THE PROCESS OF DEPLOYMENT OF CLOUD ENVIRONMENT OF AN EDUCATIONAL INSTITUTION: NETWORK SECURITY

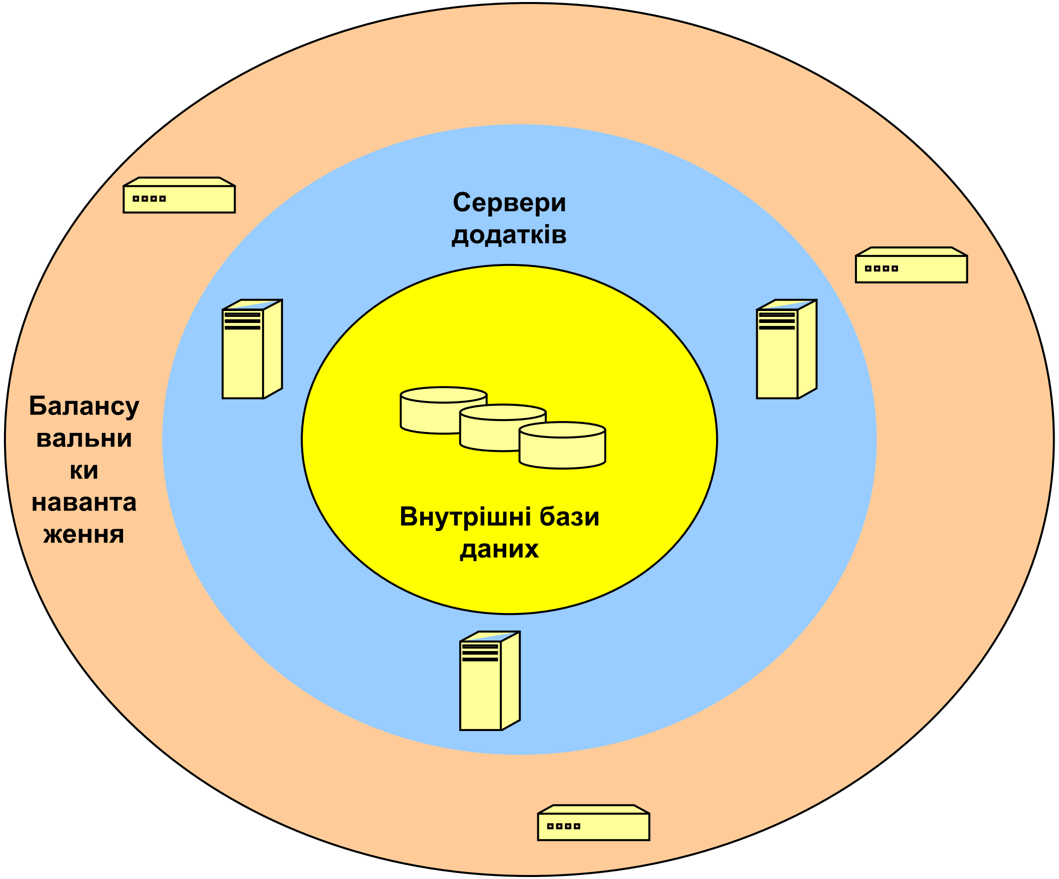
Olena Grybiuk,
National Pedagogical Dragomanov University
Institute of Information Technologies and Learning Tools National Academy of Pedagogical Sciences, Ukraine

The process of deployment of cloud environment of an educational institution: problems...

- ❑ Problems that arise between physical infrastructure of information and communication technologies and cloud environment can be partly solved by **using outsourcing services and services of SRM provider.**
- ❑ While using / working with cloud services, a user can experience an emotional challenge that is connected with **inability to visually scan the server which contains data**.
- ❑ An essential problem is limited access to **educational materials (data)**, for instance, **when a chosen cloud provider fails to protect its infrastructure components**.
- ❑ The measures to be taken: **data encryption and remote backup execution** (including backup encryption and network communications on another cloud service, encryption of network traffic together with web traffic).

The following is recommended:

- ❑ Connect to an **additional cloud provider for executing automated backup procedures,** which guarantees recovery of all data and their history, even with the main cloud provider being physically destroyed.
- ❑ Settings of the level of control on using own data in **cloud environment and data processing centre.**
- ❑ While bundling data for backup, to encrypt using strong **cryptography**, for example **Pretty Good Privacy**, which enables us to store messages (data) even in insecure environment.

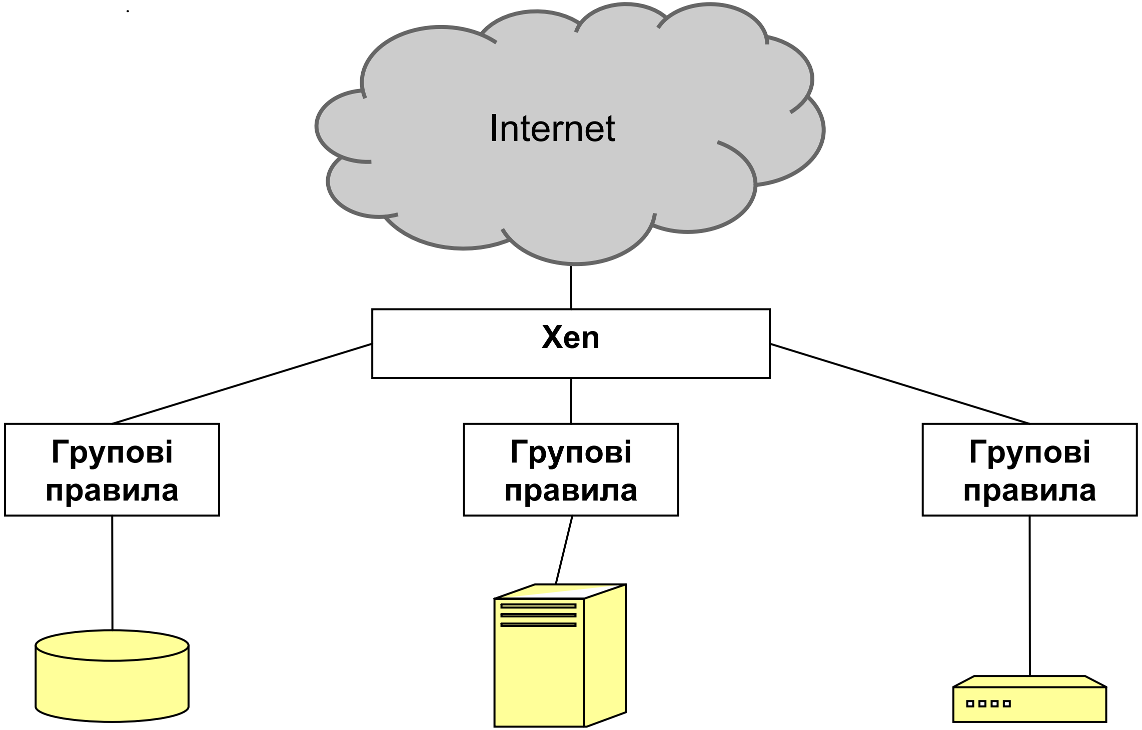

Сервери
додатків
Балансу
вальни
ки
наванта
ження
Внутрішні бази
даних

Network security support:

- ❑ While developing cloud environment it is essential to have a possibility to mount **ephemeral storage devices** when **virtual server** is used, although in **EC2** environment the failure to encrypt ephemeral storage devices poses a risk because the **system zeros** the storage out when your instance terminates.

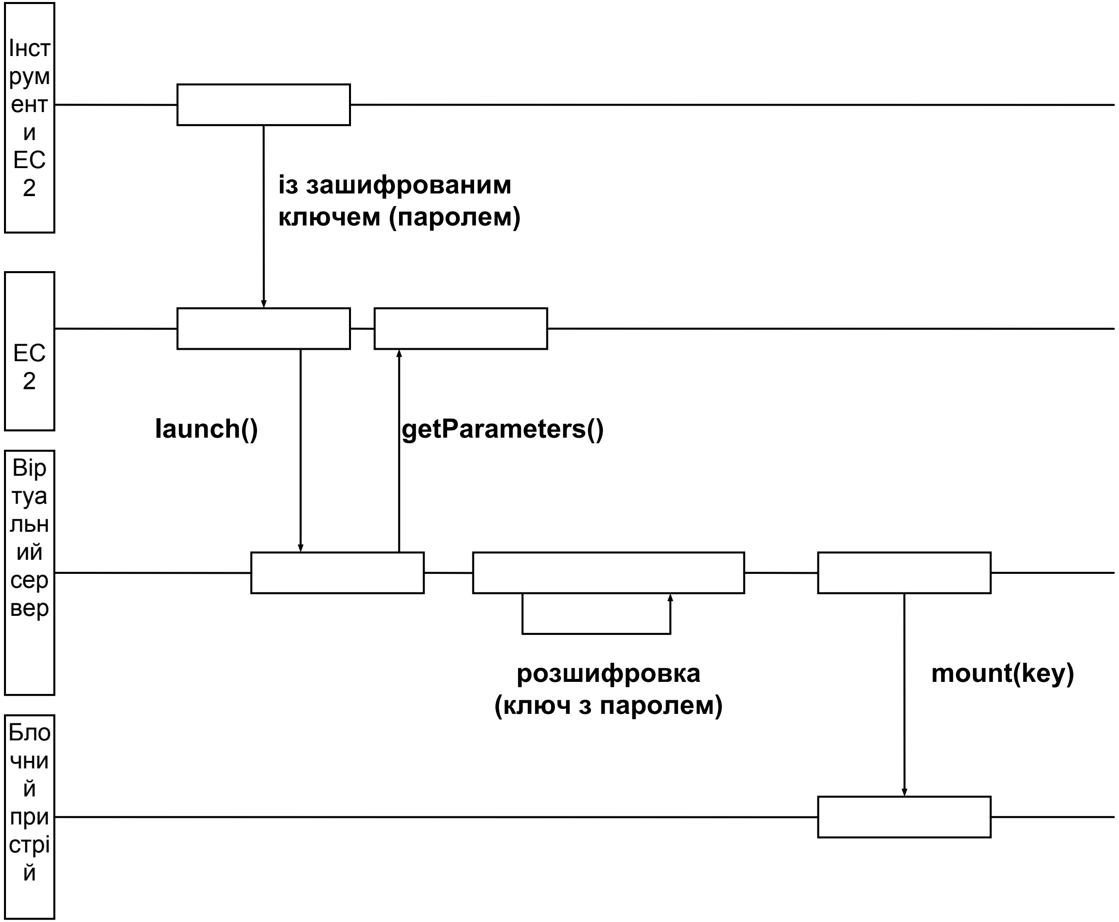
- ❑ **Encrypting filesystems** with caution helps to avoid conflicts regarding requirements to the performance level of **certain applications and data security.**

- ❑ **Security of using data in cloud environment** is provided by mounting block storage devices and ephemeral storage devices with using encrypted filesystems.


Internet
Xen
Групові правила
Групові правила
Групові правила

The process of deployment of cloud environment of an educational institution: network security support...

- ❑ Managing the start up a cloud server with using **encrypted filesystems in cloud environment is simplified** and requires advanced security level.
- ❑ It is more reasonable to store **system security passwords** in an unencrypted root filesystem than in a cloud environment.
- ❑ Such password storing is problematic, because the objective of filesystem encryption is to **protect against physical access to disk image.**
- ❑ The process of starting up a **virtual server** with using access **passwords** is shown here.



Інструменти EC2

із зашифрованим ключем (паролем)

EC2

launch()

getParameters()

Віртуальний сервер

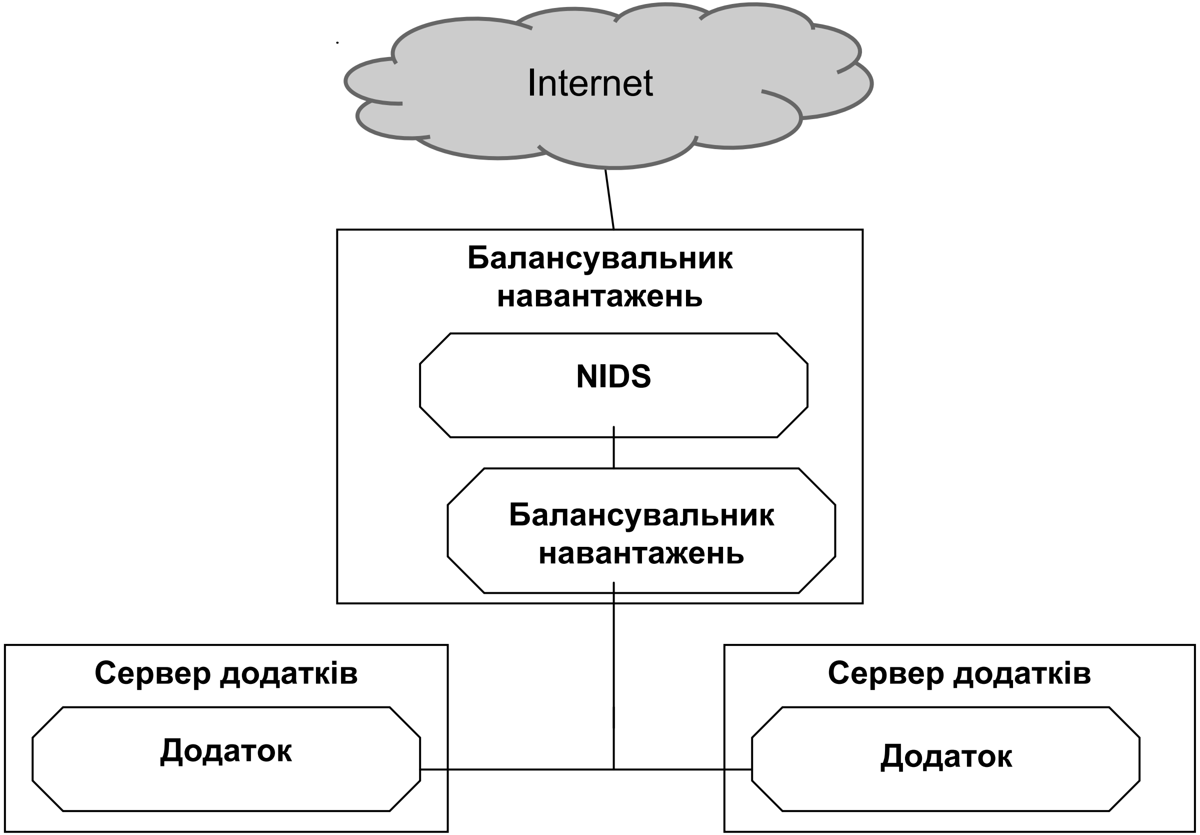
розшифровка (ключ з паролем)

mount(key)

Блочний пристрій

The process of deployment of cloud environment of an educational institution:

- **Specification of developing the system** in cloud environment is possible with implementing mixed architecture, which consists of **physical elements and some virtual elements.**
- **Cloud infrastructure, specializing in hybrid solutions, is the optimal option.**
- In a mixed environment, no sensitive data are hosted in the **cloud infrastructure**, because they are processed on servers of physical data centre which is under a user’s control.
- **The perimeter of one or more network segments** is protected by a firewall. A firewall protects the outermost perimeter, allowing in only **http, https, ftp**.


Internet
Балансувальник навантажень
NIDS
Балансувальник навантажень
Сервер додатків
Додаток
Сервер додатків
Додаток

The process of development of cloud environment of educational establishment:

- **Between the protected network segment and outermost perimeter there are border systems**, such as load balancer, that route traffic into a special area, where there are application servers.
- They make requests to the database across another firewall into internal protected network with **internal sensitive database**.
- The proposed structure is used for **gaining access to increasingly sensitive data**, and there are several layers of network protection **in the form of firewalls**.

- The disadvantage of this infrastructure is that once any internal server is compromised inside any **given segment**, full access is provided to other servers in **this segment**.

It is essential!

❑ In cloud environment there are no **perimeters and segments.**

❑ **All virtual servers** are on the same level in the network, and the traffic is managed through security groups.

There are many factors which define how **effective the network security system** in a cloud environment can be:

1. It is reasonable to run only one **network service** and **services, aimed for administration on each virtual server**.

2. **Sticking several services** on one server can lead to attack vectors for accessing the data on that server or using the server as a buffer zone to receive network's access rights.

The process of deployment of cloud environment of an educational institution:

- ❑ It is not reasonable **to open direct access to most sensitive data,** and attackers will need to exploit three different attack vectors before they can get to that data.
- ❑ Obviously, protection of each server requires using a certain port for the support of a service given.**It is appropriate to limit access of third parties to servers.**
- ❑ It is recommended to use a reverse proxy even when **load balancer using** is limited.
- ❑ A **reverse proxy forwards** a user's requests from external environment to one or several servers, logically located in internal network.

Thank you

for your attention!

Good luck!