoS-атак можна назвати TCP SYN Flooding, Ping of Death, використання мережевих черв'яків і троянських коней для організації з допомогою Distributed DoS - DDoS та інших.

Загроза атак DoS може бути знижена такими способами:

- використанням функцій анти-DoS на маршрутизаторах та мережевих екранах, що обмежують кількість напіввідкритих каналів в одиницю часу;
- обмеженням обсягу трафіку в одиницю часу (traffic rate limiting), що насамперед використовується для атак - ICMP, UDP, TCP з прапором PSH, на маршрутизаторах;
- регулярною перевіркою вірусів, оновленням антивірусних баз та системного та прикладного програмного забезпечення;
- використанням програмного забезпечення, що виявляє сканування портів.

Атаки типу Man-in-the-Middle - використання даних, що передаються по мережах. За допомогою такого рівня доступу зловмисник може перехоплювати, збирати та підмінювати інформацію користувача перш ніж передати її одержувачу. Атаки MitM широко використовуються для викрадення фінансової інформації. Існує безліч зловмисних програм та методик, які наділяють атакуючих можливостями MitM.

Посередник в мобільному телефоні (Man-In-The-Mobile або MitMo) – варіант атаки "Людина посередині", який використовується для отримання контролю над мобільним пристроєм. Заражений мобільний пристрій може отримати наказ зібрати конфіденційну інформацію користувача і відправити її нападникам. ZeuS, як приклад експлойта з

можливостями MitMo, дає змогу атакуючим непомітно перехоплювати SMS-повідомлення, які надсилаються користувачам під час проведення 2-етапної перевірки.

Для боротьби з атаками типу Man-in-the-Middle слід використовувати:

- шифрування сеансів передачі.
- регулярне встановлення виправлень операційних систем та додатків, що випускаються їх виробникам та виконання рекомендацій виробників щодо забезпечення безпеки програмного забезпечення.

Атаки на рівні програм - використання проломів у захисті серверного програмного забезпечення (HTTP, FTP, sendmail та ін.) з метою отримати доступ до системи з правами інших користувачів (наприклад, адміністратора). У цьому випадку використовуються порти та адреси, які не можуть бути закриті. Тому для захисту від атак цього типу можна рекомендувати:

- регулярний перегляд лог-файлів та їх аналіз.
- регулярне встановлення виправлень операційних систем та додатків, що їх випускають їх виробникам та виконання рекомендацій виробників щодо забезпечення безпеки програмного забезпечення.
- використання систем виявлення атак - Intrusion Detection System (IDS), які порівнюють проходять через хост (або домен) пакети з сигнатурами відомих атак і в разі збігу подають сигнал адміністратору.

Фішинг, це коли зловмисник надсилає шахрайського електронного листа, який виглядає як повідомлення від легального надійного джерела. Мета цього повідомлення - змусити одержувача встановити зловмисне ПЗ на своєму пристрої або розкрити особисту чи фінансову інформацію. Прикладом фішингу є підробка листів електронної пошти, які виглядають як повідомлення, надіслані роздрібним магазином з проханням до користувача натиснути на посиланні для участі у розігруванні призів. Посилання може переадресовувати на підроблений сайт, який запитує особисту інформацію, або може встановити вірус.

Спрямований фішинг - це цілеспрямована фішингова атака. Щоб дістатися жертв фішинг і спрямований фішинг використовують електронні листи, але спрямований фішинг націлений на конкретну особу. Переш ніж надіслати електронне повідомлення нападник вивчає інтереси жертви. Наприклад, зловмисник дізнався, що жертва цікавиться автомобілями і хоче купити конкретну модель. Зловмисник приєднується до того ж дискусійного автомобільного форуму, що і жертва, готує пропозицію продажу автомобіля і надсилає її жертві електронною поштою. Електронний лист містить посилання на фотографію автомобіля. Коли жертва натискає на посилання, шкідливе ПЗ встановлюється на її комп'ютер.

Ще один зі способів проникнення - це вдосконалені постійні загрози (advanced persistent threats - APTs). Вони складаються з багатофазних, довготривалих, непомітних та складних дій, спрямованих на конкретну жертву. APT-атаки є складними і для їх виконання необхідні досвід та високий рівень кваліфікації нападника, тому вони зазвичай добре фінансуються. APT спрямовані на організації або країни з комерційних або політичних причин.

Метою APT є розгортання спеціального шкідливого програмного забезпечення на одній або кількох системах жертви. Зазвичай атаки пов'язані зі шпигунством в мережах та залишаються невиявленими. Через багатоетапне виконання та використання декількох типів налаштовуваних шкідливих програм, які впливають на різні пристрої та

виконують визначені функції, окремий нападник часто не має навичок, ресурсів або наполегливості для виконання APT.

Пошукові системи, такі як Google, працюють шляхом ранжування сторінок та надання релевантних результатів на основі пошукових запитів користувачів. Залежно від значимості вмісту веб-сайту, він може відображатися вище або нижче в переліку результатів пошуку. Пошукова оптимізація (Search Engine Optimization, SEO) - це набір методів, що використовуються для покращення рейтингу веб-сайту в пошуковій системі. В той час як багато легальних компаній спеціалізуються на оптимізації веб-сайтів з метою їх кращого позиціонування, зловмисник може використовувати SEO для того, щоб його шкідливий веб-сайт відображався вище у результатах пошуку. Ця техніка називається "отруєння SEO".

Найпоширенішою метою отруєння SEO є збільшення трафіку на шкідливі веб-сайти, які можуть містити зловмисні програми або застосовувати прийоми соціальної інженерії. Щоб розташувати шкідливий сайт вище у результатах пошуку, зловмисники використовують популярні пошукові терміни.

Змішані атаки (Blended attacks) - це атаки, які використовують кілька методів для компрометації жертви. Використовуючи одразу декілька різних методів атаки, зловмисники застосовують шкідливі програми, які є гібридом хробаків, троянських коней, шпигунських програм, клавіатурних шпигунів, спаму та фішингових схем. Тенденція змішаних атак схильна до використання більш складного зловмисного програмного забезпечення та створює великі ризики для користувачів.

Найпоширеніший тип змішаної атаки використовує спам-листи, миттєві повідомлення або легальні веб-сайти для поширення посилань через які шкідливе або шпигунське програмне забезпечення непомітно завантажується на комп'ютер. Ще однією поширеною змішаною атакою є використання DDoS у поєднанні з фішинговими електронними листами. Спочатку DDoS-атака використовується для блокування веб-сайту популярного банку та надсилання його клієнтам електронних листів з вибаченнями за незручності. Ці електронні листи також скеровують користувачів до підробленого "аварійного сайту", де їх інформація авторизації може бути викрадена.

Більшість з найнебезпечніших комп'ютерних черв'яків, таких як Nimbda, CodeRed, BugBear, Klez і Slammer краще класифікувати як змішані атаки:

1. Деякі різновиди Nimbda розповсюджувалися через вкладення в електронні листи; завантаження файлів зі скомпрометованого веб-сервера та обмін файлами Microsoft (наприклад, через анонимні ресурси).
2. Інші різновиди Nimbda могли змінювати привілеї гостьових облікових записів системи, щоб надати зловмиснику або шкідливому коду адміністративні права.
3. До змішаних атак також належать нещодавно створені черв'яки Conficker і ZeuS/LICAT. Conficker використовував всі традиційні методи розповсюдження.

Міжмережевий екран (firewall, брендмауер) - система міжмережевого захисту, що дозволяє розділити загальну мережу на дві або більш частин і реалізувати набір правил, визначальних умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальної) мережею і глобальною мережею Internet, хоча її можна організувати і усередині корпоративної мережі підприємства. Міжмережевий екран пропускає через себе весь трафік, ухвалюючи для кожного пакету рішення - пропускати його або відкинути - на основі визначених для нього набору правил фільтрації (рис. 1).

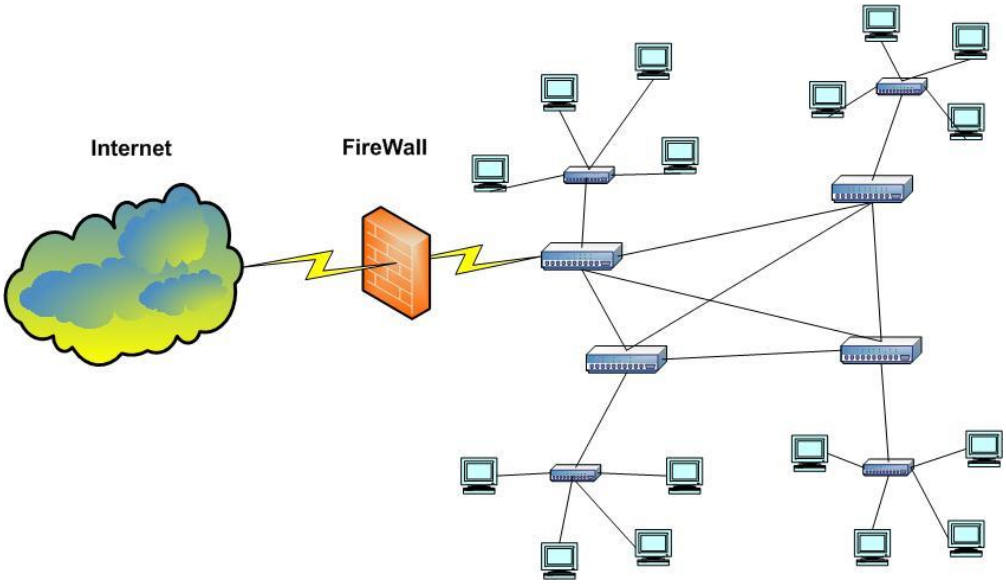


Рисунок 1 - Схема встановлення міжмережевого екрану

Існують чотири основні засоби, за допомогою яких міжмережеві екрани здійснюють контроль доступу і забезпечують реалізацію політик захисту:

- управління сервісами - визначення типів служб Internet, до яких можна дістати доступ з внутрішньої мережі назовні і із зовнішнього оточення усередину; міжмережевий екран може фільтрувати потік даних на основі IP-адрес і номерів портів TCP;
- управління напрямом руху - визначення напряму, в якому можуть ініціюватися і проходити через міжмережевий екран запити до тих або інших служб;
- управління користувачами - надання доступу до служб залежно від прав доступу користувачів, що звертаються до цих служб; ця функція звичайно застосовується до локальних користувачів; однак вона може застосовуватися і до потоку даних, що поступає від зовнішніх користувачів, що вимагає реалізації в якійсь формі технології аутентифікації, наприклад, забезпечуваної протоколом IPSec;
- управління поведінкою – контроль за використанням окремих служб; так, міжмережевий екран може фільтрувати електронну пошту, відсіваючи спам чи ж вирішувати доступ ззовні певної частини інформації, що знаходиться на локальному Web-сервері.

Можна виділити наступні типи міжмережевих екранів:

- фільтруючі маршрутизатори (packet-filtering router);
- шлюзи мережевого рівня;
- шлюзи прикладного рівня.

Звичайно міжмережеві екрани включають всі або більшість з цих компонент.

Фільтруючий маршрутизатор є маршрутизатором або працюючою на сервері програмою, що фільтрує пакети, які входять в корпоративну мережу і виходять з неї. Фільтрація пакетів звичайно здійснюється на основі інформації, що міститься в IP і TCP заголовках пакетів, найчастіше для цього використовуються:

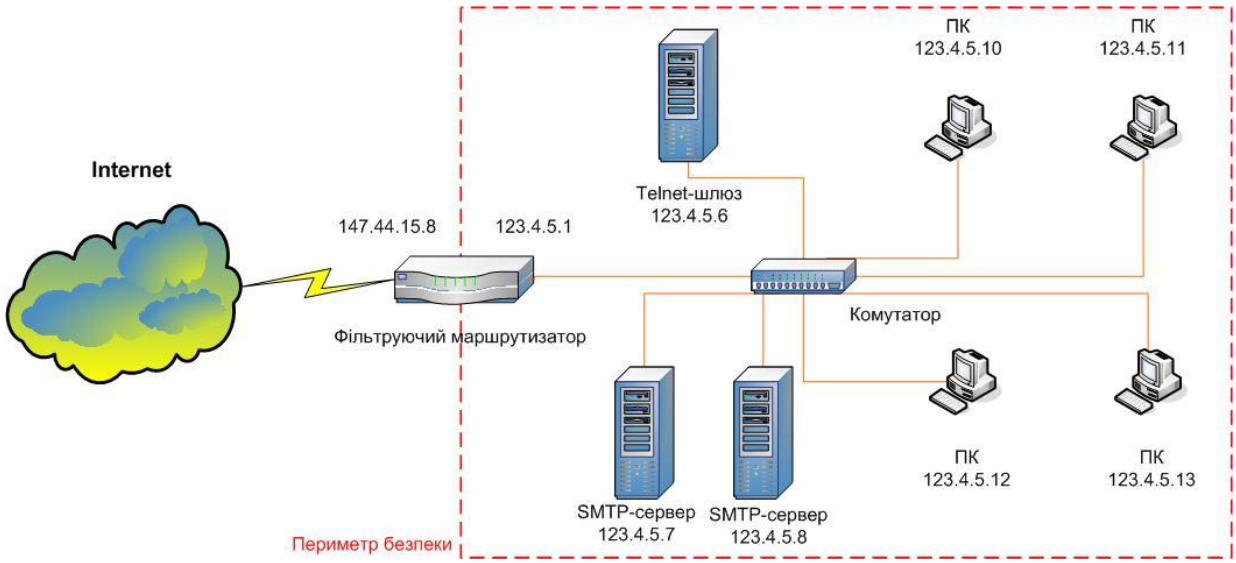
- IP адреса відправника пакету;
- IP адреса одержувача пакету;

- порт системи відправника;
- порт системи одержувача.

Фільтр пакетів звичайно представляється у вигляді списку правил, що використовують значення полів заголовків IP і TCP. Якщо виявляється відповідність одному з правил, то на підставі цього правила ухвалюється рішення про можливість передачі пакету далі. При невідповідності всім правилам виконується операція, передбачена для використання за умовчанням. Для неї існують наступні варіанти локальних політик захисту:

- Default = discard. Все, що не дозволено, заборонено.
- Default = forward. Все, що незаборонено, дозволено.

Як приклад роботи фільтруючого маршрутизатора розглянемо реалізацію політики безпеки, що допускає певні з'єднання з локальною корпоративною мережею 123.4/16 (рис. 2).



Протокол	Адреса відправника	Адреса одержувача	Порт відправника	Порт одержувача	Дія
TCP		123.4.5.6	>1023	23	allow
TCP		123.4.5.7	>1023	25	allow
TCP		123.4.5.8	>1023	25	allow
TCP	1239.6.48.254	123.4.5.9	>1023	119	allow
UDP		123.4/16	>1023	123	allow
*	*	*	*		deny

Рисунок 2 - Приклад набору правил фільтрації

При цьому з'єднання по протоколу telnet дозволені тільки з хостом 123.4.5.6, що виконує роль прикладного telnet-шлюзу, а з'єднання по протоколу SMTP - тільки з двома хостами 123.4.5.7 і 123.4.5.8, що виконують роль серверів електронної пошти. Обмін по протоколу NNTP дозволений тільки від зовнішнього сервера новин з адресою 129.6.48.254 і лише з NNTP сервером локальної мережі 123.4.5.9. Використання

мережевої служби синхронізації часу NTP дозволене для всіх комп'ютерів локальної мережі.

Позитивні якості фільтруючих маршрутизаторів:

- порівняно невисока вартість;
- гнучкість у визначенні правил фільтрації;
- невелика затримка при проходженні пакетів.

Недоліки фільтруючих маршрутизаторів:

- внутрішня мережа маршрутизується з Internet;
- правила фільтрації важкі в описі і відсутні засоби їх тестування;
- відсутня аутентифікація на призначеному для користувача рівні.

Шлюзи мережевого рівня інколи називають системами трансляції мережевих адрес (Network Address Translation - NAT), оскільки вони виключають пряму взаємодію між авторизованим клієнтом і зовнішнім хост - комп'ютером. Шлюз мережевого рівня приймає запит довіреного клієнта на конкретні послуги і після перевірки чи задовольняє клієнт базовим критеріям фільтрації (наприклад, чи може DNS - сервер визначити IP-адреса клієнта і асоційоване з ним ім'я) встановлює з'єднання із зовнішнім хостом. Шлюз мережевого рівня виконує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP адрес локальної мережі на одну "надійну" IP адресу інтерфейсу міжмережевого екрану, через який передаються всі витікаючі з локальної мережі пакети.

Кожен раз, коли витікаючий пакет передається через NAT - маршрутизатор локальна IP адреса відправника замінюється на "чесну" IP адресу (рис. 3).

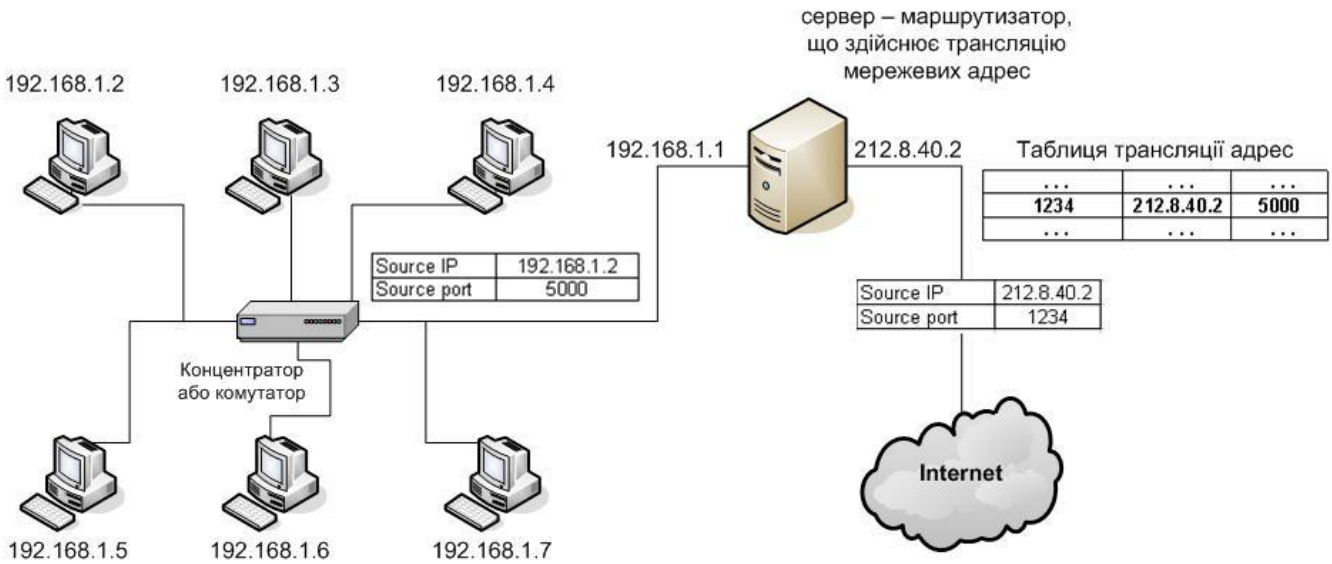


Рисунок 3 - Трансляція мережевих адрес шлюзом мережевого рівня

Окрім цього, в полі порту відправника заголовка TCP заноситься 16-бітовий індекс таблиці трансляції адрес (з максимум 65536 рядками). Кожен рядок таблиці містить цей індекс, первинну IP адресу відправника і первинний порт відправника. Після описаної заміни прораховуються контрольні суми заголовків IP і TCP і заносяться у відповідні поля пакету. Коли NAT- маршрутизатор отримує у відповідь пакети для даного процесу, значення порту одержувача в заголовку TCP використовується для пошуку індексу в таблиці трансляції адрес. З визначеного по індексу рядка витягується локальна IP адреса відправника і первинний TCP порт відправника, які заносяться у відповідні поля пакету.

Після цього знову перераховуються контрольні суми в полях IP і TCP заголовків, заносяться у відповідні поля пакету, після чого пакет прямує на робочу станцію локальної мережі.

Шлюз мережевого рівня відстежує процедуру квитування зв'язку по протоколу TCP через порядкові номери сегментів даних. Коли сеанс завершується, шлюз видаляє відповідний елемент з таблиці і розриває з'єднання. Недоліком шлюзів мережевого рівня є те, що після встановлення зв'язку вони не можуть перевіряти вміст пакетів на прикладному рівні. Також для них відсутня призначена для користувача аутентифікація.

Шлюзи прикладного рівня також виключають пряму взаємодію між авторизованим клієнтом і зовнішнім хостом, проте при цьому вони фільтрують всі вхідні і витікаючі пакети на прикладному рівні. Це досягається установкою і настройкою програмного забезпечення повноважних серверів – проксі - серверів (proxy servers), що перенаправляють через шлюз інформацію прикладного рівня, що генерується хостами (рис. 4). Користувач зв'язується з цим шлюзом за допомогою такого побудованого на основі TCP/IP застосування, як HTTP-браузер, Telnet-термінал або FTP- клієнт. Ці застосування передають шлюзу ім'я віддаленого вузла, до якого необхідно дістати доступ. Шлюз зв'язується з відповідним застосуванням віддаленого вузла і ретранслює сегменти TCP, що містять дані застосування локального користувача. Шлюз можна настроїти так, щоб він підтримував тільки певні можливості застосування, які адміністратор мережі вважає допустимими з погляду безпеки.

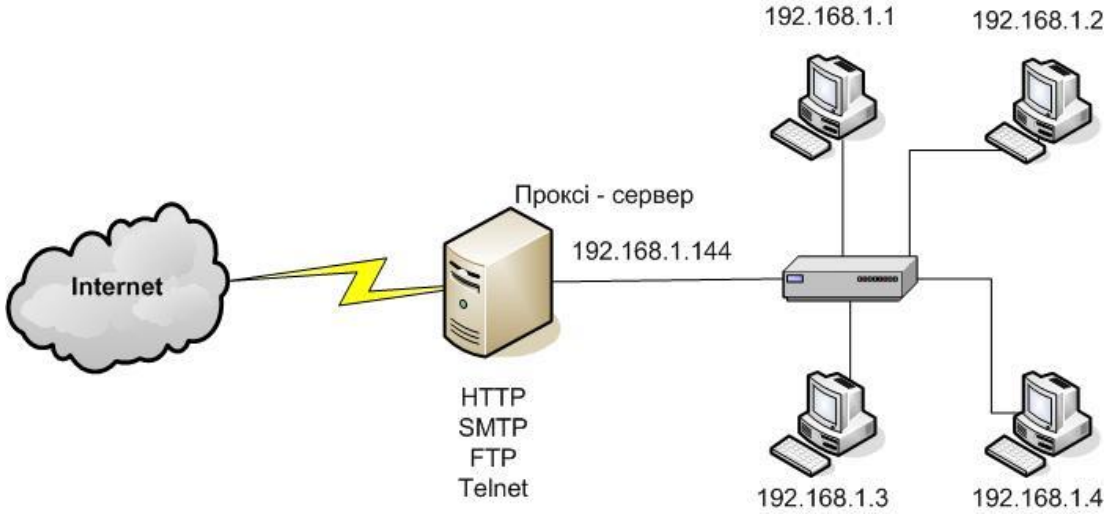


Рисунок 4 - Шлюз прикладного рівня – проксі – сервер

У загальному випадку шлюзи прикладного рівня забезпечують надійніший захист, ніж фільтри пакетів. Замість того щоб перевіряти численні можливі комбінації дозволів і заборон на рівні TCP і IP, шлюзу прикладного рівня доводиться розглядати лише обмежене число застосувань. Крім того, при цьому легко протоколювати і контролювати весь вхідний потік даних прикладного рівня. Проте, для досягнення вищого рівня безпеки і гнучкості шлюзи прикладного рівня і фільтруючі маршрутизатори можуть об'єднуватися в одному міжмережевому екрані. Переваги використання проксі-серверів:

- пропускають пакети лише тих служб, які їм доручено обслуговувати (частіше за все HTTP, HTTPS, FTP, Gopher);
- приховують структуру мережі, що захищається;

- дозволяють виконувати кешування запрошуваної Інтернет інформації і будувати ієрархію кешів;
- дозволяють виконувати аутентифікацію користувачів;
- дозволяють вести статистику відвідувань за витікаючими IP адресами.

Основним недоліком шлюзів даного типа є додаткове навантаження на процесор, що створюється кожним з'єднанням. Насправді між двома кінцевими користувачами встановлюється два зв'язані з'єднання, загальною точкою яких є шлюз, і шлюзу доводиться перевіряти весь потік даних в обох напрямах, щоб переправити його далі.

Міжмережеві екрани можуть бути інтегровані в маршрутизатори або виконані як окремі пристрої.

Основні схеми захисту на базі міжмережевих екранів:

- міжмережевий екран - фільтруючий маршрутизатор;
- міжмережевий екран на основі двопортового шлюзу;
- міжмережевий екран на основі екранованого шлюзу;
- міжмережевий екран - екранована підмережа.

Міжмережевий екран - фільтруючий маршрутизатор - найбільш простий в реалізації - виконує фільтрацію вхідних і витікаючих пакетів на основі аналізу їх адрес і портів (рис.5).

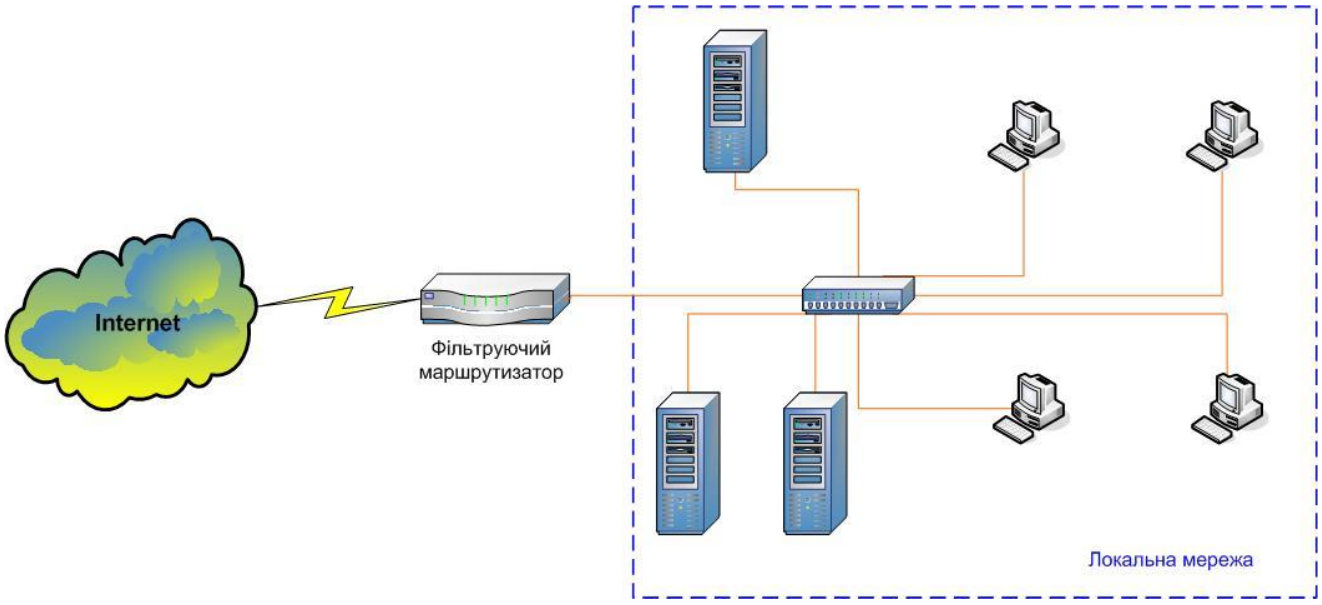


Рисунок 5 - Міжмережевий екран на основі фільтруючого маршрутизатора

Міжмережевий екран на основі двопортового шлюзу прикладного рівня часто є комп'ютером з двома мережевими інтерфейсами, при передачі даних між якими здійснюється фільтрація (рис. 6). Для забезпечення додаткового захисту між шлюзом прикладного рівня і Internet звичайно розміщують фільтруючий маршрутизатор. Між прикладним шлюзом і фільтруючим маршрутизатором утворюється внутрішня екранована підмережа - демілітаризована зона, в якій можна розташовувати доступні ззовні інформаційні сервери.

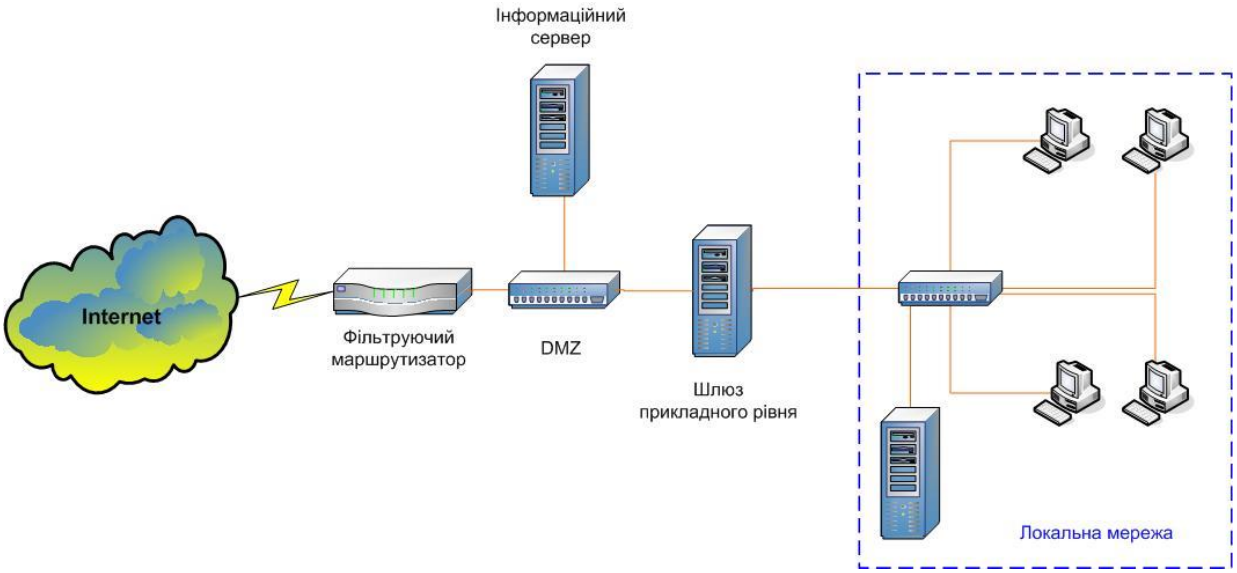


Рисунок 6 - Міжмережевий екран з шлюзом прикладного рівня і фільтруючим маршрутизатором

Міжмережевий екран на основі екранованого шлюзу прикладного рівня, реалізованого на комп'ютері лише з одним мережевим інтерфейсом, є гнучкіший варіант реалізації міжмережевого екрану, оскільки є можливість реалізувати з'єднання з Internet для деяких служб через проксі - сервер, а для деяких через фільтруючий маршрутизатор (рис. 7).

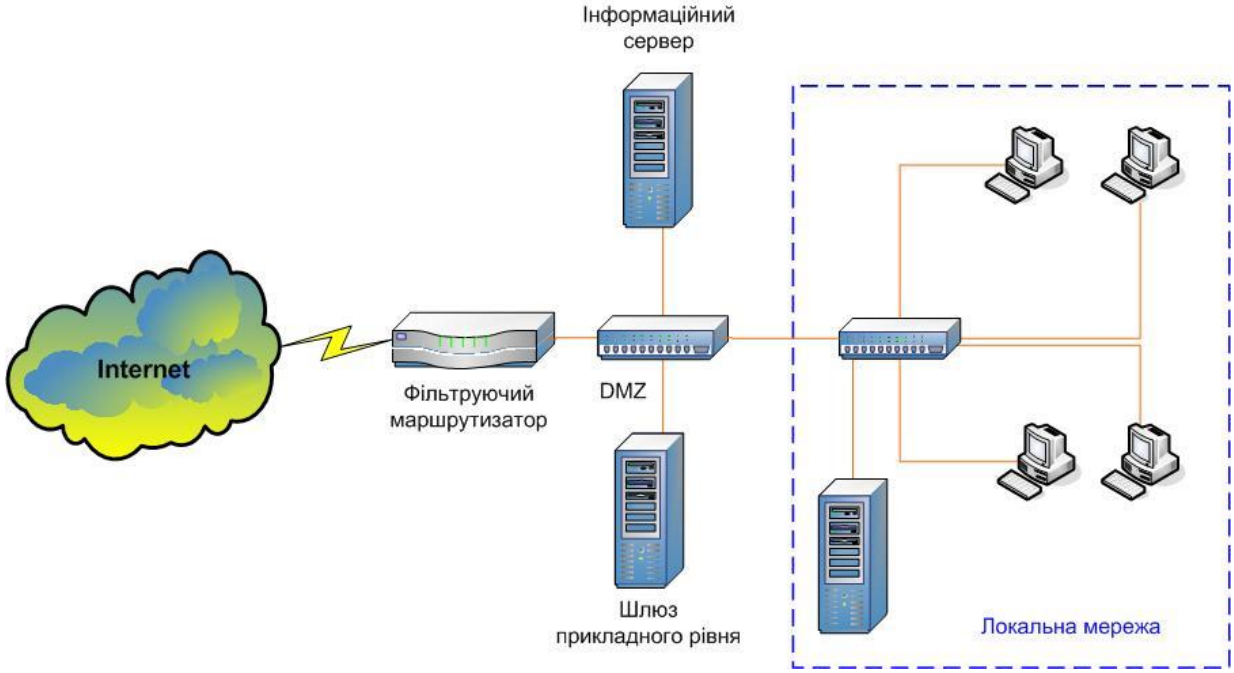


Рисунок 7 - Міжмережевий екран з екранованим шлюзом прикладного рівня і фільтруючим маршрутизатором

Міжмережевий екран, що складається з екранованою зовнішнім і внутрішнім фільтруючими маршрутизаторами підмережею показаний на рис. 8.

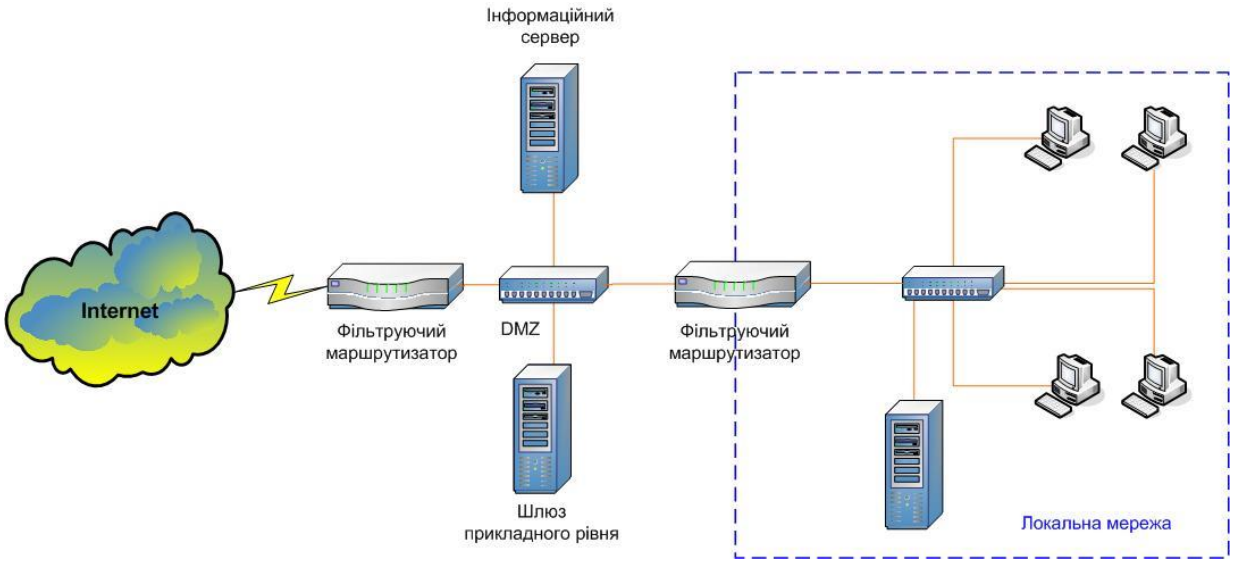


Рисунок 8 - Міжмережевий екран з екранованою фільтруючими маршрутизторами підмережею

У цій підмережі розташовується шлюз прикладного рівня і сервери. Зовнішній маршрутизатор дозволяє трафік зовнішніх користувачів лише до проксі - серверу і серверам в демілітаризованій зоні. Внутрішній маршрутизатор захищає внутрішню мережу як від Internet, так і від екранованої підмережі (у разі її компрометації).