Мережева безпека

Захист периметра

Перелік тем

- Два критерії фільтрації.
- Основи створення ACL.
- Істинна та хибна фільтрація.
- Впорядкування правил у поданні на діаграмах Венна.
- Приклади ACL (для лабораторної PT-ACL).
- Що таке периметр і де він проходить?
- Деякі «особливі» проблеми периметра.
- Варіанти DMZ.
- Комбінація фільтрів і VPN.
- Роздільне тунелювання.

Два критерії фільтрації

1. Вочевидь, блокуємо всі відомі _____ _____.

2. Але блокуємо також і _____ _____.

Основи створення ACL

- За допомогою списків контролю доступу (Access Control Lists, ACL) маршрутизатори можуть виконувати функції фільтрування та міжмережевого екрана.
- Конфігурування ACL є 2-етапним процесом:
  - створюємо список правил фільтрації (т. зв. «*набір правил*»);
  - застосовуємо цей список до інтерфейсу.
- ACL застосовується або до вхідного, або до вихідного трафіка (або ж до обох напрямків «вхід/вихід»).
- На одному інтерфейсі для кожного напрямку може бути застосований тільки один ACL.

Основи створення ACL

- **ACL тестують згори вниз:**
  - **виконується перший збіг (дозвіл або заборона);**
  - **в кінці списку є неявне правило «_____» (приховане);**
  - **впорядкування правил важливе:**
    - **з міркувань ефективності правила, збіги з якими трапляються найчастіше, слід розташовувати повище, проте, це не так важливо, як міркування безпеки;**
    - **з міркувань безпеки слід пересвідчуватися, що впорядкований набір правил дозволу та заборони не зумовлюватиме хибних спрацювань.**

Істина та хиба

- **Хибні спрацювання фільтрів:**
  - **Припустимо, що пакет містить і поганий елемент B, і хороший елемент G, а ACL виглядає так:**

    дозволити G

    заборонити B

    <далі можуть бути інші правила>
  - **Яким буде результат?**
    - **Відповідь: Станеться хибно-_____ спрацювання.**

Істина та хиба

- **Хибні спрацювання фільтрів:**
  - **Припустимо, що потрібно заборонити весь вхідний трафік, який надходить до внутрішньої мережі (поганий елемент B), якщо це не VPN-трафік (хороший елемент G), а ACL виглядає так:**

    заборонити B

    дозволити G

    <далі можуть бути інші правила>
  - **Яка хиба може статися в результаті?**
    - **Відповідь: Станеться хибно-_____ спрацювання.**

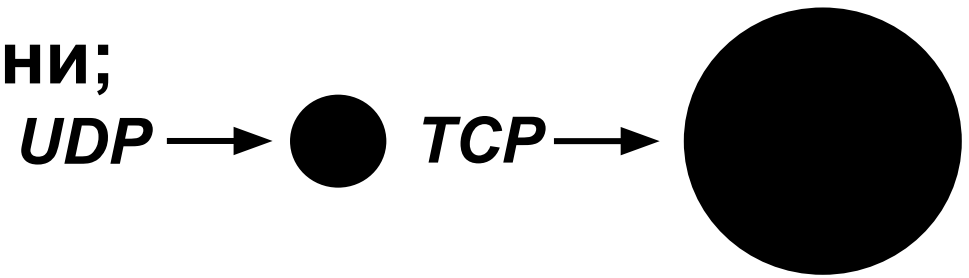
Істина та хиба

- Взагалі хотілося б не мати жодних хибних спрацювань.
- Інакше кажучи, потрібні тільки істинні.
- Розглянемо такі варіанти:
  - хибно-позитивне:
    - (мало/не мало) б відфільтруватися, але так (сталося/не сталося);
  - хибно-негативне:
    - (мало/не мало) б відфільтруватися, але так (сталося/не сталося);
  - істинно-позитивне:
    - (мало/не мало) б відфільтруватися, але так (сталося/не сталося);
  - істинно-негативне:
    - (мало/не мало) б відфільтруватися, але так (сталося/не сталося).

Візуалізація фільтрів за допомогою діаграм Венна (0)

- На подальших слайдах:
  - кола представляють трафік, який відповідає зазначеним критеріям;
  - розміри кіл є відносними ілюстраціями відсотка всього трафіка, який відповідає зазначеним критеріям;
  - чорне коло правила заборони;
  - біле коло правила дозволу.

Наприклад:

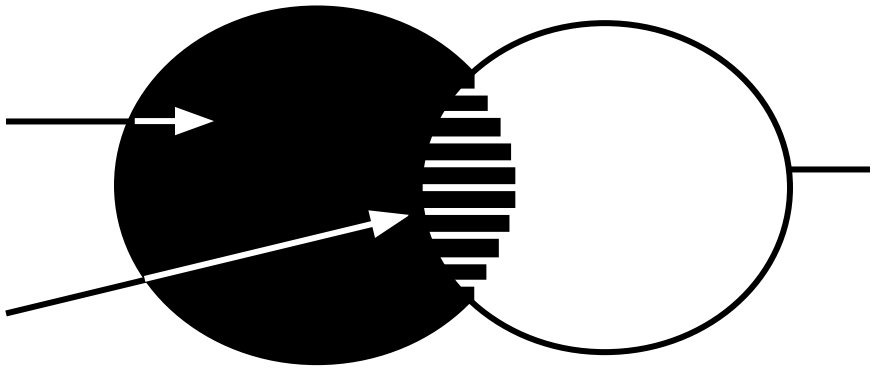


Впорядкування правил

Перетин правил дозволу та заборони означає, що потрібно звернутися до політики, щоб забезпечити належне впорядкування правил.

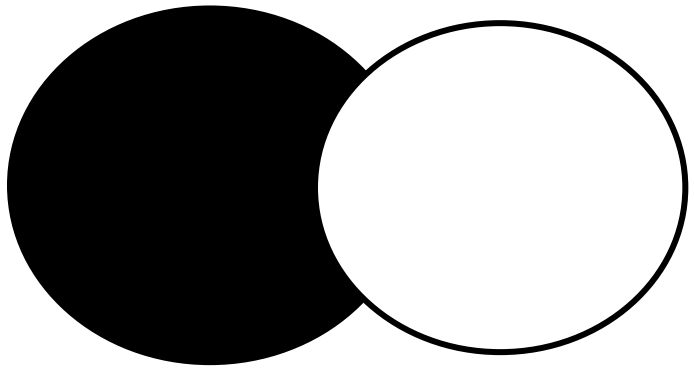
Заборонити весь SNMP-трафік

Конфлікт повинен бути розв'язаний



Дозволити весь трафік від SysAdmin за адресою A.B.C.S

Це, ймовірно, і був намір особи, яка складала політику



Тож, яке правило повинне виконуватися першим?

Візуалізація фільтрів за допомогою діаграм Венна (1)

Якщо фільтрації немає, то, вочевидь, не виконуються безпекові _____!

Тобто не вживається загально відомих та визнаних безпекових практик.

Візуалізація фільтрів за допомогою діаграм Венна (2)

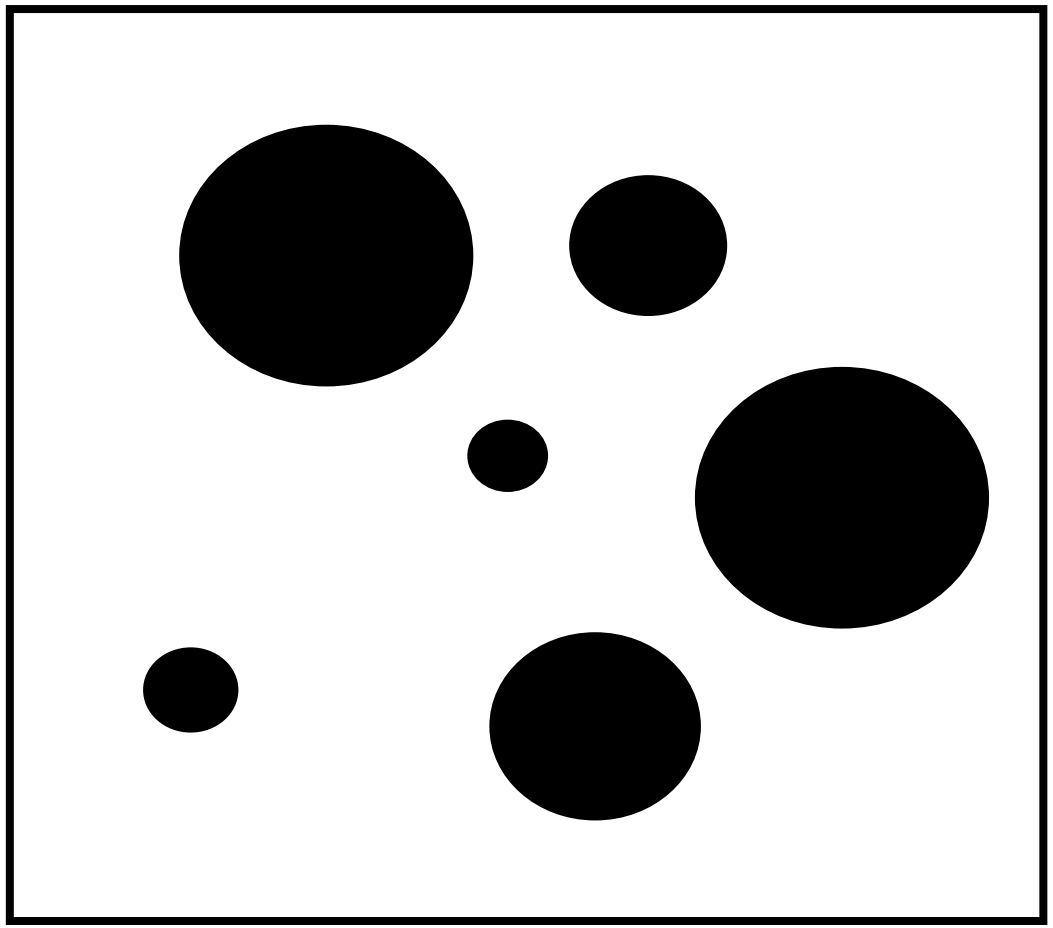
Додавання правил заборони мірою виявлення потреби в них, часто вже після інциденту, є застарілим і розвінчаним підходом

«_____

і

_____»

до безпеки.



Візуалізація фільтрів за допомогою діаграм Венна (3)

Ліпше всього почати зі стандартної відправної точки «заборонити все».

Це буде стратегією фільтрування, яка найліпше відповідає принципу

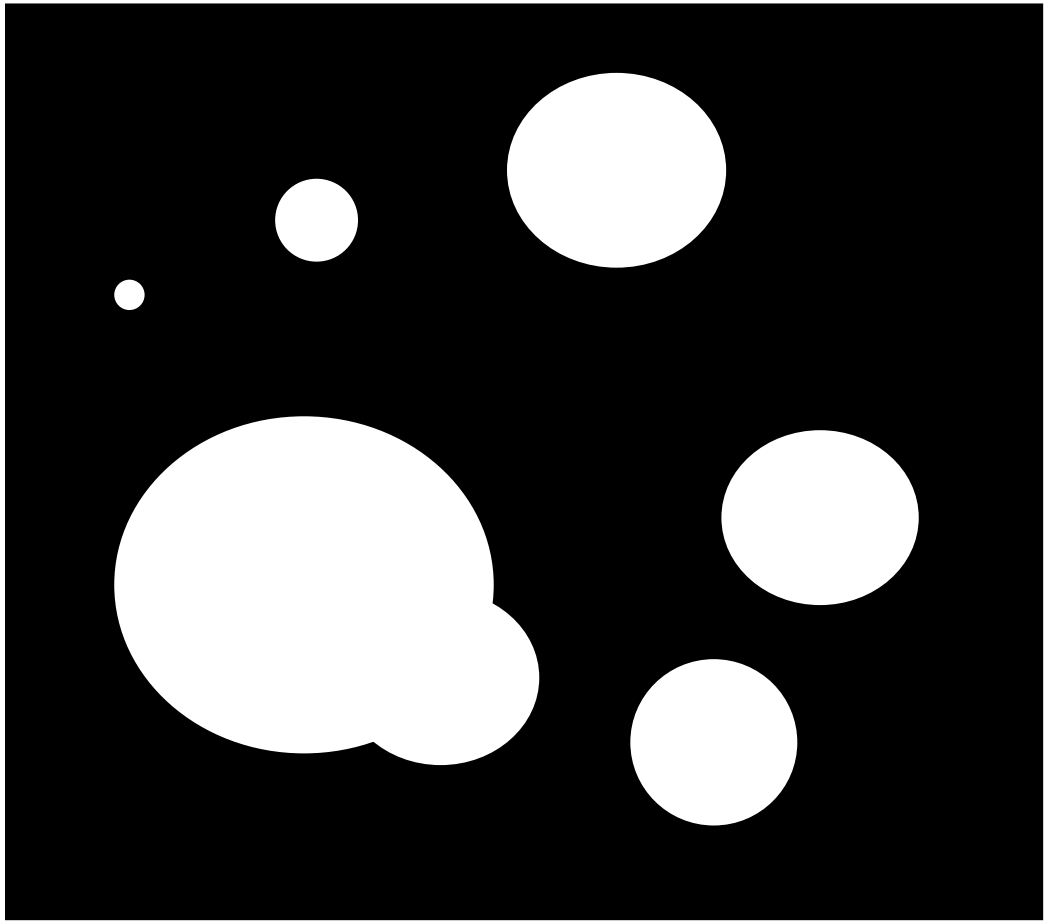
_____

_____.

Візуалізація фільтрів за допомогою діаграм Венна (4)

Виходячи з «заборонити все», додамо дозволи для трафіка, який, вочевидь, буде необхідний для певного бізнесу чи завдання.

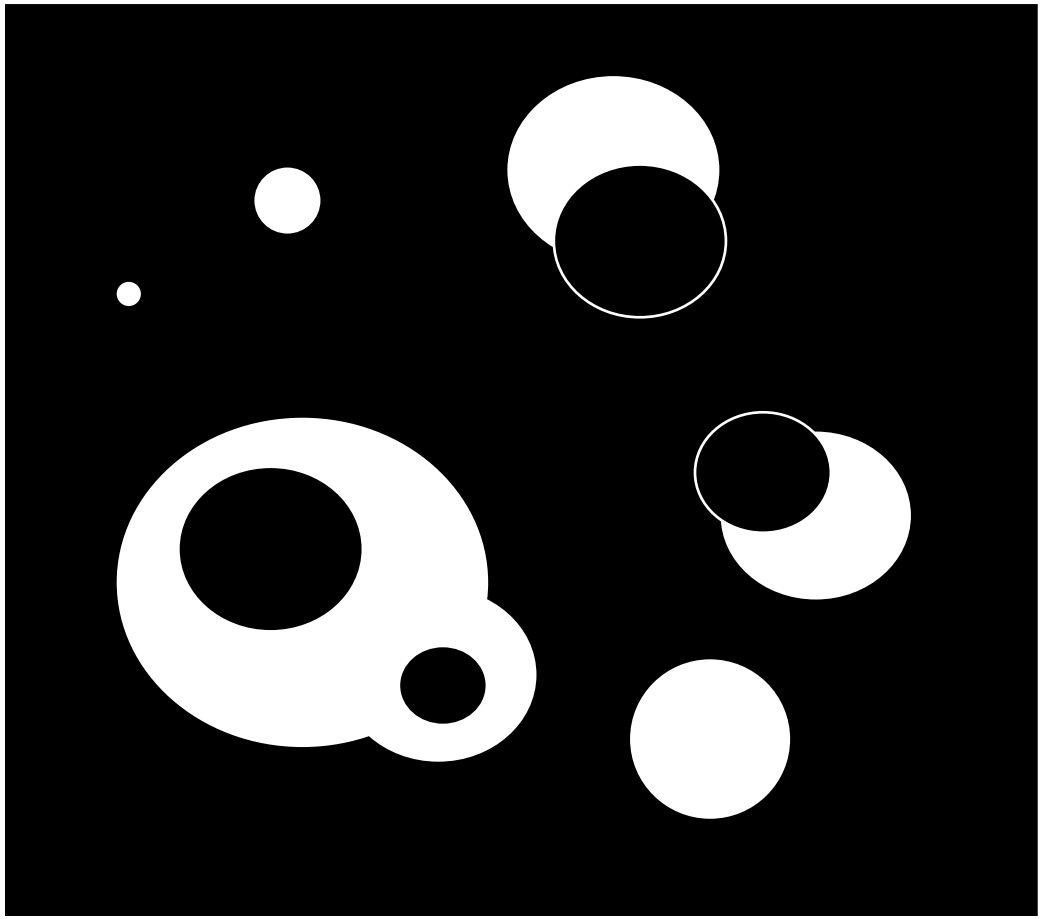
Узагальнено це називають _____.



Візуалізація фільтрів за допомогою діаграм Венна (5)

Додамо правила заборони, потрібні для протидії відомим векторам атак, які можуть накладатися на правила дозволу.

Узагальнено це називають _____.

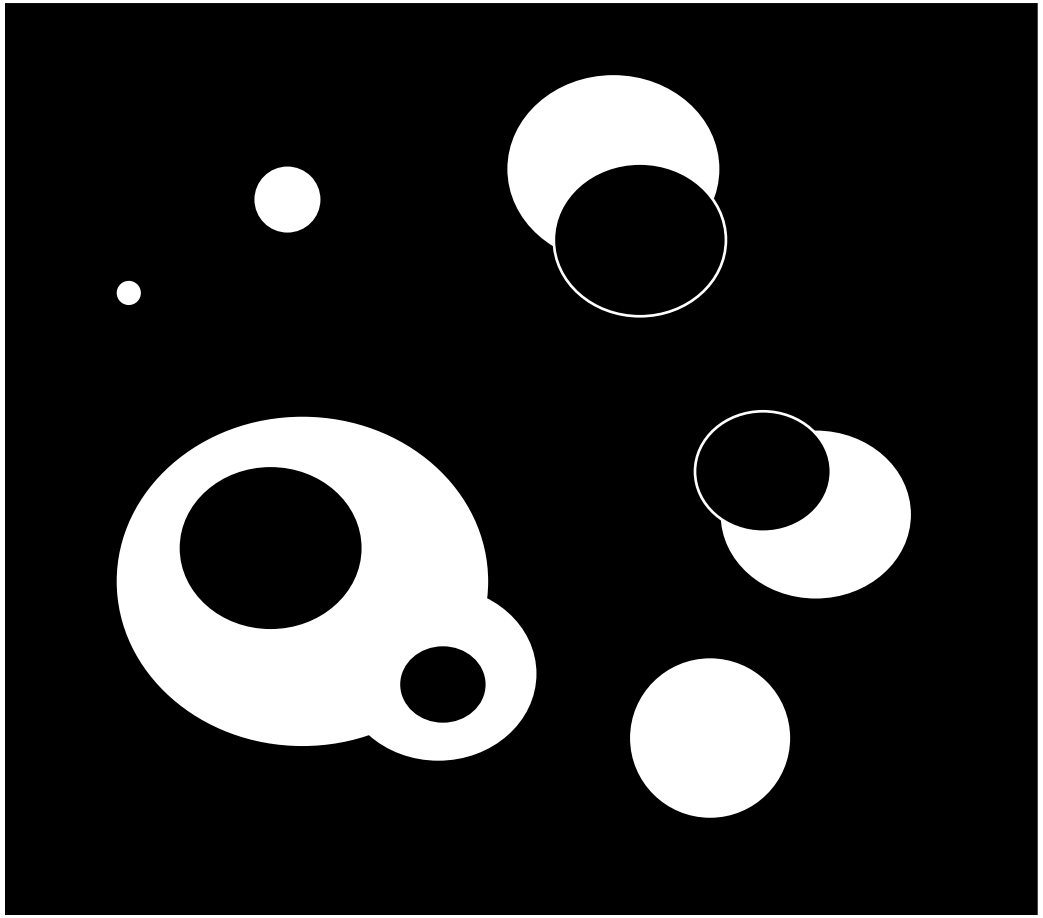


Візуалізація фільтрів за допомогою діаграм Венна (6)

Варто зазначити, що цей приклад побудований графічно ззаду наперед.

На практиці його б побудували текстово згори вниз, тобто:

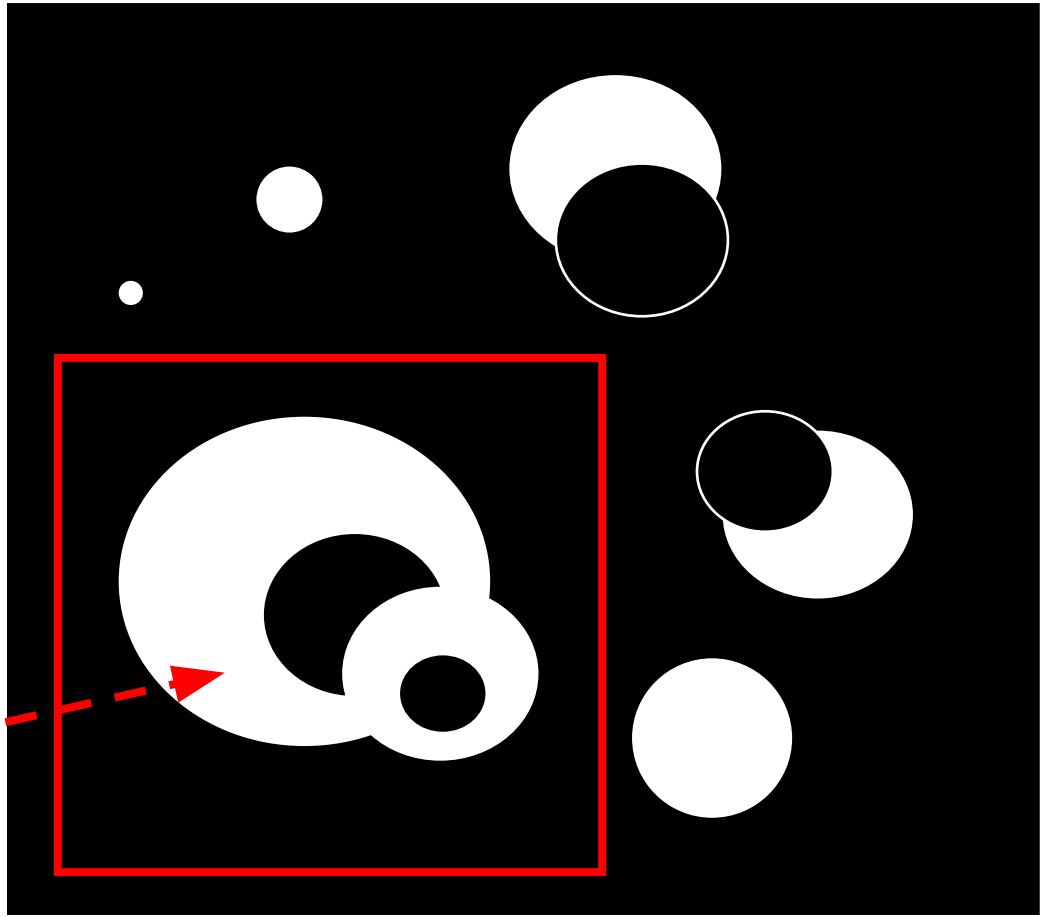
1. **перелічили б усі заборони, тоді**
2. **перелічили б усі дозволи, тоді**
3. **заборонили б усе (неявно).**



Візуалізація фільтрів за допомогою діаграм Венна (7)

Варто зауважити, що попередній приклад доволі простий: *всі* заборони йдуть перед *всіма* дозволами.

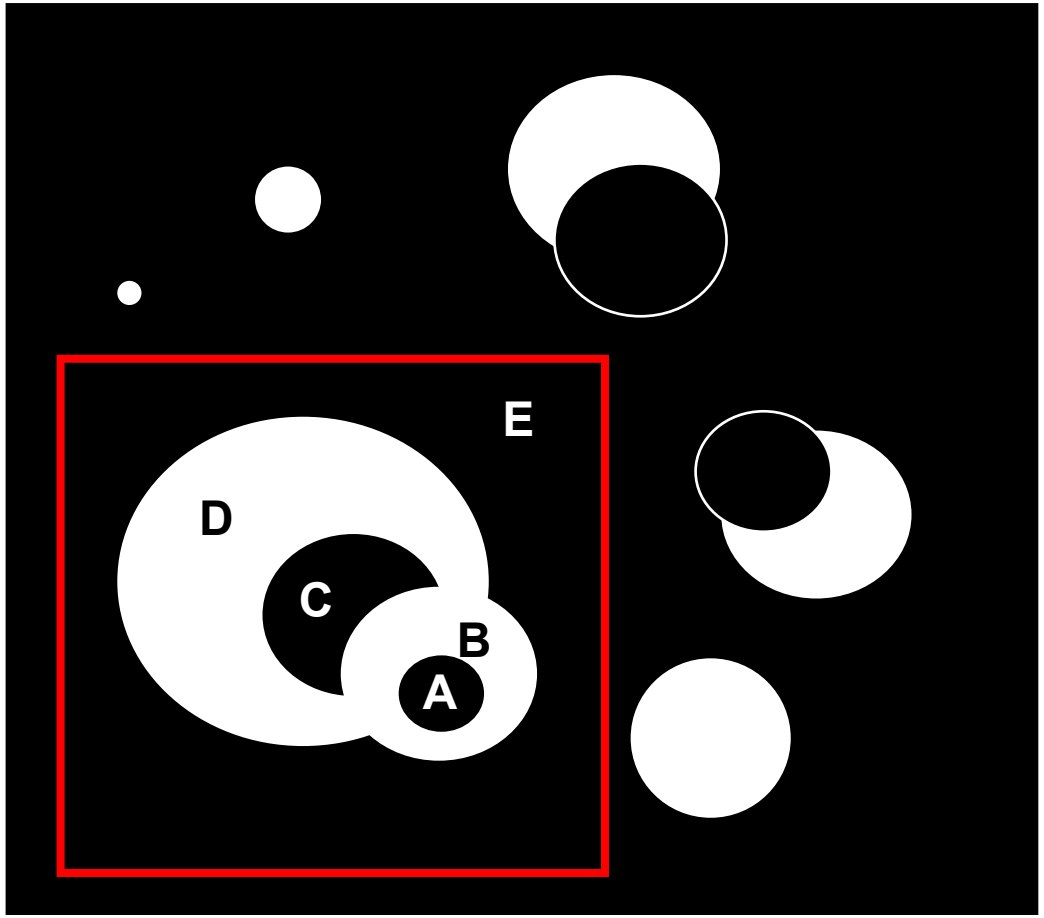
Однак може бути так, що все ускладниться додатковими міркуваннями щодо порядку, наприклад:



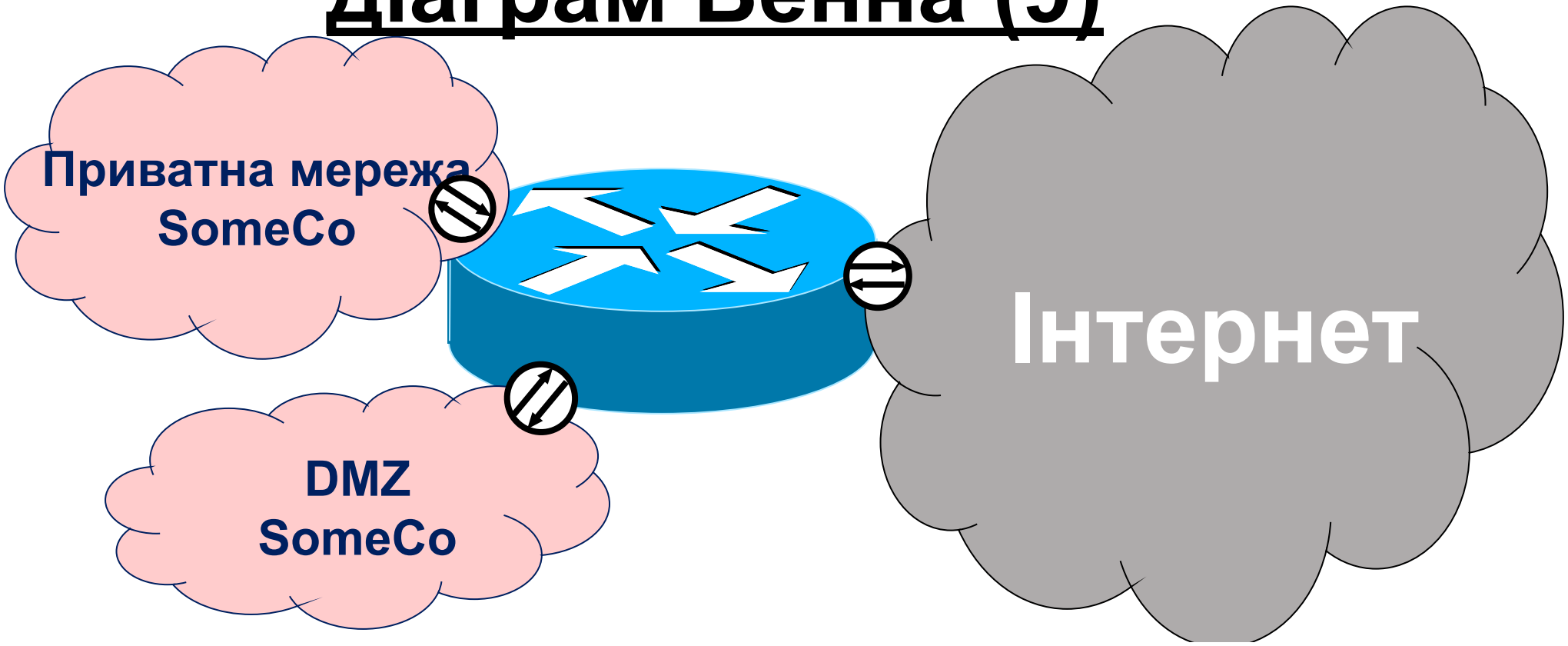
Візуалізація фільтрів за допомогою діаграм Венна (8)

Зверніть увагу на обов’язкове впорядкування правил згори вниз, передбачене цією ілюстрацією за Венном:

1. **заборонити A;**
2. **дозволити B;**
3. **заборонити C;**
4. **дозволити D;**
5. **заборонити все (E).**

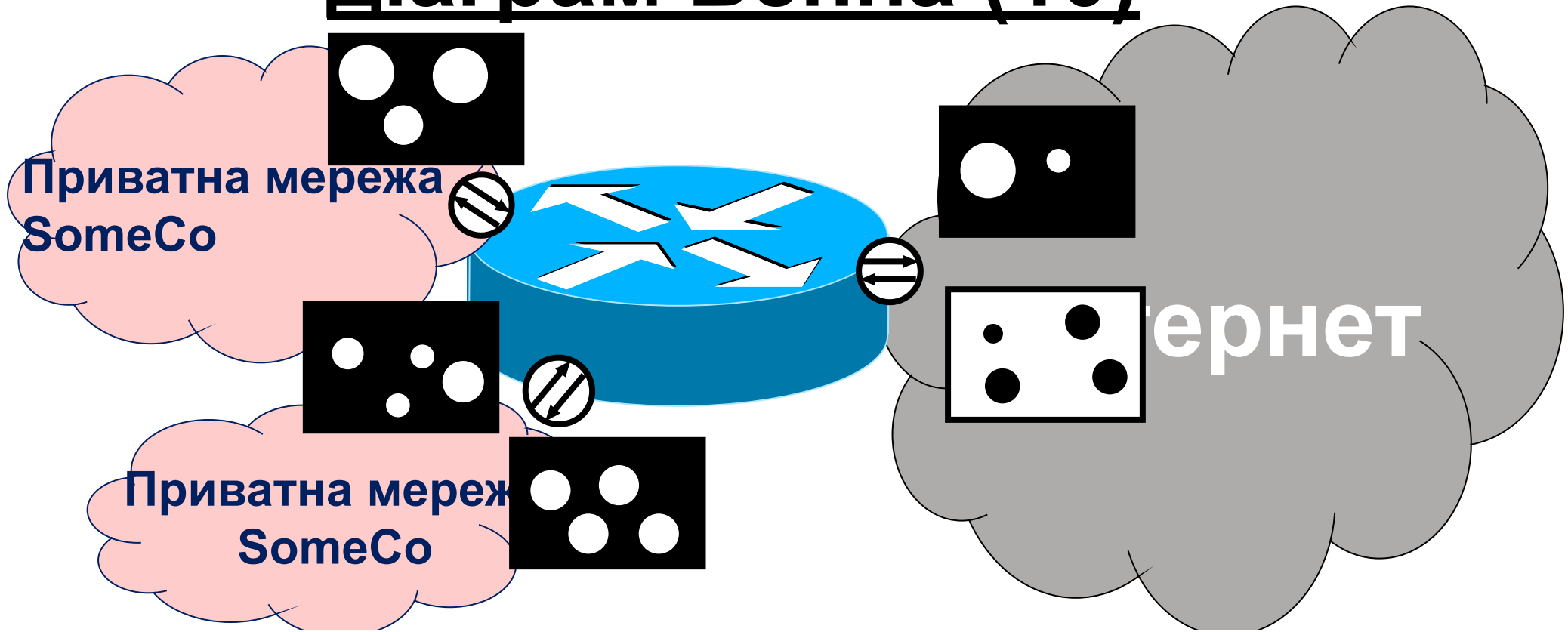


Візуалізація фільтрів за допомогою діаграм Венна (9)



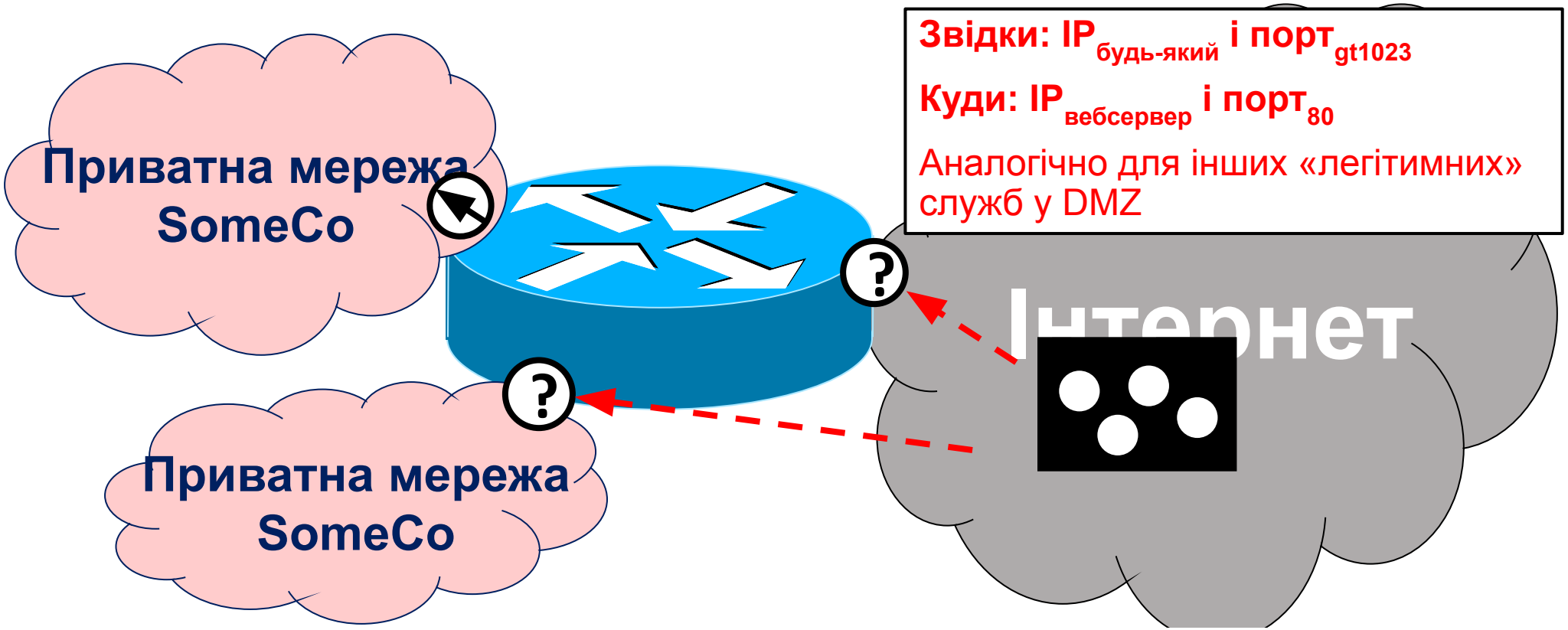
Є кілька різних мереж, тому керування вимогами до безпеки здійснюється за кожним _____ і за кожним _____.

Візуалізація фільтрів за допомогою діаграм Венна (10)



Які б не були комбінації дозволів і заборон, вони повинні працювати коректно й якомога ефективніше втілювати політику.

Міркування щодо розміщення ACL



Політика безпеки стверджує: «дозволяти проходження тільки легітимного трафіка до DMZ (демілітаризованої зони) компанії (наприклад, HTTP до вебсервера, SMTP до поштового сервера тощо)».

Запитання: на якому інтерфейсі слід розмістити цей ACL?

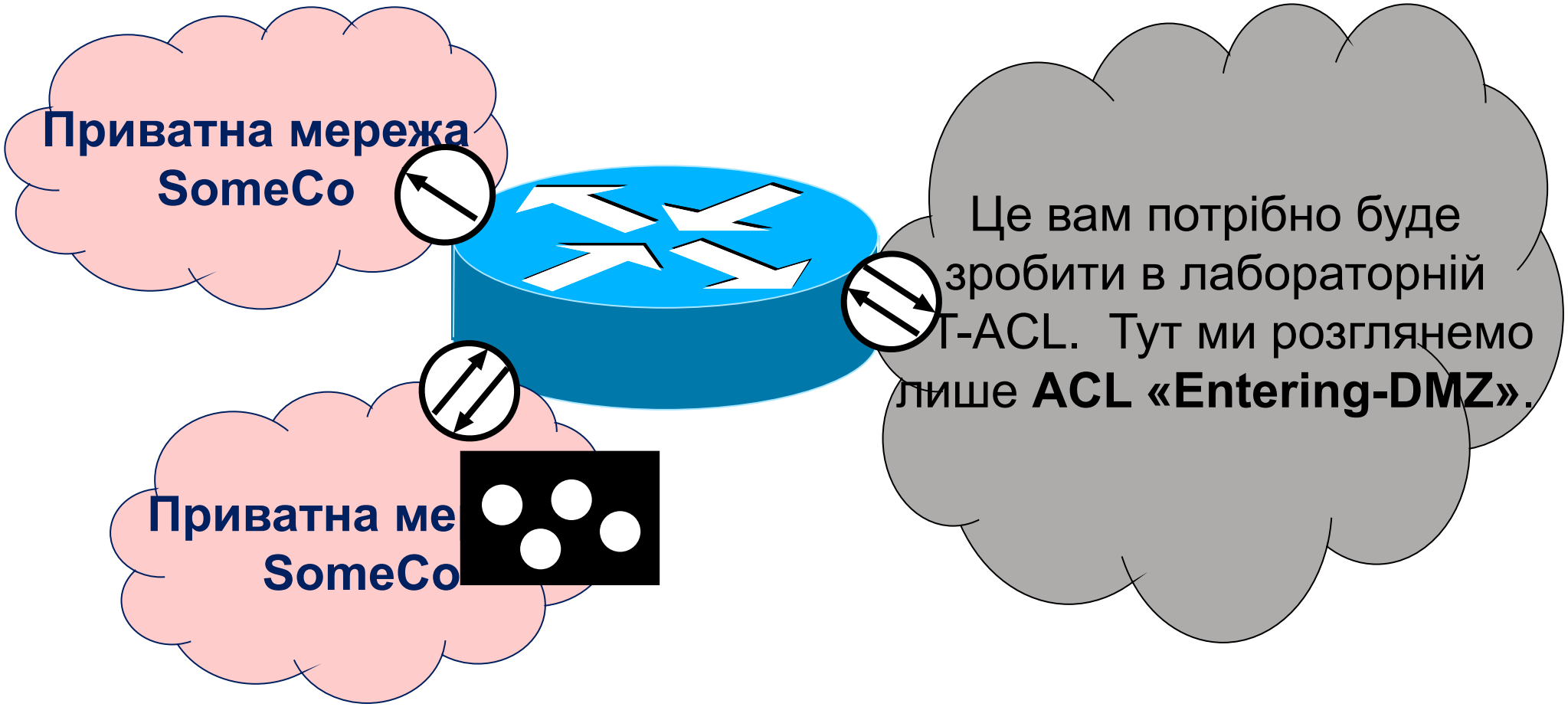
Базова структура правила ACL

- **Дозвіл** або **заборона +**
- передаваний протокол 4-го рівня (**ICMP**, **TCP**, **UDP**) або IP, якщо елемент, що підлягає фільтрації, знаходиться в заголовку 3-го рівня (IP-заголовку), +
- IP-адреса джерела:
  - **W.X.Y.Z хоста** (те саме, що **W.X.Y.Z 0.0.0.0**), або
  - будь-який (неважливо, звідки надходить трафік), або
  - **W.X.Y.0 0.0.0.255** (будь-який трафік з мережі W.X.Y.0) +
- порт джерела:
  - **eq** означає «дорівнює» (зазвичай найменування служби; наприклад, **HTTP**) або
  - **gt** означає «більше ніж» (**gt 1023** означає _____) +
- IP-адреса призначення (аналогічно IP-адресі вище) +
- порт призначення (аналогічно порту вище) +
- можливі додаткові параметри, з яких дві найважливіші:

Базова структура правила ACL

Можна скористатися вбудованою довідкою в командному рядку Cisco, і вона підкаже, які параметри команди мають стояти наступними. Ця поведінка була описана в першій лабораторній роботі з трасування пакетів. Повторіть матеріал, якщо потрібно.

Приклад ACL (SomeCo.com)



Приклад ACL (SomeCo.com)

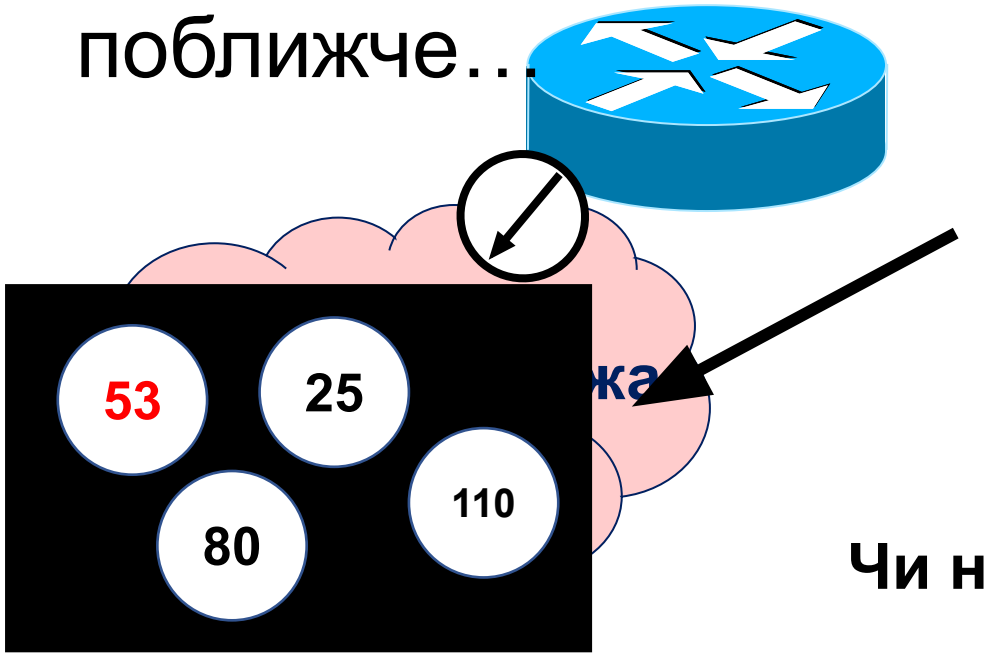
У цій лабораторній вам буде дано доволі просту політику безпеки. Відповідно до неї потрібно реалізувати фільтрування за принципом найменших привілеїв.

Які 4 послуги надаються в DMZ SomeCo.com?

1. _____
2. _____
3. _____
4. _____

Приклад ACL (SomeCo.com)

Розглянемо ситуацію поближче…



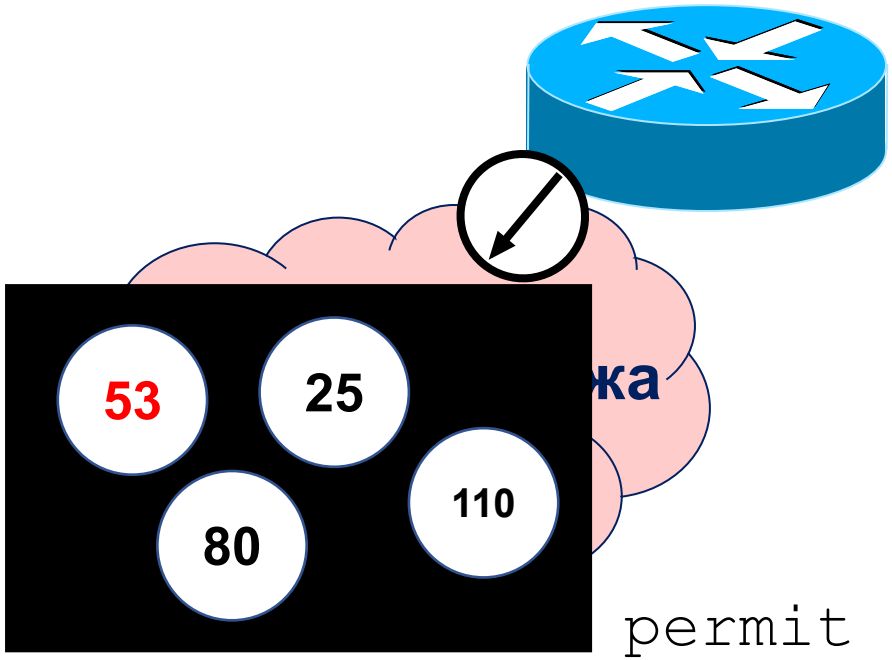
Чотири служби (за номерами портів), що пропонуються загалу в нашій (SomeCo) DMZ

Чи не мав би наш фільтр Entering-DMZ мати правило на кшталт:

```
permit udp any any eq 53
```

Чи можна — і варто — зробити краще?

Приклад ACL (SomeCo.com)



Припустимо, сервери мають такі адреси:

DNS — 170.180.190.130

Веб — 170.180.190.131

Пошта — 170.180.190.132

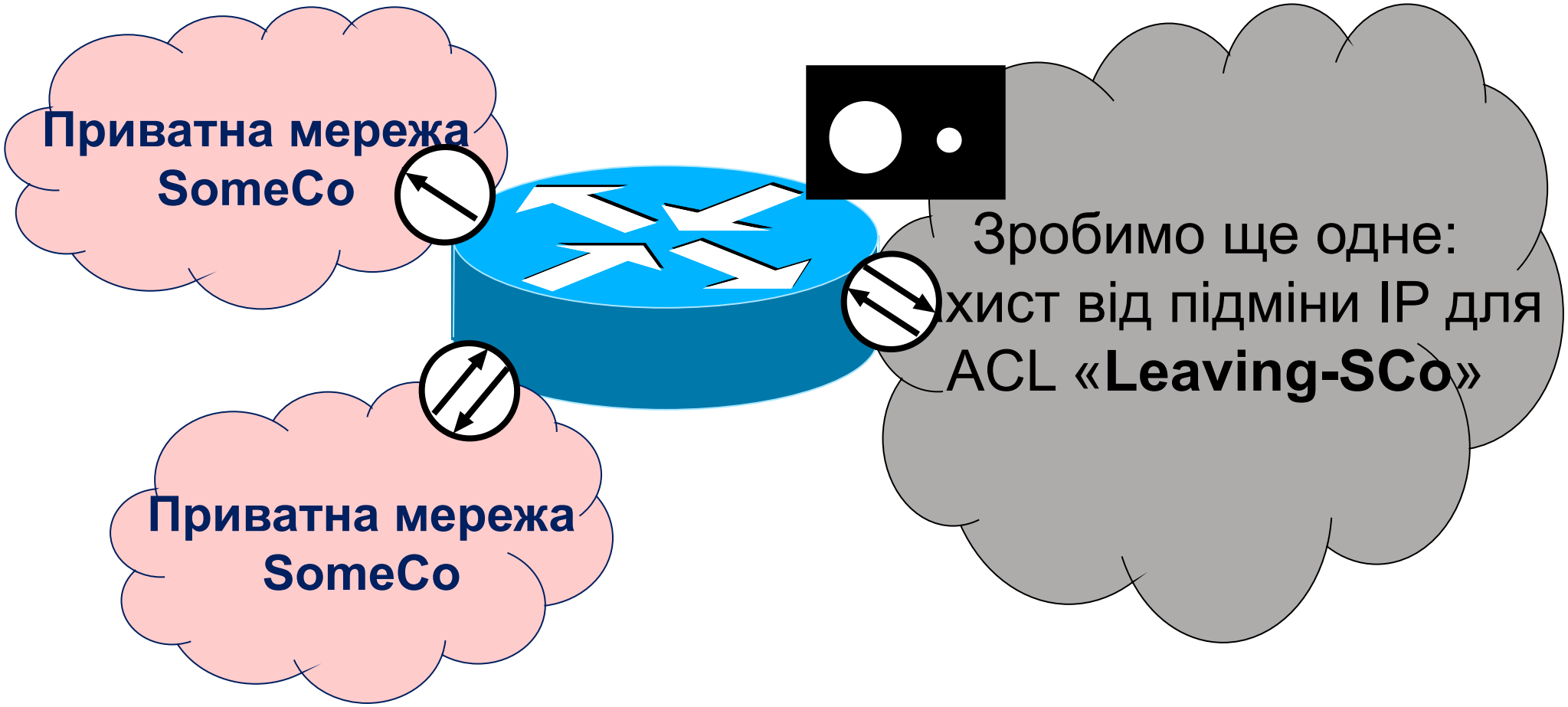
Як має виглядати правило для DNS?

`permit udp any _____ host _____ eq 53`

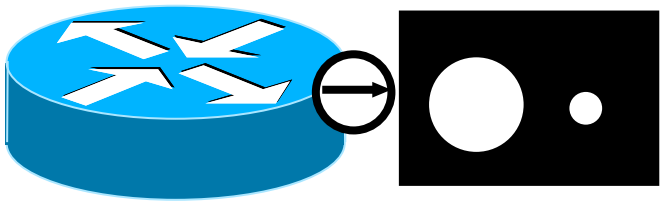
Крім того, для забезпечення нормального функціонування DNS нам потрібно це:

`permit udp any eq ____ host 170.180.190.130 gt 1023`

Приклад ACL (SomeCo.com)



Приклад ACL (SomeCo.com)

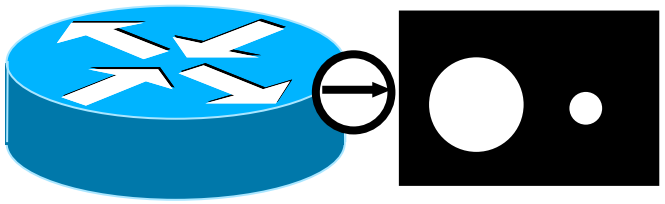


Політика безпеки передбачає запобігання підміні IP у *вихідному* трафіку. Як це зробити?

Які легітимні публічні IP-адреси, що належать SomeCo.com, слід очікувати у трафіку, що виходить з інтранету SomeCo? Тобто що представляють два білих (дозвільних) кола вище?

1. **Простір IP-адрес _____ SomeCo.com та**
2. **адреса _____, яку використовують клієнти у приватній підмережі.**

Приклад ACL (SomeCo.com)

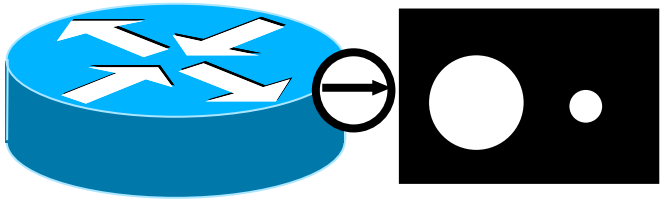


Політика безпеки передбачає запобігання підміні IP у *вихідному* трафіку. Як це зробити?

1. **Простір IP-адрес DMZ SomeCo.com та**
2. **адреса перевантаженого NAT-у, яку використовують клієнти у приватній підмережі.**

```
permit ip 170.180.190.128 _____________________ any
permit ip host ____________________ any
```

Приклад ACL (SomeCo.com)



В лабораторній PT-ACL цей ACL називається «**Leaving-SCo**»

Більш докладний приклад того, як виглядатиме конфігурація маршрутизатора в командному рядку для створення цього ACL, призначення його відповідному інтерфейсу маршрутизатора та фільтрування трафіка в належному напрямку, наведений на наступних трьох слайдах.

Лістинг командного рядка для створення та застосування решти чотирьох ACL буде аналогічним.

Зверніть увагу на кілька випадків використання знака ? для виведення контекстної довідки, наявної в IOS (тобто що має бути введене далі).

ACL «Leaving-SCo» (1 з 3)

```
SomeCoRouter>enable
SomeCoRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SomeCoRouter(config)#
SomeCoRouter(config)#ip access-list ?
   extended Extended Access List
   standard Standard Access List
SomeCoRouter(config)#ip access-list extended ?
  <100-199> Extended IP access-list number
  WORD name
SomeCoRouter(config)#ip access-list extended Leaving-SCo ?
  <cr>
SomeCoRouter(config)#ip access-list extended Leaving-SCo
SomeCoRouter(config-ext-nacl)#
SomeCoRouter(config-ext-nacl)#?
   default Set a command to its defaults
   deny Specify packets to reject
   exit Exit from access-list configuration mode
   no Negate a command or set its defaults
   permit Specify packets to forward
   remark Access list entry comment
SomeCoRouter(config-ext-nacl)#
```

Зауважте індикатор в командному рядку:

`config-ext-nacl`

який є скороченням від:

configure-extended-network-access control list

ACL «Leaving-SCo» (2 з 3)

```
SomeCoRouter(config-ext-nacl)#permit ?
        ahp Authentication Header Protocol
        eigrp Cisco's EIGRP routing protocol
        esp Encapsulation Security Payload
        gre Cisco's GRE tunneling
        icmp Internet Control Message Protocol
        ip Any Internet Protocol
        ospf OSPF routing protocol
        tcp Transmission Control Protocol
        udp User Datagram Protocol
SomeCoRouter(config-ext-nacl)#permit ip ?
        A.B.C.D Source address
        any Any source host
        host A single source host
SomeCoRouter(config-ext-nacl)#permit ip 170.180.190.128 ?
        A.B.C.D Source wildcard bits
SomeCoRouter(config-ext-nacl)#permit ip 170.180.190.128 0.0.0.63 ?
        A.B.C.D Destination address
        any Any destination host
        host A single destination host
```

Можна побачити, як утиліта раз-по-раз використовує функцію довідки ? для визначення того, що має стояти далі.

ACL «Leaving-SCo» (3 з 3)

```
SomeCoRouter(config-ext-nacl)#permit ip 170.180.190.128 0.0.0.63 any
SomeCoRouter(config-ext-nacl)#permit ip host 170.180.190.2 any
SomeCoRouter(config-ext-nacl)#exit
SomeCoRouter(config)#int fa0/1
SomeCoRouter(config-if)# ip ?
  access-group          Specify access control for packets
  address               Set the IP address of an interface
  hello-interval        Configures IP hello interval
  helper-address        Specify a destination address
  inspect               Apply inspect name
  ips                   Create IPS rule
  mtu                   Set IP Maximum Transmission Unit
  nat                   NAT interface commands
  ospf                  OSPF interface commands
  split-horizon         Perform split horizon
  summary-address       Perform address summarization
  virtual-reassembly    Virtual Reassembly
SomeCoRouter(config-if)# ip access-group Leaving-SCo out
SomeCoRouter(config-if)#
```

Це команда, яка призначає вже створений ACL визначеному інтерфейсу маршрутизатора.

Виглядає не надто інтуїтивно.

Перевірка (1 з 2)

```
SomeCoRouter(config-if)#
SomeCoRouter(config-if)#^Z
SomeCoRouter#
%SYS-5-CONFIG_I: Configured from console by console
SomeCoRouter#sh run
Building configuration...
<lots of snipped/removed stuff here...>
interface FastEthernet0/1
 ip address 170.180.190.2 255.255.255.192
 ip access-group Leaving-SCo out
 ip nat outside
 duplex auto
 speed auto
!
<additional snipped/removed stuff here...>
```

Дуже корисна команда, яка відображає поточну конфігурацію.

Її варто використовувати щоразу, коли потрібно переглянути поточну конфігурацію маршрутизатора.

Явне підтвердження того, що цей ACL застосовано до потрібного інтерфейсу і в потрібному напрямку.

Перевірка (2 з 2)

```
SomeCoRouter#sh access-lists
Standard IP access list NAT
 permit 10.10.10.0 0.0.0.255(8 match(es))
Extended IP access list Leaving-SCo
 permit ip 170.180.190.128 0.0.0.63 any (4 match(es))
 permit ip host 170.180.190.2 any (4 match(es))
SomeCoRouter#
```

Зауважте, як ця команда також забезпечує динамічне відображення того, скільки разів сталися збіги з правилами (втім, цей індикатор вимкнеться після таймауту).

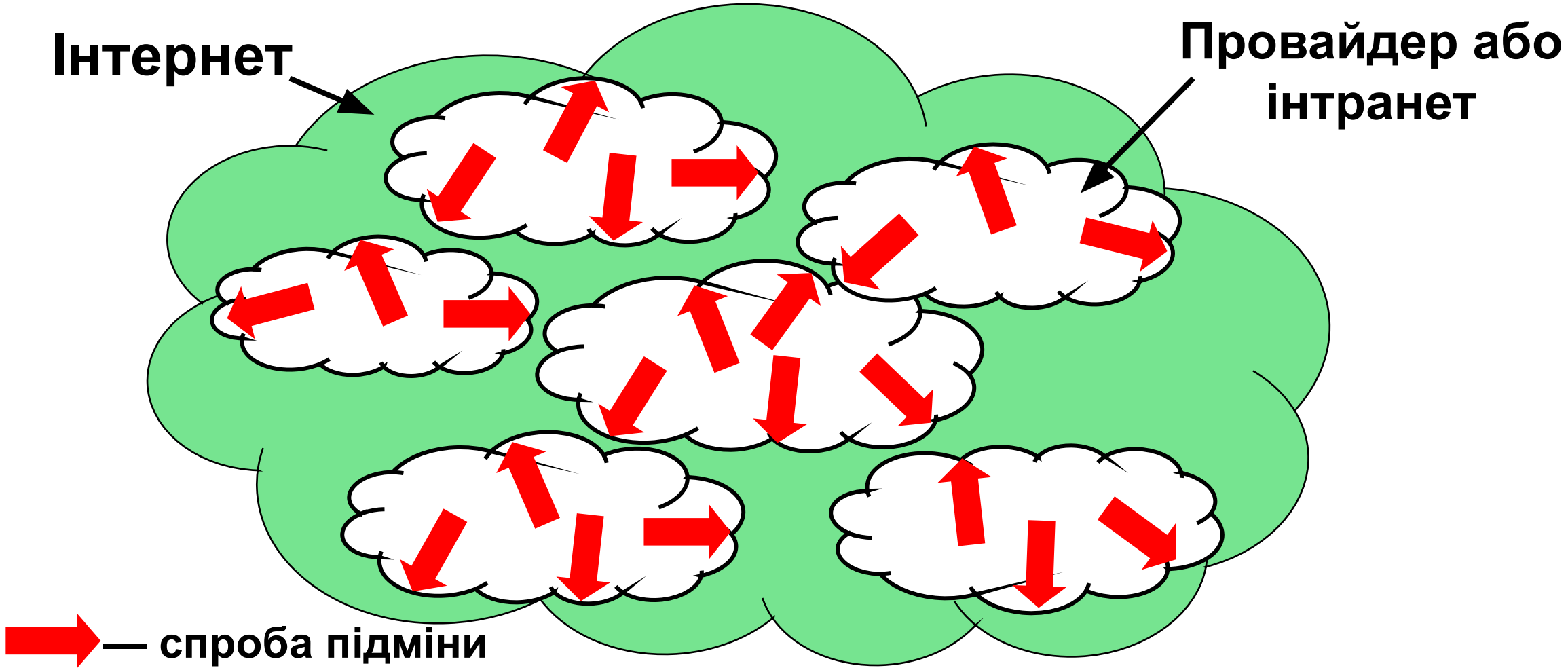
Тепер у цілях лабораторної з ACL прочитайте (й обміркуйте) надану політику безпеки, а тоді створіть відповідні ACL (тобто реалізуйте вимоги політики безпеки) для такого:

- **Entering-SCo;**
- **Entering-DMZ;**
- **Leaving-DMZ;**
- **Entering-Pvt.**

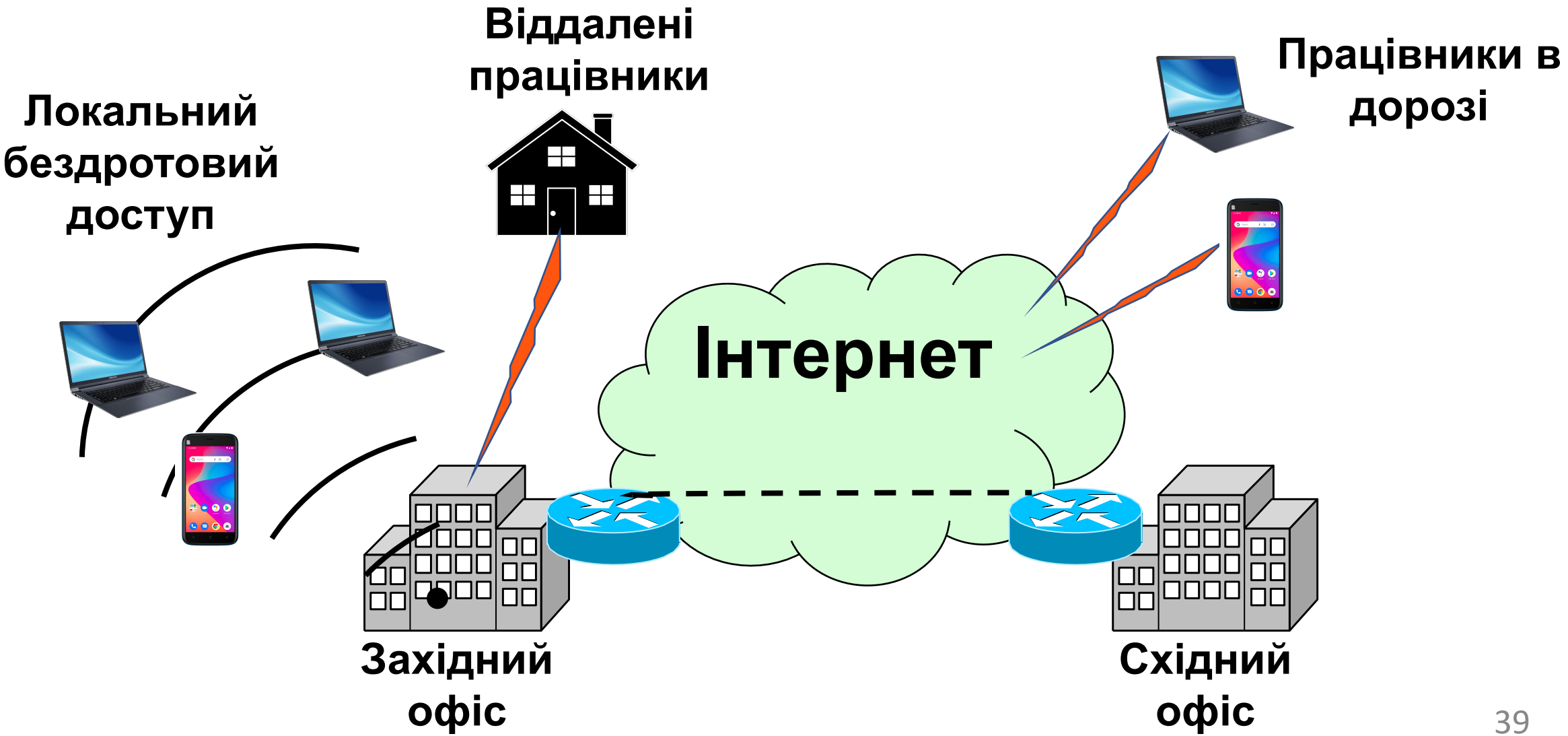
Захист від підміни у вихідному трафіку

- Невелика примітка щодо відносно простої, але дуже корисної дії.
- Початковим наміром (з точки зору самозахисту) є блокування лише вхідного трафіка з підміною (спуфінгом).
- І це правильно, але якби кожен Інтернет-провайдер дотримувався принципів «хорошого громадянина Інтернету» і також запобігав спуфінгу вихідного трафіка?
- Див. ілюстрацію на наступному слайді.

Захист від підміни у вихідному трафіку



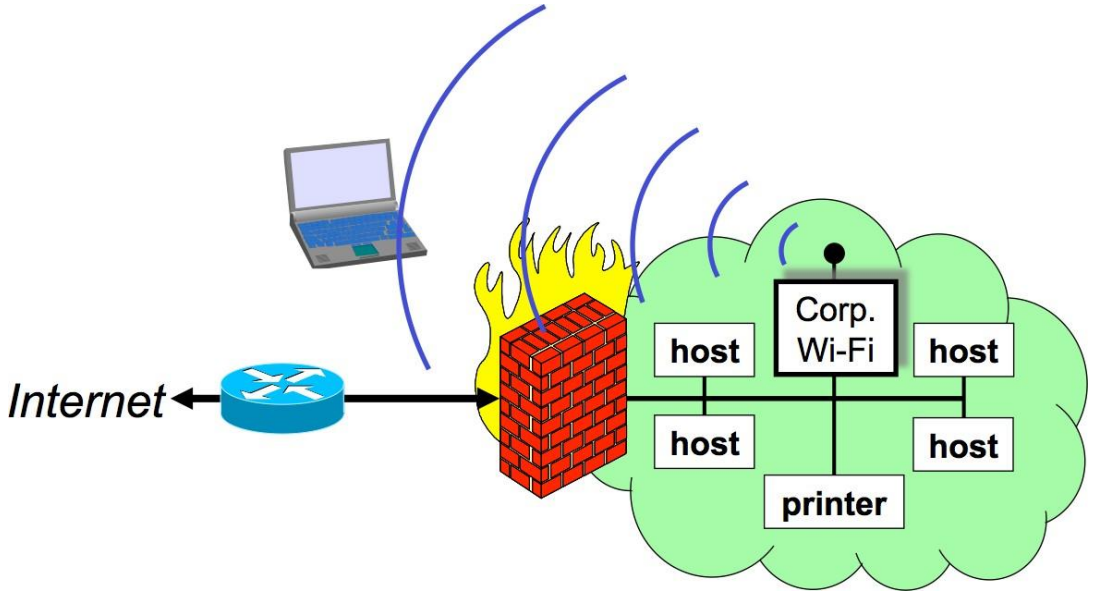
Де проходить периметр?



Де проходить периметр?

- Як зображено на попередньому слайді, «периметр» може бути «пористим» і динамічним (змінюватися з часом).
- Дуже важливим є безпековий аналіз всіх точок входу/виходу та загальної топології мережі установи.
- Бездротовий (OTA) доступ — слабке місце.
- Працівники з власними пристроями та гості — слабке місце.
- Дані, що проходять через канали загального користування (інфраструктуру), — слабке місце.
- Всі ці проблеми повинна враховувати політика, відповідно до якої і повинні працювати технології.

Бездротовий доступ — слабке місце

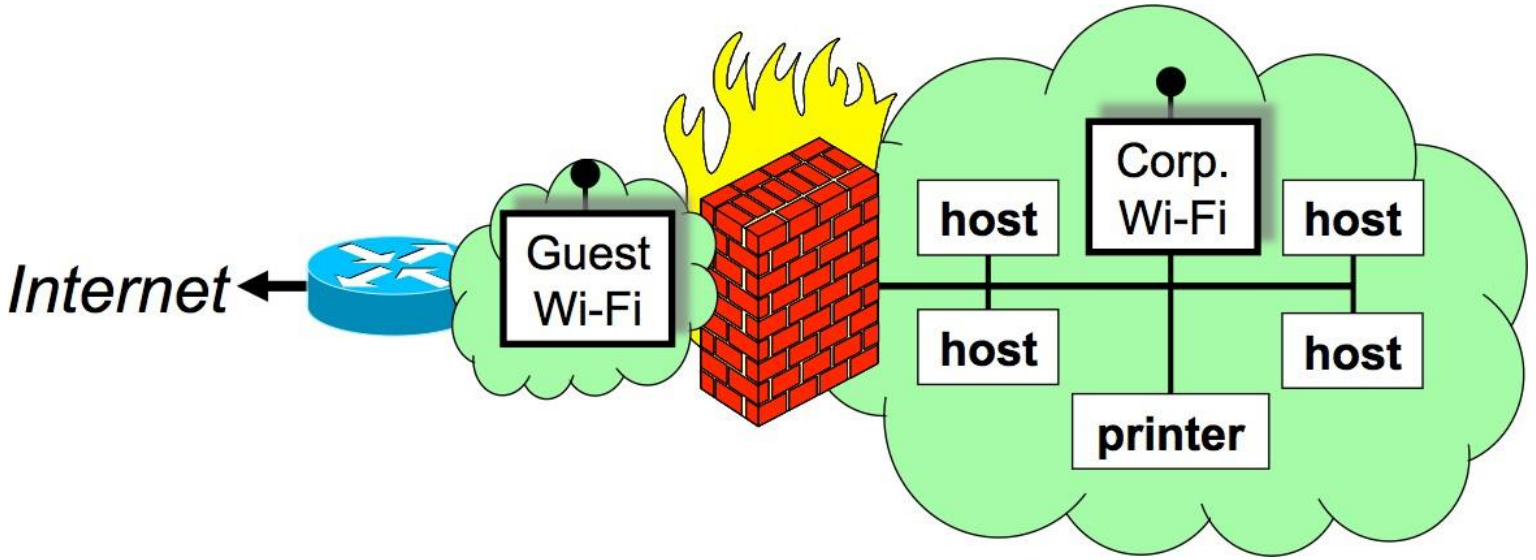


Це істотно знижує ефективність заходів контролю фізичного доступу.

Які 2 типові заходи фізичного контролю для цього використовуються?

1. **Впровадження _____ (найбільш сучасного захисту Wi-Fi) для автентифікації користувачів.**
2. **Упаковування всього бездротового трафіка у _____ для створення мірою потреби виділеної/ізольованої локальної мережі.**

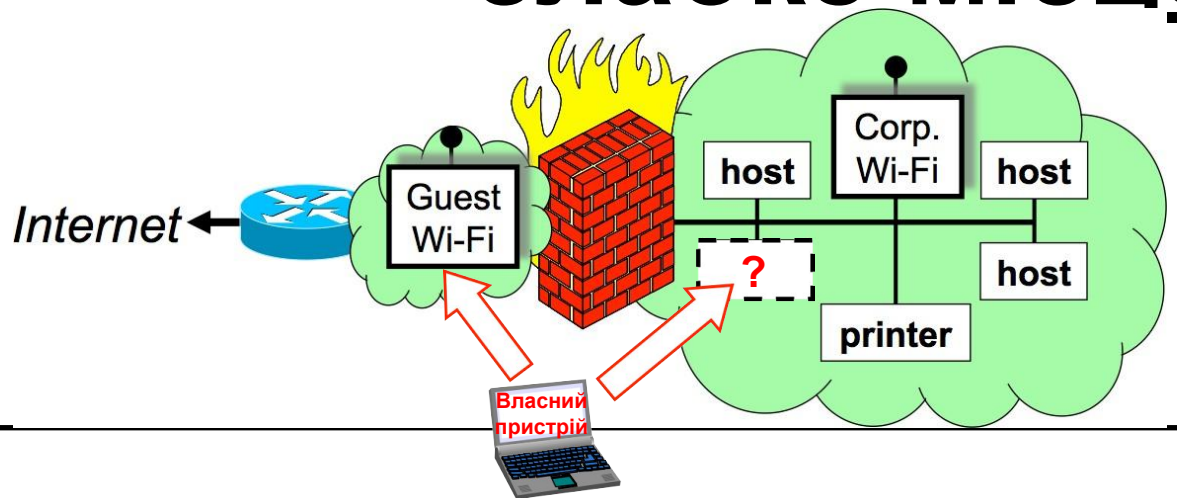
Гість — слабке місце



Ось де в нагоді стане _____.

Можна прийняти кожного з мінімальним ризиком.

Працівники із власними пристроями — слабке місце



Небезпеки:

1. Користувачі можуть приносити шкідливі програми, які «підхопили», перебуваючи поза межами корпоративної мережі.
2. Користувачі можуть не дотримуватися базових принципів кібергігієни (наприклад, регулярного оновлення ОС антивірусного ПЗ).

Заходи безпеки:

1. Контроль/обмеження доступу за MAC-адресами («безпека портів»).
2. Впровадження IEEE 802._____ (пристрій повинен автентифікуватися за допомогою сертифіката).
3. NAC — Network Access Control («контроль доступу до мережі», підтвердження стану антивірусного ПЗ й оновлень ОС перед наданням дозволу).
4. C2C — _____ to Connect («відповідність для з'єднання», більш автоматизована версія NAC).

Витяги з «Прийнятного плану мережі» НБА

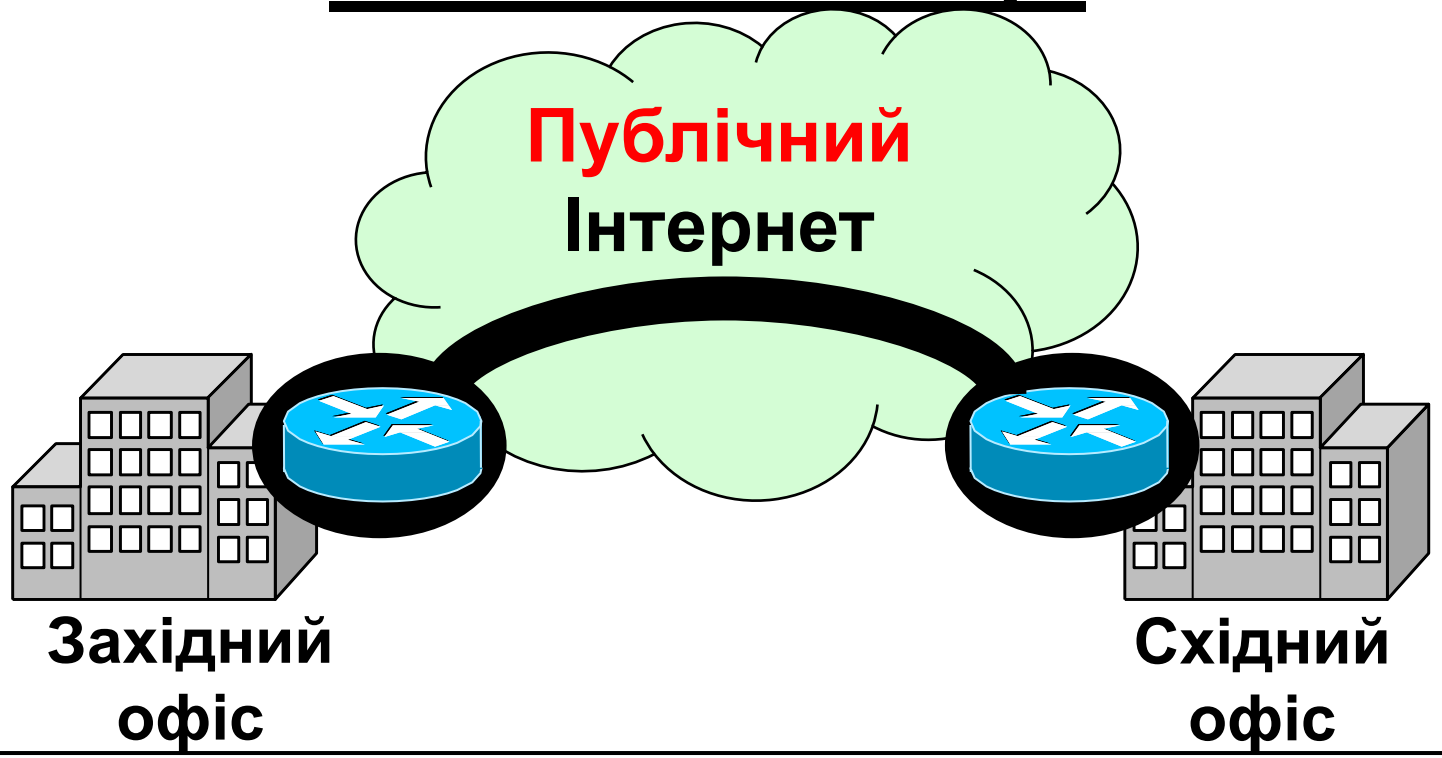
Версія 4.0 від грудня 2015 р.

Network Access Control (NAC)

When someone plugs a device into your network, that device should not automatically have access to everything. Unauthorized "rogue" devices and devices that are misconfigured, behind in patches or malware scans, etc. should be prevented from accessing your network resources, because they may open up vulnerabilities on your internal network. This applies especially in BYOD ("Bring Your Own Device") environments. Devices (and any users of the devices) should be denied access to your network resources until after a verification and authentication procedure.

- Suggestion: For basic access control, configure your network switches to only allow certain MAC addresses to connect to their physical ports (port-based authentication, or port security) or implement IEEE 802.1X, where client machines must authenticate at the network layer before gaining access to network resources.
  - Whenever possible, require client machines to authenticate using certificates (which, unlike MAC addresses, generally cannot be spoofed). Record these certificates with their associated devices in the device list from Milestone 2.
  - For your mobile devices, be sure that your NAC solution and your MDM solution are compatible.
- Suggestion: For more robust access control, use a Comply-to-Connect (C2C) solution. A C2C solution can, for example, assign machines connected to your network to separate VLANs based on device type, initial (and even ongoing) health and configuration checks and policies that you set. C2C is an automated Network Access Control (NAC) solution that verifies that an endpoint is authorized and meets security requirements before allowing access to the network. C2C can take automated security actions to enforce network security requirement and provide continuous network monitoring for deviations from these requirements.

Канали загального користування — слабке місце



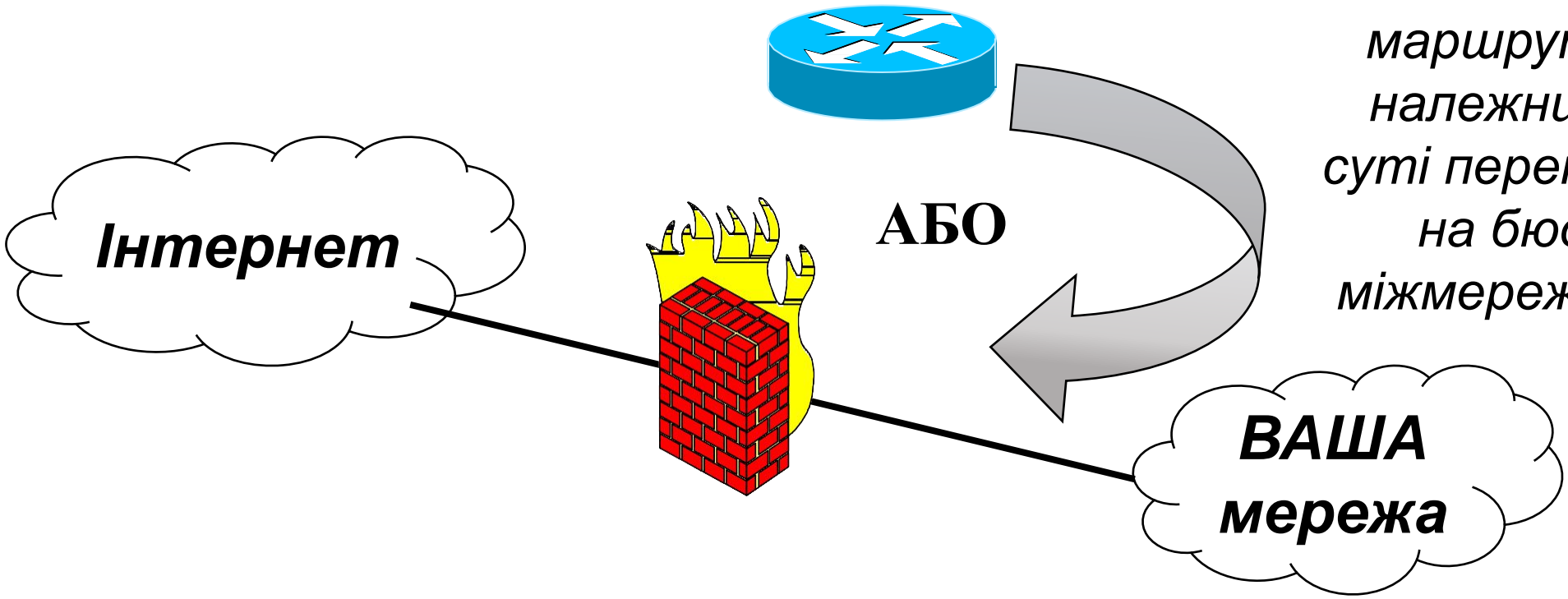
Щойно дані в русі виходять за фізичний (безпековий) периметр, їхня безпека стає залежною від належного використання _____.

Це ще називається — вельми узагальнено — технологією VPN.

Варіанти DMZ

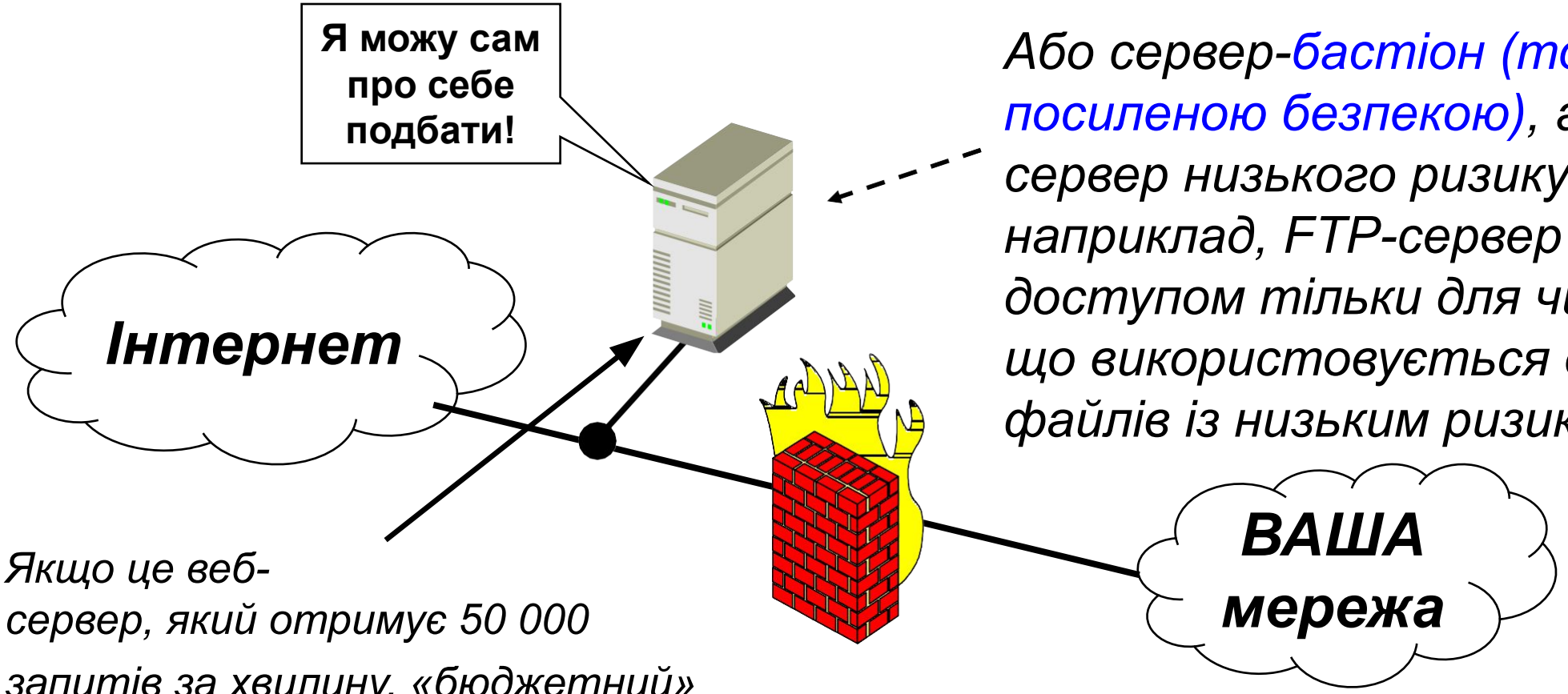
- Потреби організації часто зумовлюють створення кількох підмереж, які працюють із різними рівнями припустимого ризику.
- Потрібну гнучкість забезпечують кілька периметрів один всередині іншого.
- «Середній» рівень часто називають DMZ (демілітаризованою зоною).
- На наступних чотирьох слайдах проілюстровані базові топології периметра.

Одноpівнева (базова) топологія



Пам’ятайте: маршрутизатор із належними ACL по суті перетворюється на бюджетний міжмережевий екран.

Одноpівнева топологія (із додатковим «сервером-бастіоном»)

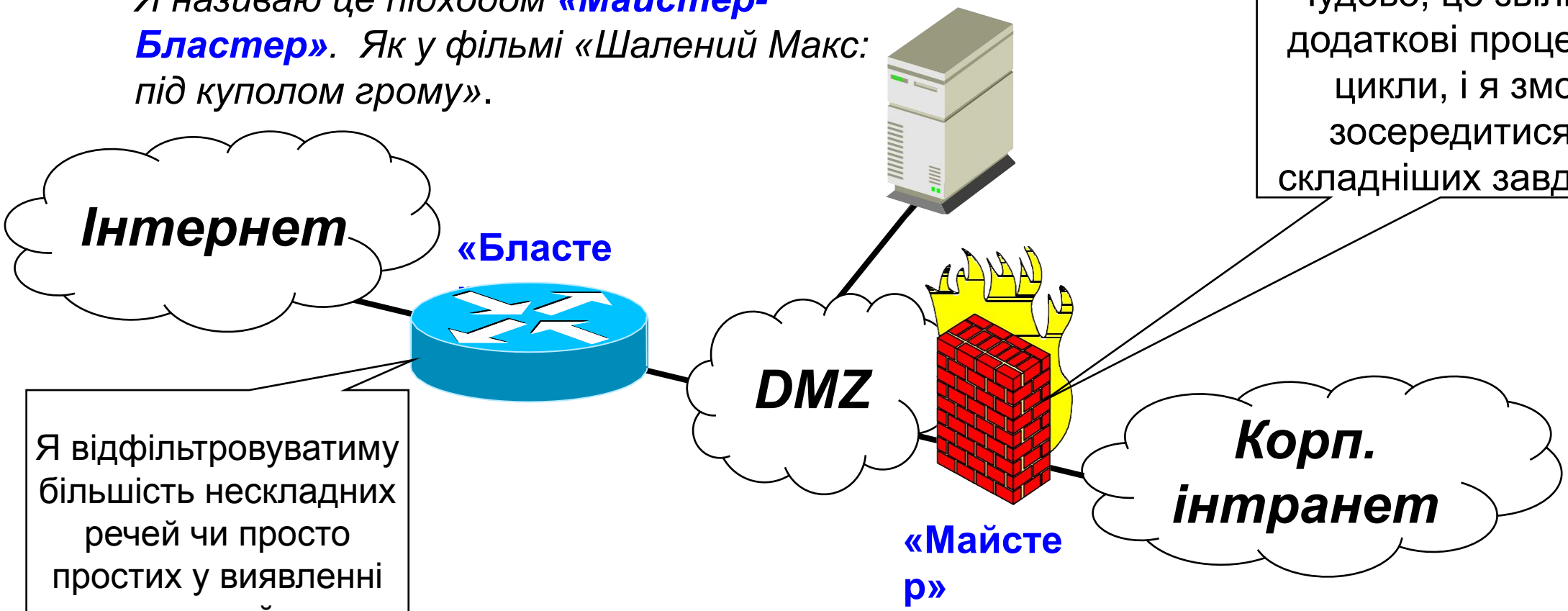


Або сервер-бастіон (тобто із посиленою безпекою), або сервер низького ризику — наприклад, FTP-сервер із доступом тільки для читання, що використовується для файлів із низьким ризиком

Якщо це веб-сервер, який отримує 50 000 запитів за хвилину, «бюджетний» міжмережевий екран може не бути спроможним опрацьовувати таку кількість трафіка;

Багаторівнева топологія (із DMZ)

*Я називаю це підходом **«Майстер-Бластер»**. Як у фільмі «Шалений Макс: під куполом грому»*.



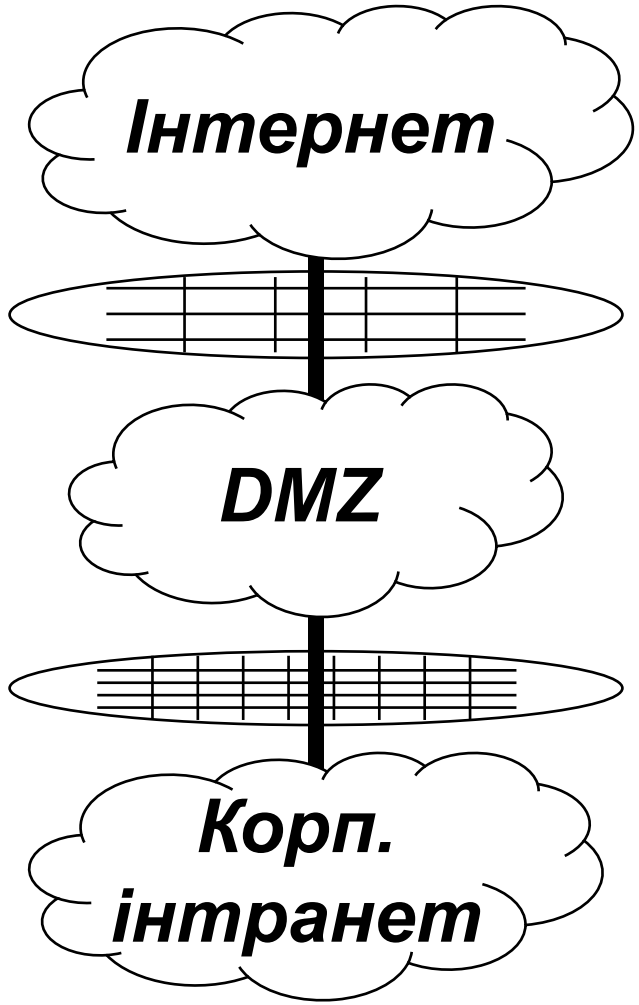
Чудово, це звільнить додаткові процесорні цикли, і я зможу зосередитися на складніших завданнях

Я відфільтровуватиму більшість нескладних речей чи просто простих у виявленні сканувань й атак

Концепція «Майстер-Бластер»

«Бластер»

«Майстер»



«Груба» фільтрація

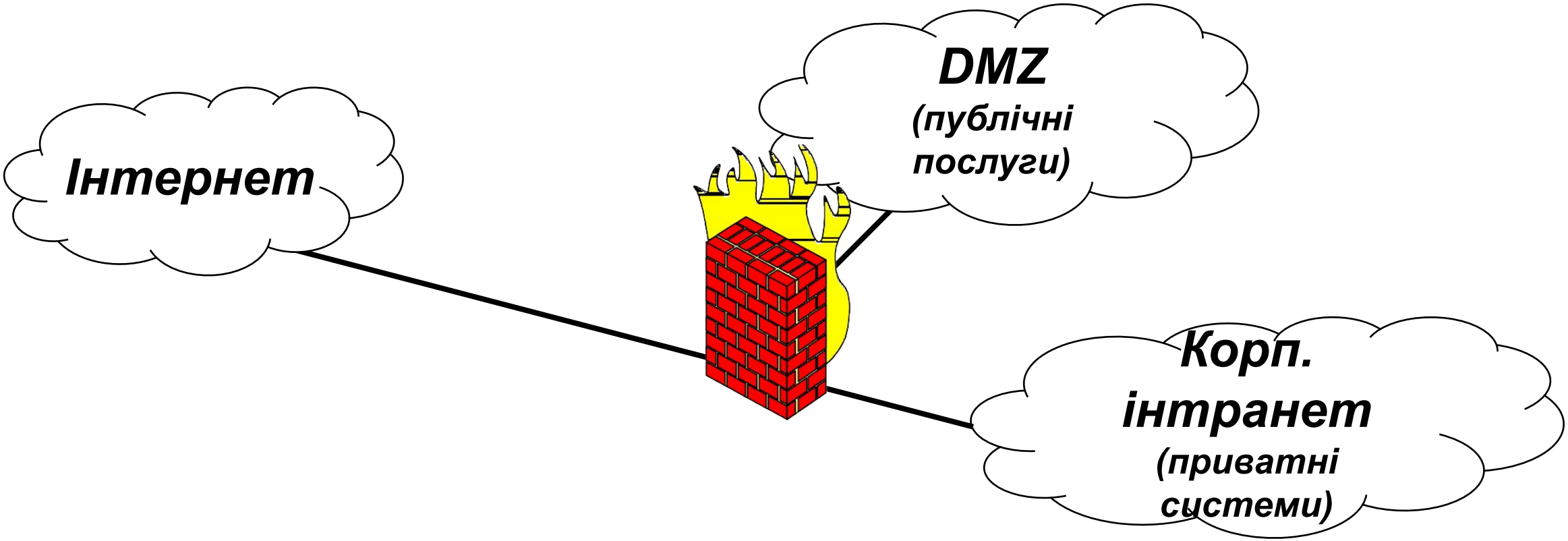
наприклад, прості дозволи та заборони на основі пари сокетів

«Тонка» фільтрація

наприклад, міжмережеві екрани на основі проксі, які фільтрують на основі корисного навантаження пакетів

«3-інтерфейсна» DMZ ( )

Також відома як DMZ «зі службовим інтерфейсом»

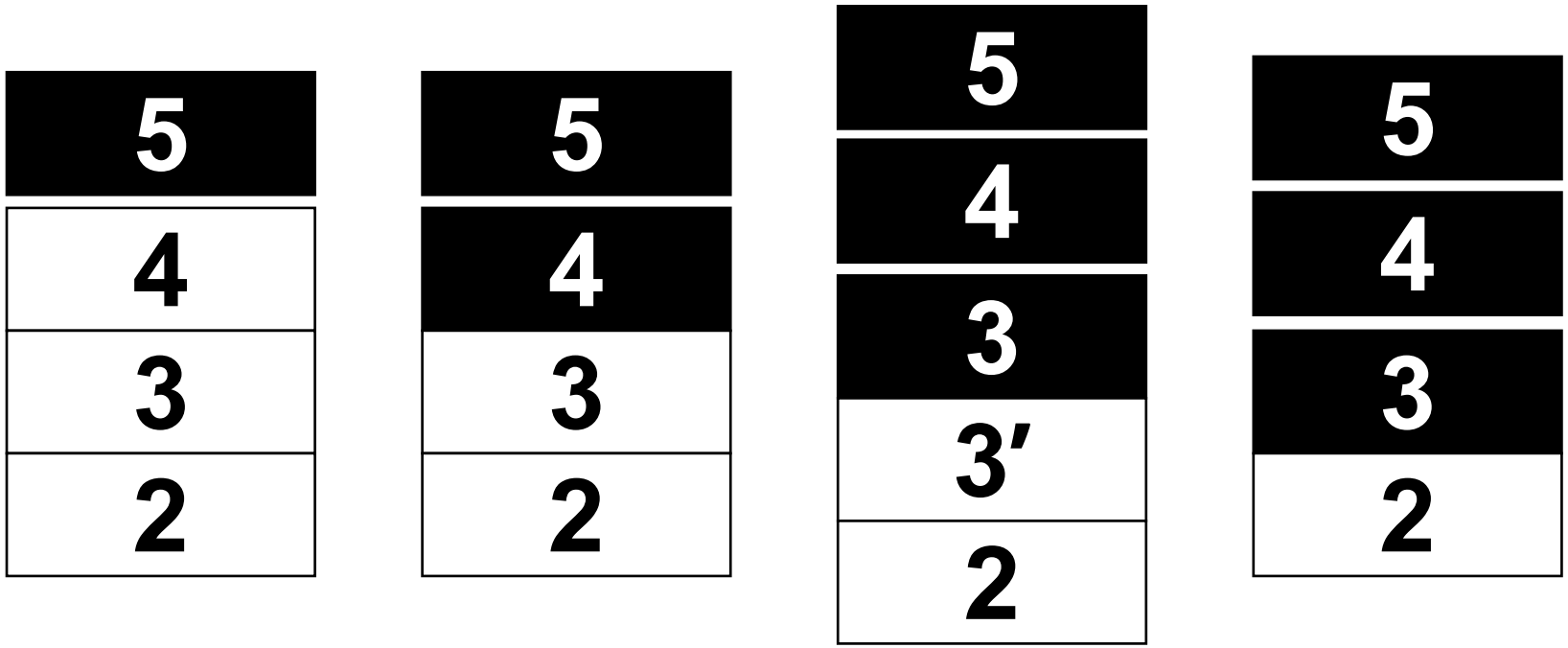


Комбінація фільтрів і VPN

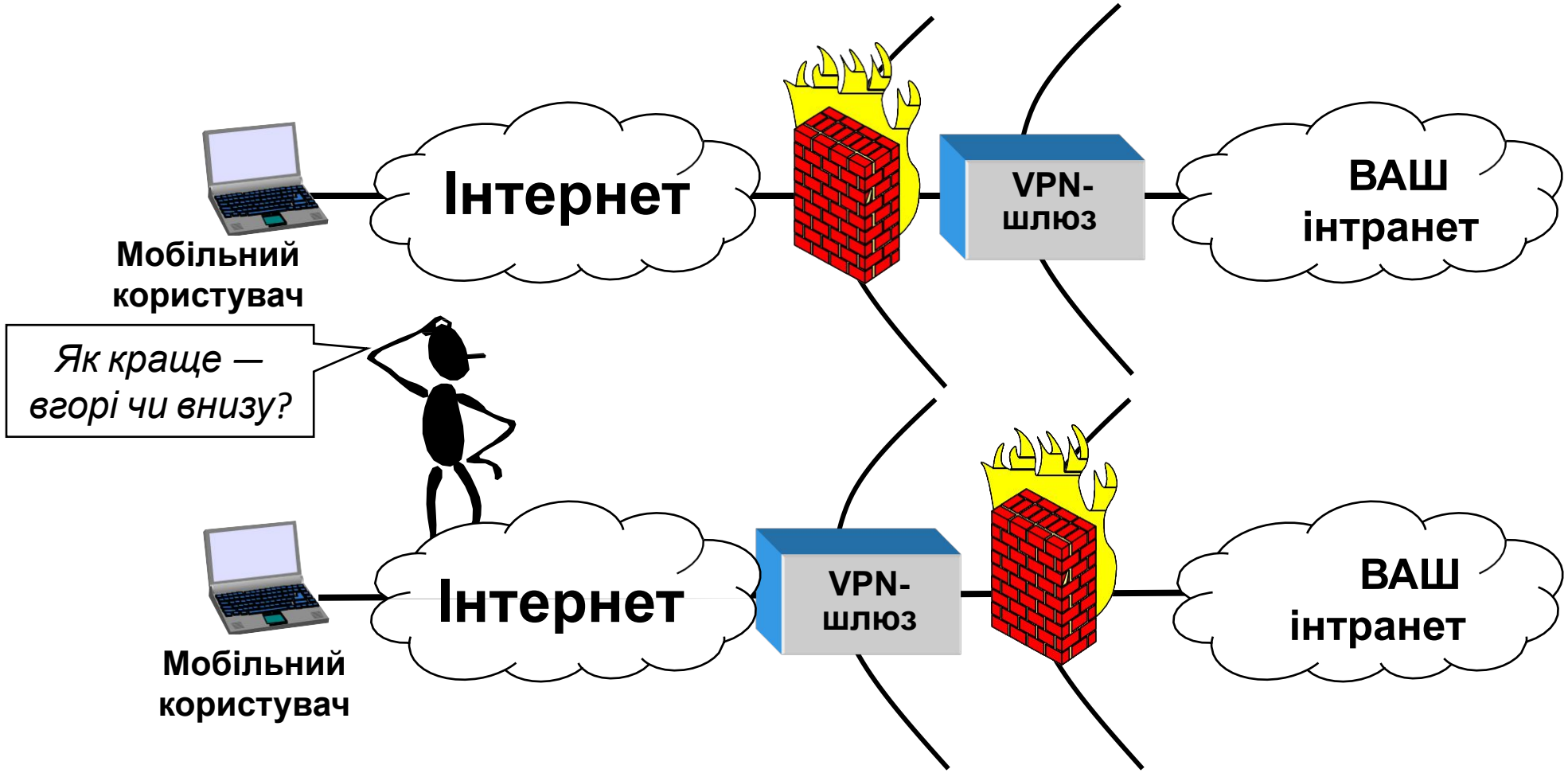
- **Комбінуючи ці дві технології безпеки, важливо враховувати наслідки цього для безпеки.**
- **Для того, щоб дати відповідь на пов'язані питання (далі буде), потрібно розглянути таке:**
  - **тип VPN з точки зору того, який(-і) _____ він має шифрувати;**
  - **чи дозволяє/забороняє локальна політика VPN роздільне тунелювання;**
  - **пропускну спроможність фільтра;**
  - **«довіра» до віддаленого користувача та його програмного забезпечення VPN-клієнта;**
  - **який тип _____ віддаленого користувача реалізовується (наприклад, автоматичний вхід до мережі/служби).**

Основні типи VPN

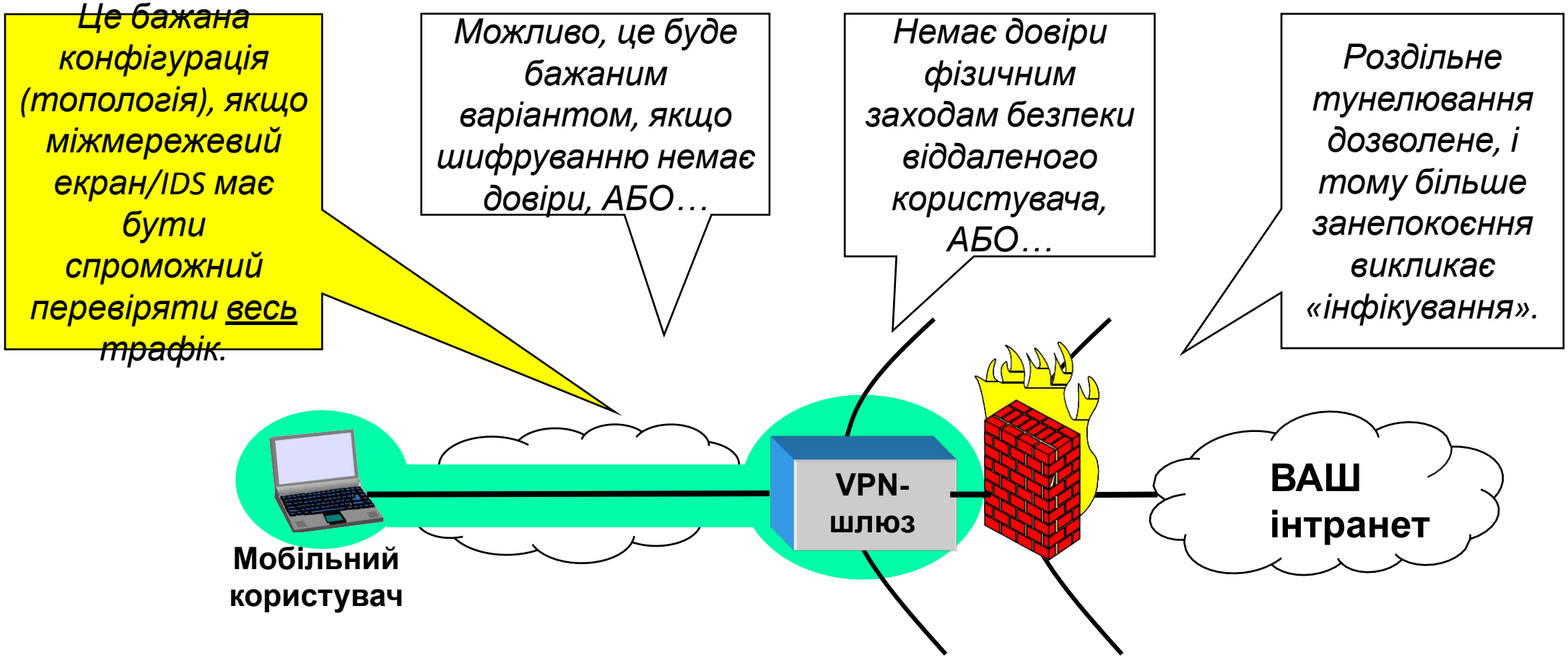
- Чорні — шифровані; білі — нешифровані.
- Запам’ятайте ці найбільш поширені.



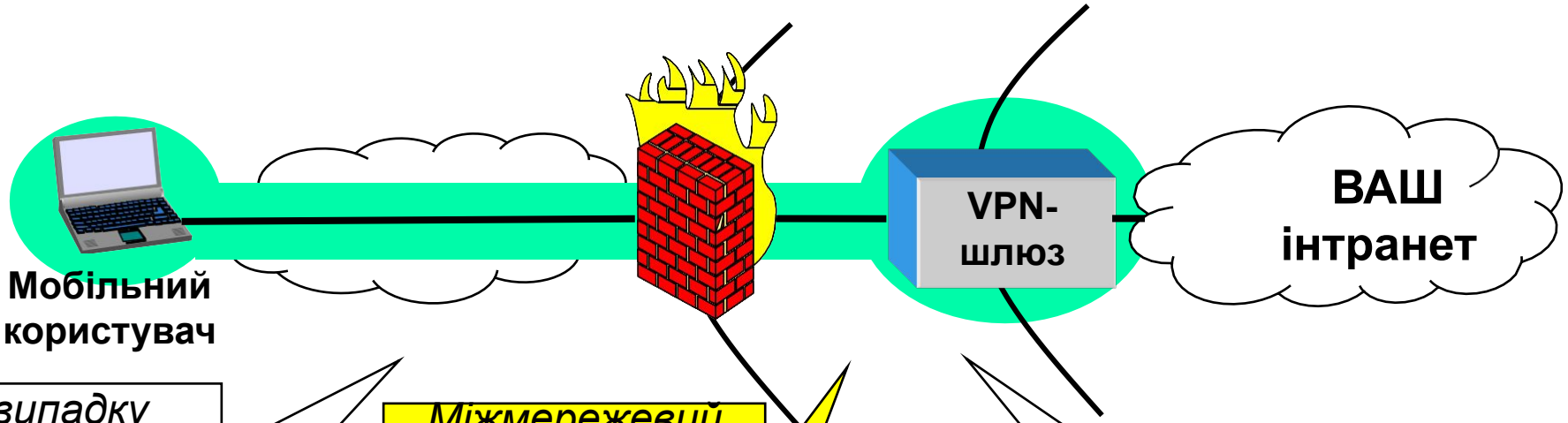
Комбінація фільтрів і VPN



Комбінація фільтрів і VPN



Комбінація фільтрів і VPN



В цьому випадку міжмережевий екран матиме менше роботи, оскільки деякий/весь шифрований трафік буде просто пропускатися.

Міжмережевий екран/IDS не зможе перевіряти один чи кілька шарів (залежно від типу VPN) у тунельованому трафіку.

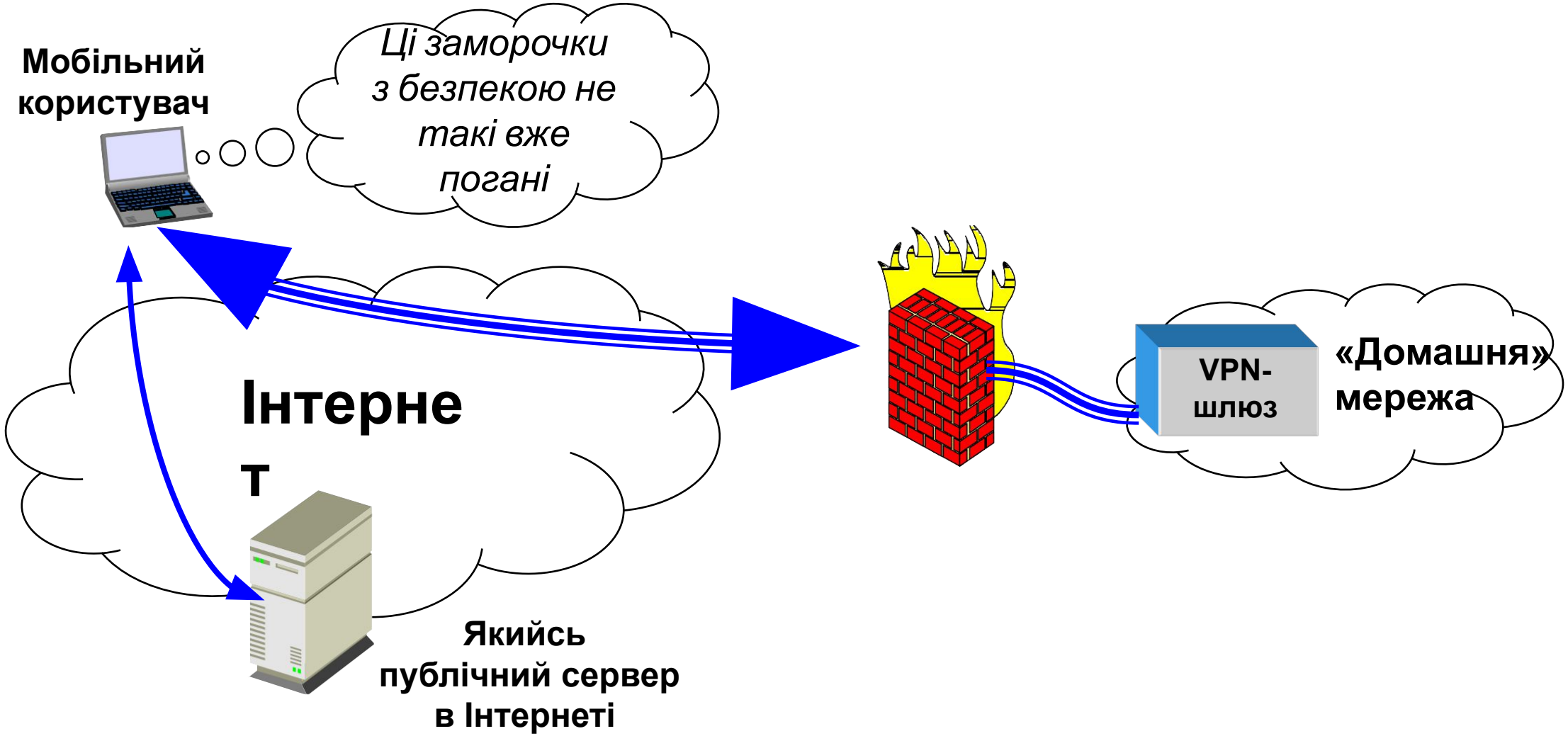
Будемо сподіватися, що поганці не отримають доступу до цього ноутбука!

Роздільне тунелювання

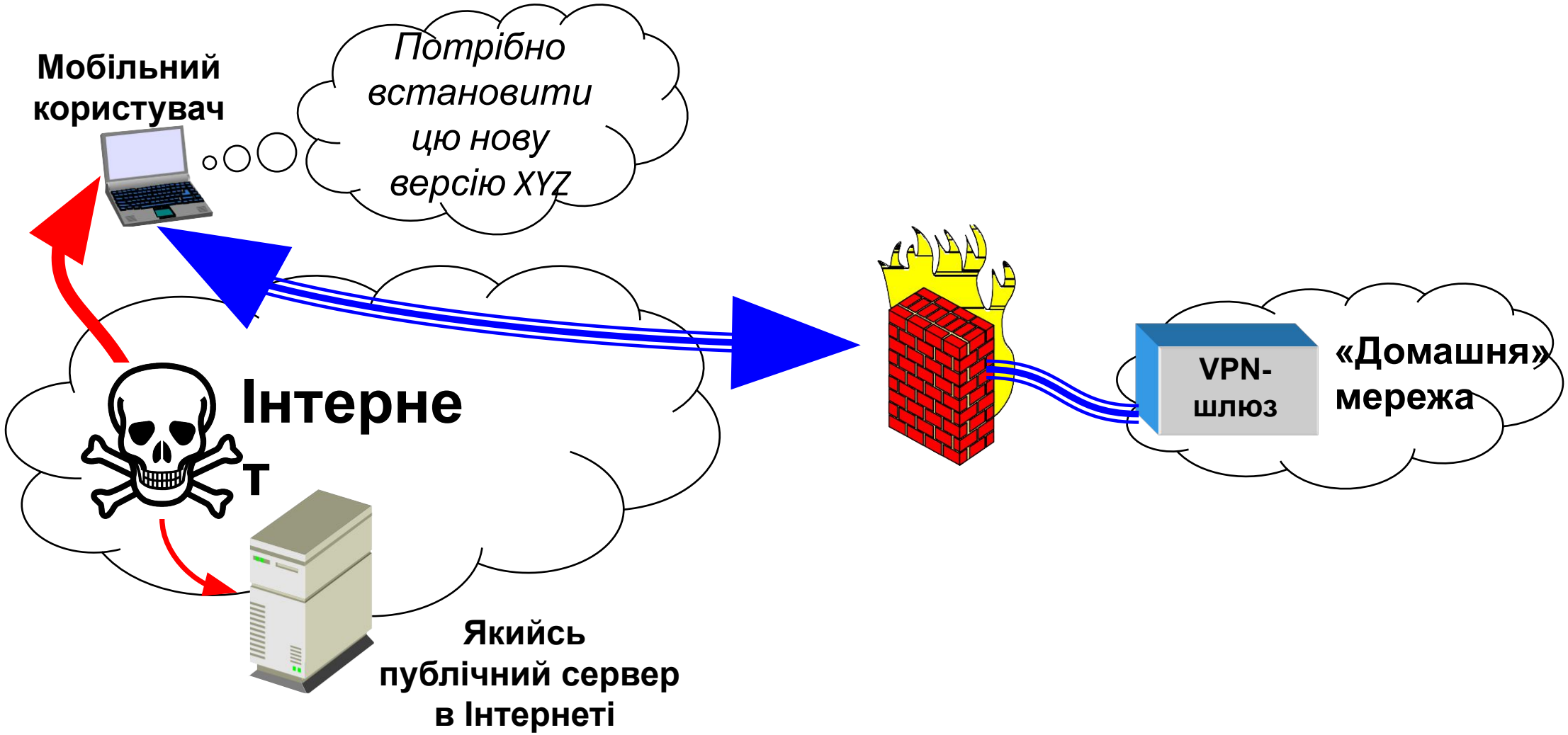
- **Роздільне тунелювання означає, що віддалений/VPN-клієнт може _____ підтримувати VPN-тунель до своєї «домашньої» мережі та вести прямий* обмін даними з не-«домашніми» мережевими системами.**
- **Це вносить ризик у роботу VPN-тунелю, оскільки _____ може проникнути з інфікованої/шкідливої Інтернет-системи до VPN-клієнта, а звідти через тунель до «домашньої» мережі.**

***Тією мірою, як маршрутизаційна інфраструктура буде спрямовувати його, причому він може не проходити спершу через «домашню» мережу.**

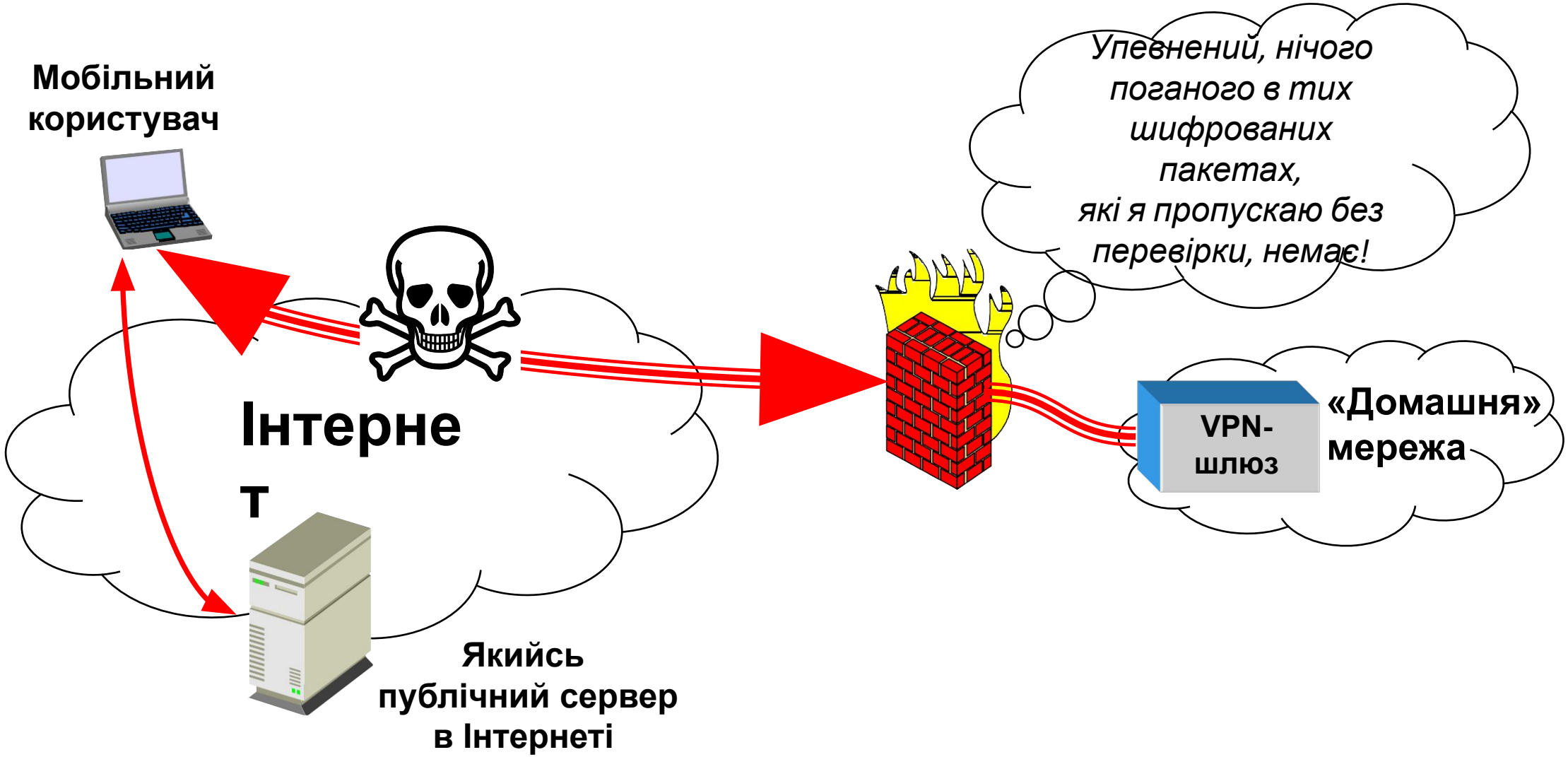
Роздільне тунелювання (дозволене)



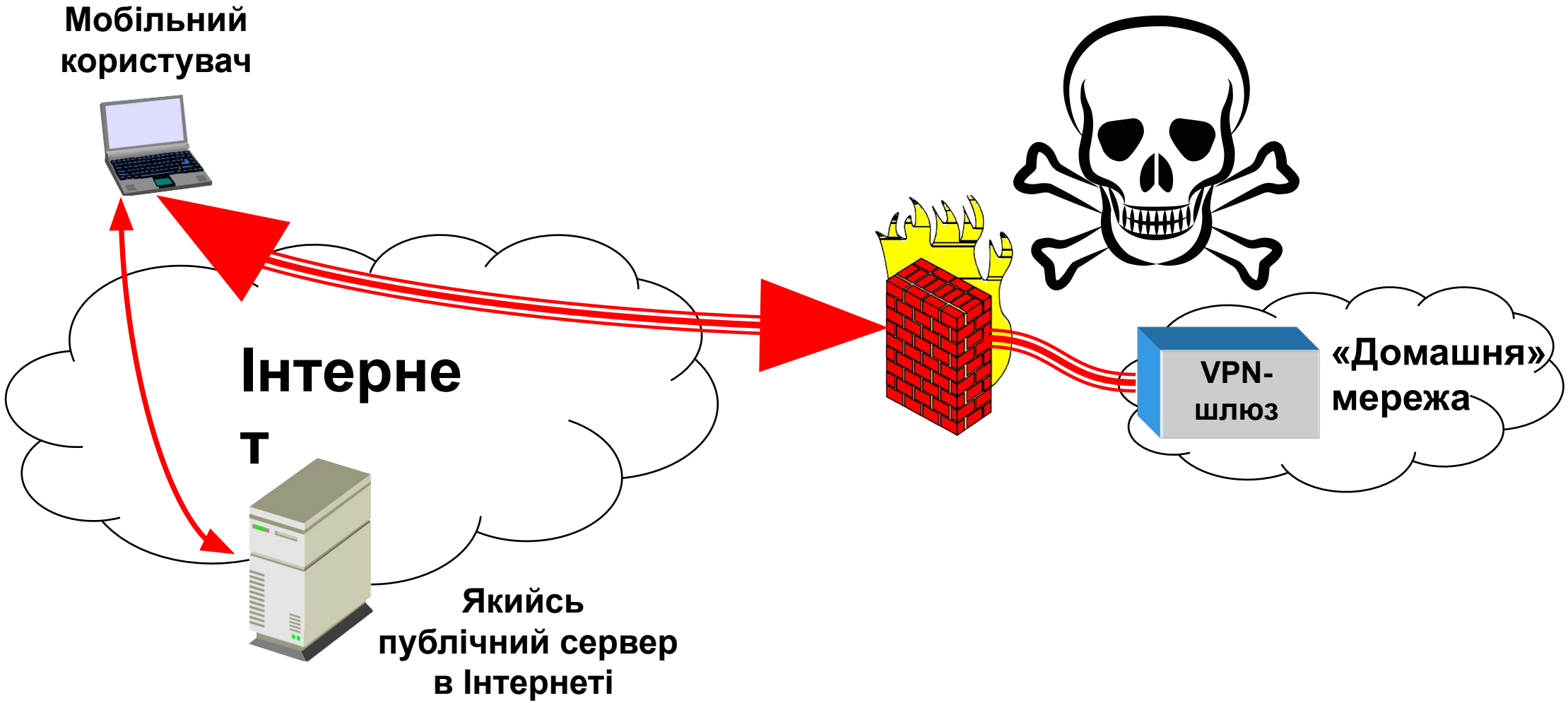
Роздільне тунелювання (дозволене)



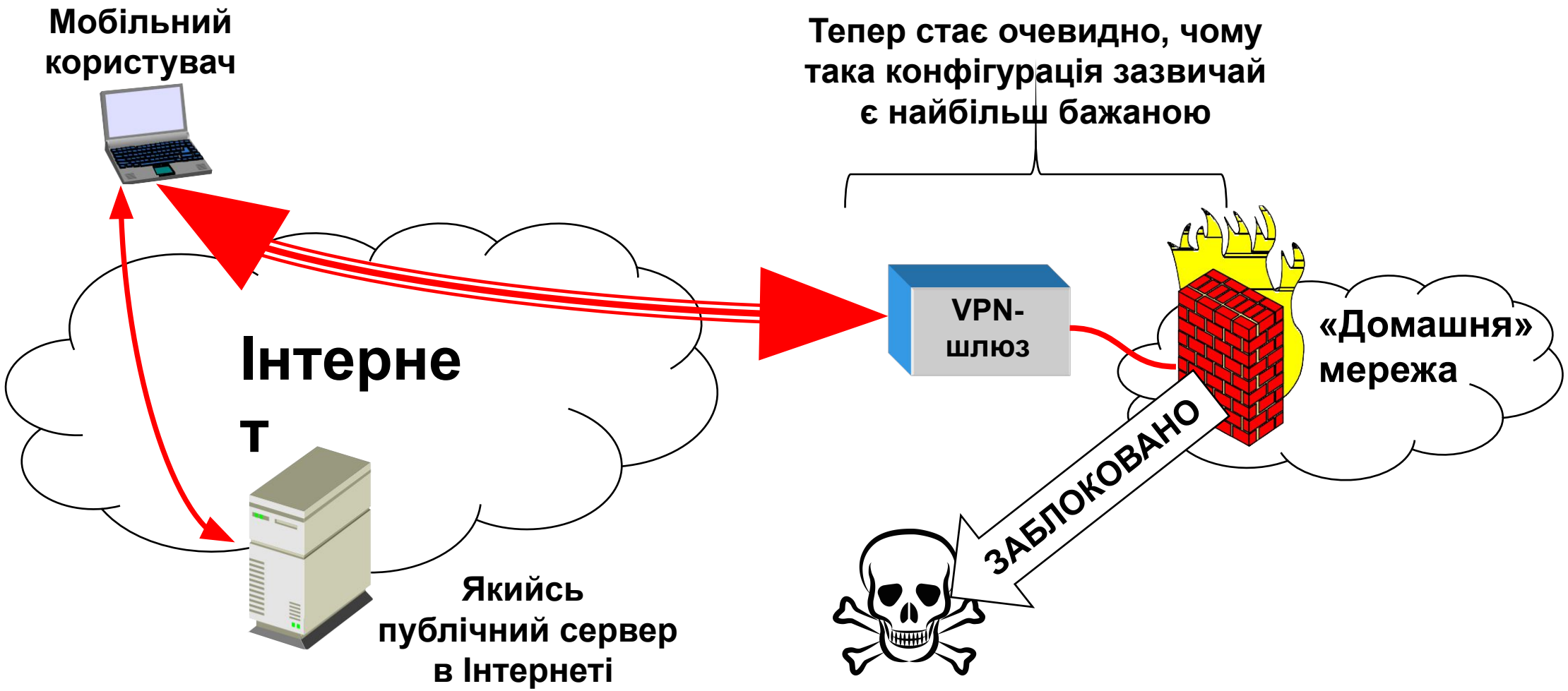
Роздільне тунелювання (дозволене)



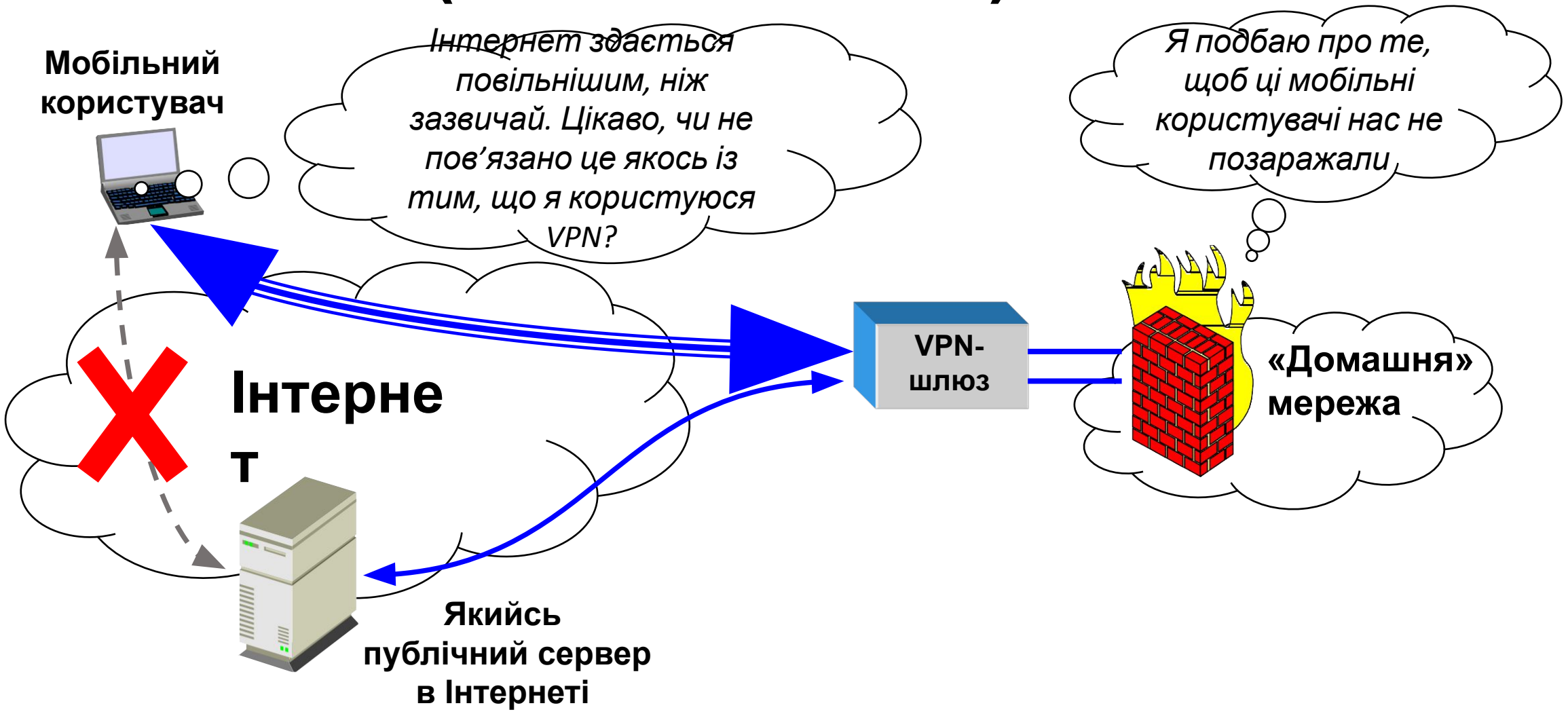
Роздільне тунелювання (дозволене)



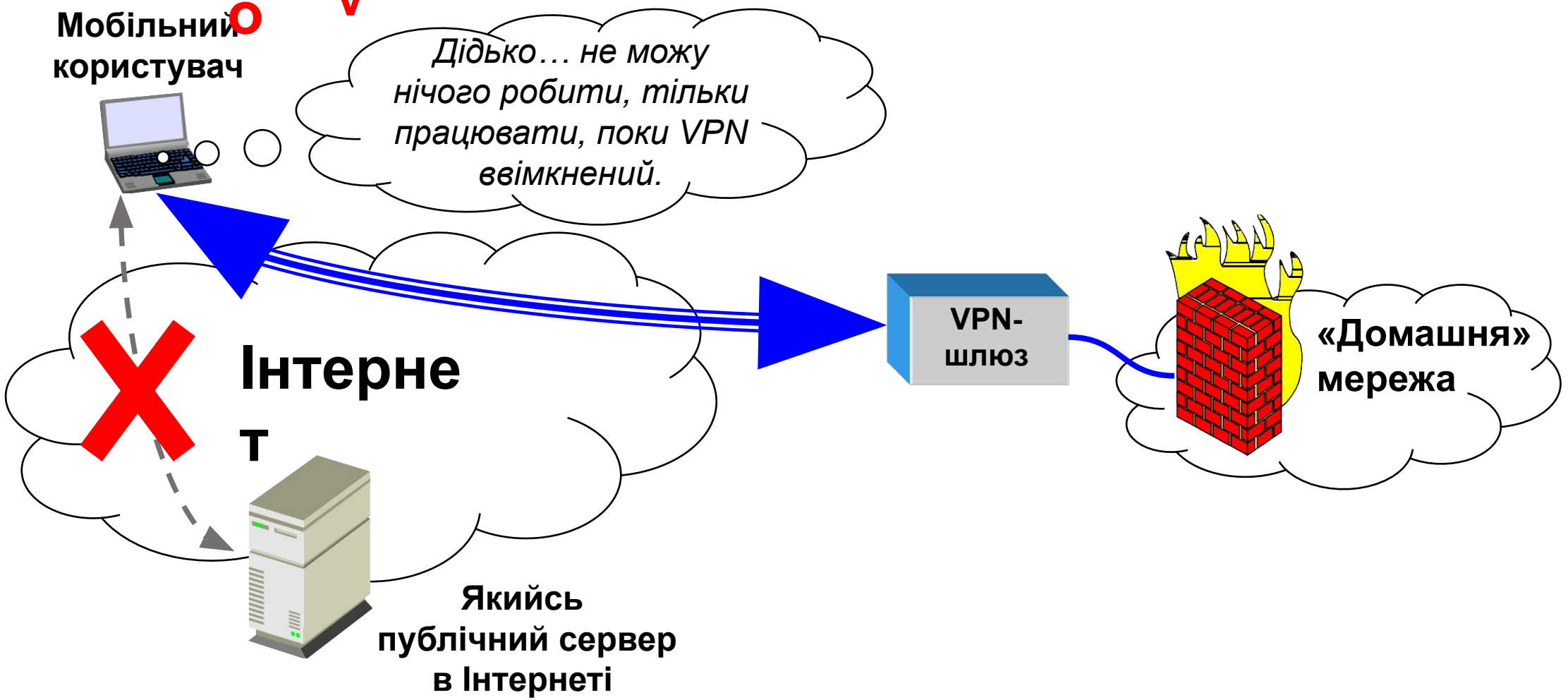
Роздільне тунелювання (дозволене)



Роздільне тунелювання (не дозволене)



Роздільне тунелювання (не дозволене)



Еволюція фільтрування

- Загалом «еволюція» проходила якось так (вгорі старіше, в напрямку вниз новіше):
  - фільтрація пакетів без фіксації стану (тільки рівні 3 і 4);
  - фільтрація пакетів із фіксацією стану (все ще тільки рівні 3 і 4);
  - «інспектування» із фіксацією стану;
  - міжмережевий екран із фільтром на основі проксі (прозорий);
  - міжмережевий екран із фільтром на основі проксі (непрозорий).
- Мірою спускання списком вище
  - зростають витрати та обчислювальне навантаження.

Фільтрація пакетів без фіксації стану

- **Найпростіша форма фільтрації:**
  - **немає потреби в зберіганні _____, що створювало би велике навантаження на пам'ять і процесор;**
  - **немає потреби в перевірці/розумінні широке розмаїття інформації в _____.**
- **Поля заголовків 3-го і 4-го рівнів просто зіставляються з правилами фільтра дозволу/заборони.**
- **Не дуже «оригінально», але дуже дієво, адже відносно просто, а тому добре підходить для грубого фільтрування великих обсягів трафіка («бластер»).**

Статична фільтрація пакетів

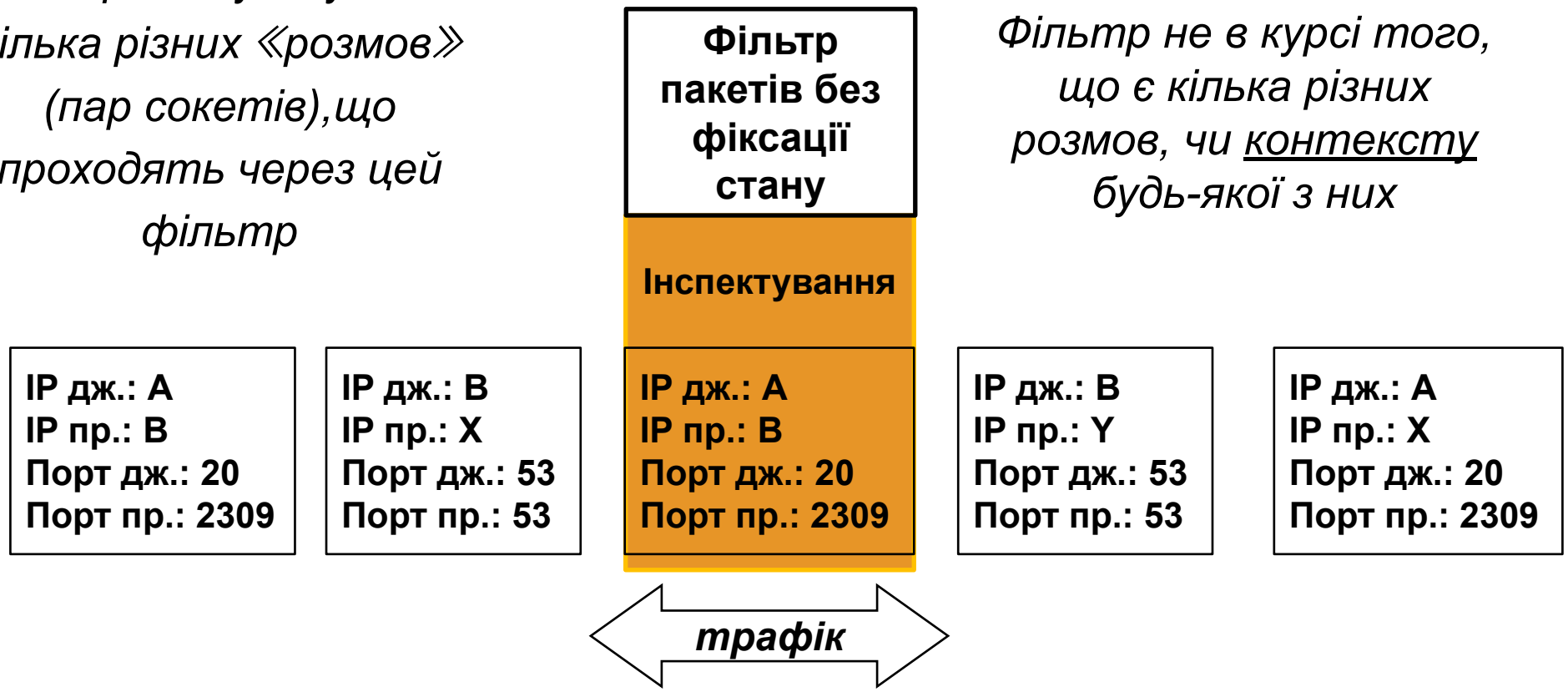
- **Хороші застосування для статичної фільтрації:**
  - **блокування підміни IP-адрес в обох напрямках;**
  - **блокування всього простору приватних IP-адрес (див. RFC 1918);**
  - **блокування всього нерозподіленого простору IP-адрес (див. IANA);**
  - **блокування адреси _____ (127.*.*.*);**
  - **блокування занесених до «чорного списку» доменів (топ-10 з incidents.org);**
  - **контроль напрямку ініціювання сеансу (SYN);**
  - **блокування непотрібного (тобто не пов'язаного з бізнесом) трафіка;**
  - **блокування пакетів, маршрутизованих від джерела;**
  - **блокування перенаправлень ICMP, exo-запитів тощо;**
  - **блокування доступу dogotomypc.com (тощо).**

Фільтрація пакетів із фіксацією стану

- Пристрій «запам'ятовує» попередні пакети, які він бачив, що дає змогу забезпечувати більш інтелектуальну фільтрацію.
- Важлива інформація стосовно пакетів зберігається у таблиці станів чи з'єднань (в ОЗП).
- Звернення до таблиці здійснюється під час прийняття рішення щодо дозволу/заборони для поточного пакета.
- Наслідки з точки зору обчислювального навантаження очевидні.

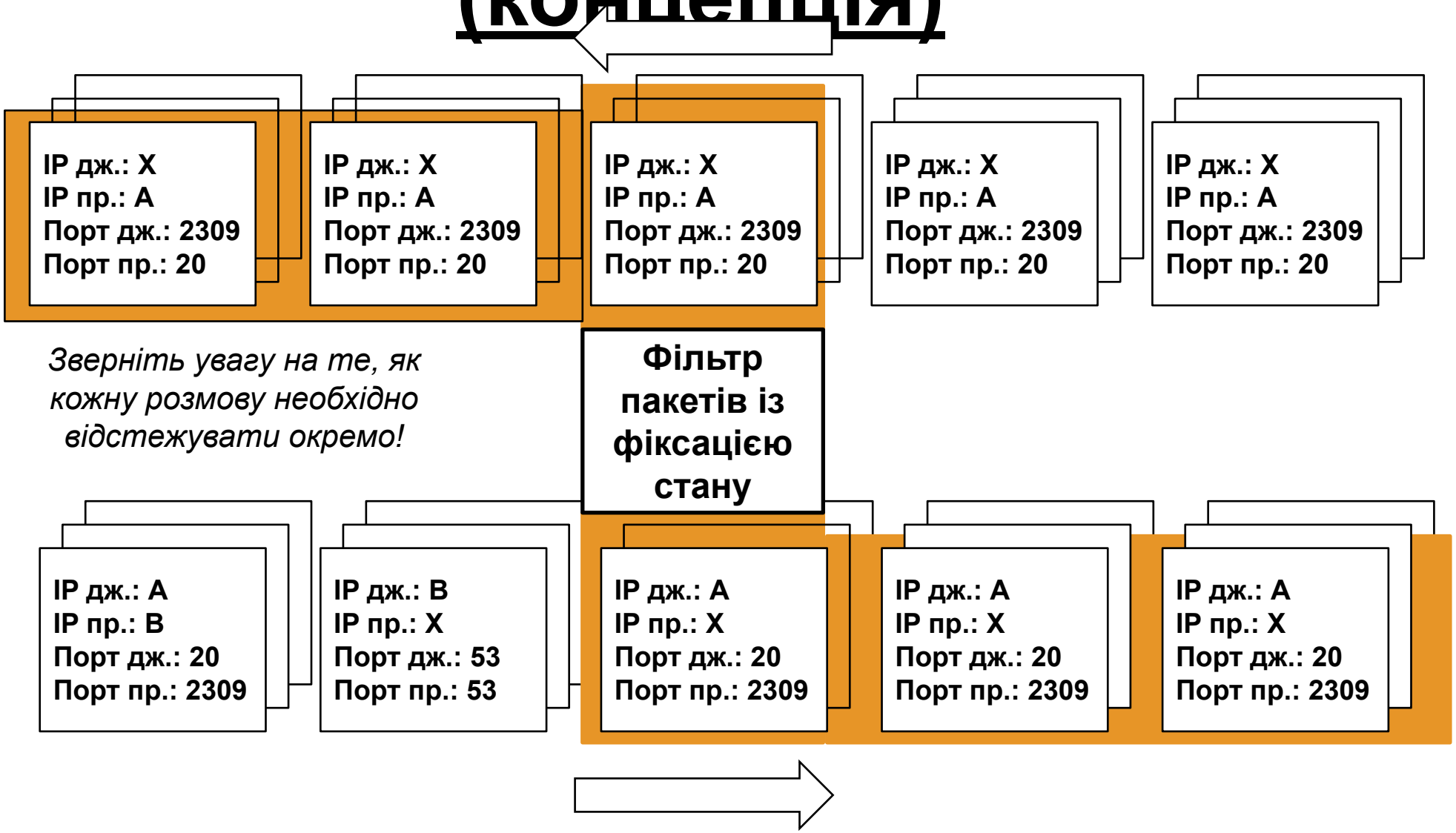
Фільтрація без фіксації стану (концепція)

Зверніть увагу на кілька різних «розмов» (пар сокетів),що проходять через цей фільтр



Фільтр не в курсі того, що є кілька різних розмов, чи контексту будь-якої з них

Фільтрація із фіксацією стану (концепція)

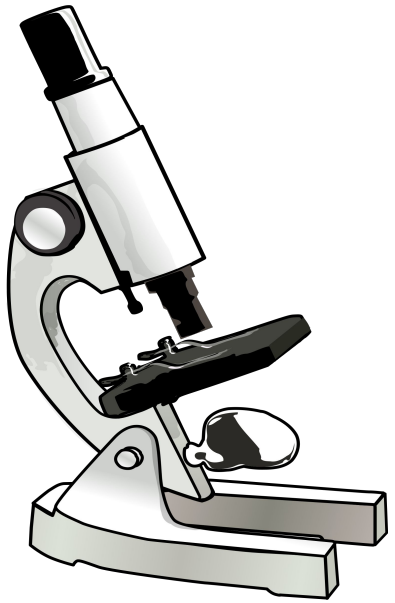


Незнання корисного навантаження

Транспортоване корисне навантаження жодним чином не пов’язане з протоколами, що його транспортують, тож варто остерігатися «брудної гри»

Інспектування із фіксацією стану

- **Інспектування із фіксацією стану означає, що фільтрувальний пристрій дивиться «глибше» в пакет, тобто до самого корисного навантаження** (хоча *dexto* вважає цей термін синонімом старої доброї фільтрації з фіксацією стану).



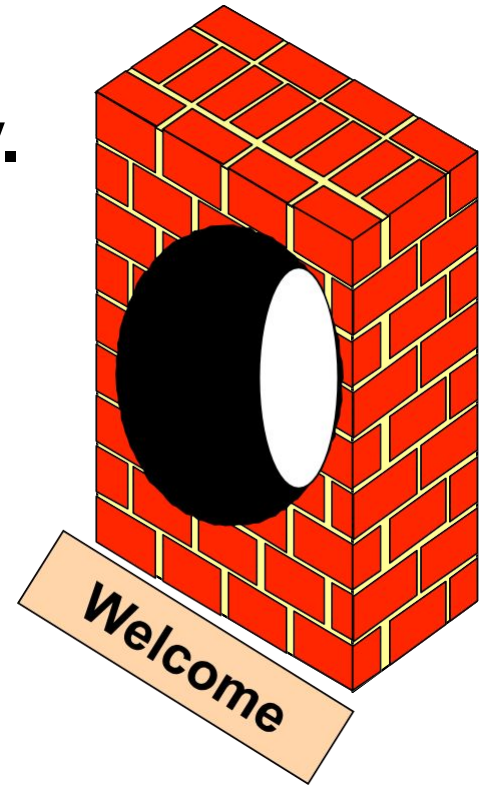
- **Як можна уявити, це зумовлює більше навантаження на пристрій (його процесор/пам'ять), оскільки він повинен розуміти протоколи _____ рівня. Втім, це дає більш «*інтелектуальну*» фільтрацію.**

Інспектування із фіксацією стану

- FTP і його унікальна схильність створювати «подвійні сеанси» представляє простий приклад для розгляду переваг інспекції із фіксацією стану.
- Про проблему безпеки слід згадувати в контексті кожної версії FTP:
  - активний FTP: міжмережевий екран на боці клієнта повинен відкрити всі порти > 1023 для сеансу обміну даними, ініційованого сервером;
  - пасивний FTP: міжмережевий екран на боці сервера повинен відкрити всі порти > 1023 для сеансу обміну даними, ініційованого клієнтом.

Інспектування із фіксацією стану

- Поміркуйте про значення безпеки «периметра». Чого ви загалом прагнете?
  - Якомога менше точок входу/виходу.
  - Якомога менші точки входу/виходу.
- Тобто великі діри (наприклад, будь-які порти чи gt 1023) є менш бажаними.
- Розглянемо, як інспектування» із фіксацією стану може допомогти.



Приклад інспектування із фіксацією стану

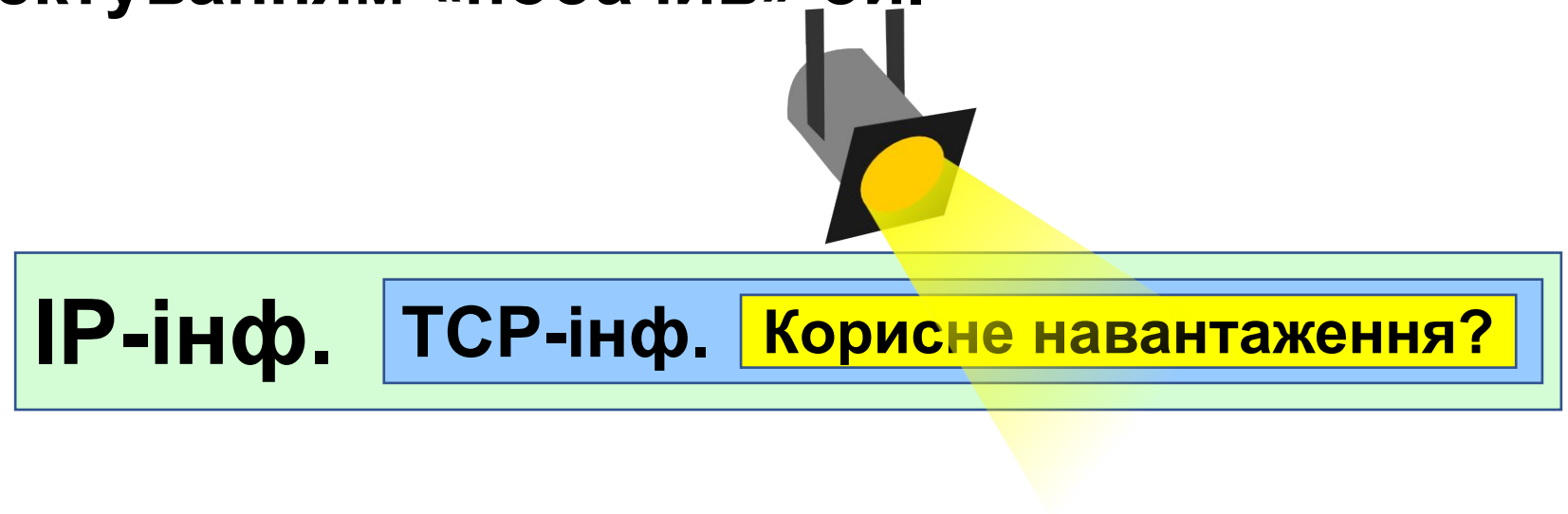
1	136.84.111.13.1118 > 207.46.133.140.21: P ack
2	207.46.133.140.21 > 136.84.111.13.1118: P ack
3	136.84.111.13.1118 > 207.46.133.140.21: P ack
4	207.46.133.140.21 > 136.84.111.13.1118: P ack
5	136.84.111.13.1120 > 207.46.133.140.3880: S
6	207.46.133.140.3880 > 136.84.111.13.1120: S ack
7	136.84.111.13.1120 > 207.46.133.140.3880: ack

Що відбувається?_____

_____

Приклад інспектування із фіксацією стану

- Звідки береться інформація порту 3880?
  _____
- Чи знав би про це міжмережевий екран без інспектування? _____
- **Нумо проллємо трохи світла на корисне навантаження пакета 4, щоб зрозуміти, що міжмережевий екран із інспектуванням «побачив» би.**



Приклад інспектування із фіксацією стану

Джерело: 207.46.133.140 (207.46.133.140)

Призначення: 127.84.111.13 (127.84.111.13)

Порт джерела: 21 (21)

Порт призначення: 1118 (1118)

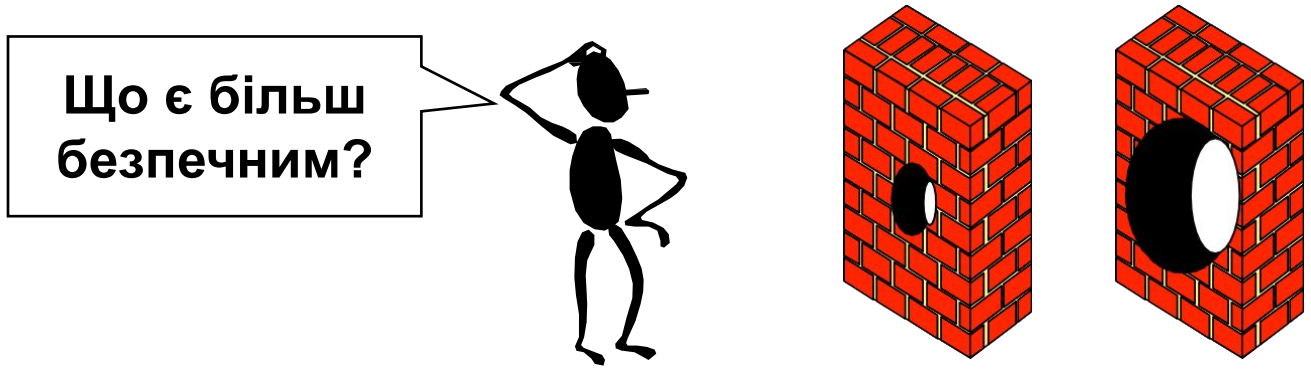
Прапорці: 0x0018 (PSH, ACK)

Tcpdump показує:
- інформацію заголовка;
- вихідний вміст всього пакета в шістнадцятковому поданні;
- представлення шістнадцяткових даних в ASCII-поданні.

```
0  0002 2d09 9610 0080 c8be 6d58 0800 4500    ..-.......mX..E.
10 005b 7e12 4000 3106 51aa cf2e 858c c0a8    .[~.@.1.Q.......
20 647d 0015 045e 94e2 78b1 003f e23c 5018    d}...^..x..?.<p.
30 4420 498c 0000 3232 3720 456e 7465 7269    D I...227 Enteri
40 6e67 2050 6173 7369 7665 204d 6f64 6520    ng Passive Mode
50 2832 3037 2c34 362c 3133 332c 3134 302c    (207,46,133,140,
60 3135 2c34 3029 2e0d 0a33                   15,40)...3
```

Приклад інспектування із фіксацією стану

- Запам’ятайте формат видачі IP-адреси та порту для FTP-трансакції: X,X,X,X,P_1,P_0, де:
  - X.X.X.X — IP-адреса (в десятковому поданні з крапками);
  - P1 × 256 + P_0 = № порту (десятковий).
- На попередньому слайді міжмережевий екран із інспектуванням побачив би 15 і 40 і збагнув би, що потрібно динамічно відкрити порт 3880 — і ТІЛЬКИ порт 3880!



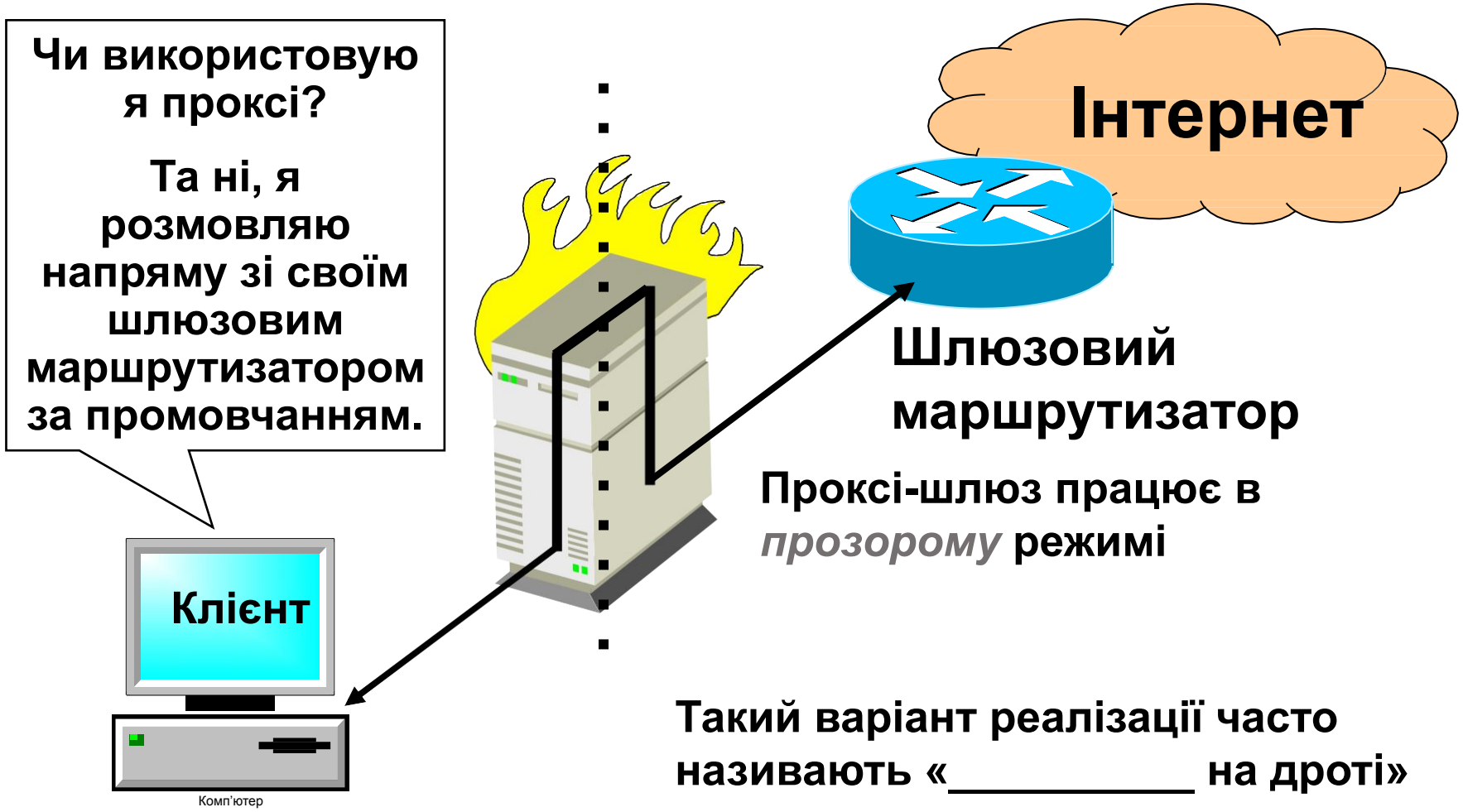
Проксі-фільтри

- **Називаються проксі-серверами, проксі-шлюзами та (іноді) серверами пересилки.**
- **По суті це інспектування із фіксацією стану — з тієї точки зору, що вони в курсі прикладного рівня та враховують інформацію в корисному навантаженні під час прийняття рішення щодо дозволу/заборони.**
- **Проксі відрізняються від фільтрів інспектування із фіксацією стану кількома фундаментальними рисами; наприклад, проксі:**
  - **забезпечують більш ретельну _____;**
  - **здійснюють менше дій дозволу/заборони, аніж**
  - **дій «_____»;**
  - **в певному сенсі відіграють роль _____ серверів.**

Прозорість

- **Прозорість (або її відсутність) з точки зору клієнта під захистом:**
- **Прозорий проксі:**
  - **клієнт не потребує жодної спеціальної конфігурації для використання проксі-фільтра, тобто йому навіть не потрібно знати, що він є;**
- **непрозорий проксі:**
  - **клієнт повинен бути спеціально сконфігурованим для перенаправлення всього трафіка на єдиний порт проксі;**
  - **це здійснюється за допомогою програмам, що виявляють присутність проксі, чи встановлення спеціального програмного клієнта.**

Прозорий шлюз



Шлюзовий маршрутизатор

Проксі-шлюз працює в *прозорому* режимі

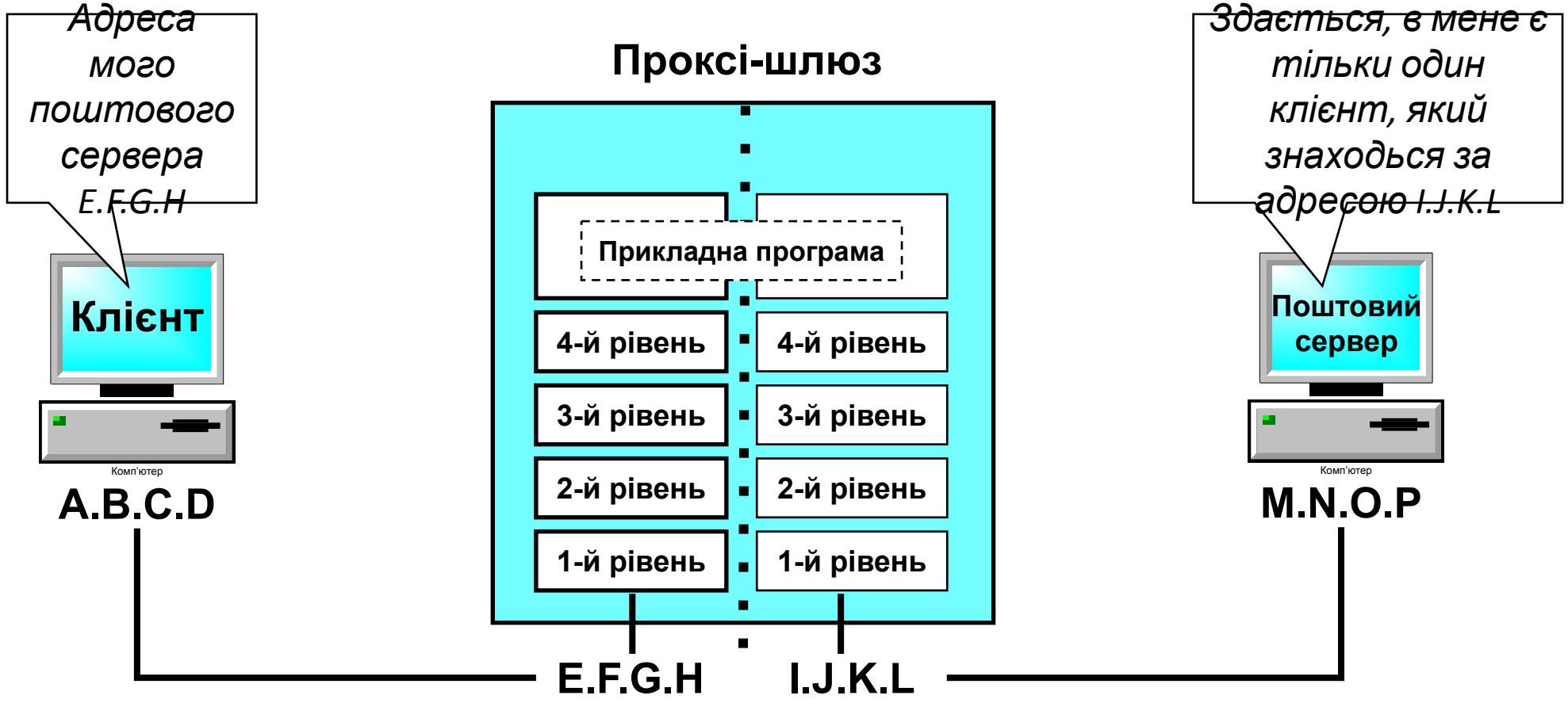
Такий варіант реалізації часто називають «_____ на дроті»

Непрозорий

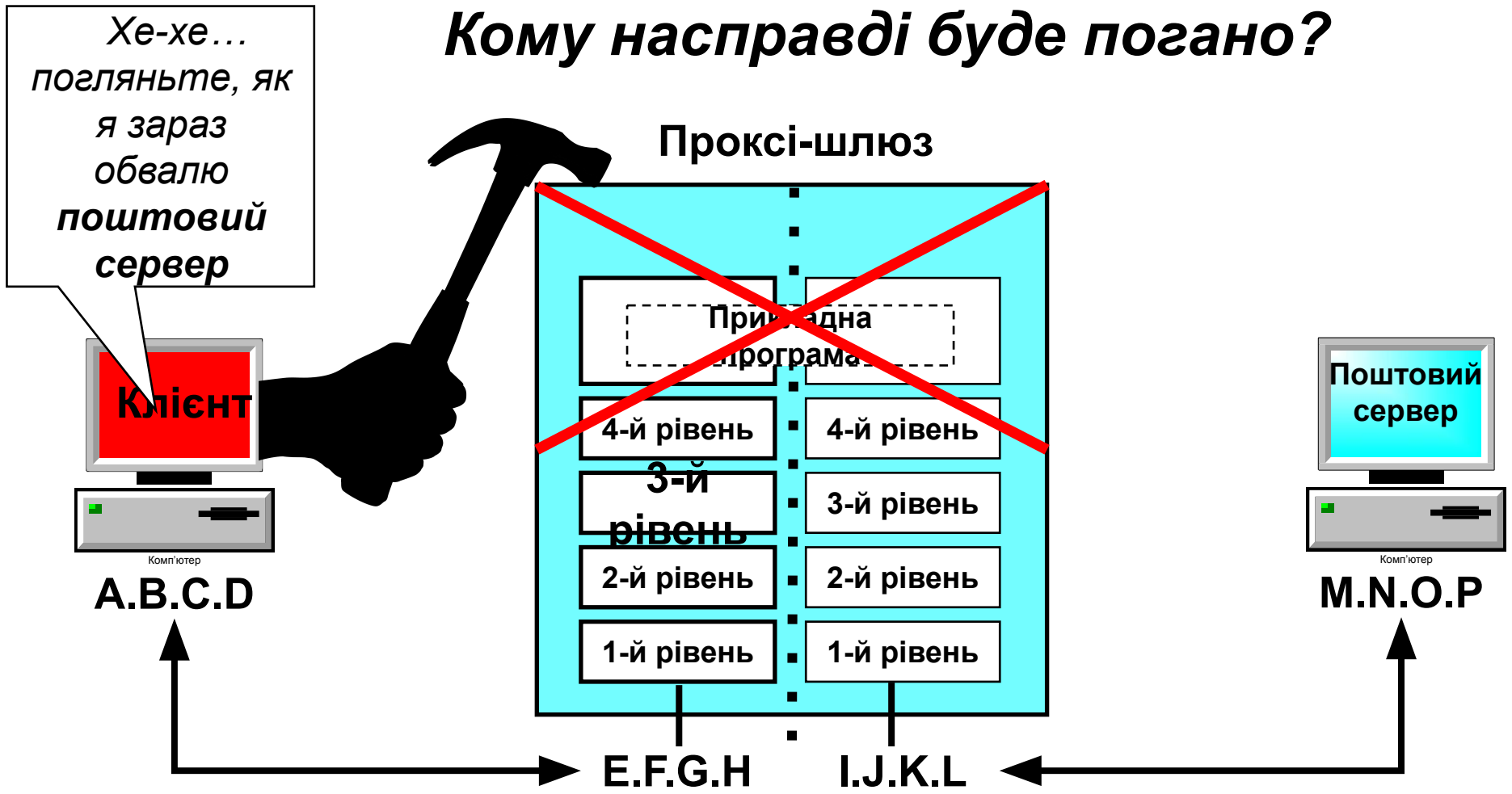
- **Непрозорий проксі, вочевидь, набагато складніше налаштувати, але він забезпечить набагато вищу захищеність, наприклад:**
  - **клієнтам більше не потрібно мати таблиці маршрутизації;**
  - **весь клієнтський трафік може бути «тунельований» через призначений порт проксі чи порт, який прослуховує мережу;**
- **приклад реалізації — протокол SOCKS:**
  - **весь клієнтський трафік «тунелюється» через TCP-порт 1080 або 8080;**
  - **робить прослуховування трафіка складнішим;**
  - **може також передбачати шифрування, утворюючи міні-VPN.**

Проксі як ізолятор

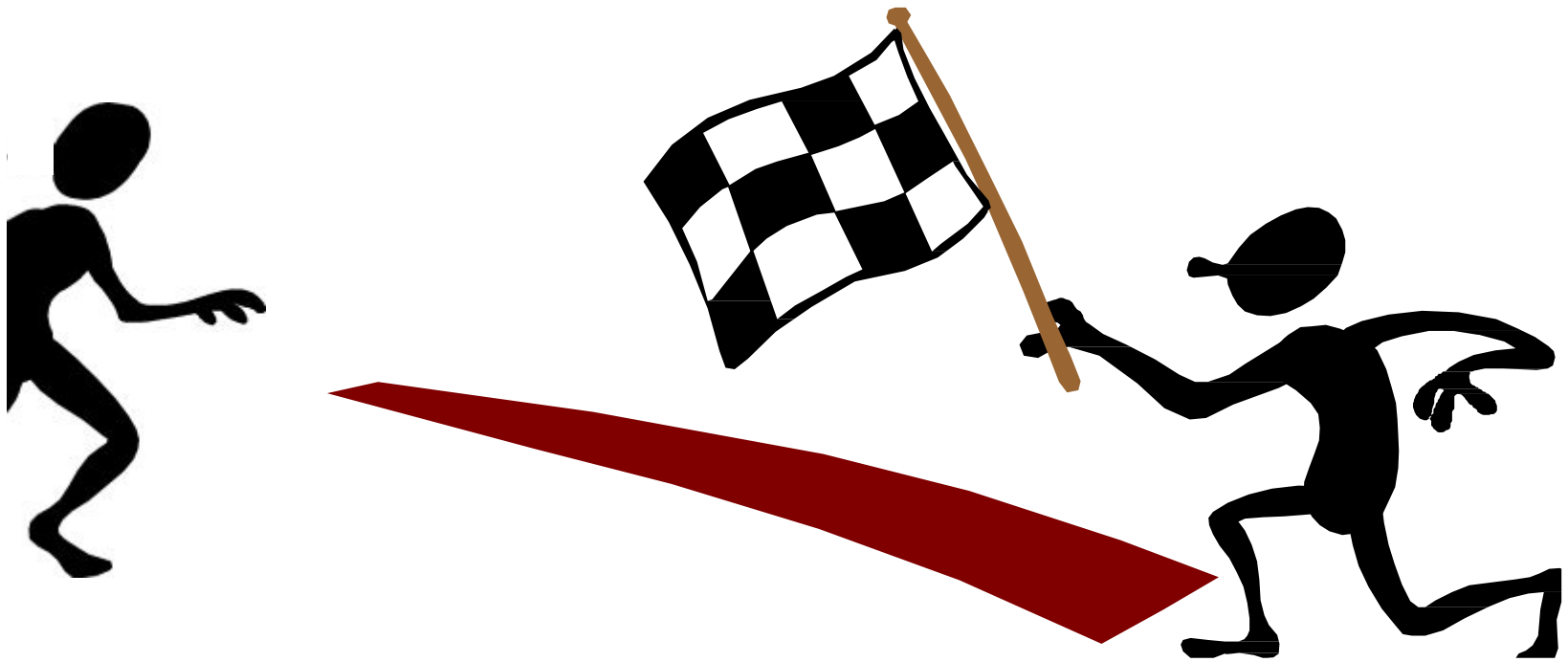
- **Чи він прозорий, чи непрозорий? _____.**



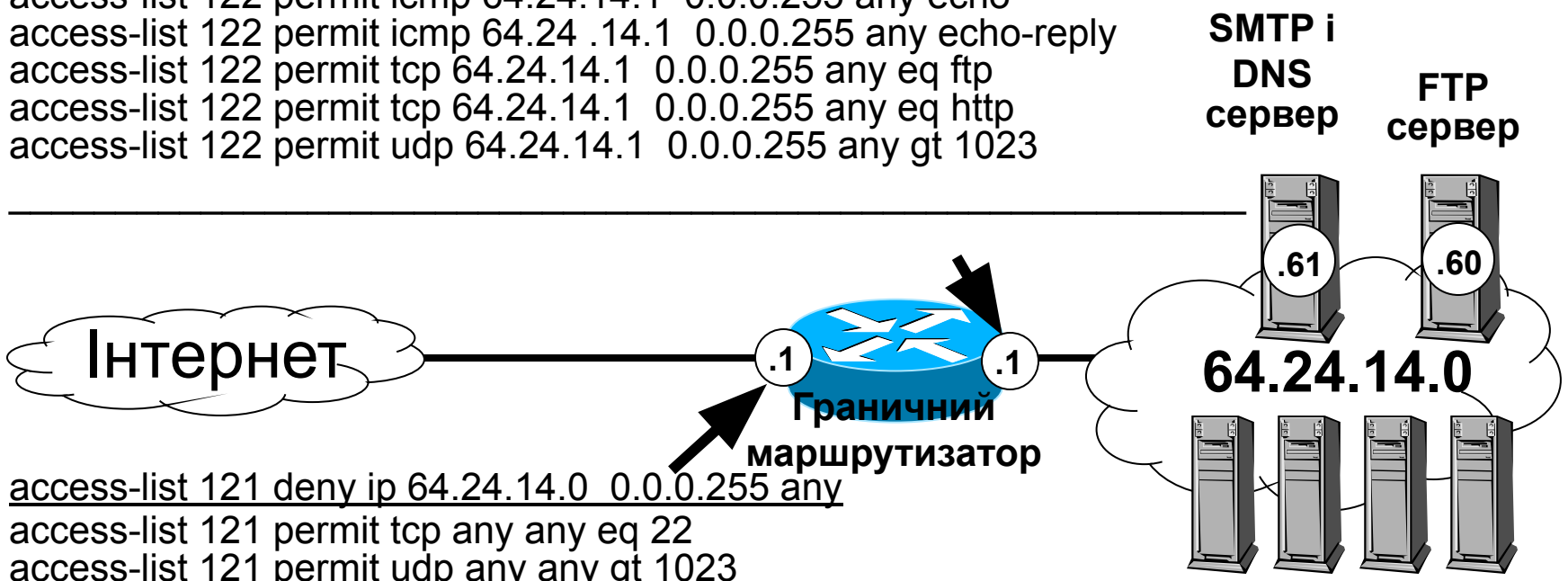
Проксі як «жертовний» сервер



Кінець



```
1  access-list 122 permit tcp 64.24.14.1  0.0.0.255 any eq 22
2  access-list 122 permit udp 64.24.14.1  0.0.0.255 any eq domain
3  access-list 122 permit icmp 64.24.14.1  0.0.0.255 any echo
4  access-list 122 permit icmp 64.24 .14.1  0.0.0.255 any echo-reply
5  access-list 122 permit tcp 64.24.14.1  0.0.0.255 any eq ftp
6  access-list 122 permit tcp 64.24.14.1  0.0.0.255 any eq http
7  access-list 122 permit udp 64.24.14.1  0.0.0.255 any gt 1023
7a ----------------------------------------------------------------
```




```
8  access-list 121 deny ip 64.24.14.0  0.0.0.255 any
9  access-list 121 permit tcp any any eq 22
10 access-list 121 permit udp any any gt 1023
11 access-list 121 permit tcp any any gt 1023 established
12 access-list 121 permit icmp any any echo-reply
13 access-list 121 permit icmp any any unreachable
14 access-list 121 permit icmp any any admin-prohibited
15 access-list 121 permit icmp any any time-exceeded
16 access-list 121 permit icmp any any packet-too-big
17 access-list 121 permit tcp any  host 64.24.14.60 eq ftp
18 access-list 121 permit tcp any  host 64.24.14.61 eq smtp
19 access-list 121 permit tcp any  host 64.24.14.61 eq domain
20 access-list 121 permit udp any host 64.24.14.61 eq domain
```

ip access-group 121 in
команда, що видається зовнішньому інтерфейсу маршрутизатора

ip access-group 122 in
команда, що видається внутрішньому інтерфейсу маршрутизатора

Пояснення/мета правил

1. Дозволяти вихідні _____-сеанси в напрямку Інтернету;
2. дозволяти _____-запити в напрямку Інтернету;
3. дозволяти _____ в напрямку Інтернету;
4. дозволяти відповіді на пінг-запити з Інтернету;
5. дозволяти ініціювання FTP-сеансів у напрямку Інтернету (зауважимо, що це стосується тільки порту 21 (FTP), додати також слід порт 20 (дані FTP), відсутній цьому прикладі);
6. дозволяти ініціювання _____-сеансів з Інтернету;
7. дозволяти _____;

7a. дозволяти TCP-трафік у відповідь на ініційований <u>ззовні</u> TCP-трафік (тобто SMTP, FTP і DNS);

8. запобігати надходженню _____;
9. дозволяти вхідні _____-сеанси з Інтернету;
10. дозволяти вхідні _____-відповіді;

Пояснення/мета правил

11. дозволяти _____-трафік у відповідь на ініційований зсередини трафік;
12. дозволяти відповіді на _____;
13. показувати повідомлення про недосяжність (хоста чи порту);
14. дозволяти сповіщення щодо повідомлень про фільтрацію трафіку;
15. дозволяти сповіщення про TTL = 0 і втрачені фрагменти;
16. дозволяти сповіщення про запити на фрагментування;
17. дозволяти вхідний FTP-трафік до нашого FTP-сервера;
18. дозволяти вхідним поштовим повідомленням надходити на наш SMTP-сервер;
19. дозволяти передачі DNS-_____ на наш DNS-сервер;
20. дозволяти Інтернет-клієнтам отримувати визначення імен від нашого DNS-сервера.