Тема 15-16. Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера (Firewall).

Захист комп'ютерних мереж та персональних комп'ютерів за допомогою брандмауера

Брандмауер (Firewall) – це захисна стіна, що стоїть між мережним адаптером та операційною системою. Будь-який IP-пакет, перш ніж потрапити на обробку операційної системи (наприклад, для маршрутизації або передачі його web-серверу) проходить через суворий контроль. Будь-який вихідний пакет також натрапляє на цю стіну, і може бути пропущений, відкинутий, підрахований або змінений. Якщо пакет проходить через операційну систему наскрізь (маршрутизується), то його перевірка відбувається як на вході, так і на виході. При складній обробці пакету він може проходити через брандмауер і більшу кількість разів.

Поза комп'ютерної сфери брандмауером (або firewall) називають стіну, зроблену з негорючих матеріалів і перешкоджає поширенню пожежі. У сфері комп'ютерних мереж міжмережевий екран є бар'єр, що захищає від фігуральнї пожежі - спроб зловмисників вторгнутися у внутрішню мережу для того, щоб скопіювати, змінити або стерти інформацію або скористатися пам'яттю чи обчислювальною потужністю працюючих у цій мережі комп'ютерів. Міжмережевий екран покликаний забезпечити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Брандмауери можуть бути виконані у вигляді як апаратного, так і програмного комплексу, записаного в комутуючий пристрій або сервер доступу (сервер-шлюз, просто сервер, хост-комп'ютер і т.д.), вбудованого в операційну систему або представляти собою програму, що працює під її управлінням.

Робота брандмауера полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропуску пакетів у внутрішню мережу (сегмент мережі) або повному їх фільтруванні. Ефективність роботи міжмережевого екрану, що працює під управлінням Windows, обумовлена тим, що він повністю заміщає реалізований стек протоколів TCP \ IP, і тому порушувати його роботу з допомогою спотворення протоколів зовнішньої мережі (що часто робиться хакерами) неможливо.

Міжмережеві екрани зазвичай виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі (внутрішньої підмережі) від зовнішніх каналів зв'язку;
- багатоетапну ідентифікацію запитів, що надходять в мережу (ідентифікація серверів, вузлів зв'язку про інших компонентів зовнішньої мережі);
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі (у внутрішній підмережі може використовуватися локальна система адресації серверів);
- приховування IP адрес внутрішніх серверів з метою захисту від хакерів.

Брандмауери можуть працювати на різних рівнях протоколів моделі OSI.

На мережевому рівні виконується фільтрація пакетів, заснована на IP адресах (наприклад, не пропускати пакети з Інтернету, направлені на ті сервери, доступ до яких зовні заборонено; не пропускати пакети з фальшивими зворотними адресами або IP адресами, занесеними до «чорного списку», і т.д.). На транспортному рівні фільтрація припустима ще й за номерами портів TCP і прапорів, що містяться в пакетах (наприклад, запитів на встановлення з'єднання). На прикладному рівні може виконуватися аналіз прикладних протоколів (FTP, HTTP, SMTP і т.д.) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Можливо в брандмауері створювати експертну систему, яка, аналізуючи трафік, діагностує

події, що можуть становити загрозу безпеки внутрішньої мережі, та інформує про це адміністратора. Експертна система здатна також у разі небезпеки (спам, наприклад) автоматично посилювати умови фільтрації і т.д.

Брандмауери бувають апаратними або програмними.

Апаратний брандмауер представляє собою пристрій, фізично підключається до мережі. Це пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення. Це забезпечує безпеку, допомагаючи запобігти небажаним проникнення в мережу або на комп'ютер.

Програмний брандмауер виконує ті ж функції, використовуючи не зовнішній пристрій, а встановлену на комп'ютері програму.

На одному і тому ж комп'ютері можуть використовуватися як апаратні, так і програмні брандмауери.

Брандмауер представляє собою захисну кордон між комп'ютером (або комп'ютерною мережею) і зовнішнім середовищем, користувачі або програми якої можуть намагатися отримати несанкціонований доступ до комп'ютера. Зазвичай зломщики використовують спеціальні програми для пошуку в Інтернеті незахищених підключень. Така програма відправляє на комп'ютер дуже маленьке повідомлення. За відсутності брандмауера комп'ютер автоматично відповідає на повідомлення, виявляючи свою незахищеність. Встановлений брандмауер отримує такі повідомлення, але не відповідає на них; таким чином, зломщики навіть не підозрюють про існування даного комп'ютера.

Існує кілька шляхів звести нанівець або піддати ризику захист братмауерів. Виходячи з того, що основною метою встановлення більшості брандмауерів є блокування доступу, очевидно, що виявлення будь-ким лазівки, що дозволяє проникнути в систему, веде до повного краху всієї захисту даної системи. Якщо ж несанкціонованому користувачеві вдалося проникнути в брандмауер і переконфігурувати його, ситуація може прийняти ще більш загрозливого характеру. З метою розмежування термінології приймемо, що в першому випадку ми маємо справу зі зломом захисту Firewall, а в другому - з повним її руйнуванням. Ступінь впливу, який може спричинити за собою руйнування захисту братмауера, визначити неймовірно складно. Найбільш повні відомості про надійність такого захисту може дати тільки інформація про діяльність, спробі злому, зібрана цим брандмауером. Найгірше відбувається із системою захисту саме тоді, коли при повному руйнуванні брандмауера не залишається жодних слідів, що вказують на те, як це відбувалося. У кращому ж випадку брандмауер сам виявляє спробу злому і ввічливо інформує про це адміністратора. Спроба при цьому приречена на провал.

Один зі способів визначити результат спроби злому захисту Firewall - перевірити стан речей в так званих зонах ризику. Якщо мережа підключена до Internet без брандмауера, об'єктом нападу стане вся мережа. Така ситуація сама по собі не передбачає, що мережа стає вразливою для кожної спроби злому. Однак якщо вона приєднується до загальної незахищеної мережі, адміністраторові доведеться забезпечувати безпеку кожного вузла окремо. У разі утворення проломів в брандмауері зона ризику розширюється і охоплює всю захищену мережу. Зломщик, що отримав доступ до входу в брандмауер, може вдатися до методу "захоплення островів" і, користуючись брандмауером як базою, охопити всю локальну мережу. Подібна ситуація все ж дасть слабку надію, бо порушник може залишити сліди в брандмауері, і його можна буде викрити. Якщо ж брандмауер повністю виведений з ладу, локальна мережа стає відкритою для нападу з будь-якої зовнішньої системи, і визначення характеру цього нападу стає практично неможливим.

Загалом, цілком можливо розглядати брандмауер як засіб звуження зони ризику до однієї точки пошкодження. Однак практикою підтверджено, що будь-яка досить велика мережа включає, щонайменше, декілька вузлів, уразливих при спробі злому навіть не дуже досвідченим порушником, якщо у нього достатньо для цього часу. Багато великих компаній мають на озброєнні організаційну політику забезпечення безпеки вузлів, розроблену з урахуванням цих недоліків. Однак було б не надто розумним цілком покладатися виключно на правила. Саме за допомогою брандмауера можна підвищити надійність вузлів, направляючи порушника в такий вузький тунель, що з'являється реальний шанс

виявити і вистежити його, до того як він завдасть шкоди.

Зазвичай міжмережеві екрани захищають внутрішню мережу підприємства від "вторгнень" з глобальної мережі Internet, однак вони можуть використовуватися і для захисту від "нападів" з корпоративної мережі, до якої підключена локальна мережа підприємства. Жоден міжмережевий екран не може гарантувати повного захисту внутрішньої мережі при всіх можливих обставин. Однак для більшості комерційних організацій установка міжмережевого екрану є необхідною умовою забезпечення безпеки внутрішньої мережі. Головний аргумент на користь застосування міжмережевого екрану полягає в тому, що без нього системи внутрішньої мережі наражаються на небезпеку з боку слабо захищених служб мережі Internet, а також зондування і атакам з будь-яких інших хост - комп'ютерів зовнішньої мережі.

Проблеми недостатньої інформаційної безпеки є "вродженими" практично для всіх протоколів і служб Internet. Велика частина цих проблем пов'язана з історичною залежністю Internet від операційної системи UNIX. Відомо, що мережа Arpanet (прабатько Internet) будувалася як мережа, що зв'язує дослідні центри, наукові, військові та урядові установи, великі університети США. Ці структури використовували операційну систему UNIX в якості платформи для комунікацій і вирішення власних завдань. Тому особливості методології програмування в середовищі UNIX та її архітектури наклали відбиток на реалізацію протоколів обміну і політики безпеки в мережі. Через відкритості та поширеності система UNIX стала улюбленою здобиччю хакерів. Тому зовсім не дивно, що набір протоколів TCP / IP, який забезпечує комунікації в глобальній мережі Internet, має "вроджені" недоліки захисту. Те ж саме можна сказати і про ряд служб Internet.

Набір протоколів управління передачею повідомлень в Internet (Transmission Control Protocol / Internet Protocol - TCP / IP) використовується для організації комунікацій в неоднорідному мережевому середовищі, забезпечуючи сумісність між комп'ютерами різних типів. Сумісність - одна з основних переваг TCP / IP, тому більшість локальних комп'ютерних мереж підтримує ці протоколи. Крім того, протоколи TCP / IP надають доступ до ресурсів глобальної мережі Internet. Оскільки TCP / IP підтримує маршрутизацію пакетів, він зазвичай використовується в якості міжмережевого протоколу. Завдяки своїй популярності TCP / IP став стандартом де фактора для міжмережевої взаємодії.

У заголовках пакетів TCP / IP зазначається інформація, яка може піддатися нападам хакерів. Зокрема, хакер може підмінити адресу відправника у своїх "шкідливих" пакетах, після чого вони будуть виглядати, як пакети, що передаються авторизованим клієнтом.

Функціональні вимоги до міжмережевих екранів включають:

- вимоги до фільтрації на мережевому рівні;
- вимоги до фільтрації на прикладному рівні;
- вимоги по налаштуванню правил фільтрації та адміністрування;
- вимоги до засобів мережевої аутентифікації;
- вимоги щодо впровадження журналів та обліку.

Більшість компонентів міжмережевих екранів можна віднести до однієї з трьох категорій:

- фільтруючі маршрутизатори;
- шлюзи мережевого рівня;
- шлюзи прикладного рівня.

Ці категорії можна розглядати як базові компоненти реальних міжмережевих екранів. Лише деякі міжмережеві екрани включають тільки одну з перерахованих категорій. Тим не менше, ці категорії відображають ключові можливості, що відрізняють міжмережеві екрани один від одного.

Фільтруючий маршрутизатор являє собою маршрутизатор або працюючий на сервері програму, сконфігуровану таким чином, щоб фільтрувати вхідні і вихідні пакети. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP-і IP-заголовках пакетів.

Фільтруючі маршрутизатори звичайно мають можливості фільтрувати IP-пакет на основі групи наступних полів заголовка пакету:

- IP-адреса відправника (адреса системи, яка послала пакет);

- IP-адресу одержувача (адреса системи, яка приймає пакет);
- порт відправника (порт з'єднання в системі відправника);
- порт одержувача (порт з'єднання в системі одержувача);

Порт - це програмне поняття, яке використовується клієнтом або сервером для здійснення та отримання повідомлень; порт ідентифікується 16 - бітовим числом.

В даний час не всі фільтруючі маршрутизатори фільтрують пакети по TCP / UDP - порт відправника, однак багато виробників маршрутизаторів почали забезпечувати таку можливість. Деякі маршрутизатори перевіряють, з якого мережевого інтерфейсу маршрутизатора прийшов пакет, і потім використовують цю інформацію як додатковий критерій фільтрації.

Фільтрація може бути реалізована в різний спосіб для блокування сполук з певними хост - комп'ютерами або портами. Наприклад, можна блокувати з'єднання, що надходять від конкретних адрес тих хост-комп'ютерів і мереж, які вважаються ворожими або ненадійними.

Додавання фільтрації по портах TCP і UDP до фільтрації по IP-адресам забезпечує більшу гнучкість. Відомо, що такі сервери, як домен TELNET, зазвичай пов'язані з конкретними портами (наприклад, порт 23 протоколу TELNET). Якщо міжмережевий екран може блокувати з'єднання TCP або UDP з певними портами або від них, то можна реалізувати політику безпеки, при якій деякі види з'єднань встановлюються лише з конкретними хост - комп'ютерами.

До позитивних якостей фільтруючих маршрутизаторів слід віднести:

- порівняно невисоку вартість;
- гнучкість у визначенні правил фільтрації;
- невелику затримку при проходженні пакетів.

Недоліками фільтруючих маршрутизаторів є:

- правила фільтрації пакетів важкі в описі і вимагають дуже хороших знань технологій TCP і UDP;
- при порушенні працездатності брандмауера з фільтрацією пакетів всі комп'ютери за ним стають повністю незахищеними або недоступними;
- аутентифікацію з використанням IP-адреси можна обдурити шляхом підміни IP-адреси (атакуюча система видає себе за іншу, використовуючи її IP-адресу);
- відсутня аутентифікація на рівні користувача.

Шлюзи мережевого рівня

Шлюз мережевого рівня іноді називають системою трансляції мережевих адрес або шлюзом сеансового рівня моделі OSI. Такий шлюз виключає, пряма взаємодія між авторизованим клієнтом і зовнішнім хост-комп'ютером. Шлюз мережевого рівня приймає запит довіреного клієнта на конкретні послуги, і після перевірки допустимості запитаного сеансу встановлює з'єднання із зовнішнім хост - комп'ютером. Після цього шлюз копіює пакети в обох напрямках, не здійснюючи їх фільтрації.

Шлюз стежить за підтвердженням зв'язку між авторизованим клієнтом і зовнішнім хост - комп'ютером, визначаючи, чи є запитуваний сеанс зв'язку допустимим.

Фактично більшість шлюзів мережевого рівня не є самостійними продуктами, а поставляються в комплекті зі шлюзами прикладного рівня. Прикладами таких шлюзів є Gauntlet Internet Firewall компанії Trusted Information Systems, Alta Vista Firewall компанії DEC і ANS Interlock компанії ANS. Наприклад, Alta Vista Firewall використовує канальні посередники прикладного рівня для кожної з шести служб TCP / IP, до яких належать, зокрема, FTP, HTTP (Hyper Text Transport Protocol) і Telnet. Крім того, міжмережевий екран компанії DEC забезпечує шлюз мережевого рівня, що підтримує інші загальнодоступні служби TCP / IP, такі як Gopher і SMTP, для яких міжмережевий екран не надає посередників прикладного рівня.

Шлюз мережевого рівня виконує ще одну важливу функцію захисту: він використовується в якості сервера-посередника. Цей сервер-посередник виконує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP-адрес в одну "надійну" IP-адресу. Ця адреса асоціюється з міжмережевим екраном, з якого передаються всі вихідні пакети. У результаті в мережі зі шлюзом

мережевого рівня всі вихідні пакети виявляються відправленими з цього шлюзу, що виключає прямий контакт між внутрішньою (авторизованої) мережею і потенційно небезпечною зовнішньою мережею. IP-адреса шлюзу мережевого рівня стає єдино активною IP-адресою, яка потрапляє в зовнішню мережу. Таким чином, шлюз мережевого рівня та інші сервери-посередники захищають внутрішні мережі від нападів типу підміни адрес.

Шлюзи прикладного рівня

Для усунення ряду недоліків, властивих фільтруючим маршрутизаторам, міжмережеві екрани повинні використовувати додаткові програмні засоби для фільтрації повідомлень сервісів типу TELNET і FTP. Такі програмні засоби називаються повноважними серверами (серверами-посередниками), а хост-комп'ютер, на якому вони виконуються, - шлюзом прикладного рівня.

Шлюз прикладного рівня виключає пряму взаємодію між авторизованим клієнтом і зовнішнім хост - комп'ютером. Шлюз фільтрує всі вхідні і вихідні пакети на прикладному рівні. Пов'язані з додатком сервери - посередники перенаправляють через шлюз інформацію, що генерується конкретними серверами.

Для досягнення більш високого рівня безпеки та гнучкості шлюзи прикладного рівня і фільтруючі маршрутизатори можуть бути об'єднані в одному міжмережному екрані. Як приклад розглянемо мережу, в якій за допомогою фільтруючого маршрутизатора блокуються вхідні з'єднання TELNET і FTP. Цей маршрутизатор допускає проходження пакетів TELNET або FTP тільки до одного хост - комп'ютера - шлюзу прикладного рівня TELNET / FTP. Зовнішній користувач, який хоче з'єднатися з деякою системою в мережі, повинен спочатку з'єднатися зі шлюзом прикладного рівня, а потім вже з потрібним внутрішнім хост-комп'ютером.

На додаток до фільтрації пакетів багато шлюзи прикладного рівня реєструють всі виконувані сервером дії і, що особливо важливо, попереджають мережевого адміністратора про можливі порушення захисту. Наприклад, при спробах проникнення в мережу ззовні BorderWare Firewall Server компанії Secure Computing дозволяє фіксувати адреси відправника і одержувача пакетів, час, в який ці спроби були зроблені, і використовуваний протокол. Міжмережевий екран Black Hole компанії Milkyway Networks реєструє всі дії сервера і попереджає адміністратора про можливі порушення, посилаючи йому повідомлення по електронній пошті або на пейджер. Аналогічні функції виконують і ряд інших шлюзів прикладного рівня.

Шлюзи прикладного рівня дозволяють забезпечити найбільш високий рівень захисту, оскільки взаємодія із зовнішнім світом реалізується через мало прикладних повноважних програм-посередників, повністю контролюють весь вхідний і вихідний трафік.

Шлюзи прикладного рівня мають ряд переваг у порівнянні зі звичайним режимом, при якому прикладної трафік пропускається безпосередньо до внутрішніх хост - комп'ютерів. Розглянемо ці переваги.

– Невидимість структури мережі, що захищається з глобальної мережі Internet. Імена внутрішніх систем можна не повідомляти зовнішнім системам через DNS, оскільки шлюз прикладного рівня може бути єдиним хост - комп'ютером, ім'я якого повинно бути відомо зовнішнім системам.

– Надійна аутентифікація та реєстрація. Прикладної трафік може бути аутентифікований, перш ніж він досягне внутрішніх хост-комп'ютерів, і може бути зареєстрований більш ефективно, ніж за допомогою стандартної реєстрації.

– Оптимальне співвідношення між ціною і ефективністю. Додаткові або апаратні засоби для аутентифікації або реєстрації потрібно встановлювати тільки на шлюзі прикладного рівня.

– Прості правила фільтрації. Правила на фільтруючому маршрутизаторі виявляються менш складними, ніж вони були б, якщо б маршрутизатор сам фільтрував прикладний трафік і відправляв його великому числу внутрішніх систем. Маршрутизатор повинен пропускати прикладної трафік, призначений тільки для шлюзу прикладного рівня, і блокувати весь інший трафік.

– Можливість організації великого числа перевірок. Захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, що знижує ймовірність злому з використанням

"дірок" у програмному забезпеченні.

До недоліків шлюзів прикладного рівня відносяться:

– більш низька продуктивність у порівнянні з фільтруючими маршрутизаторами; зокрема, при використанні клієнт-серверних протоколів, таких як TELNET, потрібно двокрокова процедура для вхідних та вихідних з'єднань;

– більш висока вартість у порівнянні з фільтруючим маршрутизатором.

Крім TELNET і FTP шлюзи прикладного рівня зазвичай використовуються для електронної пошти, Windows і деяких інших служб.

Одним з важливих компонентів концепції міжмережевих екранів є автентифікація (перевірка дійсності користувача). Перш ніж користувачеві буде надано право скористатися тим чи іншим сервісом, необхідно переконатися, що він дійсно той, за кого себе видає.

Одним із способів аутентифікації є використання стандартних UNIX-паролів. Однак ця схема найбільш вразливе з точки зору безпеки - пароль може бути перехоплений і використаний іншою особою. Багато інцидентів в мережі Internet відбулися через уразливість традиційних паролів. Зловмисники можуть спостерігати за каналами в мережі Internet і перехоплювати що передаються в них відкритим текстом паролі, тому схему аутентифікації з традиційними паролями слід визнати застарілою.

Для подолання цього недоліку розроблено ряд засобів посиленою аутентифікації: смарт-карти, персональні жетони, біометричні механізми і т.п. Хоча в них задіяні різні механізми аутентифікації, загальним для них є те, що паролі, які генеруються цими пристроями, не можуть бути повторно використані порушником, що спостерігає за встановленням зв'язку. Оскільки проблема з паролями в мережі Internet є постійною, міжмережевий екран для з'єднання з Internet, не має в своєму розпорядженні засобів посилення аутентифікації або не використовує їх, втрачає всякий сенс.

Ряд найбільш популярних засобів посиленою аутентифікації, що застосовуються в даний час, називаються системами з одноразовими паролями. Наприклад, смарт-карти або жетони аутентифікації генерують інформацію, яку хост-комп'ютер використовує замість традиційного пароля. Результатом є одноразовий пароль, який, навіть якщо він буде перехоплений, не може бути використаний зловмисником під виглядом користувача для встановлення сеансу з хост - комп'ютером.

Так як міжмережеві екрани можуть централізувати управління доступом в мережі, вони є підходящим місцем для установки програм або пристроїв посиленою аутентифікації. Хоча кошти посиленою аутентифікації можуть використовуватися на кожному хост - комп'ютері, більш практично їх розміщення на межсетевом екрані. Якщо хост - комп'ютери не застосовують заходів посиленої аутентифікації, зловмисник може спробувати зламати паролі або перехопити мережевий трафік з метою знайти в ньому сеанси, в ході яких передаються паролі.

У цьому випадку сеанси TELNET або FTP, що встановлюються з боку мережі Internet з системами мережі, повинні проходити перевірку за допомогою засобів посиленою аутентифікації, перш ніж вони будуть дозволені, Системи мережі можуть запитувати для дозволу доступу і статичні паролі, але ці паролі, навіть якщо вони будуть перехоплені зловмисником, не можна буде використовувати, тому що кошти посиленою аутентифікації та інші компоненти міжмережевого екрану запобігають проникнення зловмисника або обхід ними міжмережевого екрану.

Основні схеми мережевого захисту на базі міжмережевих екранів

При підключенні корпоративної або локальної мережі до глобальних мереж адміністратор мережевої безпеки має вирішувати такі завдання:

– захист корпоративної або локальної мережі від несанкціонованого доступу з боку глобальної мережі;

– приховування інформації про структуру мережі та її компонентів від користувачів глобальної мережі,

– розмежування доступу в мережу, що захищається з глобальної мережі і з мережі, що захищається в глобальну мережу.

Необхідність роботи з віддаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається. При цьому часто виникає потреба в організації у складі корпоративної мережі декількох сегментів з різними рівнями безпеки:

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

Для захисту корпоративної або локальної мережі застосовуються такі основні схеми організації міжмережевих екранів:

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

Міжмережевий екран, заснований на фільтрації пакетів, є поширеним і найбільш простим в реалізації. Він складається з фільтруючого маршрутизатора, розташованого між що захищається мережею і мережею Internet. Фільтруючий маршрутизатор налаштований для блокування або фільтрації вхідних і вихідних пакетів на основі аналізу їх адрес і портів. Комп'ютери, що знаходяться в мережі, що захищається, мають прямий доступ в мережу Internet, в той час як більша частина доступу до них з Internet блокується. Часто блокуються такі небезпечні служби, як X Windows, NIS і NFS.

Міжмережевий екран на базі двопортового прикладного шлюзу включає дводомний хост-комп'ютер з двома мережевими інтерфейсами. При передачі інформації між цими інтерфейсами і здійснюється основна фільтрація. Для забезпечення додаткового захисту між прикладним шлюзом та мережею Internet зазвичай розміщують фільтруючий маршрутизатор. У результаті між прикладним шлюзом та маршрутизатором утворюється внутрішня екранована підмережа. Цю підмережу можна використовувати для розміщення доступних ззовні інформаційних серверів.

Міжмережевий екран на основі екранованого шлюзу об'єднує фільтруючий маршрутизатор і прикладної шлюз, дозволяються з боку внутрішньої мережі. Прикладної шлюз реалізується на хост - комп'ютері і має тільки один мережевий інтерфейс.

Міжмережевий екран, що складається з екранованої підмережі, являє собою розвиток схеми міжмережевого екрану на основі екранованого шлюзу. Для створення екранованої підмережі використовуються два екрануючих маршрутизатора. Зовнішній маршрутизатор розташовується між мережею Internet і під мережею, що екранується, а внутрішній - між підмережею, що екранується і захищається внутрішньою мережею. Ця підмережа містить прикладної шлюз, а також може включати інформаційні сервери та інші системи, що вимагають контрольованого доступу. Ця схема міжмережевого екрану забезпечує хорошу безпеку завдяки організації екранованої підмережі, яка ще краще ізолює внутрішню мережу, що захищається від Internet.

Можливості брандмауер Windows

- Блокувати комп'ютерним вірусам і «черв'якам» доступ на комп'ютер.
- Здійснити запит до користувача про вибір блокування або дозволу для певних запитів на підключення.
- Вести облік (журнал безпеки) - за бажанням користувача - записуючи дозволені та заблоковані спроби підключення до комп'ютера. Цей журнал може виявитися корисним для діагностики помилок.

Відсутні можливості брандмауер Windows

- Виявити або знешкодити комп'ютерні віруси, якщо вони вже потрапили на комп'ютер. З цієї причини необхідно також встановити антивірусне програмне забезпечення та своєчасно оновлювати його, щоб запобігти пошкодження комп'ютера вірусами, «черв'яками» та іншими небезпечними об'єктами, а також не допустити використання даного комп'ютера для поширення на інші комп'ютери.

– Заборонити користувачеві відкривати повідомлення електронної пошти з небезпечними вкладеннями. Не відкривайте вкладення в повідомленнях електронної пошти від незнайомих відправників. Слід проявляти обережність, навіть якщо джерело повідомлення електронної пошти відоме і заслуговує довіри. При отриманні від знайомого користувача електронного листа з вкладенням уважно прочитайте тему повідомлення перед тим, як відкрити його. Якщо тема повідомлення являє собою безладний набір знаків або не має сенсу, не відкривайте лист, поки не зв'яжетеся з відправником для отримання підтвердження.

– Блокувати спам або несанкціоновані поштові розсилки, щоб вони не надходили в папку вхідних повідомлень. Однак деякі програми електронної пошти здатні робити це.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається брандмауером?
2. Які основні функції брандмауера?
3. Дайте визначення апаратному та програмному міжмережевим екранам.
4. Що включають в себе функціональні вимоги до міжмережевих екранів?
5. Назвіть основні категорії компонентів між мережевих екранів.
6. Дайте визначення фільтруючому маршрутизаторі.
7. Назвіть переваги та недоліки фільтруючих маршрутизаторів.
8. Охарактеризуйте шлюзи мережевого рівня.
9. Дайте визначення шлюзам прикладного рівня.
10. Які ви знаєте основні схеми мережевого захисту на базі міжмережевих екранів.
11. Назвіть можливості брандмауер Windows.