Призначення, можливості, і основні захисні механізми міжмережевих екранів (брандмауерів). Основні захисні механізми мереж. Політика безпеки при доступі до мережі загального користування.

Із часом до Інтернету під'єднується дедалі більше користувачів. Якщо раніше мережа використовувалась лише в якості середи для передачі файлів та повідомлень електронної пошти, то сьогодні вирішуються складніші завдання розподіленого доступу до ресурсу. Зараз будь-яка людина може отримати доступ до даних, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Internet, який раніше слугував виключно дослідницьким та учбовим групам, стає все більш популярною у діловому світі. Компанії спокушають швидкість, дешевий глобальний зв'язок, зручність для проведення спільних робіт, доступні програми, унікальна база даних мережі. Вони розглядають глобальну мережу, як доповнення до власних локальних мереж.

Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, ускладнюючи їх виявлення й покарання. Зловмисники розміщують шкідливі програми на веб-ресурсах, «маскують» їх під корисне й безкоштовне програмне забезпечення. Тому важливо запобігти небезпеці, уникнути можливих загроз. Саме тому, важливим є захист інформації у всесвітній мережі Internet.

Якщо комп'ютер підключений до Інтернету, то будь-який користувач, також підключений до Інтернету, може отримати доступ до інформаційних ресурсів цього комп'ютера.

Є різні механізми проникнення з Інтернету на локальний комп'ютер і в локальну мережу:

- веб-сторінки, що завантажуються в браузер, можуть містити активні елементи, здатні виконувати *деструктивні дії* на локальному комп'ютері;

- деякі веб-сервери розміщують на локальному комп'ютері текстові файли cookie, використовуючи які, можна отримати конфіденційну інформацію про користувача локального комп'ютера; електронні листи або дописи в соціальних мережах можуть містити *шкідливі посилання*;

- за допомогою спеціальних програм можна отримати доступ до дисків і файлів локального комп'ютера тощо.

Що таке "cookie-файл"?

"Cookie-файл" (**HTTP-cookie**, «**Ку́кі**» або «**реп'яшки**» (англ. *Cookies*- тістечка, печиво)) - це невеликий файл, який містить ряд символів, що надсилається до вашого комп'ютера при перегляді веб-сайта. Застосовується для збереження даних, специфічних для даного користувача.

Таким чином веб-сервер помічає браузер користувача при відвідуванні. Куки створюються за ініціативою скриптового сценарію на стороні веб-браузера. При наступному візиті сервер буде знати, що користувач вже тут був. За допомогою кукі-технології можна вивчити вподобання відвідувача. Кукі є одним із найточніших засобів визначення унікального користувача.

Google використовує cookie-файли, щоб покращити якість надання послуг і краще розпізнавати бажання користувачів до взаємодії. Увімкнення cookie-файлів необхідне для користування обліковим записом Google.

В комп'ютерних системах використовуються такі засоби мережевого захисту інформації:

1) Брандмауери (або ***міжмережеві екрани*** *(Firewall)*) — для блокування атак, це окремі пристрої чи спеціальні програми, які створюють бар'єр між комп'ютером і мережею, між внутрішньою локальною мережею організації та Інтернетом.

Термін брандмауер походить від нім. brand — пожежа та mauer — стіна; його англійський еквівалент — firewall, асоціюється з вогнестійкою капітальною стіною, що перешкоджає поширенню пожежі. Термін виник приблизно в 1995 р.

Мережеві екрани керують проходженням мережевого трафіку відповідно до правил (*policies*) захисту, контролюють трафік, що входить в мережу і що виходить з неї.

За допомогою програм-брандмауерів відслідковуються всі під'єднання й за необхідності дозволяється чи блокується доступ до комп'ютера. Використовуючи інтерфейс налаштувань профілю доступу міжмережевого екрану, є можливість для кожного користувача створити свій профіль, який буде визначати не тільки права доступу цього користувача до мережі Інтернет, але і права доступу до цього користувача з Інтернет. Міжмережевий екран може блокувати спроби хакерів, вірусів і черв'яків отримати доступ до вашого комп'ютера через Інтернет. Добре сконфігурований міжмережевий екран спроможний зупинити більшість відомих комп'ютерних атак.

Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі.

2) Іншим пристроєм ефективного захисту в комп'ютерних мережах є ***маршрутизатор***. Він здійснює фільтрацію пакетів даних для передачі і, тим самим, з'являється можливість заборонити доступ деяким користувачам до певного "хосту", програмно здійснювати детальний контроль адрес відправників та одержувачів та ін

Міжмережеві екрани працюють з програмами маршрутизації та фільтрами всіх мережевих пакетів, щоб визначити, чи можна пропустити інформаційний пакет, а якщо можна, то відправити його до певної комп'ютерної служби за призначенням. Для того щоб міжмережевий екран міг зробити це, необхідно визначити правила фільтрації. Отже, міжмережевий екран є немовби віртуальним кордоном, на якому перевіряється цілісність фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.

3) ***системи виявлення втручань*** — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі.

4) ***засоби аналізу захищеності*** — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

5) ***засоби створення віртуальних приватних мереж*** (*Virtual Private Network*) — для організації захищених каналів передачі даних через незахищене середовище.

Віртуальні приватні мережі (virtualprivatenetworks, VPN) - територіально розподілені корпоративні мережі, які використовують для зв'язку між окремими сегментами Інтернет.

Часто корпоративні мережі зв'язують офіси, розкидані в місті, регіоні, країні або всьому світі. Провідні постачальники міжмережевих екранів і маршрутизаторів запропонували ***технологію S/WAN***. Протоколи S/WAN допомагають досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників. Іншими словами, компанії зможуть створювати власні віртуальні приватні мережі (virtualprivatenetworks, VPN) і використовувати Інтернет як альтернативу традиційним каналам зв'язку, які орендуються за високу плату .

Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.

Засоби захисту VPN - це інтегровані з віртуальними мережами засоби захисту мережі, в цілому, її сегментів та кожного клієнта мережі окремо (захист TCP/IP трафіку, створюваного будь-якими додатками і програмами; захист робочих станцій, серверів WWW, баз даних і додатків; автопроцесингу, трансакцій для фінансових та банківських додатків і платіжних систем). Вони реалізуються в рамках програмно-апаратних рішень VVPN-шлюзів. Серед основних функцій VPN-шлюзів: автентифікація

(MD5, SHA1), шифрування (DES, 3DES, AES), тунелювання пакетів даних через IP. Певні шлюзи підтримують також функції firewall.

Однак міжмережеві екрани не є універсальним вирішенням усіх проблем безпеки в Інтернет. Брандмауер може блокувати доступ до комп'ютера вірусів і хробаків, але він не здійснює перевірку на віруси і не здатен забезпечити цілісність даних.

6) Використання антивірусних засобів вважається необхідною умовою при підключенні до Internet, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами.

Антивірус - програма, що виявляє або виявляє та знищує комп'ютерні віруси. *Мережеві антивіруси* - використовують для захисту від вірусів однієї або кількох OS, протоколів та команди комп'ютерних мереж і електронної пошти. Використання автоматизованих засобів перевірки мережі на можливі уразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз та значно понизити вірогідність ефективних атак на корпоративну мережу або персональний комп'ютер.

SKIPBridge - система, яка встановлюється на інтерфейсі внутрішня / зовнішня мережа (локальна мережа або комунікаційний провайдер), забезпечує захист (шифрування) трафіка, що направляється з внутрішньої мережі у зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіка, який поступає із зовнішньої мережі у внутрішню. IP-пакети, що приймаються із зовнішньої мережі, обробляються протоколом SKIP (розшифровуються, фільтруються відкриті пакети в режимі тільки захищеного трафіка, контролюється і забезпечується імітозахист). Пакети, які пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIP-Bridge. Програмне забезпечення вирішує завдання адміністративної безпеки (забезпечуючи пакетну фільтрацію), і потім системи SKIPBridge, який маршрутизує пакети на адаптер локальної мережі.

Використання Proxy та анонімних серверів дозволяє залишатись умовно анонімним при діях в мережі Internet та знизити ризики, пов'язані із збиранням та моніторингом мережевої інформації на користь третіх осіб, потоком непотрібної та шкідливої інформації у системі.

Використання систем обмеження доступу до мережевих ресурсів Internet, використання маршрутизаторів та надійних постачальників мережевих послуг, короткочасного каналу зв'язку дозволяє скоротити збір та моніторинг мережевої інформації на користь третіх осіб, потік непотрібної та шкідливої інформації.

Захист даних в Інтернеті.

Для захисту даних під час роботи в Інтернеті доцільно використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням Google шифрує з'єднання з Gmail, а також при виборі інших сервісів Google, наприклад Google Диск, активується протокол шифрування SSL, який використовується до завершення сеансу роботи.

Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу — вона починається з https://. Це, на відміну від протоколу http, — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка, це означає, що з'єднання захищене й більш безпечне.

HTTPS (від англ. HyperText Transfer Protocol Secure) — розширення протоколу http для підтримки шифрування з метою підвищення безпеки.

Браундмаєр

Перш ніж під'єднати комп'ютер до Інтернету, бажано підключити брандмауер. Наприклад, щоб підключити брандмауер в операційній системі Windows 7, треба виконати вказівку Пуск/Панель керування та обрати Брандмауер Windows.

У вікні, що відкрилося, слід встановити режим Підключено та за необхідності задати додаткові параметри.

Після встановлення міжмережевого екрана при кожному першому запуску мережевих програм брандмауер видаватиме вікно з попередженням, що деяка програма намагається одержати доступ до мережевого ресурсу.

Користувачеві пропонується на вибір: одноразово чи назавжди дозволити або заборонити доступ до комп’ютера для обраної програми.

Крім брандмауера, вбудованого у Windows 7, є багато інших засобів, що мають гнучкі параметри налагодження.

Поради:

• Якщо у вас будинку до Інтернету підключено кілька комп'ютерів, або вони з'єднані в мережу, важливо захистити кожен з них. Для захисту мережі слід використовувати апаратний брандмауер (наприклад, маршрутизатор), однак, щоб запобігти поширенню вірусу в самій мережі в разі зараження одного з комп'ютерів, на кожному з них необхідно включити програмний брандмауер.

• Якщо ваш комп'ютер підключений до корпоративної, шкільної або мережі іншої організації, дотримуйтесь політиці, встановленої адміністратором даної мережі .

• При використанні комп'ютера вдома, найперший крок, який слід зробити для його захисту , - включити брандмауер.

За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад, хробаків) через мережу або Інтернет. Крім того, брандмауер запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші.

У брандмауер Windows вбудований журнал безпеки, який дозволяє фіксувати ip-адреси і інші дані, що відносяться до з'єднань в домашніх і офісною мережах або в Інтернеті. Можна записувати як успішні підключення, так і пропущені пакети. Це дозволяє відстежувати, коли комп'ютер в мережі підключається, наприклад, до web-сайту. Дана можливість за умовчанням відключена (її може включити системний адміністратор).