Лабораторна робота №4. Планування між мережевих екранів.

Мета роботи

Метою роботи є отримання навичок розміщення брандмауерів в підходящих місцях, що задовольняють вимогам безпеки.

Теоретичні відомості

З швидким зростанням інтересу до Інтернету і операційній системі Windows NT безпеку мережі стала важливим завданням для багатьох компаній у всьому світі. Той факт, що інформація про злом і проникненні в корпоративні мережі та засоби, необхідні для цього, легко і широко доступні, ще більше посилює актуальність проблем безпеки. У зв'язку з цим адміністратори мережі часто витрачають набагато більше зусиль і часу на захист мереж, ніж на установку програм і адміністрування. Нові засоби, перевіряючі мережу на присутність слабких вузлів, типу Security Administrator Tool for Analyzing Networks (SATAN), безсумнівно, допомагають адміністраторам, але вони лише показують вразливі місця мережі, не забезпечуючи захисту. Давайте подивимося, від чого потрібно захищатися при роботі в мережі, щоб відповісти на питання: чому ви маєте потребу в firewall?

Проблеми з безпекою при з'єднанні з інтернетом

Коли ви підключаєте вашу приватну мережу до Інтернету, ви фізично з'єднуєтеся більш ніж з 50 тис. Невідомих мереж і всіма їх користувачами. Таке з'єднання відкриває вам шлях до багатьох корисних програмам і забезпечує величезні можливості поділу інформації, проте більшість приватних і корпоративних мереж містить інформацію, яка не повинна бути доступна іншим користувачам Інтернету. Крім того, не всі дії користувачів Інтернету є законними. Звідси випливають два основні питання:

Як захистити конфіденційну інформацію від тих, хто не має права доступу до неї?

1. Як захистити мережу та її ресурси від зловмисних користувачів і випадковостей, які відбуваються поза вашої мережі?

2. Будемо надалі називати атакою спробу доступу до прихованої інформації або просто проникнення в мережу, завжди маючи на увазі, що це не бажане для вас дію. Людину, яка виробляє таку дію, будемо називати зломщиком.

Захист конфіденціальної інформації

Конфіденційна інформація (як і будь-яка інформація в мережі) може або перебувати на носії інформації, або передаватися по мережі у вигляді пакетів. В обох станах інформація може стати предметом злому з боку як внутрішніх, так і зовнішніх користувачів. Ми обмежимося розглядом другого стану, коли інформація «в дорозі». Ось основні п'ять способів, які використовуються для отримання доступу до інформації:

- «винюхування» мережевих пакетів (network packet sniffers);
- містифікація пакетів IP (IP spoofing);
- взлом пароля (password attacks);
- перенаправлення пакетів зовні (distribution of sensitive information).
- використання проміжного комп'ютера (man-in-the-middle attacks)

При захисті інформації від таких атак ви хочете в першу чергу запобігти крадіжкам, руйнування, псування інформації або введення інформації ззовні. Стисло опишемо вищеперелічені способи злому.

«Винюхуванню» мережевих пакетів - це просто якийсь спосіб стеження за пакетами, що проходять по мережі. Зазвичай це програма, запущена на якомусь комп'ютері мережі.

Містифікація пакетів IP- це посилка пакетів з невірною інформацією про відправника, одержувача, номері порту або типі самого пакета. Наприклад, запис в пакет адреси відправника, що збігається з адресою машини внутрішньої мережі, може збільшити пріоритет обробки цього пакета.

Злом пароля зустрічається дещо частіше інших методів. Виробляється спроба будь-яким способом дізнатися пароль або отримати привілеї користувача root на який-небудь машині мережі.

Перенаправлення пакетів зовні є спробою направити назовні з вашої мережі інформацію, доступ до якої обмежено або заборонено.

Використання проміжного комп'ютера (man-in-the-middle attacks) - явне використання доступу до інформації вашої мережі. Приміром, це ситуація, коли користувач, що має офіційний доступ до інформації, намагається пересилати її в зовнішню мережу

Захист мережі: підтримка цілісності мережі

При захисті інформації важливу роль відіграє підтримка цілісності мережі. Порушення налагодженої роботи мережі може привести до великих витрат часу на відновлення, а також відкрити нові можливості для зовнішніх атак, тобто стати першим етапом злому мережі. Ось методи, які для цього використовуються:

• «винюхування» мережевих пакетів (network packet sniffers);

• містифікація пакетів IP (IP spoofing);

• взлом пароля (password attacks);

• збій роботи (denial of service);

• атаки на рівні програм (application layer attacks).

Збій роботи - це не атака з метою злому. Це - спроба порушити або повністю блокувати роботу якогось вузла мережі, окремої програми або фізично знищити інформацію на носіях.

Атаки на рівні програм ставлять своєю метою одержання або знищення інформації за допомогою модифікації існуючих або установки нових, спеціально підготовлених програм. Аналогом таких атак є віруси.

Опису ідеї firewall як найбільш поширеного способу захисту мереж та інформації від злому присвячена інша частина статті.

Розвиток firewall

Очевидно, що необхідність захисту мереж породило цілий напрямок в комп'ютерній індустрії - технологію захисту мереж, яке в основному обертається навколо ідеї firewall.

Firewall - це точка поділу вашої мережі і тієї, до якої ви під'єднані. Цією точкою може бути комп'ютер, на якому запущено програмний firewall, або апаратно реалізований firewall. Firewall може бути простим, як звичайний маршрутизатор, фільтруючий пакети, або складним, що поєднує в собі функції багатозадачною маршрутизації, фільтрації пакетів і програмного proxy-сервера.

Перше покоління firewall (packet filtering firewalls), яке з'явилося в 1985 році, представляло собою перше покоління звичайних маршрутизаторів, що включають фільтрацію пакетів.

Друге покоління з'явилося в 1990-х і відомо як firewall ланцюгового рівня (circuit level firewalls).

Третє покоління - це firewall програмного рівня (application layer firewall).

Четверте покоління firewall засновано на динамічній фільтрації пакетів (dynamic packet filter firewalls), а першою його реалізацією була програма CheckPoint, випущена однойменною фірмою.

П'яте покоління firewall, яке з'явилося в 1996 році, базується на архітектурі kernel proxy. Зараз цей метод теж має як програмні, так і апаратні реалізації.

Лінія захисту (Security Perimeter)

Коли ви визначаєте тактику захисту мережі, ви повинні визначити спосіб охорони мережі та інформації, а також користувачів від пошкодження і втрати даних. Тактика захисту мережі заснована на управлінні рухом пакетів і контролем використання мережі. Ви повинні повністю описати мережу, встановити її «вузькі місця» і визначити дії, які робитимуться при порушенні захисту. При цьому ви точно обумовлюєте кордону, в яких діє ваша захист. Ці кордони і є мережа лінії захисту (perimeter networks).

Perimeter networks

Щоб встановити таку мережу захисту, ви повинні визначити мережу комп'ютерів, які потребують захисту, і визначити механізм їх захисту. Необхідним є умова, щоб firewall-сервер був шлюзом (gateway) між внутрішніми і зовнішніми мережами. Кожна мережа може містити мережі захисту всередині себе. Розрізняють зовнішні, середні і внутрішні мережі захисту. Зовнішня захист розділяє мережу, якою ви керуєте, і ту, якої ви не можете управляти. Середній рівень розділяє підмережі всередині вашої мережі або відокремлює доступні для зовнішніх користувачів комп'ютери від тих, до яких доступ заборонений. Внутрішній рівень дозволяє розділяти мережі всередині недоступних і зовні доступних частин вашої мережі.

Для подальшого викладу введемо три поняття: Trusted networks - мережі, які ви захищаєте і якими можете управляти (всередині perimeter network); Untrusted networks - мережі, якими ви не керуєте (зазвичай зовні), але з якими, проте, повинні обмінюватися інформацією; і Unknown networks - мережі, про які не можна сказати нічого певного, крім того, що вони існують.

Архітектура firewall

Firewall - це шлюз мережі, забезпечений правилами захисту. Він може бути апаратним або програмним. Відповідно до закладеними правилами обробляється кожен пакет, що проходить назовні або всередину мережі, причому процедура обробки може бути задана для кожного правила. Виробники програм і машин, що реалізують firewall-технології, забезпечують різні способи завдання правил і процедур. Зазвичай firewall створює контрольні записи, деталізують причину і обставини виникнення позаштатних ситуацій. Аналізуючи такі контрольні записи, адміністратори часто можуть виявити джерело атаки і способи її проведення, тим самим забезпечуючи себе додатковою інформацією про атаку.

Як працює фільтрація пакетів (packet filtering firewalls)

Кожен IP-пакет перевіряється на збіг закладеної в ньому інформації з допустимими правилами, записаними в firewall.

Параметри, які можуть перевірятися:

• фізичний інтерфейс руху пакета;

• адресу, з якої прийшов пакет (джерело);

• адресу, куди йде пакет (одержувач);

• тип пакета (TCP, UDP, ICMP);

• порт джерела;

• порт одержувача.

З цього переліку видно, що фільтрація пакетів не має справи з їх вмістом. Це дозволяє використовувати безпосередньо ядро операційної системи для завдання правил. По суті, створюються два списки: заперечення (deny) і дозвіл (permit). Всі пакети повинні пройти перевірку за всіма пунктами цього списку. Далі використовуються такі методи:

• якщо ніяке правило відповідності не знайдено, то видалити пакет з мережі;

• якщо відповідне правило знайдено в списку дозволів, то пропустити пакет;

• якщо відповідне правило знайдено в списку заперечень, то видалити пакет з мережі.

На додаток до цього firewall, заснований на фільтрації пакетів, може змінювати адреси джерел пакетів, що виходять назовні, щоб приховати тим самим топологію мережі (метод address translation).

Відзначимо переваги firewall, заснованого на фільтрації пакетів:

• фільтрація пакетів працює швидше інших firewall-технологій, бо використовується менша кількість перевірок;

• цей метод легко реалізуємо апаратно;

• одне-єдине правило може стати ключовим при захисті всієї мережі;

• фільтри не вимагають спеціальної конфігурації комп'ютера;

• метод address translation дозволяє приховати реальні адреси комп'ютерів в мережі.

Однак є й недоліки:

• немає перевірки вмісту пакетів, що не дає можливості, наприклад, контролювати, що передається по FTP. В цьому сенсі application layer і circuit level firewall набагато практичніше;

• немає інформації про те, який процес або програма працювали з цим пакетом, і відомостей про сесії роботи;

• робота ведеться з обмеженою інформацією пакета;

• в силу «низькорівневі» методу не враховується особливість переданих даних;

• слабо захищений сам комп'ютер, на якому запущено firewall, тобто предметом атаки може стати сам цей комп'ютер;

• немає можливості сигналізувати про позаштатних ситуаціях або виконувати при їх виникненні будь-які дії;

Firewall ланцюгового рівня (circuit level firewalls)

Оскільки при передачі великої порції інформації вона розбивається на маленькі пакети, цілий фрагмент складається з декількох пакетів (з ланцюга пакетів). Firewall ланцюгового рівня перевіряє цілісність всього ланцюга, а також те, що вона вся йде від одного джерела до одного одержувачу, і інформація про ланцюги всередині пакетів (а вона там є при використанні TCP) збігається з реально проходять пакетами. Причому ланцюг спочатку збирається на комп'ютері, де встановлений firewall, а потім вирушає одержувачу. Оскільки перший пакет ланцюга містить інформацію про всю ланцюга, то при попаданні першого пакета створюється таблиця, яка видаляється лише після повного проходження ланцюга.

Зміст таблиці такий:

• унікальний ідентифікатор сесії передачі, який використовується для контролю;

• стан сесії передачі: встановлено, передано або закрито;

• інформація про послідовність пакетів;

• адресу джерела ланцюга;

• адресу одержувача ланцюга;

• фізичний інтерфейс, використовуваний для отримання ланцюга;

• фізичний інтерфейс, використовуваний для відправлення ланцюга.

Ця інформація застосовується для перевірки допустимості передачі ланцюга. Правила перевірки, як і у випадку фільтрації пакетів, задаються у вигляді таблиць в ядрі.

Основні переваги firewall ланцюгового рівня:

• firewall ланцюгового рівня швидше програмного, так як виробляє менше перевірок;

• firewall ланцюгового рівня дозволяє легко захистити мережу, забороняючи з'єднання між певними адресами зовнішньої і внутрішньої мережі;

• можливо приховування внутрішньої топології мережі.

Недоліки firewall ланцюгового рівня:

• важко реалізувати цей алгоритм для не-TCP-протоколів;

• немає перевірки пакетів на програмному рівні;

• слабкі можливості запису інформації про нештатні ситуації, окрім інформації про сесії передачі;

• немає перевірки переданих даних;

• важко перевірити дозвіл або заперечення передачі пакетів.

Firewall програмного рівня

- Крім цілісності ланцюгів, правильності адрес і портів, перевіряються також самі дані, передані в пакетах. Це дозволяє перевіряти цілісність даних і відстежувати передачу таких відомостей, як паролі. Разом з firewall програмного рівня використовується proxy-сервіс, який кешируєт інформацію для більш швидкої її обробки. При цьому виникають такі нові можливості, як, наприклад, фільтрація URL і встановлення автентичності користувачів. Всі з'єднання внутрішньої мережі з зовнішнім світом відбуваються через proxy, який є шлюзом. У proxy дві частини: сервер і клієнт. Сервер приймає запити, наприклад на telnet-з'єднання з внутрішньої мережі з зовнішньою, обробляє їх, тобто перевіряє на допустимість передачі даних, а клієнт працює з зовнішнім комп'ютером від імені реального клієнта. Природно, спочатку всі пакети проходять перевірку на нижніх рівнях.

Гідності proxy:

• розуміє і обробляє протоколи високого рівня типу HTTP і FTP;

• зберігає повну інформацію про сесії передачі даних як низького, так і високого рівня;

• можлива заборона доступу до деяких мережевих сервісів;

• є можливість управління пакетами даних;

• є приховування внутрішніх адрес і топології мережі, так як proxy є фільтром;

• залишається видимість прямого з'єднання мереж;

• proxy може перенаправляти запити мережевих сервісів на інші комп'ютери;

• є можливість кешування http-об'єктів, фільтрації URL і встановлення автентичності користувачів;

• можливе створення докладних звітних записів для адміністратора.

Недоліки proxy:

• вимагає зміни мережевого стека на машині, де стоїть firewall;

• не можна напряму запустити мережеві сервіси на машині, де стоїть firewall, так як proxy перехоплює роботу портів;

• неминуче уповільнює роботу, тому всі дані обробляються двічі: «рідний» програмою і власне proxy;

• так як proxy повинен вміти працювати з даними будь-якої програми, то для кожної програми потрібен свій proxy;

• немає proxy для UDPi RPC;

• іноді необхідна спеціальна настройка клієнта для роботи з proxy;

• proxy не захищений від помилок в самій системі, а його робота сильно залежить від наявності останніх;

• коректність роботи proxy безпосередньо пов'язана з правильністю обробки мережевого стека;

• використання proxy може вимагати додаткових паролів, що незручно для користувачів.

Динамічна фільтрація пакетів (dynamic packet filter firewalls)

В основному цей рівень повторює попередній, за двома важливими винятками:

• можлива зміна правил обробки пакетів «на льоту»;

• включена підтримка UDP.

Рівень kernel proxy

Рівень kernel proxy виник досить недавно. Основна його ідея - спроба помістити описаний вище алгоритм firewall програмного рівня в ядро операційної системи, що позбавляє комп'ютер від зайвих витрат часу на передачу даних між ядром і програмою proxy. Це підвищує продуктивність і дозволяє виробляти більш повну перевірку проходить інформації.

Коротко про реалізації firewall

Як вже було сказано, firewall може бути реалізований як програмно, так і апаратно. Апаратна реалізація являє собою якийсь спеціалізований комп'ютер, єдиною функцією якого є робота в якості firewall. Причому ця програма зашита в його залізо. Це дозволяє домагатися великої продуктивності. Однією з провідних фірм, що виробляють такі комп'ютери, є Cisco (серія Cisco Access Servers). Програмна реалізація - це просто програма, яка виконується на комп'ютері-шлюзі і виконує описані вище функції (наприклад, LanGuard, Cisco IOS Software, Checkpoint). Очевидно, що для роботи такої програми необхідний досить потужний комп'ютер з великим об'ємом пам'яті, причому нерозумно сильно завантажувати цей комп'ютер іншою роботою. Для прикладу наведу короткий опис програми LanGuard, яка має один з найвищих рейтингів.

Програма написана під Windows NT і працює по четвертому, описаного вище рівню. Вона безкоштовна обмежений час, після чого дозволяє працювати, якщо мережа складається не більше ніж з п'яти комп'ютерів. Програма виконує наступні функції:

• захищає мережу від доступу зовнішніх користувачів, в тому числі і сам шлюз, дозволяючи розписувати правила по портам, додаткам і мережевим адресам;

• відстежує програми sniffer;
• відстежує кількість проходить по мережі інформації;
• відстежує використання Інтернет і конкретну зв'язок з сайтами, дозволяючи вводити правила, наприклад заборона використання будь-яких сайтів;
• відстежує віруси типу троянських коней;
• може створювати докладні звіти про використання мережі;
• видає попередження адміністратору.

Нижче на малюнках представлено декілька екранів, що наочно демонструють LanGuard.

На закінчення скажемо, що зараз firewall де-факто є стандартом захисту мереж. Більш того, він входить до складу багатьох операційних систем сімейства UNIX. Щорічно проводяться форуми, присвячені firewall, постійно удосконалюються наявні та створюються нові програми, що реалізують firewall. Зараз firewall існує для всіх відомих платформ. Більшість фірм сьогодні пропонують останній, п'ятий рівень firewall, що забезпечує роботу proxy на рівні ядра операційної системи.

Завдання на лабораторну роботу

Ви є техніком, що здійснює підтримку роботи мережі середнього підприємства. В процесі росту підприємства відкритий науково-дослідний відділ, що працює над новим, вельми секретним проектом. Існування проекту залежить від захисту даних, використовуваних науково-дослідницькою групою.

Ви є техніком, що здійснює підтримку роботи мережі середнього підприємства. В процесі росту підприємства відкритий науково-дослідний відділ, що працює над новим, вельми секретним проектом. Існування проекту залежить від захисту даних, використовуваних науково-дослідницькою групою.

Сценарій 1. Захист мережі від хакерів.

Так як в компанії підвищені вимоги до безпеки, рекомендується встановити міжмережевий екран для захисту мережі від хакерів, працюючих в Інтернеті. Дуже важливо обмежити доступ до внутрішньої мережі з Інтернету.

В міжмережевому екрані Firewall_1 попередньо налаштовані правила для забезпечення необхідної клієнту безпеки. Встановіть цей брандмауер в мережі клієнта і перевірте правильність його функціонування.

Крок 1. Заміна маршрутизатора Router_A брандмауером Firewall_1.

а. Демонтуйте маршрутизатор Router_A і замініть його брандмауером Firewall_1
Підключіть інтерфейс технології Fast Ethernet 0/0 брандмауера Firewall_1 до інтерфейсу Fast Ethernet 0/1 комутатора Switch_A.
б. Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall_1 до інтерфейсу Ethernet 6 хмари мережі ISP. (Використовуйте прямий кабель для обох сполук.)
в. Підтвердіть ім'я мережевого вузла для Firewall_1 - "Firewall_1".
г. На Firewall_1 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1 209.165.200.225 і 255.255.255.224, відповідно.
д. На брандмауері Firewall_1 виберіть IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 192.168.1.1 і 255.255.255.0.

Крок 2. Перевірка конфігурації брандмауера Firewall_1

Для перевірки настройки використовуйте команду **show run**. Нижче наводиться частина зразкового лістингу:

а.

```
Firewall_1#show run
Building configuration...

hostname Firewall_1
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
 interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip access-group 100 in
 ip nat outside
 duplex auto
 speed auto
!
 interface Vlan1
 no ip address
 shutdown
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.1.2
ip route 192.168.3.0 255.255.255.0 192.168.1.3
!
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 100 deny ip any host 209.165.200.225
<выходные данные опущены>
!
end
```

З комп'ютера ПК_В, відправте луна-запит 209.165.200.225, щоб переконатися, що у внутрішнього комп'ютера мається доступ в Інтернет.

б.

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=107ms TTL=120
Reply from 209.165.200.225: bytes=32 time=98ms TTL=120
Reply from 209.165.200.225: bytes=32 time=104ms TTL=120
Reply from 209.165.200.225: bytes=32 time=95ms TTL=120

Ping statistics for 209.165.200.225:
         Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
         Minimum = 95ms, Maximum = 107ms, Average = 101ms
```

В привілейованому режимі EXEC брандмауера Firewall_1 збережіть поточну конфігурацію в початкову за допомогою команди copy run start.

Сценарій 2. Захист мережі відділу досліджень і розробок

Тепер, коли вся мережа захищена від трафіку, що надходить з Інтернету, прийшов час захистити мережу відділу досліджень і розробок (підмережа Subnet C) від можливих проникнень з внутрішньої області мережі. Для проведення досліджень науково-дослідницькій групі необхідний доступ до серверів, розташованих в підмережі B, і до Інтернету. Комп'ютерам підмережі B повинно бути відмовлено в доступі до підмережі науково-дослідного відділу.

В міжмережевому екрані Firewall_2 попередньо налаштовані правила для забезпечення необхідної клієнту безпеки. Встановіть цей брандмауер в мережі клієнта. Перевірте правильність його функціонування.

Крок 1. Заміна маршрутизатора Router_C брандмауером Firewall_2.

а. Видаліть маршрутизатор Router_C і замініть його брандмауером Firewall_2.

б. Підключіть інтерфейс Fast Ethernet 0/1 брандмауера Firewall_2 до інтерфейсу Fast Ethernet 0/3 комутатора Switch_A. Підключіть інтерфейс Fast Ethernet 0/0 брандмауера Firewall_2 до інтерфейсу Fast Ethernet 0/1 комутатора Switch_C. (Використовуйте прямий кабель для обох сполук.)

в. Підтвердіть ім'я мережевого вузла для Firewall_2 - "Firewall_2".

г. На Firewall_2 налаштуйте IP-адресу глобальної мережі та маску підмережі для інтерфейсу Fast Ethernet 0/1: 192.168.1.3 і 255.255.255.0, відповідно.

д. На брандмауері Firewall_1 виберіть IP-адресу локальної мережі та маску підмережі для інтерфейсу FastEthernet 0/0: 192.168.3.1 і 255.255.255.0.

Крок 2. Проверка конфигурации брандмауэра Firewall_2

Для перевірки налаштувань використовуйте команду "show run". Далі представлена частина вихідних даних.

a.
```
Firewall_2#show run
Building configuration...
...
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.3 255.255.255.0
 ip access-group 100 in
 ip nat outside
 duplex auto
 speed auto
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 100 permit ip host 192.168.2.10 any
access-list 100 permit ip host 192.168.1.1 any
<выходные данные опущены>
!
```

```
end
```

За запитом команди на ПК_B використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet B не можуть отримати доступ до комп'ютерів в підмережі Subnet C.

б.
```
PC>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Request timed out. Request timed out. Request timed out. Request timed out.

Ping statistics for 192.168.3.10: Packets: Sent = 4, Received = 0, Lost = 4
(100% loss),
```

За запитом команди на ПК_C використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet C мають доступ до сервера в підмережі Subnet B.

в.
```
PC>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time=164ms TTL=120
Reply from 192.168.2.10: bytes=32 time=184ms TTL=120
Reply from 192.168.2.10: bytes=32 time=142ms TTL=120

Ping statistics for 192.168.2.10:
         Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
         Minimum = 142ms, Maximum = 184ms, Average = 163ms
```

За запитом команди на ПК_C використовуйте команду ping, щоб переконатися, що комп'ютери в підмережі Subnet C мають доступ до Інтернету.

г.
```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=97ms TTL=120
Reply from 209.165.200.225: bytes=32 time=118ms TTL=120
Reply from 209.165.200.225: bytes=32 time=100ms TTL=120
Reply from 209.165.200.225: bytes=32 time=110ms TTL=120

Ping statistics for 209.165.200.225:
         Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
         Minimum = 97ms, Maximum = 118ms, Average = 106ms
```

д. В привілейованому режимі EXEC брандмауера Firewall_2 збережіть поточну конфігурацію в початкову за допомогою команди copy run start.

е. Для перевірки зробленої роботи натисніть кнопку Check Results (Перевірити результати) в нижній частині вікна інструкцій.

Контрольні питання

а. Навіщо потрібно встановлювати брандмауер у внутрішній мережі?

б. Яким чином маршрутизатор, налаштований для використання довідки NAT, дозволяє захистити комп'ютерні системи, розташовані всередині маршрутизатора NAT?

в. Вивчіть розташування брандмауерів Firewall_1 і Firewall_2 в завершеною топології мережі. Які мережі можна вважати надійними і ненадійними для брандмауера Firewall_1? Які мережі вважаються надійними і ненадійними для брандмауера Firewall_2?