

Лекція 3. Класифікація firewall-ів і визначення політики firewall-у

1.1. Модель OSI.

1.2. Особливості протоколів, що використовуються в локальних і глобальних мережах.

1.3. Класифікація фільтрів.

1.4. Трансляція мережних адресів (NAT).

2. Різні типи середовищ навколо firewall-у

2.1. Принципи побудови оточуючого firewall середовища.

2.2. DMZ-мережі .

2.3. Віртуальні приватні мережі (VPN) .

2.4. Інтранет та екстранет.

2.5. Розміщення серверів в DMZ-мережах.

2.6. Політика безпеки firewall-у.

2.7. Адміністрування firewall-у.

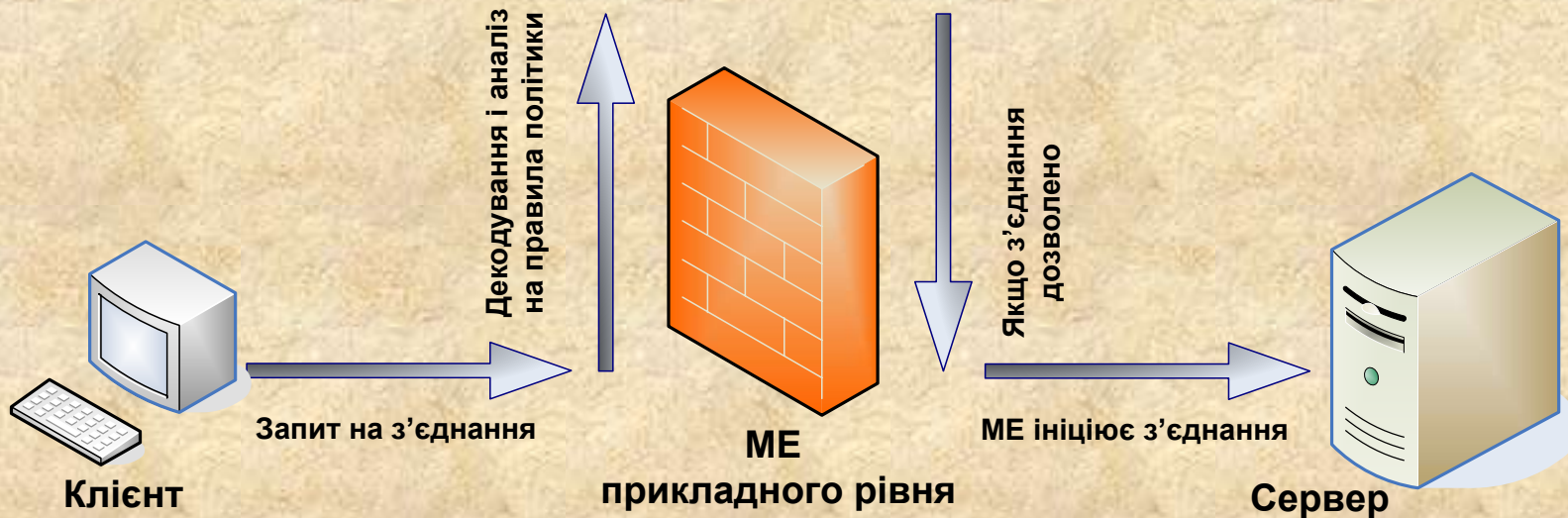
*Firewall'и **призначені** для захисту комп'ютерів і мереж від спроб несанкціонованого доступу з використанням вразливостей в сукупності протоколів TCP/IP.*



Існують різні **типи** firewall'ів:

- *пакетні фільтри*, вбудовані в пограничні роутери які можуть забезпечити управління доступом для IP-пакетів)
- *firewall'и*, які можуть перекривати вразливості на різних рівнях сукупності протоколів TCP/IP
- *firewall'и*, які можуть фільтрувати потік інформації і аналізувати вміст пакетів.

Аналіз пакету на відповідність політиці безпеки.
Якщо пакет дозволений – передається на сервер



Технологічні можливості *firewall*'ів

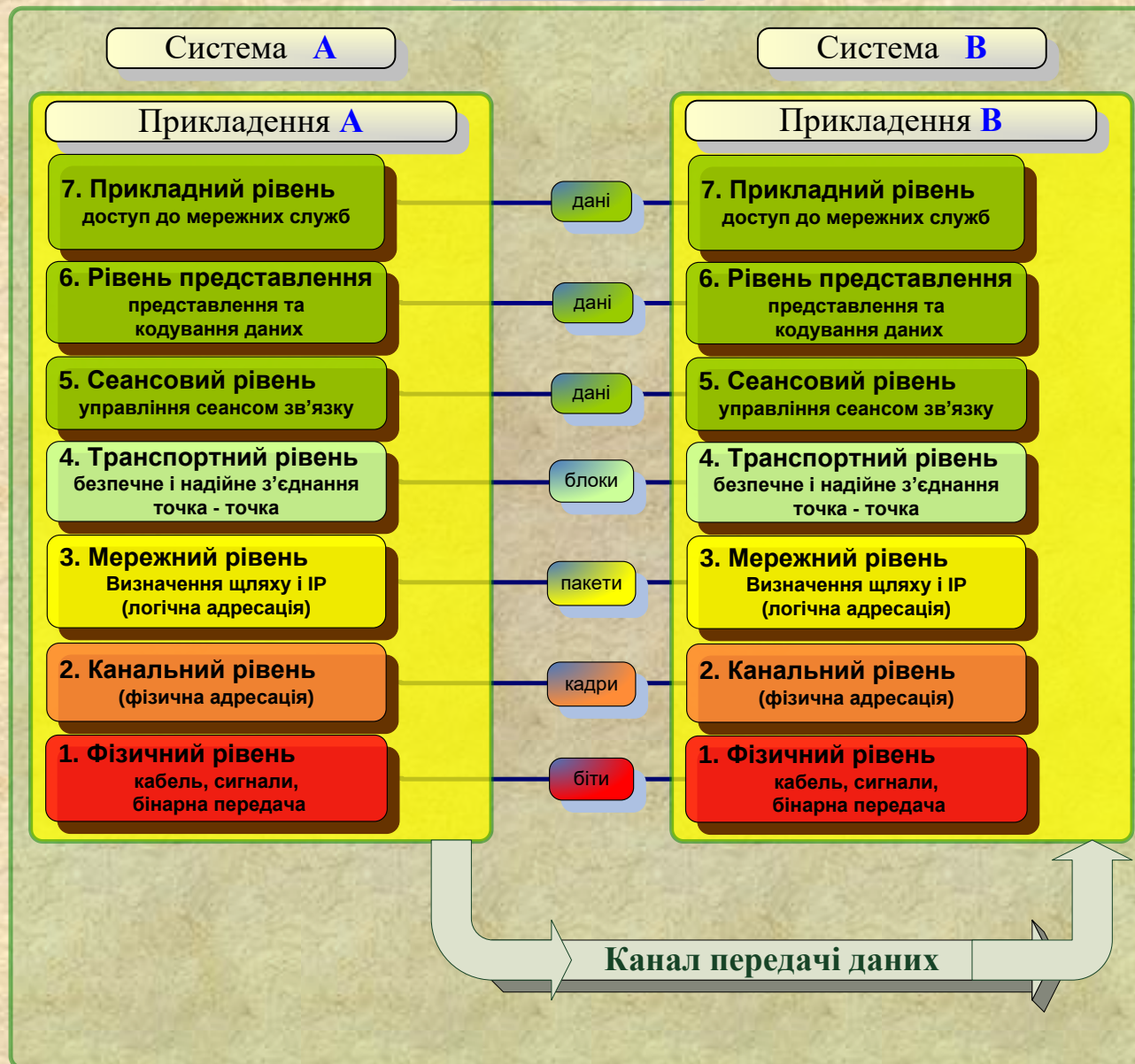
сучасні *firewall*'и працюють у сукупності з системами виявлення вторгнень і сканерами змісту e-mail або web з метою виявлення вірусів або небезпечного коду.

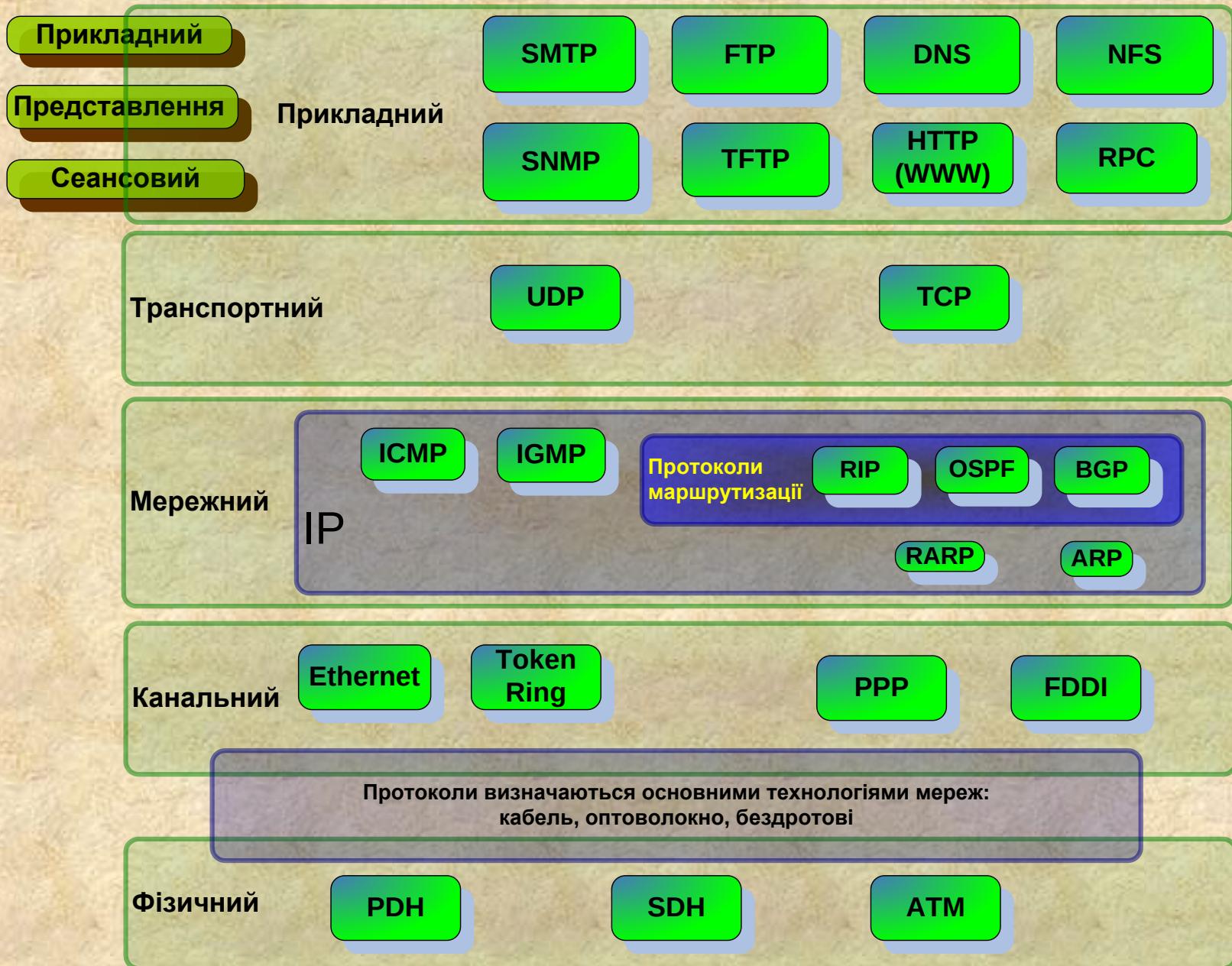
firewall не забезпечує повного захисту від усіх проблем, породжених Інтернетом і є однією частиною архітектури ІБ.

Основні поняття, пов'язані з *firewall*'ами є

- модель OSI і на яких рівнях функціонують різні типи *firewall*'ів (*пакетні фільтри*, *stateful inspection firewall*'и і прикладні проксі).
- політика *firewall*'а і сукупність правил (принципи, якими користуються при адмініструванні і конфігурації політики *firewall*'у)
- причини вибору, того чи іншого фільтра
- розгортання і управління *firewall*'ом
- функціональне оточення *firewall*'у
- різні топології мереж з використанням *firewall*'ів.
- додаткові функції сучасних *firewall*'ів
 - використання в якості точок під'єднання VPN,
 - трансляція IP-адресов,
 - фільтрація вмісту web або e-mail.

Модель OSI

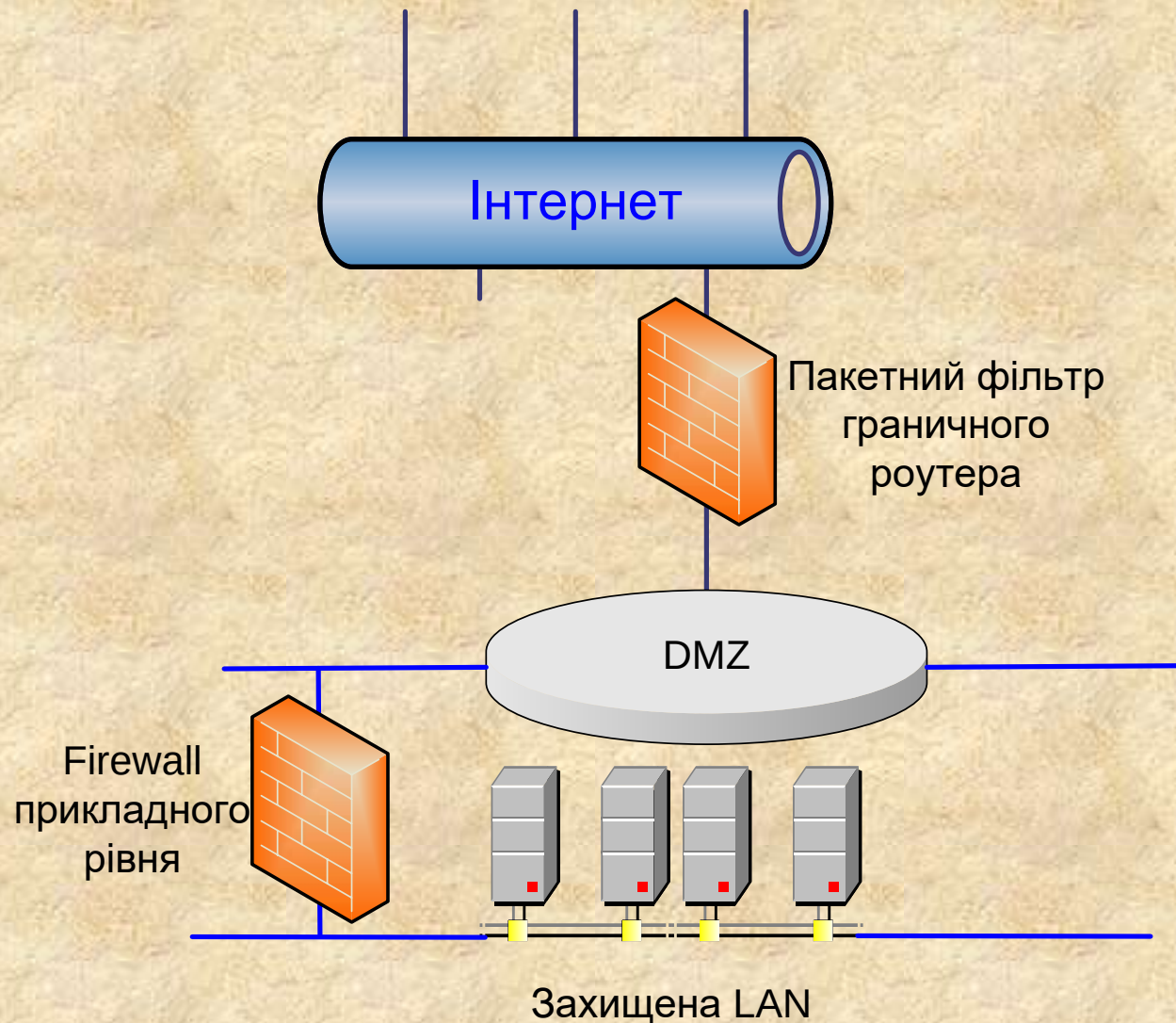






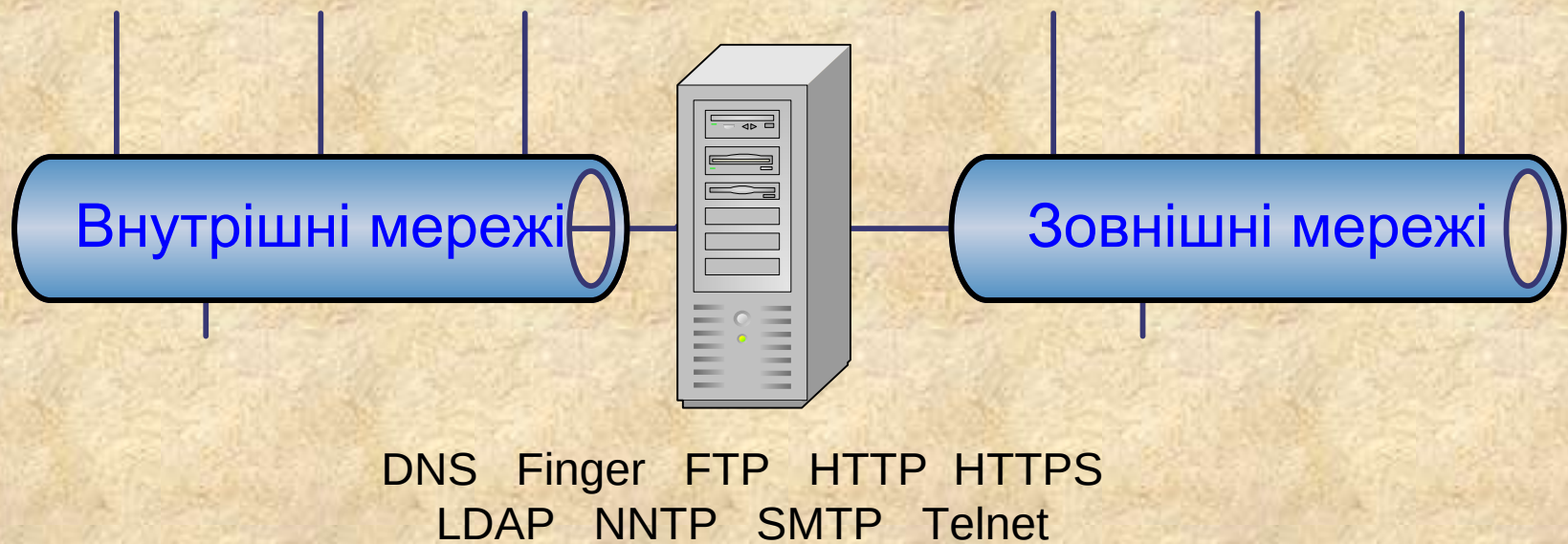
Співвідношення рівнів стеку протоколів Інтернету і адресів

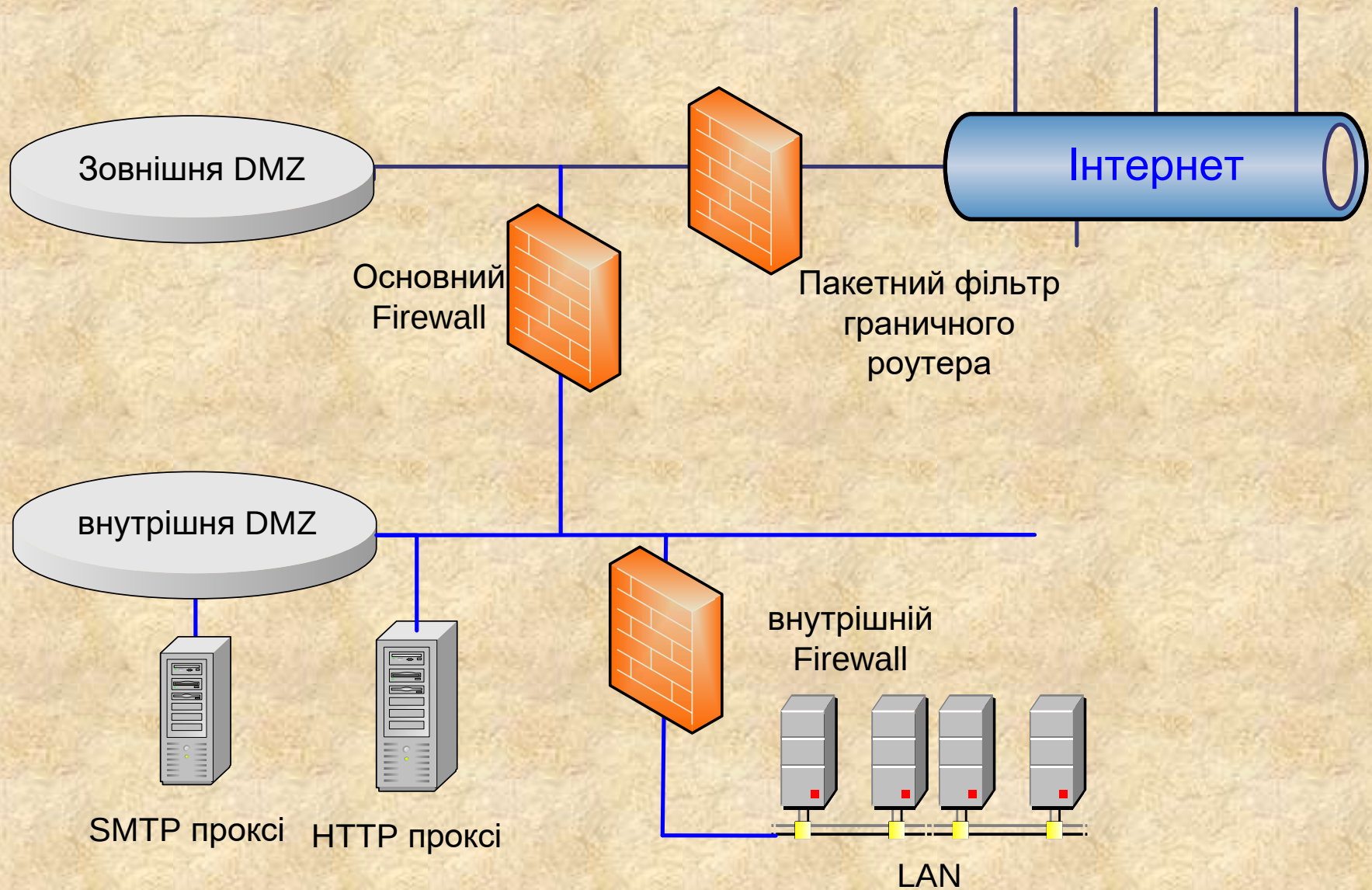




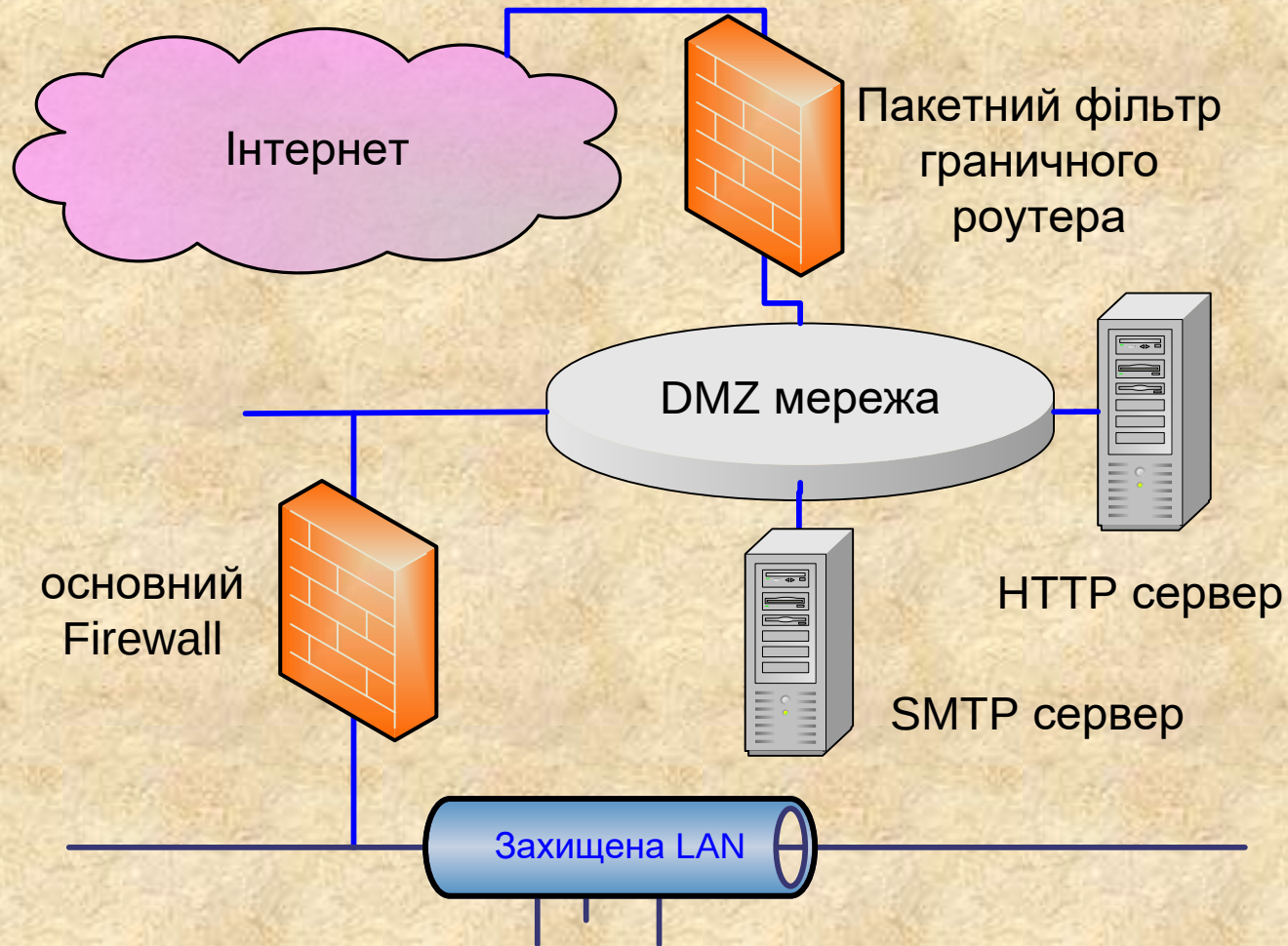
Сукупність правил пакетного фільтра

	Адрес відправника	Порт відправника	Адрес призначення	Порт призначення	Дія	Опис
1	Any	Any	192.168.1.0 (робоча станція)	>1023	Allow	Правило дозволяє повертати TCP-з'єднання у внутрішню мережу, тобто користувачі внутрішньої мережі можуть виходити в Інтернет
2	192.168.1.1 (пакетний фільтр)	Any	Any	Any	Deny	Захищає сам <i>пакетний фільтр</i> від безпосереднього з'єднання з будь-ким
3	Any	Any	192.168.1.1	Any	Deny	Запобігає безпосередній доступ усіх користувачів до пакетного фільтра
4	192.168.1.0	Any	Any	Any	Allow	Внутрішні користувачі можуть мати доступ до зовнішніх серверів
5	Any	Any	192.168.1.2 (SMTP-сервер)	SMTP	Allow	Дозволяє усім (і зовнішнім і внутрішнім) користувачам надсилати e-mail для внутрішніх користувачів
6	Any	Any	192.168.1.3 (HTTP-сервер)	HTTP	Allow	Дозволяє зовнішнім користувачам доступ до WWW-сервера
7	Any	Any	Any	Any	Deny	"Заборонити все": правило – все, що не дозволено, то заборонено

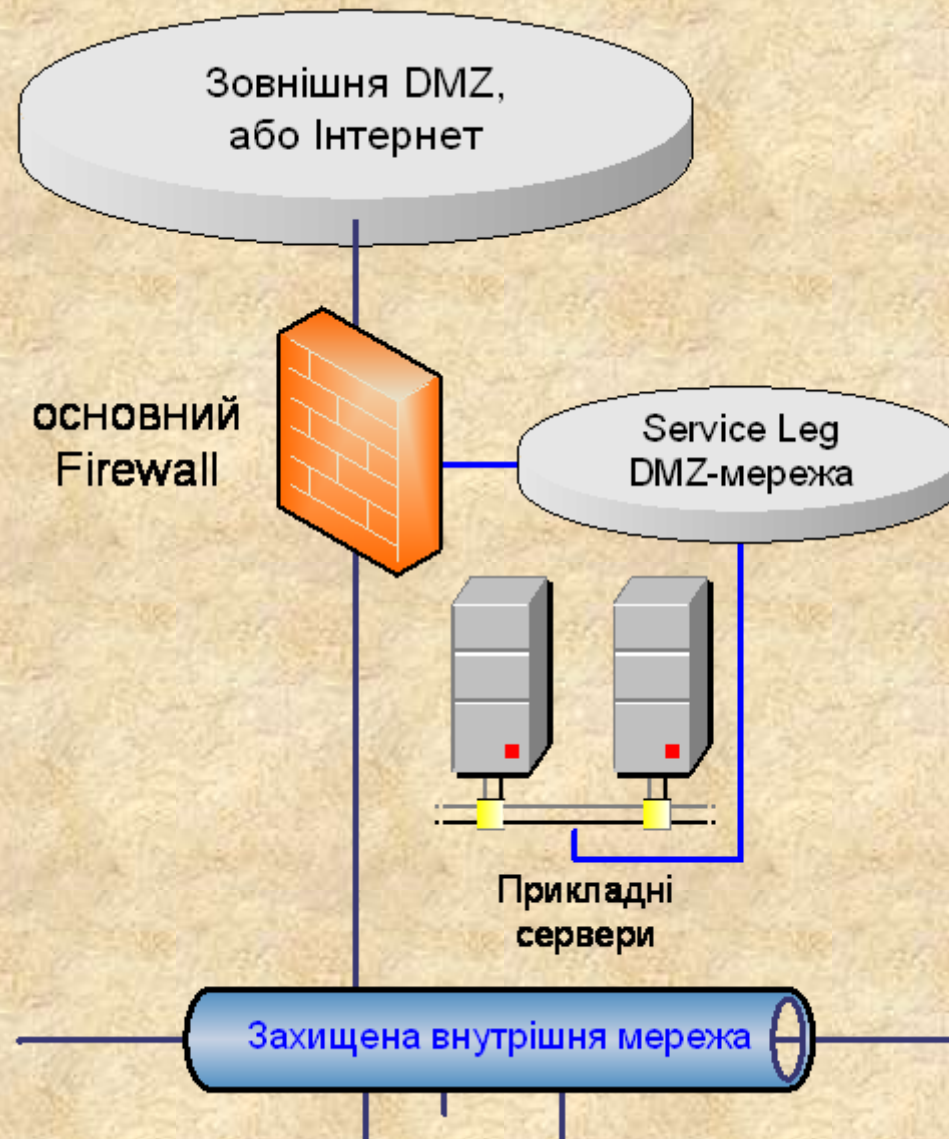




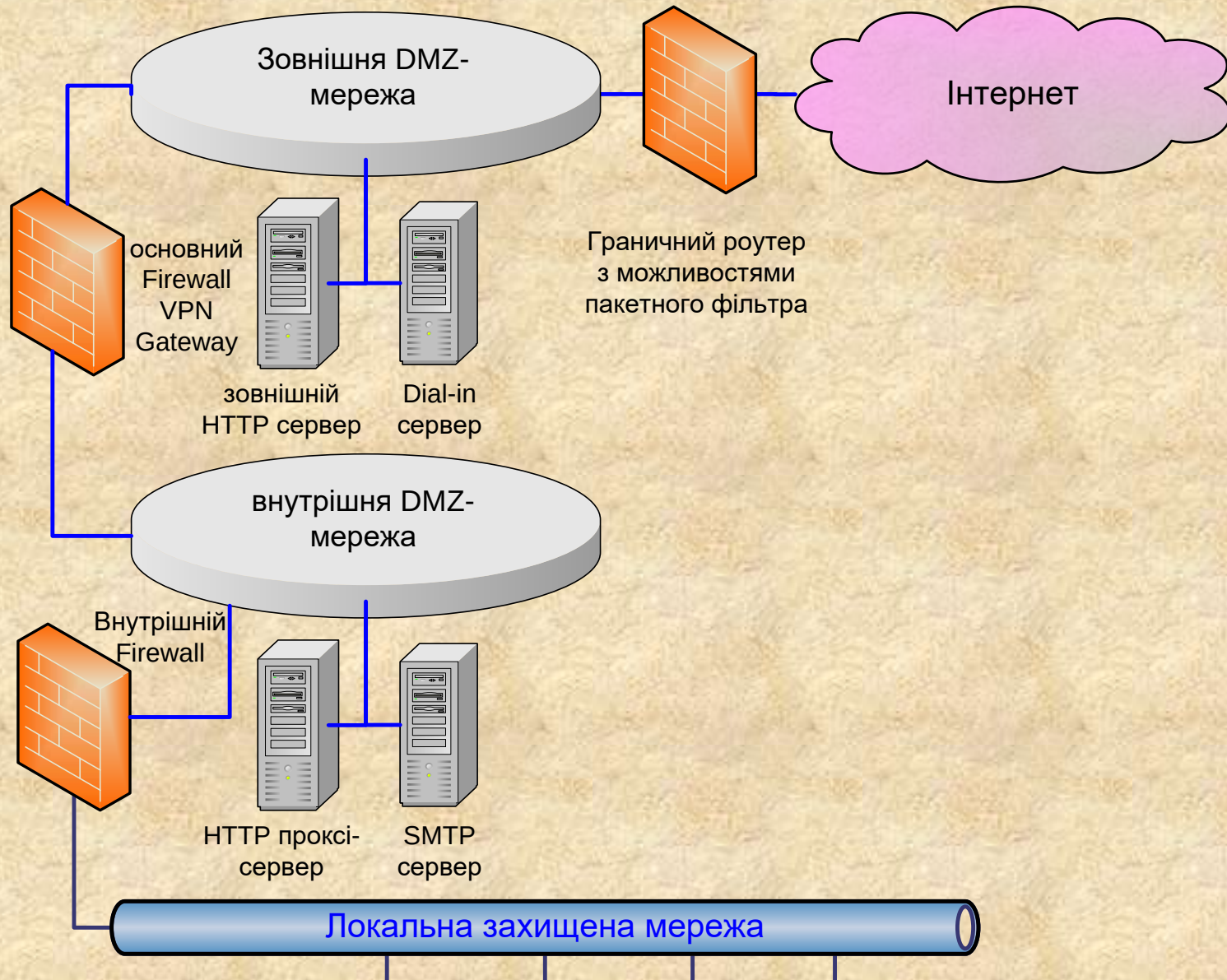




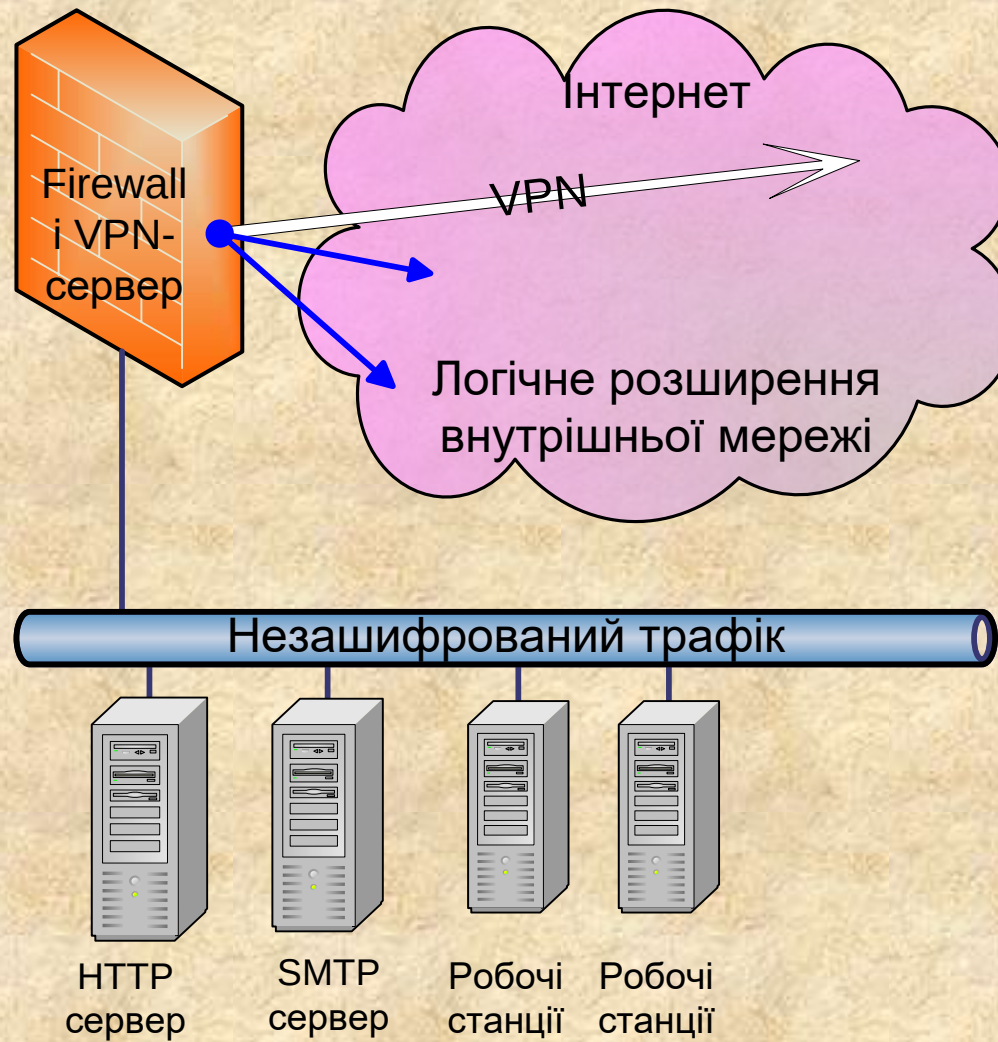
Приклад мережі з firewall-ом і однією DMZ



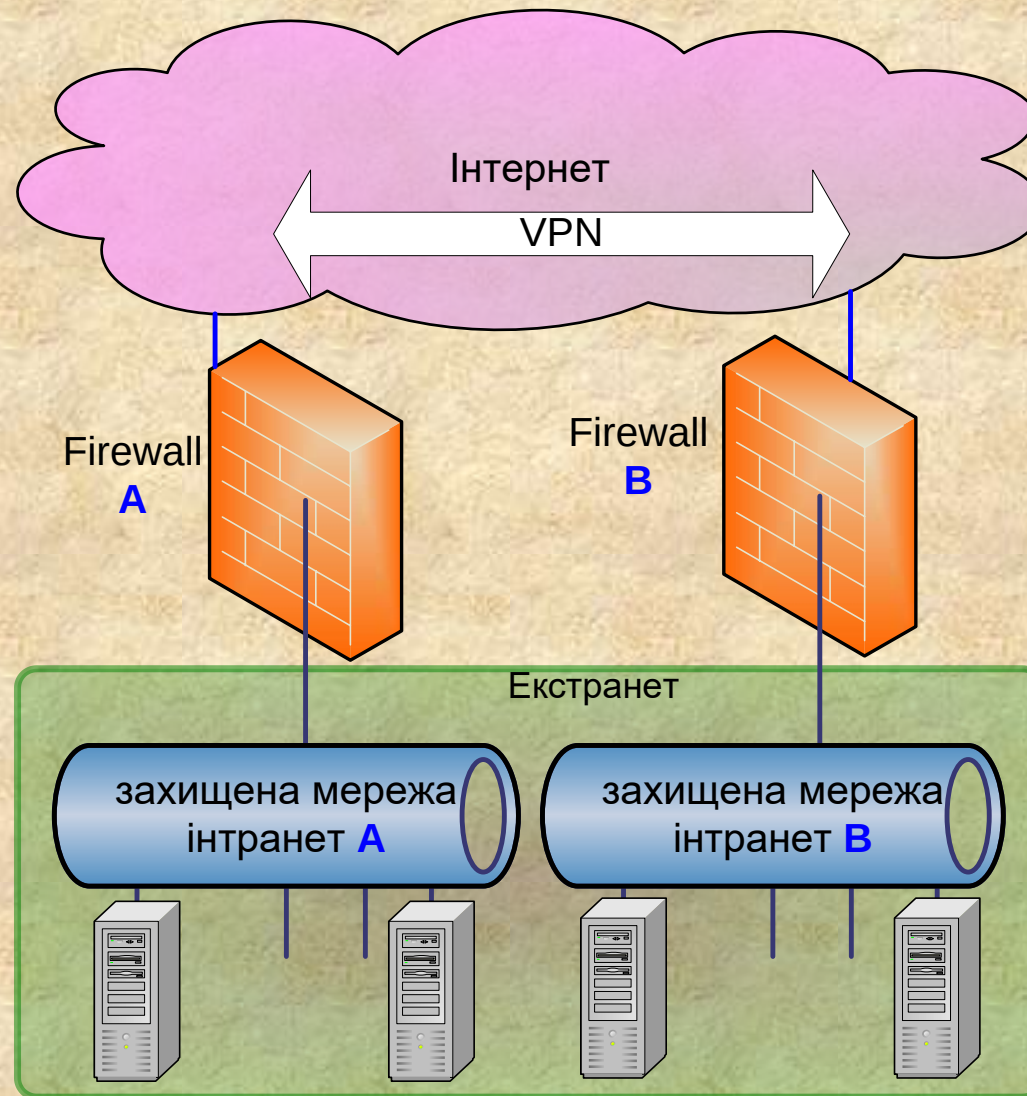
Конфігурація Service Leg DMZ



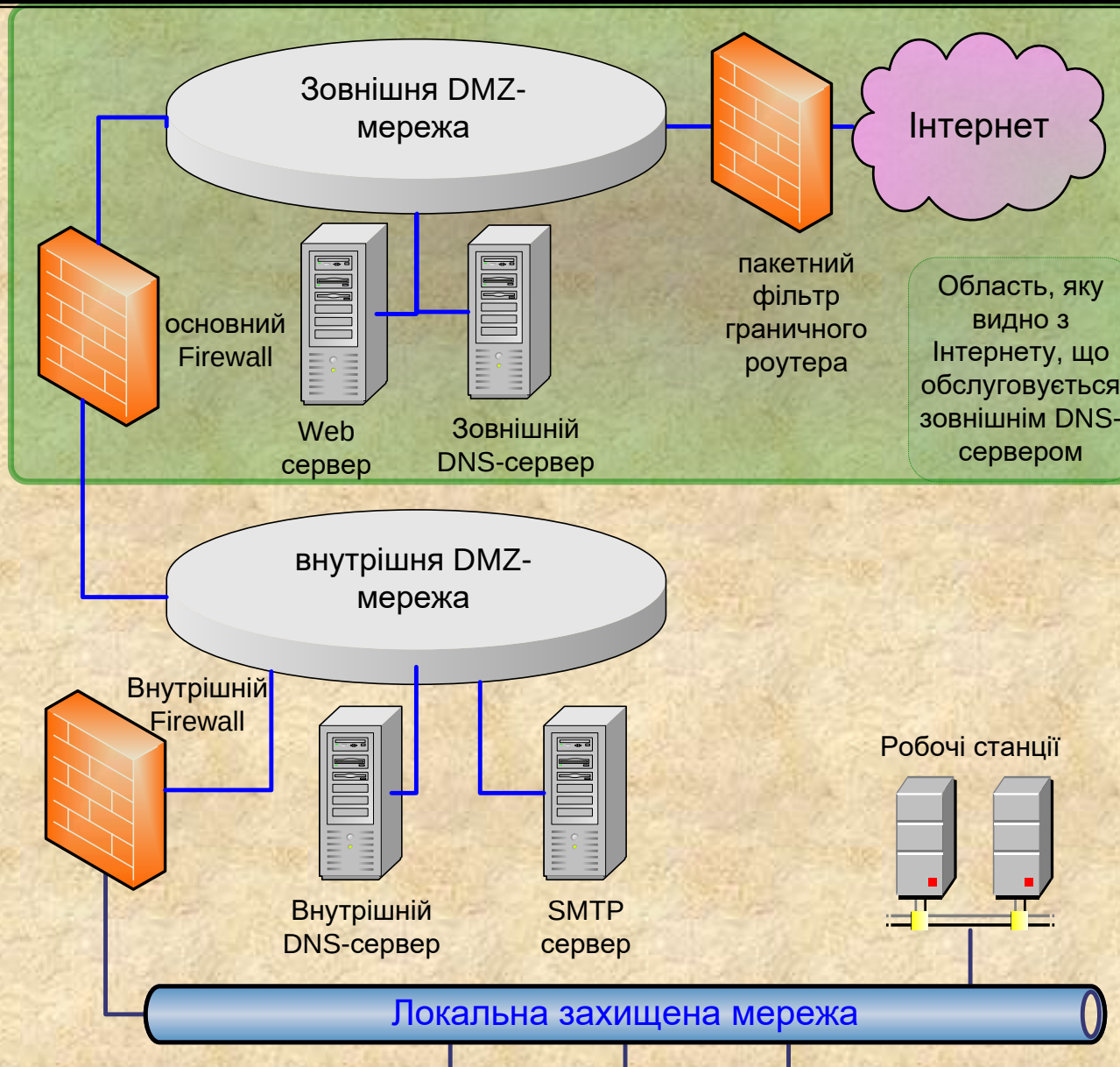
Конфігурація з двома DMZ-мережами



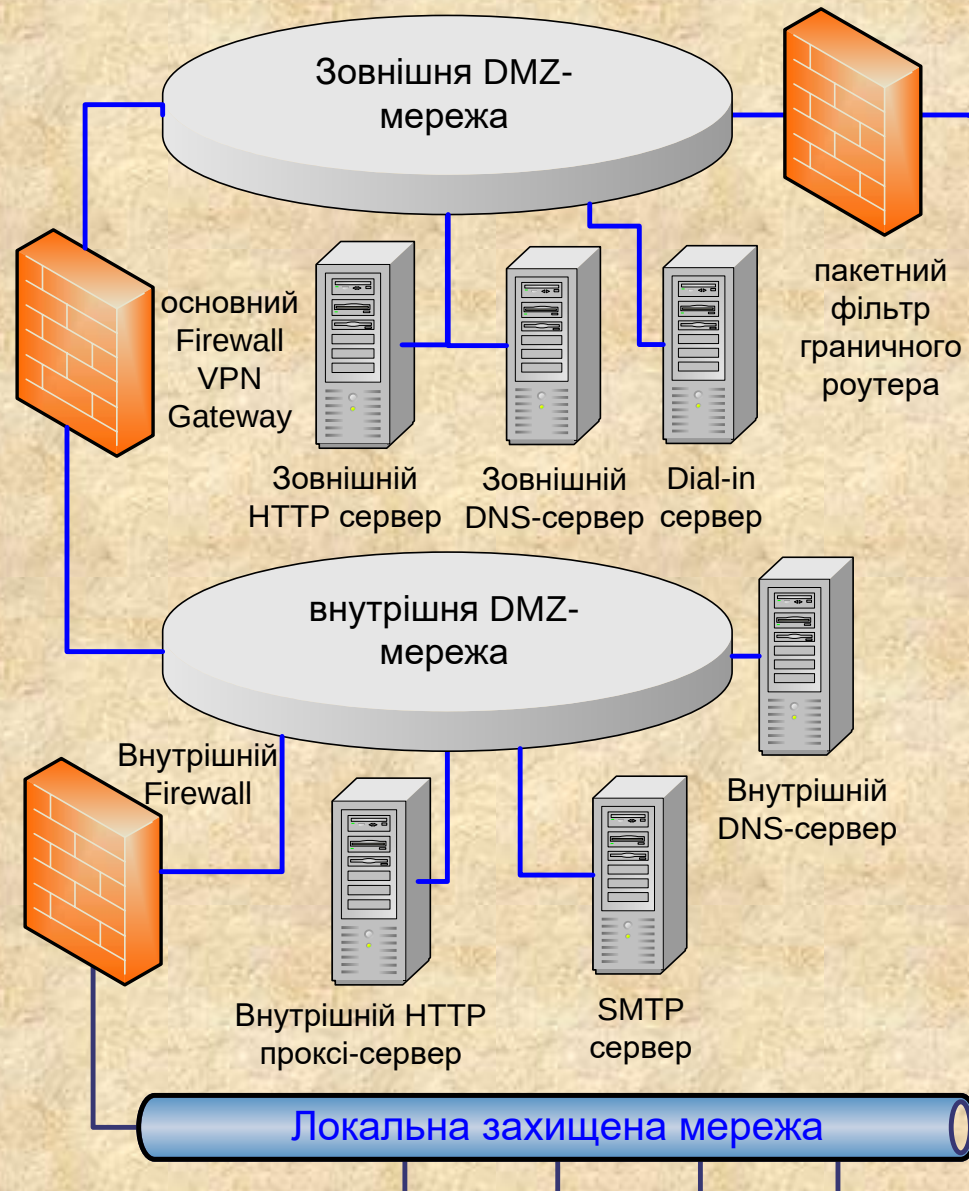
Приклад суміщення firewall-а і VPN



VPN і екстранет, що з'єднують дві інтранет мережі



Приклад топології мережі з двома DNS-серверами



Приклад топології мережі з двома DMZ

Поля, які входять в набір правил *firewall*'а:

- адрес відправника пакета (IP-адрес);
- адрес призначення пакета;
- тип трафіка - конкретний мережний протокол, який використовується для взаємодії систем відправника і отримувача (TCP або UDP);
- деякі характеристики комунікаційної сесії 4-го рівня (можливо)
 - протокол (TCP) і порти відправника і отримувача (TCP:80 для порта призначення, що належить web-серверу, TCP:1320 для порта відправника, який отримує доступ до сервера);
- інформація про інтерфейси роутерів від якого і для якого надійшов пакет (деколи)
(використовується для роутерів з трьома і більше мережними інтерфейсами);
- дії:
Deny, Block, Drop – коли пакет блокується firewall-ом
Allow, Pass, Accept - коли пакет пропускається через firewall.

Набір правил firewall'a повинен завжди блокувати такі типи трафіка:

- **Вхідний трафік від неаутентифікованого джерела з адресою призначення самого firewall'a.**
Даний тип пакета зазвичай є зондуванням або атакою на firewall.
Виключення: firewall забезпечує доставку вхідного e-mailу (SMTP на порт 25) - тоді firewall повинен дозволити вхідному з'єднанню до себе, але лише на порт 25;
- **Вхідний трафік з зовнішньої мережі з адресою відправника, яка вказує ніби пакет отримано з мережі позаду firewall'a.**
Даний тип пакету зазвичай є спробою spoofing'у (підробки);
- **Вхідний трафік, що містить ICMP-трафік, оскільки ICMP може використовуватися для визначення мереж позаду firewall'a;**
- **Вхідний або вихідний трафік від системи, що використовує адрес відправника з діапазону адрес, які зарезервовані для приватних мереж:**
з 10.0.0.0 до 10.255.255.255;
з 172.16.0.0 до 172.31.255.255;
з 192.168.0.0 до 192.168.255.255.
- **Вхідний трафік від неаутентифікованого джерела, який містить SNMP- трафік.**
Ці пакети вказують на зондування мережі. Можливо в деяких випадках організація дозволяє вхідний SNMP-трафік, але в загальному, він повинен бути заблокованим;
- **Вхідний або вихідний мережний трафік, який містить адрес відправника або отримувача 127.0.0.1 (localhost).**
Такий трафік зазвичай є деяким різновидом атаки на сам firewall;
- **Вхідний або вихідний мережний трафік, який містить адрес відправника або отримувача 0.0.0.0.**
Деякі ОС інтерпретують цей адрес як localhost або broadcast-адрес, в обох випадках такі пакети можуть використовуватися для атаки;
- **Вхідний або вихідний мережний трафік, який містить directed broadcast адреса.**
Directed broadcast часто використовують для початку broadcast'ового розповсюдження атаки. Directed broadcast дозволяє одному комп'ютеру відсилати broadcast'ове повідомлення з підробленою адресою відправника. Люба система, яка відповідає на directed broadcast, відсилає свою відповідь системі, вказаній в якості відправника, а не справжньому відправнику. Такі пакети можна використовувати для створення "шторму" мережного трафіка, наприклад, для блокування деяких сайтів.

Необхідні дії для процедури укріплення:

- Всі мережні протоколи, які не використовуються мають бути видалені з ОС, на якій працює firewall, оскільки можуть бути використані для доступу до firewall'у.
- Всі мережні сервіси або прикладення, що не використовуються мають бути видалені або заборонені (можуть бути використані для атаки на firewall'и). Окрім цього, мережні сервіси або прикладення, що не використовуються зазвичай встановлюються в конфігурації за замовчуванням, які, як правило, не є безпечними.
- Всі користувацькі або системні акаунти, що не використовуються мають бути видалені.
- Застосування всіх відповідних patches ОС також є критичними. Бо patches і hot fixes зазвичай вирішують проблеми безпеки і тому мають бути інтегрованими в процес побудови firewall'у. Patches завжди треба протестувати на невиробничій системі перед встановленням їх на діючу.
- Усі фізичні мережні інтерфейси, які не використовуються повинні бути видалені з сервера.

Приклади firewall:

```

shared@linuxhint: ~
root@linuxhint:~# ufw status
Status: active

To Action From
--
1194 ALLOW Anywhere
80 ALLOW Anywhere
443 ALLOW Anywhere
1194 (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)

root@linuxhint:~# █

```

