

Лабораторна робота

Налаштування політик IP-безпеки. Брандмауер

Завдання.

Пропонується для виконання лабораторної роботи скористатись віртуальною операційною системою.

Виконати налаштування базових політик безпеки.

За допомогою вбудованих політик IP-безпеки потрібно налаштувати доступ до окремих протоколів та портів передачі даних.

Налаштувати блокування всіх вхідних та вихідних з'єднань, крім HTTP (порт 80) та HTTPS (порт 443); налаштувати дозвіл на внутрішні з'єднання у мережі, але блокування зовнішніх з'єднань.

Створити правила для різних типів програм.

Налаштувати журналування всіх подій брандмауера для подальшого аналізу.

Налаштувати моніторинг мережевої активності для виявлення аномалій.

Оскільки, заборона дозволу для різних протоколів відбувається однотипним чином, то пропонується, для лабораторної роботи, використовувати протокол ICMP. Відповідно до виданого варіанту, вибирати діапазон IP-адрес для дозволу проходження пакетів протоколом ICMP, проходження пакетів із інших адрес повинно бути заборонено. Також у кожного діапазону є додаткова IP-адреса. Якщо вказана адреса входить до первинного діапазону, то потрібно додатково заборонити надходження запитів із вказаної адреси, якщо адреса не входить до вказаного діапазону, то, навпаки, дозволити доступ із додаткової IP-адреси.

Налаштувати мережевий адаптер віртуального комп'ютеру таким чином, щоб він входив до мережі 192.168.1.0/24.

№ варіанту	Діапазон для дозволу доступу	Додаткова адреса
1	192.168.1.0-192.168.1.63	192.168.1.150
2	192.168.1.64-192.168.1.127	192.168.1.151
3	192.168.1.128-192.168.1.191	192.168.1.152
4	192.168.1.192-192.168.1.255	192.168.1.153
5	192.168.1.0-192.168.1.63	192.168.1.154
6	192.168.1.64-192.168.1.127	192.168.1.155
7	192.168.1.128-192.168.1.191	192.168.1.156
8	192.168.1.192-192.168.1.255	192.168.1.157
9	192.168.1.0-192.168.1.63	192.168.1.158
10	192.168.1.64-192.168.1.127	192.168.1.159
11	192.168.1.128-192.168.1.191	192.168.1.160

№ варіанту	Діапазон для дозволу доступу	Додаткова адреса
12	192.168.1.192-192.168.1.255	192.168.1.161
13	192.168.1.0-192.168.1.63	192.168.1.162
14	192.168.1.64-192.168.1.127	192.168.1.163
15	192.168.1.128-192.168.1.191	192.168.1.164

Контрольні питання

1. Які існують типи мережевих екранів, чим вони відрізняються?
2. Яке призначення мережевого екрану, де він повинен бути встановлений?
3. Яке призначення протоколу ICMP?
4. Функціонування мережевого екрану із пакетною фільтрацією.
5. Основні принципи роботи мережевого екрану прикладного рівня.
6. Які наявні рішення мережевих екранів і яких компаній Ви можете назвати?
7. Яким чином здійснюється доступ до налаштувань IP-політик в операційній системі Windows?
8. Які переваги персональних мережевих екранів перед вбудованими IP-політиками ви можете назвати?
9. Які додаткові функціональні можливості мережеві фільтри можуть запропонувати користувачеві?
10. Які персональні мережеві екрани Ви можете назвати?
11. Яким чином можна здійснити розподіл мережі на підмережі за допомогою маски?
12. У якому випадку використання мережевого екрану буде неефективним?

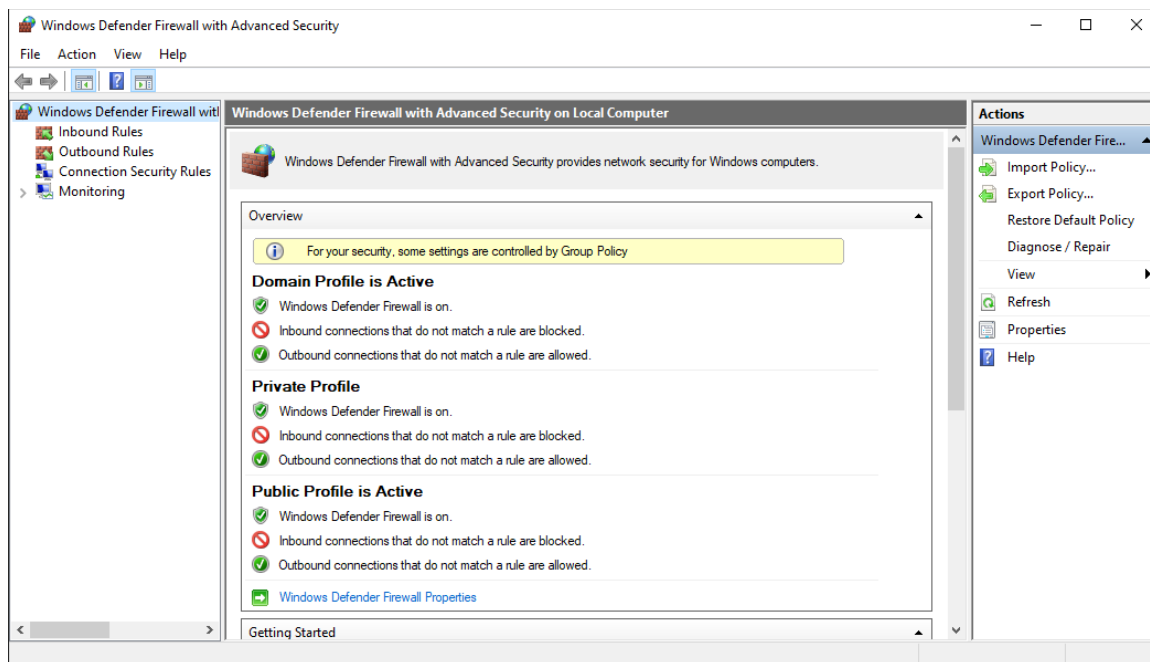
Теоретичні відомості для виконання лабораторної роботи

Захисник Windows Брандмауер у режимі підвищеної безпеки забезпечує двосторонню фільтрацію мережевого трафіку на основі вузла та блокує несанкціонований мережевий трафік, що надходить на локальний пристрій або з нього. Налаштування брандмауера Windows на основі наступних рекомендацій допоможе оптимізувати захист пристроїв у мережі. Ці рекомендації охоплюють широкий спектр розгортань, включаючи домашні мережі та корпоративні настільні та серверні системи.

Щоб відкрити брандмауер Windows, перейдіть до меню Пуск , виберіть Виконати, введіть WF.msc, а потім натисніть кнопку ОК.

Зберегти параметри за замовчуванням

Під час першого відкриття брандмауера Windows Defender ви побачите стандартні параметри, які застосовуються до локального комп'ютера. На панелі Огляд відображаються параметри безпеки для кожного типу мережі, до якої може підключатися пристрій.

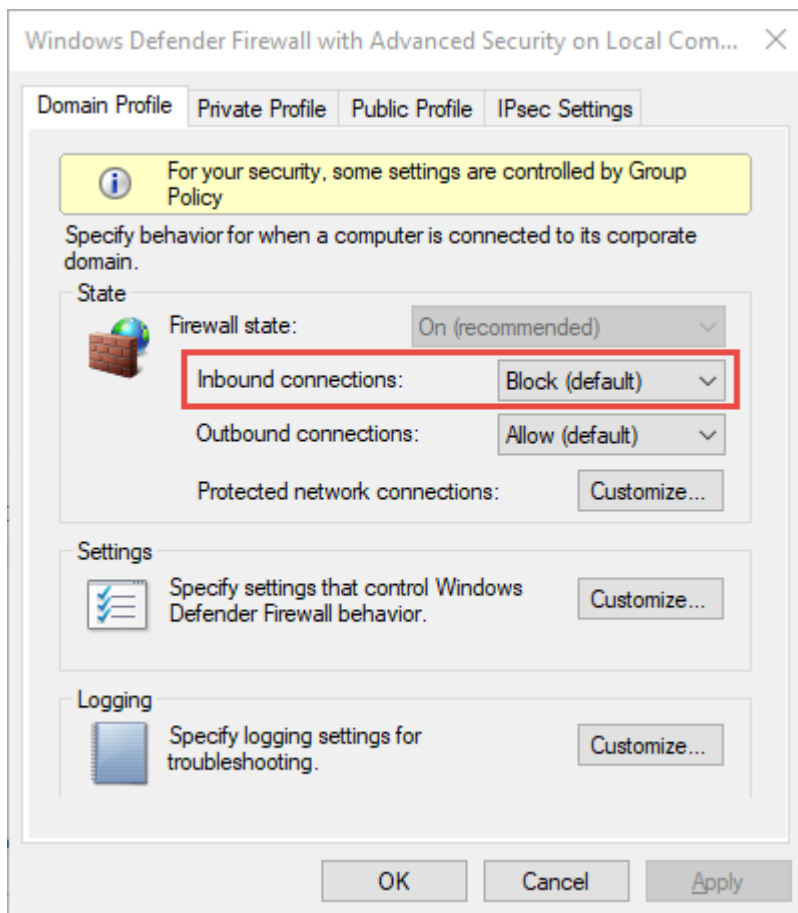


Мал. 1. Брандмауер Захисник Windows

1. **Профіль домену:** використовується для мереж, у яких є система автентифікації облікового запису на контролері домену Active Directory.
2. **Приватний профіль:** призначений та найкраще використовується у приватних мережах, таких як домашня мережа.
3. **Загальнодоступний профіль:** розроблено з урахуванням вищого рівня безпеки для загальнодоступних мереж, таких як Wi-Fi гарячі точки, кафе, аеропорти, готелі або магазини

Щоб переглянути докладні параметри для кожного профілю, клацніть правою кнопкою миші вузол Windows Defender Брандмауер у режимі підвищеної безпеки в лівій області та виберіть пункт Властивості.

За можливості зберігайте параметри за промовчанням у брандмауері Windows Defender. Ці параметри призначені для захисту пристрою для використання у більшості мережевих сценаріїв. Одним з ключових прикладів є поведінка стандартного блоку для вхідних підключень.



Мал. 2. Параметри вхідного та вихідного трафіку за замовчуванням

Важливо!

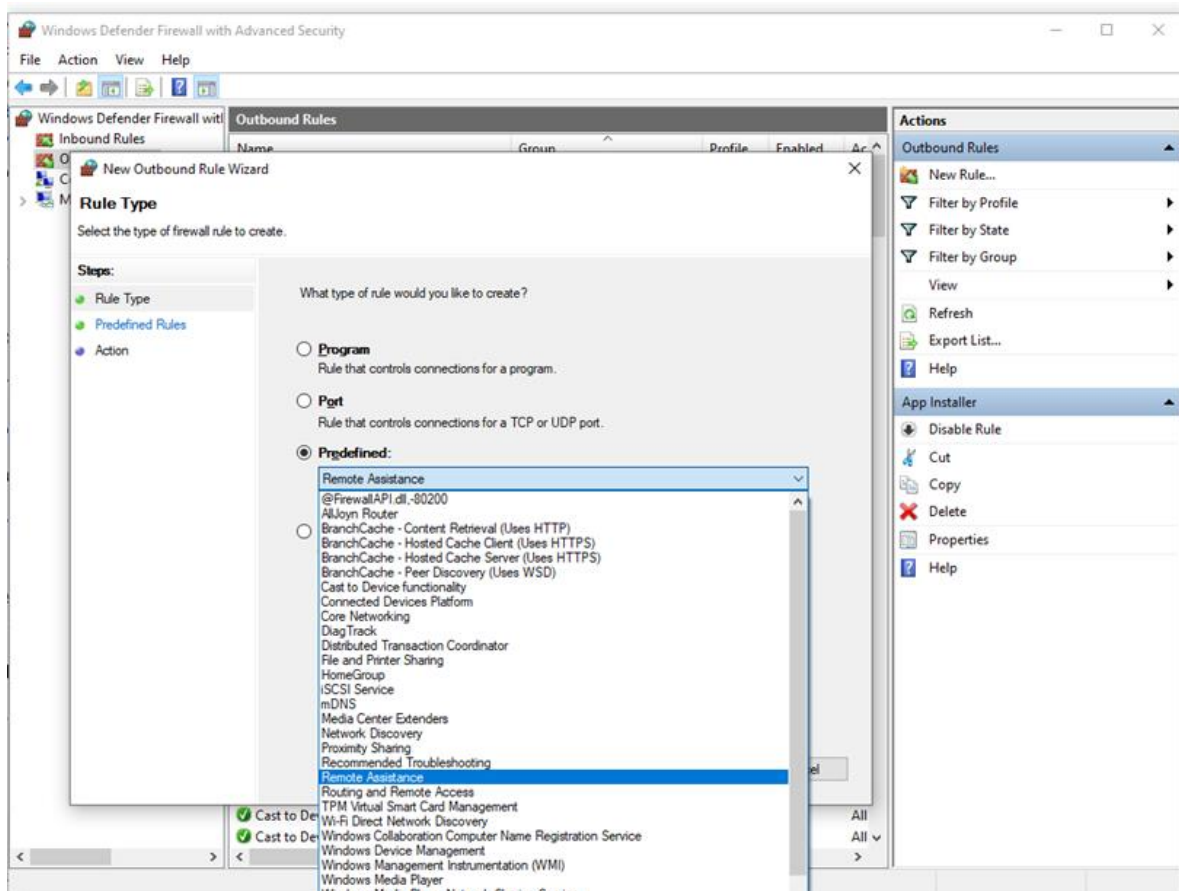
Щоб забезпечити максимальну безпеку, не змінюйте параметр блокування за промовчанням для вхідних підключень.

Загальні відомості про пріоритет правил для вхідних правил

У багатьох випадках наступним кроком для адміністраторів буде налаштування цих профілів за допомогою правил (іноді званих фільтрами), щоб вони могли працювати з програмами користувача або іншими типами програмного забезпечення. Наприклад, адміністратор або користувач може додати правило для розміщення програми, відкрити порт або протокол або дозволити певний тип трафіку.

Це завдання додавання правил можна виконати, клацнувши правою кнопкою миші правила для вхідного трафіку або Правила для вихідного

трафіку і вибравши Створити правило. Інтерфейс для додавання нового правила виглядає так:



Мал. 3. Майстер створення правил

У багатьох випадках для роботи програм у мережі потрібна роздільна здатність певних типів вхідного трафіку. Адміністратори повинні пам'ятати про таку поведінку пріоритету правил при вирішенні цих винятків.

1. Очевидно, певні правила дозволів матимуть пріоритет над параметром блоку за замовчуванням.
2. Явні правила блокування матимуть пріоритет над будь-якими правилами дозволу, що конфліктують.
3. Більш конкретні правила будуть мати пріоритет над менш конкретними правилами, за винятком випадків, коли існують явні блокові правила, як згадувалося в 2. (Наприклад, якщо параметри правила 1 включають діапазон IP-адрес, а параметри правила 2 включають одну IP-адресу вузла, правило 2 матиме пріоритет.)

Через значення 1 і 2 важливо переконатися, що при розробці набору політик ви переконаєтеся, що немає інших явних правил блокування, які могли б випадково перекриватися, тим самим запобігаючи потоку трафіку, який ви хочете дозволити.

Загальні рекомендації щодо безпеки при створенні правил для вхідного трафіку повинні бути якомога конкретнішими. Однак, якщо необхідно створити нові правила, що використовують порти або IP-адреси, розгляньте можливість використання послідовних діапазонів або підмереж замість окремих адрес або портів, де це можливо. Такий підхід дозволяє уникнути створення кількох фільтрів під капотом, знижує складність та допомагає уникнути зниження продуктивності.

Примітка

Брандмауер Захисник Windows не підтримує традиційне зважування правил адміністратора. Ефективний набір політик з очікуваною поведінкою можна створити, враховуючи кілька узгоджених та логічних правил, описаних вище.

Створення правил для нових програм перед першим запуском

Правила дозволу для вхідного трафіку

Під час першого встановлення мережні програми та служби виконують виклик прослуховування, вказуючи відомості про протокол або порт, необхідні для правильної роботи. Оскільки в брандмауері Windows Defender є дія блокування за промовчанням, необхідно створити правила для вхідних винятків, щоб дозволити цей трафік. Зазвичай програма або інсталятор додатків додають це правило брандмауера. В іншому випадку користувачу (або адміністратору брандмауера від імені користувача) необхідно створити вручну правило.

Якщо немає активних правил дозволів, визначених програмою або адміністратором, діалогове вікно запропонує користувачеві дозволити або заблокувати пакети програми при першому запуску програми або спробі взаємодіяти через мережу.

- Якщо користувач має дозволи адміністратора, буде запропоновано. Якщо вони відповідають ні або скасовують

запит, буде створено правила блокування. Зазвичай створюються два правила, по одному для трафіку TCP та UDP.

- Якщо користувач не є локальним адміністратором, він не запитуватиметься. У більшості випадків буде створено блокові правила.

У будь-якому з описаних вище сценаріїв, після додавання цих правил, вони повинні бути видалені, щоб знову створити запит. В іншому випадку трафік буде, як і раніше, заблокований.

Примітка

Параметри стандартного брандмауера призначені для забезпечення безпеки. Якщо дозволити всі вхідні підключення за промовчанням, мережа ознайомиться з різними загрозами. Тому створення винятків для вхідних підключень із стороннього програмного забезпечення має визначатися довіреними розробниками додатків, користувачем або адміністратором від імені користувача.

Відомі проблеми з автоматичним створенням правил

При розробці набору політик брандмауера для мережі рекомендується налаштувати правила дозволів для будь-яких мережних програм, розгорнутих на вузлі. Наявність цих правил до того, як користувач вперше запустить програму, допоможе забезпечити безпроблемну роботу.

Відсутність цих проміжних правил не обов'язково означає, що в кінцевому підсумку програма не зможе взаємодіяти через мережу. Однак поведінка, пов'язана з автоматичним створенням правил програми під час виконання, вимагає взаємодії з користувачем та прав адміністратора. Якщо очікується, що пристрій буде використовуватись користувачами без прав адміністратора, слід дотримуватися рекомендацій та надати ці правила перед першим запуском програми, щоб уникнути непередбачених проблем із мережею.

Щоб визначити, чому деякі програми заблоковані для обміну даними в мережі, перевірте наступні екземпляри:

1. Користувач із достатніми привілеями отримує повідомлення про запит про те, що додаток необхідно внести зміни до політики брандмауера. Не повністю розуміючи запит, користувач скасовує або відхиляє запит.

2. Користувач не має достатніх привілеїв, тому їй не пропонується дозволити додатку вносити відповідні зміни до політики.
3. Локальне злиття політик вимкнено, що не дозволяє програмі або мережній службі створювати локальні правила.

Створення правил програми під час виконання також може бути заборонено адміністраторами за допомогою програми "Параметри" або групова політика.



Мал. 4. Діалогове вікно для дозволу доступу

Створіть правила програми або служби для вхідного трафіку

Щоб дозволити вхідний мережевий трафік до зазначеної програми або служби, створіть правила брандмауера Windows Defender у оснащенні MMC керування групова політика. Цей тип правила дозволяє програмі прослуховувати та отримувати вхідний мережевий трафік на будь-якому порту.

Примітка: Цей тип правила часто узгоджується з правилом програми або служби. При об'єднанні типів правил ви отримаєте правило брандмауера, яке обмежує трафік вказаним портом і дозволяє трафік лише при запуску вказаної програми. Програма не може отримувати мережний трафік на інших портах, інші програми не можуть отримувати мережний трафік на вказаному порту.

Облікові дані адміністратора

Для цих процедур необхідно бути учасником групи адміністраторів домену або мати делеговані дозволи на зміну об'єктів групової політики.

Створення правила брандмауера для вхідного трафіку для програми чи служби

1. Відкрийте консоль управління груповою політикою у вузлі

Відкриття об'єкта групової політики у брандмауері Windows у режимі підвищеної безпеки

1. Відкрийте консоль управління групової політики.
2. У області навігації розгорніть вузол Forest:YourForestName, домени, YourDomainName, групова політика Об'єкти, клацніть правою кнопкою миші об'єкт групової політики, який потрібно змінити, і виберіть команду Змінити.
3. В області навігації редактора керування групова політика перейдіть до розділу Політики>конфігурації>комп'ютера Параметри>windows Параметри> безпекиБрандмауер Windows у режимі підвищеної безпеки>Брандмауер Windows у режимі підвищеної безпеки — LDAP://cn={GUID},cn=....
2. В області навігації натисніть Правила для вхідного трафіку.
3. Клацніть Дія, а потім Створити правило.
4. На сторінці Тип правила майстра створення правила для вхідного трафіку натисніть кнопку Користувач, а потім натисніть кнопку Далі.

Примітка: Хоча ви можете створити правила, вибравши Програма або Порт, ці параметри обмежують кількість сторінок, представлених майстром. Якщо вибрати Користувач, ви побачите всі сторінки і будете максимально гнучкими при створенні правил.

5. На сторінці Програма клацніть пункт Цей шлях до програми.
6. Введіть шлях до програми у текстовому полі. Використовуйте змінні середовища, якщо це застосовується, щоб забезпечити правильну роботу програм, встановлених у різних розташуваннях на різних комп'ютерах.
7. Виконайте одну з таких дій.
 - Якщо файл, що виконується, містить одну програму, натисніть кнопку Далі.
 - Якщо файл, що виконується, є контейнером для декількох служб, яким має бути дозволено отримувати вхідний мережевий трафік, натисніть кнопку Налаштувати, виберіть Застосувати тільки до служб, натисніть кнопку ОК і натисніть кнопку Далі.
 - Якщо файл, що виконується, є контейнером для однієї служби або містить кілька служб, але правило застосовується лише до однієї з них, натисніть кнопку Налаштувати, виберіть Застосувати до цієї служби, а потім виберіть службу зі списку. Якщо служба не відображається у списку, натисніть кнопку Застосувати до служби з цим коротким ім'ям служби та введіть коротке ім'я служби у текстовому полі. Натисніть кнопку ОК та натисніть кнопку Далі.

Важливо Щоб використовувати параметри Apply to this service (Застосувати до цієї служби) або Apply to service with this service short name (Застосувати до цієї служби), необхідно налаштувати службу з ідентифікатором безпеки (SID) з типом RESTRICTED або UNRESTRICTED. Щоб перевірити тип ідентифікатора служби безпеки, виконайте таку команду:

scqsidtype<ServiceName>

Якщо результат NONE, то правило брандмауера не може бути застосоване до цієї служби.

Щоб вказати тип ідентифікатора безпеки для служби, виконайте таку команду:

Scsidtype<ServiceName><Type>

У попередній команді значення <Type> може бути НЕОБМЕЖЕНЕ або RESTRICTED. Хоча команда також дозволяє значення NONE, цей параметр означає, що службу не можна використовувати у правилі брандмауера, як описано тут. За замовчуванням більшість служб Windows налаштовані як UNRESTRICTED. Якщо змінити тип ідентифікатора безпеки на RESTRICTED, служба може не запуститись. Рекомендовано змінити тип ідентифікатора безпеки лише для служб, які ви хочете використовувати у правилах брандмауера, та змінити тип ідентифікатора безпеки на UNRESTRICTED.

8. Рекомендується обмежити правило брандмауера для програми лише портами, які вона має працювати. На сторінці Протоколи та порти можна вказати номери портів для дозволеного трафіку. Якщо програма намагається прослуховувати порт, відмінний від зазначеного тут, блокується. Налаштування параметрів протоколу та порту натисніть кнопку Далі.
9. На сторінці Область можна вказати, що правило застосовується лише до мережевого трафіку до IP-адрес, зазначених на цій сторінці, або від неї. Налаштуйте відповідну конфігурацію та натисніть кнопку Далі.
10. На сторінці Дія виберіть Дозволити з'єднання та натисніть кнопку Далі.
11. На сторінці Профіль виберіть типи мережевих положень, до яких застосовується це правило, і натисніть кнопку Далі.
12. На сторінці Ім'я введіть ім'я та опис правила, а потім натисніть кнопку Готово.

Створення правила порту для вхідного трафіку

Щоб дозволити вхідний мережевий трафік лише за вказаним номером порту TCP або UDP, використовуйте вузол Брандмауер Windows Defender у режимі підвищеної безпеки у оснащенні MMC "Управління групова політика" для створення правил брандмауера. Цей тип правила дозволяє будь-якій програмі, яка прослуховує зазначений порт TCP або UDP, отримувати мережевий трафік, що надсилається на цей порт.

Облікові дані адміністратора

Для цих процедур необхідно бути учасником групи адміністраторів домену або мати делеговані дозволи на зміну об'єктів групової політики.

Створення правила вхідного порту

1. Відкрийте консоль управління груповою політикою у вузлі
2. В області навігації натисніть Правила для вхідного трафіку.
3. Клацніть Дія, а потім Створити правило.
4. На сторінці Тип правила майстра створення правила для вхідного трафіку натисніть кнопку Користувач, а потім натисніть кнопку Далі.

Примітка

Хоча ви можете створити правила, вибравши Програма або Порт, ці параметри обмежують кількість сторінок, представлених майстром. Якщо вибрати Користувач, ви побачите всі сторінки і будете максимально гнучкими при створенні правил.

5. На сторінці Програма клацніть Усі програми, а потім натисніть кнопку Далі.

Примітка

Цей тип правила часто узгоджується з правилом програми або служби. При об'єднанні типів правил ви отримаєте правило брандмауера, яке обмежує трафік вказаним портом і дозволяє трафік лише при запуску вказаної програми. Зазначена програма не може отримувати мережний трафік на інших портах, а інші програми не можуть отримувати мережний трафік на вказаному порту.

На сторінці Протокол і порти виберіть тип протоколу, який Ви бажаєте дозволити. Щоб обмежити правило вказаним номером порту, потрібно вибрати TCP або UDP. Так як це вхідне правило зазвичай налаштовується тільки номер локального порту.

При виборі іншого протоколу через брандмауер дозволено лише ті пакети, поле протоколу яких у заголовку IP-адрес відповідає цьому правилу.

Щоб вибрати протокол за його номером, виберіть у списку Користувач, а потім введіть номер у полі Номер протоколу.

Налаштувавши протоколи та порти, натисніть кнопку Далі.

6. На сторінці Область можна вказати, що правило застосовується лише до мережевого трафіку до IP-адрес, зазначених на цій сторінці, або від неї. Налаштуйте відповідну конфігурацію та натисніть кнопку Далі.
7. На сторінці Дія виберіть Дозволити з'єднання та натисніть кнопку Далі.
8. На сторінці Профіль виберіть типи мережевих положень, до яких застосовується це правило, і натисніть кнопку Далі.

Примітка

Якщо цей об'єкт групової політики призначений для серверних комп'ютерів під керуванням Windows Server 2008, які ніколи не переміщуються, спробуйте змінити правила, щоб вони застосовувалися до всіх профілів типів мережевих розташування. Це запобігає непередбаченим змінам застосовуваних правил, якщо тип мережного розташування змінюється через встановлення нового мережного картку або відключення існуючого мережного картку кабелю. Вимкнена мережна картка автоматично призначається типу розташування загальнодоступної мережі.

9. На сторінці Ім'я введіть ім'я та опис правила, а потім натисніть кнопку Готово.

Увімкнення стандартних правил для вхідного трафіку

Брандмауер Windows Defender в режимі підвищеної безпеки включає безліч визначених правил для загальних мережевих ролей і функцій. При встановленні нової ролі сервера на пристрої або увімкнення функції мережі на клієнтському пристрої установник зазвичай включає правила, необхідні для цієї ролі, а не створює нові. При розгортанні правил брандмауера на пристроях у мережі можна скористатися перевагами цих визначених правил, а не створювати нові. Використання цієї переваги допомагає забезпечити узгодженість та точність, оскільки правила були ретельно протестовані та готові до використання.

Облікові дані адміністратора

Для цих процедур необхідно бути учасником групи адміністраторів домену або мати делеговані дозволи на зміну об'єктів групової політики.

Розгортання визначених правил брандмауера, які дозволяють вхідний мережевий трафік для загальних мережевих функцій

1. Відкрийте консоль управління груповою політикою у вузлі
2. В області навігації натисніть Правила для вхідного трафіку.
3. Клацніть Дія, а потім Створити правило.
4. На сторінці Тип правила майстра створення правила для вхідного трафіку клацніть Вибрані, виберіть категорію правил у списку та натисніть кнопку Далі.
5. На сторінці Передбачені правила відображається список правил, визначених у групі. За замовчуванням усі вони вибрані. Для правил, які не потрібно розгортати, зніміть прапорці перевірки поруч із правилами і натисніть кнопку Далі.
6. На сторінці Дія виберіть Дозволити з'єднання та натисніть Готово.

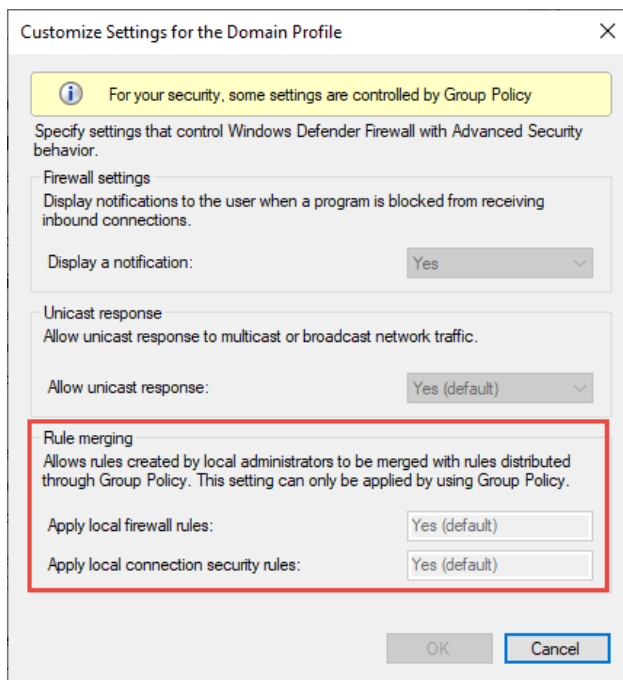
Встановлення правил злиття локальних політик та додатків

Можна розгорнути правила брандмауера:

1. Локальне використання оснастки брандмауера (WF.msc)
2. Локально за допомогою PowerShell
3. Віддалене використання групової політики, якщо пристрій є членом імені Active Directory, System Center Configuration Manager або Intune (при підключенні до робочого місця)

Параметри злиття правил управляють способом поєднання правил із різних джерел політик. Адміністратори можуть налаштовувати різні варіанти поведінки злиття для доменних, приватних та загальнодоступних профілів.

Параметри злиття правил дозволяють або забороняють локальним адміністраторам створювати власні правила брандмауера на додаток до правил, отриманих з групової політики.



Мал. 5. Параметр злиття правил

Порада

У постачальника служби конфігурації брандмауера еквівалентним параметром є AllowLocalPolicyMerge. Цей параметр можна знайти у кожному відповідному вузлі профілю, DomainProfile, PrivateProfile та PublicProfile.

Якщо з'єднання локальних політик відключено, для будь-якої програми, якій потрібне підключення, потрібне централізоване розгортання правил.

Адміністратори можуть відключити LocalPolicyMerge у середовищах з високим рівнем безпеки, щоб забезпечити суворіший контроль над кінцевими точками. Цей параметр може вплинути на деякі програми та служби, які автоматично створюють локальну політику брандмауера після встановлення, як описано вище. Щоб ці типи програм та служб працювали, адміністратори повинні централізовано надсилати правила за допомогою групової політики (GP), мобільного Управління пристроями (MDM) або обох (для гібридних середовищ або середовищ спільного керування).

Брандмауер CSP та CSP політики також мають параметри, які можуть вплинути на злиття правил.

Рекомендується виводити список та реєструвати такі програми, включаючи мережні порти, які використовуються для обміну даними. Як правило, на веб-сайті програми можна знайти порти, які мають бути відкриті для цієї

служби. Для більш складних розгортань або розгортань клієнтських додатків може знадобитися ретельніший аналіз за допомогою засобів збору мережних пакетів.

Як правило, для забезпечення максимальної безпеки адміністратори повинні надсилати виключення брандмауера лише для додатків та служб, які налаштовані на законні цілі.

Примітка

Використання шаблонів з знаками підстановки, таких як `C:\teams.exe`, не підтримується в правилах додатків. В даний час підтримуються лише правила, створені за допомогою повного шляху до додатків.

Створення правила ICMP для вхідного трафіку

Щоб дозволити вхідний мережний трафік ICMP, використовуйте вузол Брандмауер Windows Defender з підвищеною безпекою в оснащенні MMC управління групова політика, щоб створити правила брандмауера. Цей тип правила дозволяє надсилати та отримувати запити та відповіді ICMP комп'ютерами в мережі.

Створення правила ICMP для вхідного трафіку

1. Відкрийте консоль управління груповою політикою у вузлі Брандмауер Windows Defender у режимі підвищеної безпеки.
2. В області навігації натисніть Правила для вхідного трафіку.
3. Клацніть Дія, а потім Створити правило.
4. На сторінці Тип правила майстра створення правила для вхідного трафіку натисніть кнопку Користувач, а потім натисніть кнопку Далі.
5. На сторінці Програма клацніть Усі програми, а потім натисніть кнопку Далі.
6. На сторінці Протокол і порти виберіть ICMPv4 або ICMPv6 у списку Тип протоколу. Якщо в мережі використовуються протоколи IPv4 та IPv6, необхідно створити окреме правило ICMP для кожного з них.
7. Натисніть кнопку Налаштувати.

8. У діалоговому вікні Налаштування параметрів ICMP виконайте одну з таких дій.
 - Щоб дозволити весь мережний трафік ICMP, клацніть Усі типи ICMP і натисніть кнопку ОК.
 - Щоб вибрати один із стандартних типів ICMP, клацніть Визначені типи ICMP, а потім виберіть кожний тип зі списку, який ви хочете дозволити. Натисніть кнопку ОК.
 - Щоб вибрати тип ICMP, який не відображається у списку, клацніть Визначені типи ICMP, виберіть у списку номер типу , у списку виберіть номер коду , натисніть кнопку Додати, а потім виберіть щойно створений запис зі списку. Натисніть ОК
9. Натисніть кнопку "Далі".
10. На сторінці Область можна вказати, що правило застосовується лише до мережевого трафіку до IP-адрес, зазначених на цій сторінці, або від неї. Налаштуйте відповідну конфігурацію та натисніть кнопку Далі.
11. На сторінці Дія виберіть Дозволити з'єднання та натисніть кнопку Далі.
12. На сторінці Профіль виберіть типи мережевих положень, до яких застосовується це правило, і натисніть кнопку Далі.
13. На сторінці Ім'я введіть ім'я та опис правила, а потім натисніть кнопку Готово.

Загальні відомості про обробку групова політика

Параметри брандмауера Windows, налаштовані за допомогою групової політики, зберігаються у реєстрі. За промовчанням групові політики оновлюються у фоновому режимі кожні 90 хвилин із випадковим усуненням від 0 до 30 хвилин.

Брандмауер Windows відстежує зміни в реєстрі, і якщо щось записується до реєстру, він повідомляє платформу фільтрації Windows (ЗПС), яка виконує такі дії:

- Читання всіх правил та параметрів брандмауера
- Застосування нових фільтрів
- Видаляє старі фільтри

Примітка

Дії активуються щоразу, коли щось записується або видаляється з реєстру, де зберігаються параметри об'єкта групової політики, незалежно від того, чи справді відбулася зміна конфігурації. Під час процесу підключення за протоколом IPsec вимикаються.

Багато реалізації політики вказують, що вони оновлюються лише за зміни. Однак вам може знадобитися оновити без змін політики, наприклад, повторно застосувати потрібний параметр політики, якщо користувач змінив його. Для управління поведінкою групової політики реєстру можна використовувати політику Computer Configuration > Administrative Templates > System > Group Policy > Configure registry policy processing. Процес, навіть якщо об'єкти групової політики не змінилися, оновлює параметри і повторно застосовує політики, навіть якщо політики не змінилися. Цей параметр вимкнено за замовчуванням.

Якщо увімкнути параметр Обробити, навіть якщо об'єкти групова політика не змінилися, фільтри ЗПС будуть повторно застосовані при кожному фоновому оновленні. Якщо у вас є десять групових політик, фільтри ЗПС будуть повторно застосовані десять разів протягом інтервалу оновлення. Якщо під час обробки політики виникає помилка, застосовані параметри можуть бути неповними, що призводить до таких проблем:

- брандмауер Захисник Windows блокує вхідний або вихідний трафік, дозволений груповими політиками
- Параметри локального брандмауера застосовуються замість параметрів групової політики
- Неможливо встановити підключення IPsec

Тимчасовим рішенням є оновлення параметрів групової політики за допомогою команди `gpupdate.exe /force`, яка потребує підключення до контролера домену.

Щоб уникнути цієї проблеми, залиште політику Computer Configuration > Administrative Templates > System > Group Policy > Configure registry policy processing за промовчанням Не налаштовано або, якщо вона вже налаштована, налаштуйте її значення Вимкнено.

Важливо!

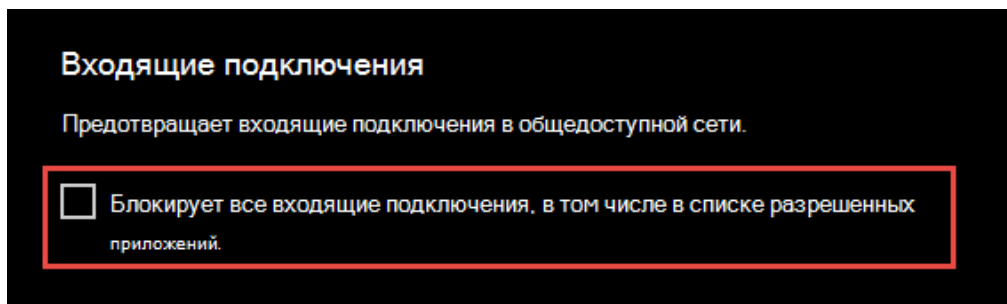
Прапорець поруч із полем Обробка, навіть якщо об'єкти групова політика не змінилися, має бути знято. Якщо цей прапорець не встановлено, фільтри МПП записуються лише у разі зміни конфігурації.

Якщо потрібно примусове видалення та перезапис реєстру, вимкніть фонову обробку, встановивши прапорець Не застосовувати під час періодичної фонові обробки.

Використання режиму "екранування вгору" для активних атак

Важливою функцією брандмауера, яка може бути використана для усунення збитків під час активної атаки, є режим "екранування вгору". Це неофіційний термін, що означає простий метод, який адміністратор брандмауера може використовувати для тимчасового підвищення безпеки перед активною атакою.


Екранування можна досягти, встановивши прапорець Блокувати всі вхідні з'єднання, у тому числі у списку дозволених програм, який знаходиться у програмі "Параметри Windows" або у файлі попередніх версій firewall.cpl.




Мал. 6. Параметри Windows App/Безпека Windows/Firewall Protection/Network Type

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.


 For your security, some settings are managed by your system administrator.

Domain network settings


 ☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app


 ☐ Turn off Windows Defender Firewall (not recommended)

Private network settings


 ☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app


 ☐ Turn off Windows Defender Firewall (not recommended)

Public network settings

 ☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app

 ☐ Turn off Windows Defender Firewall (not recommended)

Мал. 7. Застаріла *firewall.cpl*

За промовчанням брандмауер Windows Defender блокує все, якщо не створено правило виключення. Цей параметр перевизначає винятки.

Наприклад, функція віддаленого робочого столу автоматично створює правила брандмауера під час увімкнення. Однак за наявності активного експлойта з використанням кількох портів і служб на вузлі можна замість відключення окремих правил використовувати режим екранування для блокування всіх вхідних підключень, перевизначаючи попередні винятки, включаючи правила віддаленого робочого столу. Правила віддаленого робочого столу залишаються недоторканими, але віддалений доступ не працюватиме, доки активовані екрани.

Після аварійної ситуації зніміть прапорець, щоб відновити звичайний мережевий трафік.

Створення правил для вихідного трафіку

Нижче наведено кілька загальних рекомендацій щодо налаштування правил для вихідного трафіку.

- Стандартна конфігурація заблокована для правил вихідного трафіку може розглядатися для деяких середовищ з високим рівнем безпеки. Однак, конфігурацію правила для вхідного трафіку ніколи не слід змінювати таким чином, щоб дозволити трафік за замовчуванням.
- Рекомендується дозволити вихідний трафік за замовчуванням для більшості розгортань, щоб спростити розгортання додатків, якщо тільки підприємство не віддає перевагу суворим засобам управління безпекою, ніж простоті використання.
- У середовищі з високим рівнем безпеки адміністратор або адміністратори повинні виконувати інвентаризацію всіх корпоративних додатків та реєструвати їх у журналі. Записи повинні вказувати, чи потрібне мережеве підключення, що використовується. Адміністраторам потрібно створити нові правила, що стосуються кожної програми, якій потрібне мережеве підключення, і надсилати ці правила централізовано за допомогою групової політики (GP), мобільного Управління пристроями (MDM) або обох (для гібридних середовищ або середовищ спільного керування).

Документування змін

При створенні правила для вхідного або вихідного трафіку слід вказати відомості про саму програму, що використовується діапазон портів і важливі нотатки, такі як дата створення. Правила повинні бути добре документовані для зручності перевірки, як вами, так і іншими адміністраторами. Ми настійно рекомендуємо приділити час, щоб спростити роботу з перевірки правил брандмауера на пізнішому етапі. І ніколи не створюйте непотрібні дірки у брандмауері.

Налаштування правил брандмауера Windows за допомогою політик тегів WDAC

Брандмауер Windows тепер підтримує використання тегів ідентифікатора програми (AppID) Захисник Windows керування програмами (WDAC) у правилах брандмауера. За допомогою цієї можливості правила брандмауера Windows тепер можуть бути обмежені програмою або групою програм шляхом посилення на теги процесів, не використовуючи абсолютний шлях або не жертвуючи безпекою. Для цієї конфігурації потрібно виконати два кроки.

Крок 1. Розгортання політик тегів AppId WDAC

Необхідно розгорнути політику керування програмами Windows Defender (WDAC), яка вказує окремі програми або групи програм для застосування тега PolicyAppId до маркерів процесу. Потім адміністратор може визначити правила брандмауера, які відносяться до всіх процесів, помічених відповідним PolicyAppId.

Крок 2. Налаштування правил брандмауера за допомогою тегів PolicyAppId

- **Розгортання правил брандмауера за допомогою Intune:** При створенні правил брандмауера за допомогою правил брандмауера Intune Microsoft Defender вкажіть тег AppId у параметрі Ідентифікатор програми політики. Властивості надходять безпосередньо від постачальника служби конфігурації брандмауера (CSP) та застосовуються до платформи Windows. Це можна зробити за допомогою Центру адміністрування Intune у розділі Брандмауер безпеки кінцевих точок. Шаблони політик можна знайти в розділі Створення > Windows 10, Windows 11 і Windows Server > Microsoft Defender брандмауера або правил брандмауера Microsoft Defender.

АБО

- **Створення правил локального брандмауера за допомогою PowerShell.** Для налаштування можна використовувати PowerShell, додавши правило брандмауера за допомогою команди New-NetFirewallRule і вказавши –PolicyAppId тег. Під час створення правил брандмауера можна вказати по одному тегу. Підтримується декілька ідентифікаторів користувачів.