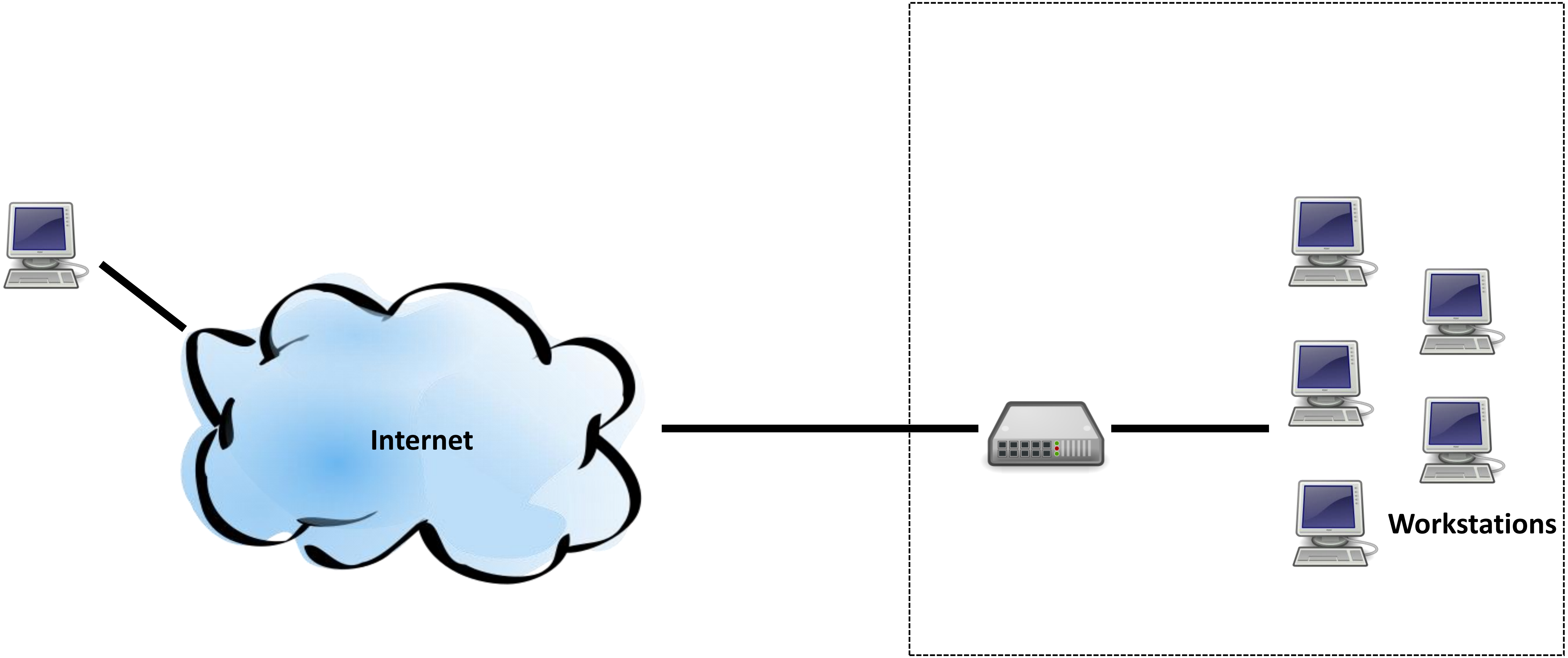
CompSci 401: Cloud Computing

Security in Local Infrastructures

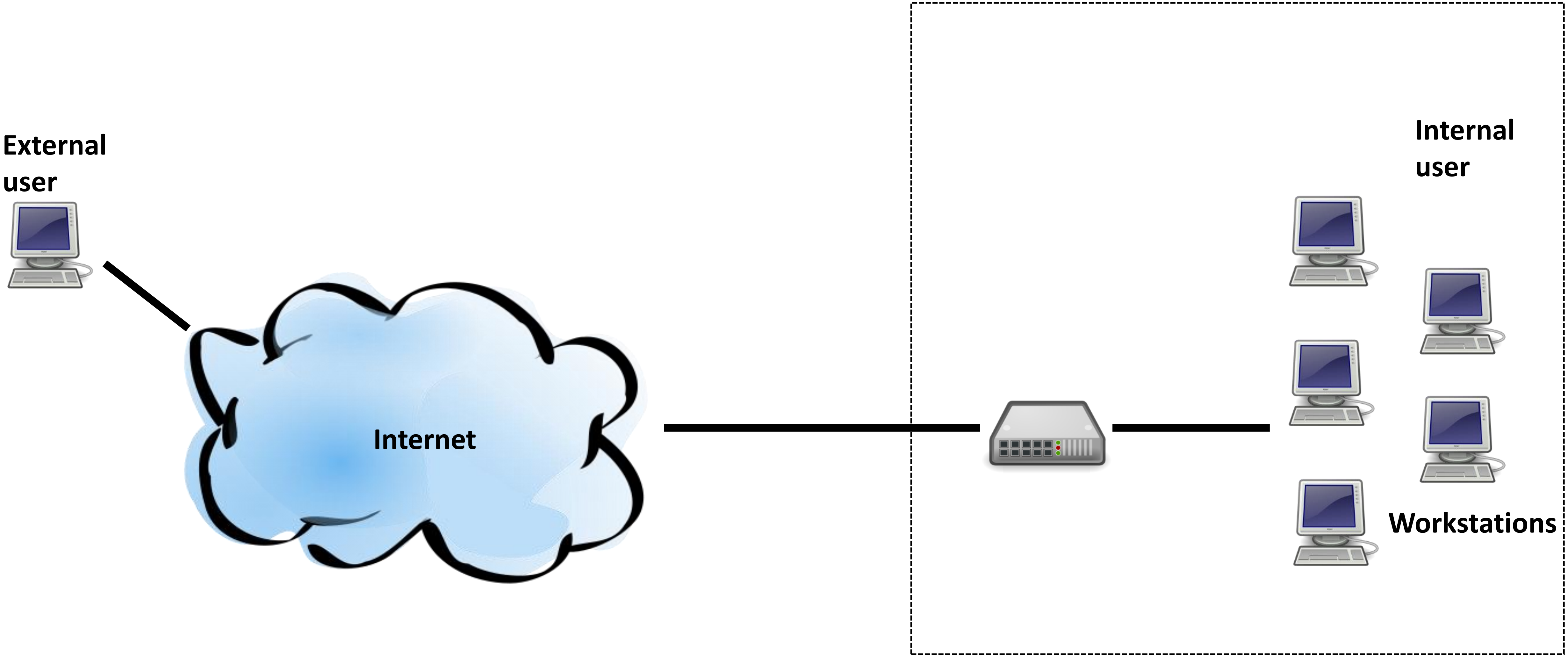
Prof. Ítalo Cunha

昆山杜克大学
DUKE KUNSHAN UNIVERSITY

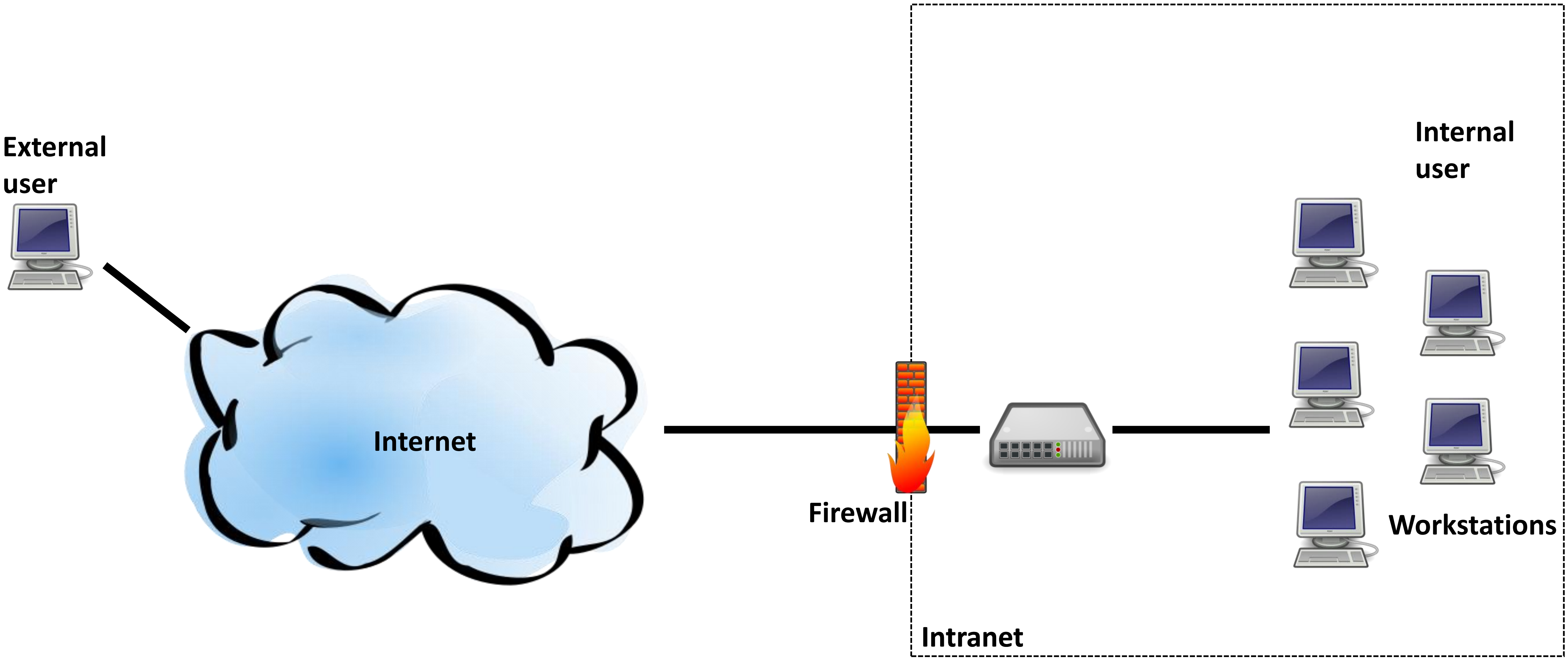
Security in Local Infrastructures



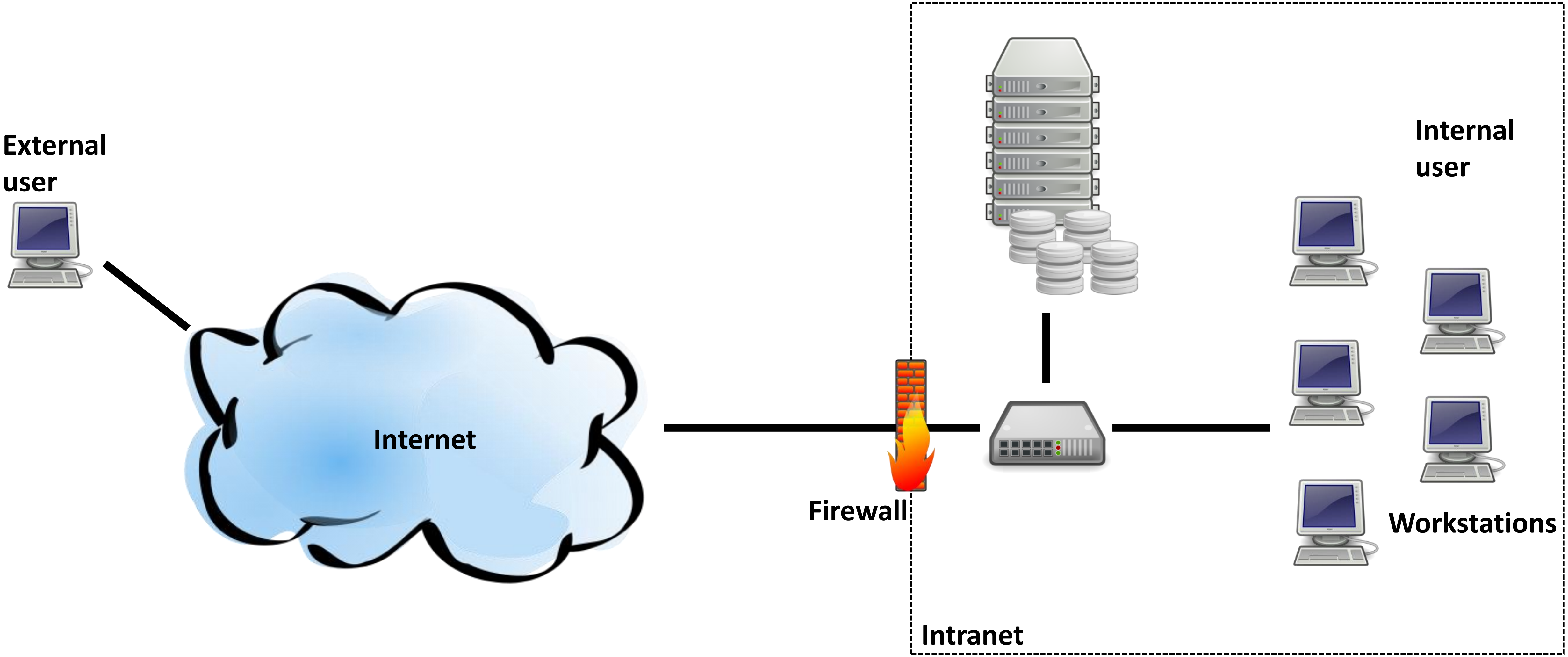
Security in Local Infrastructures



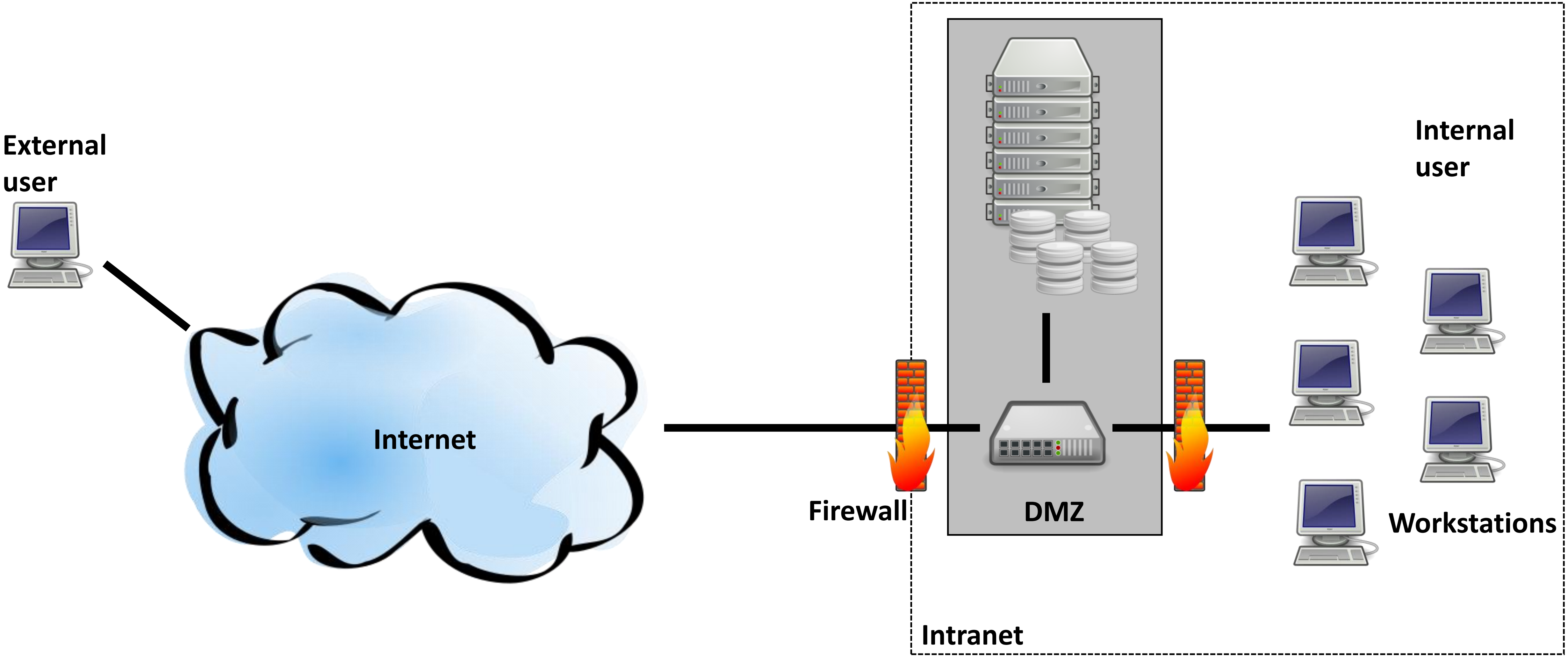
Security in Local Infrastructures



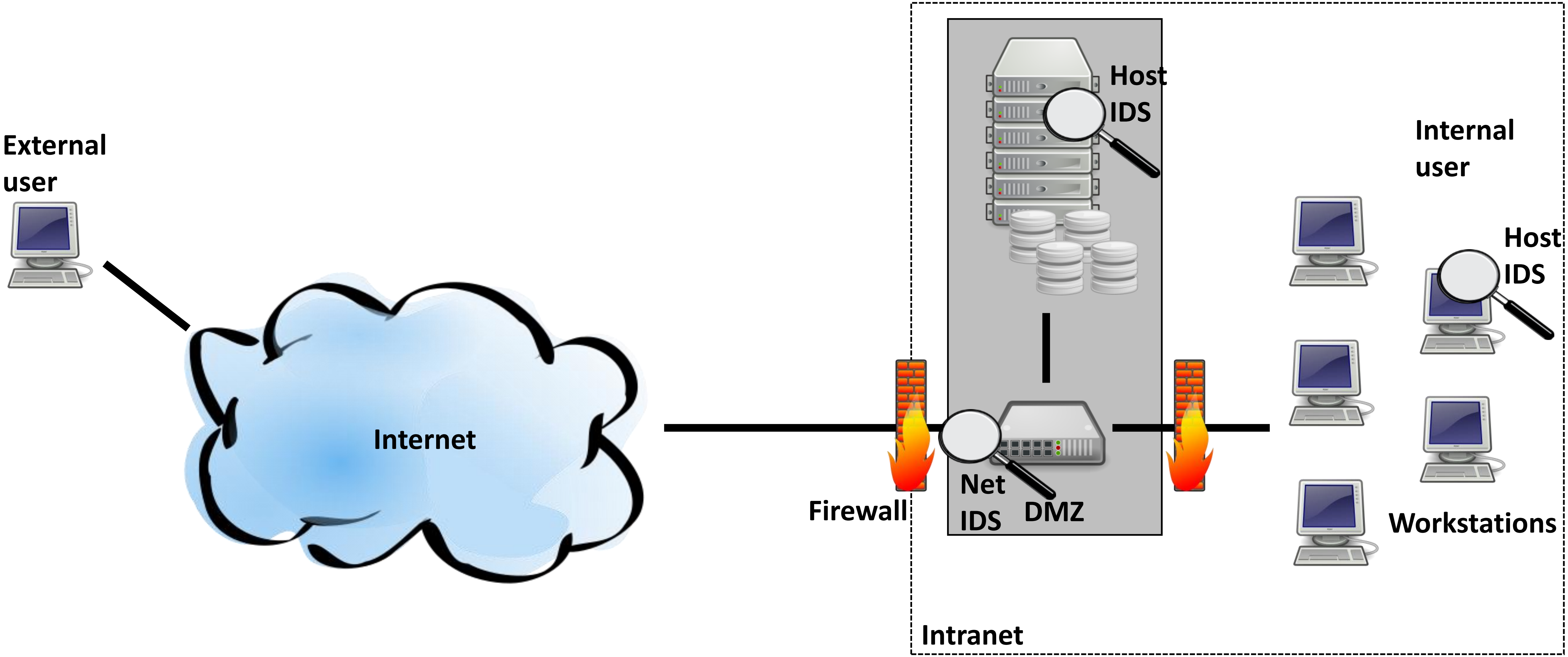
Security in Local Infrastructures



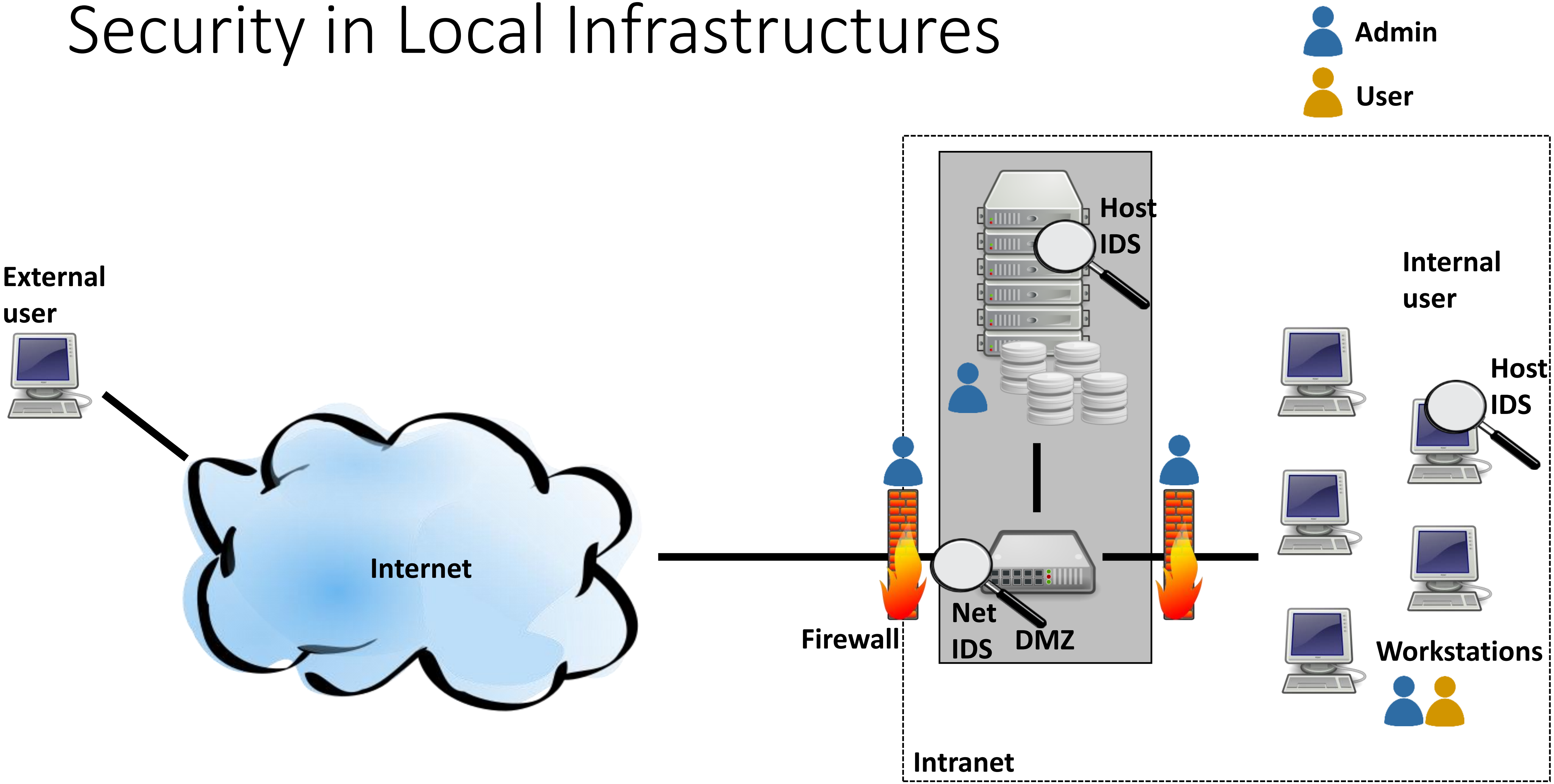
Security in Local Infrastructures



Security in Local Infrastructures



Security in Local Infrastructures



Incompatibilities of the classical approach with cloud computing

- No network perimeter
    - Logical perimeter defined by virtual network
    - Isolation is delegated to cloud operator
    - No control over *shared* physical devices
- Firewall and IDS configurations need to be coordinated with provider
    - Border firewall executes on the cloud provider’s resources
    - Provider needs to update policies whenever client changes configuration
- Coarse-grained access control may be insufficient

Security challenges in the cloud

- Lack of control and visibility
  - Tenant has limited ability to investigate issues
    - Hard to differentiate between failure on underlying infrastructure (the provider’s fault), on the application (the developer’s fault) or an attack (a third-party’s fault)
  - Depends on cloud provider to identify the root cause of the problem
- Shared infrastructure
  - Isolation from virtualization, but compute, memory, and network still shared
  - Increased security risk, for example if isolation is not perfect
- Everyone is remote: employees, IT staff, users, clients

Security challenges of cloud-native applications

- Many services with interdependencies
  - Microservices can be secured, but their number increases the attack surface
- Dynamic execution environment
  - Orchestration, autoscaling, rollouts, rollbacks, canaries: multiple systems operating in parallel with the application are confounding factors
- Reliance on software from the cloud provider
  - Cloud software may be subject to security vulnerability in the cloud infrastructure and software stack

CompSci 401: Cloud Computing

Security in the Cloud

Prof. Ítalo Cunha

昆山杜克大学
DUKE KUNSHAN UNIVERSITY

Collaboration with cloud providers

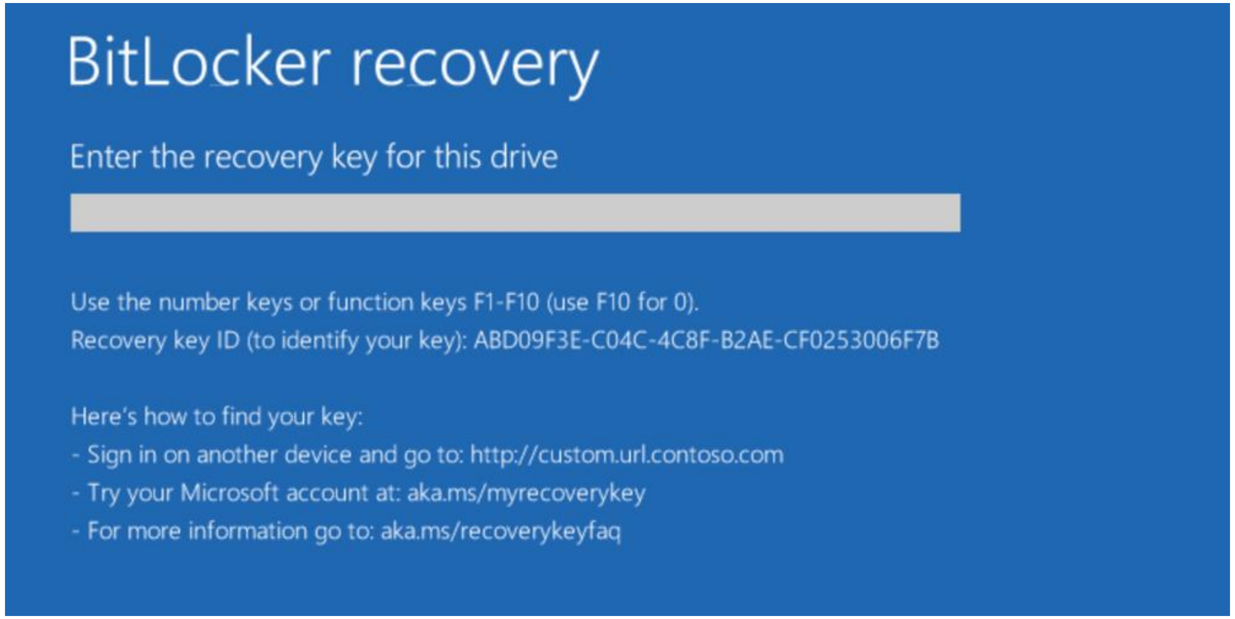
- Cloud providers have implemented security mechanisms
  - Virtualization technologies to protect their hardware and isolate tenants
  - Several security-related solutions
    - Fine-grained access control
    - Firewalls
    - Load balancers and packet filters
    - Private connections
- Tenants need to learn how to employ these mechanisms
- Collaboration with cloud providers is essential
  - Speed up issue resolution
  - Identify requirements of new solutions to cover existing gaps

Protecting remote access

- Every access is remote in a cloud environment
- Protect and isolate business data
  - Laptops and cell phones are encrypted
  - Hard to extract information from lost or stolen devices

Protecting remote access

- Every access is remote in a cloud environment
- Protect and isolate business data
  - Laptops and cell phones are encrypted
  - Hard to extract information from lost or stolen devices



BitLocker recovery

Enter the recovery key for this drive

Use the number keys or function keys F1-F10 (use F10 for 0).
Recovery key ID (to identify your key): ABD09F3E-C04C-4C8F-B2AE-CF0253006F7B

Here's how to find your key:
- Sign in on another device and go to: http://custom.url.contoso.com
- Try your Microsoft account at: aka.ms/myrecoverykey
- For more information go to: aka.ms/recoverykeyfaq

SAMSUNG Knox

Protecting remote access

- Every access is remote in a cloud environment
- Protect and isolate business data
  - Laptops and cell phones are encrypted
  - Hard to extract information from lost or stolen devices
- Protect communication
  - End-to-end encryption
- Workflow security
  - Guarantee access and protection policies are enforced
  - Identity management and user authentication
- Enforce encryption and authentication everywhere
  - Virtual Private Network (VPN)

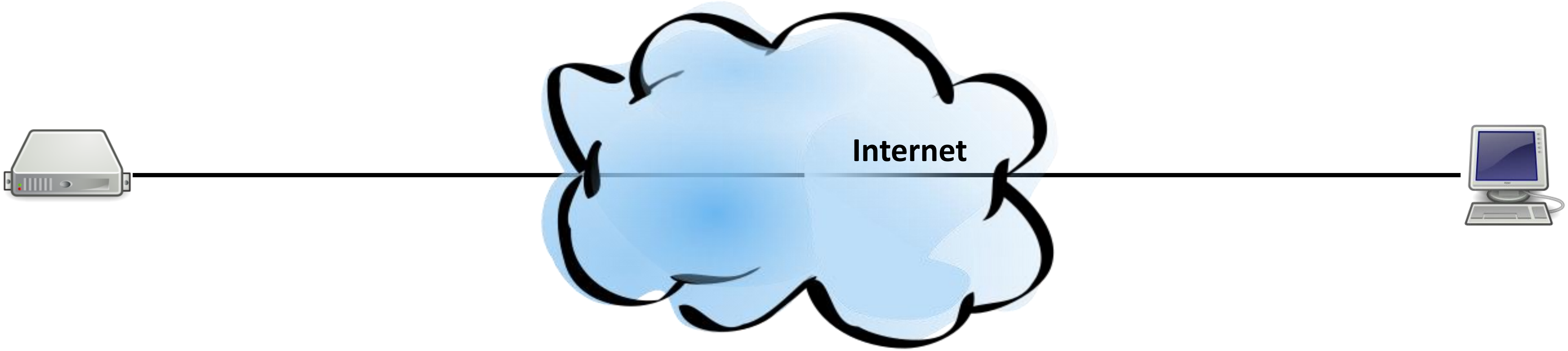
CompSci 401: Cloud Computing

End-to-end Encryption

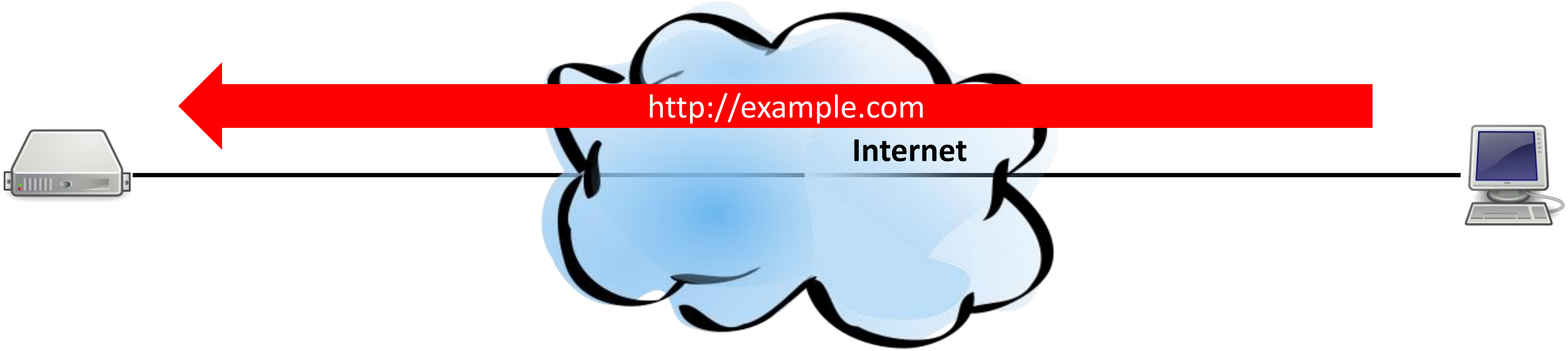
Prof. Ítalo Cunha

昆山杜克大学
DUKE KUNSHAN
UNIVERSITY

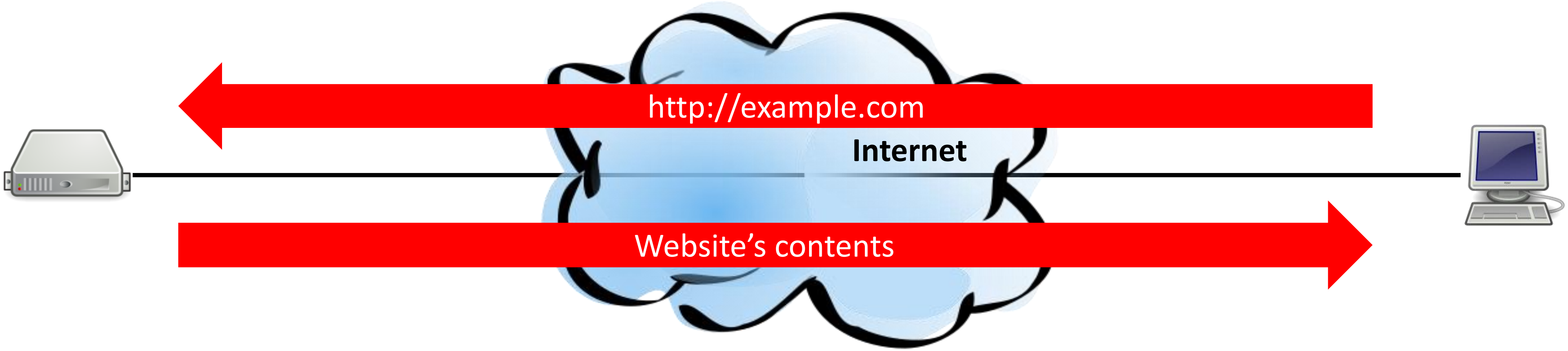
End-to-end encryption



End-to-end encryption



End-to-end encryption

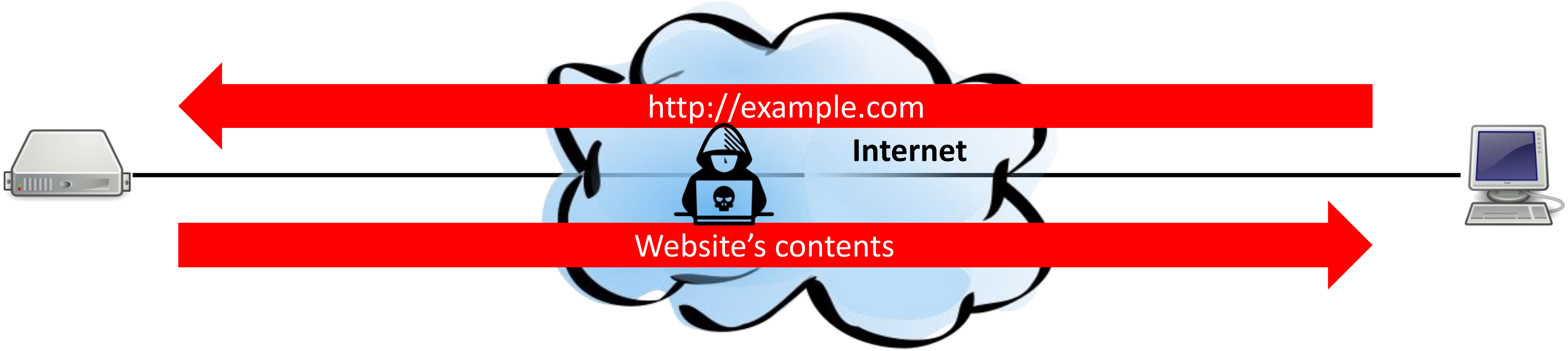


http://example.com

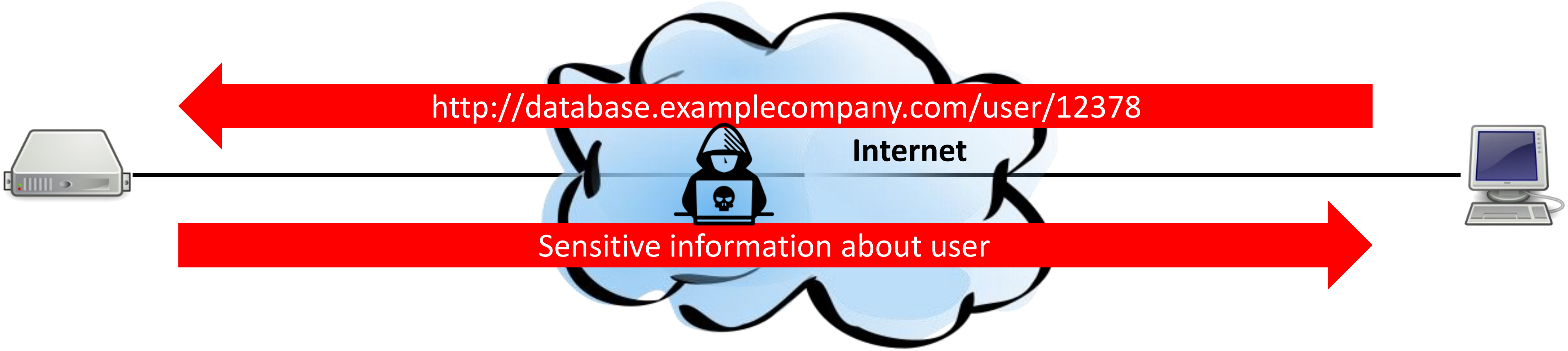
Internet

Website’s contents

End-to-end encryption

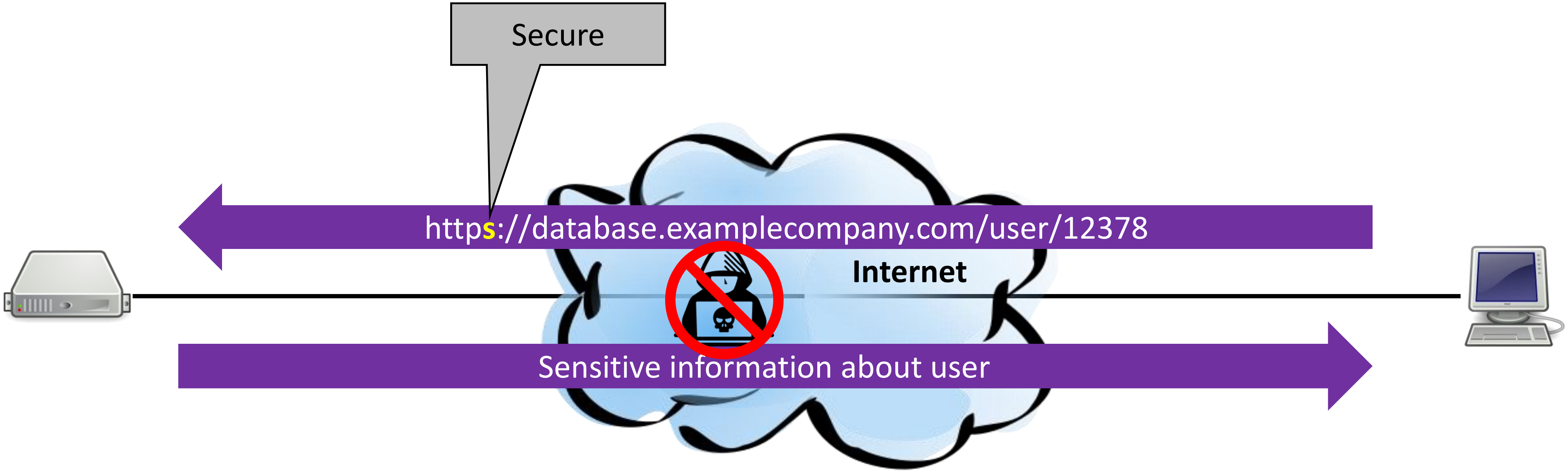


End-to-end encryption



http://database.examplecompany.com/user/12378
Internet
Sensitive information about user

End-to-end encryption



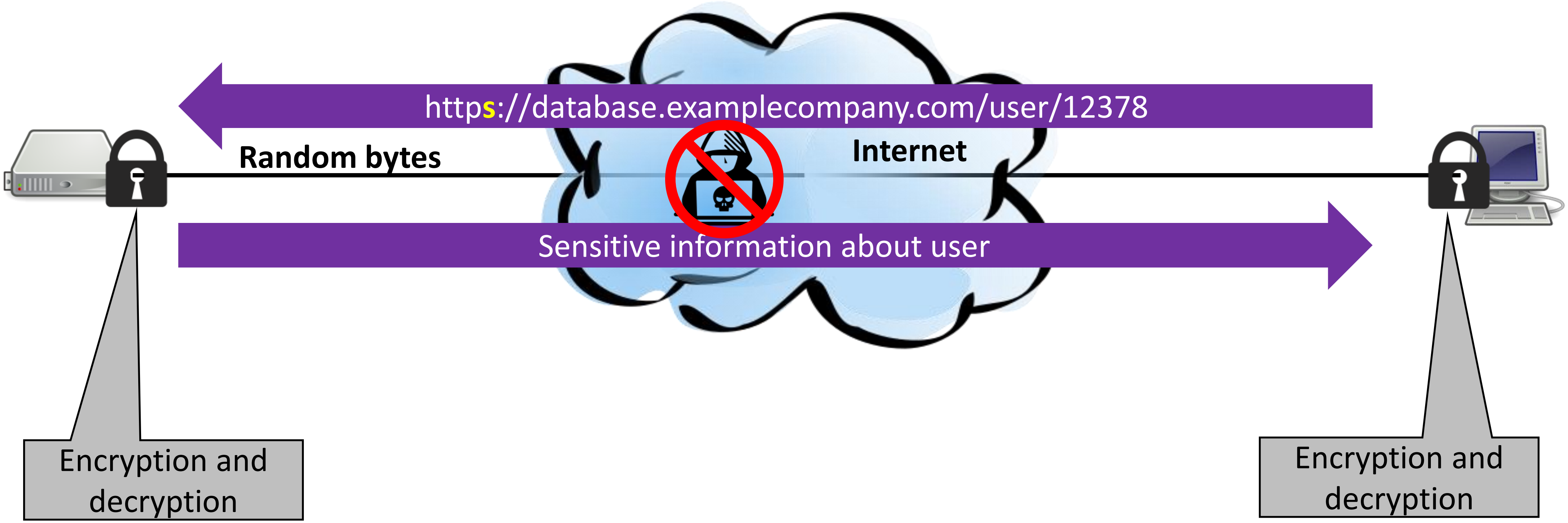
Secure

https://database.examplecompany.com/user/12378

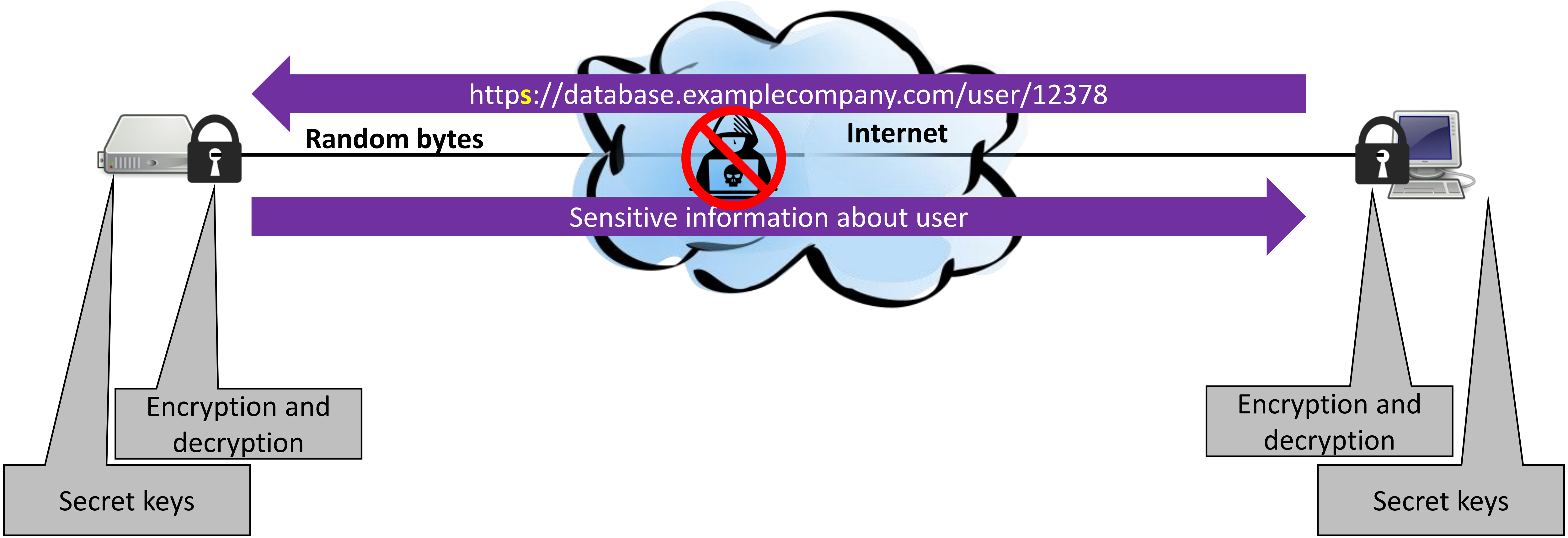
Internet

Sensitive information about user

End-to-end encryption


https://database.examplecompany.com/user/12378
Random bytes
Internet
Sensitive information about user
Encryption and decryption
Encryption and decryption

End-to-end encryption


https://database.examplecompany.com/user/12378
Random bytes
Internet
Sensitive information about user
Encryption and decryption
Secret keys
Encryption and decryption
Secret keys

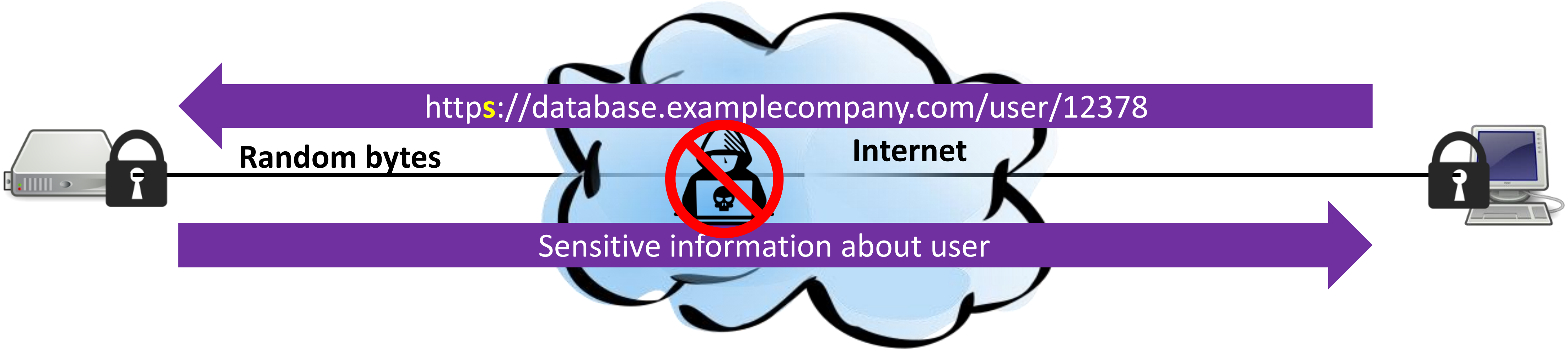
CompSci 401: Cloud Computing

Identity Management

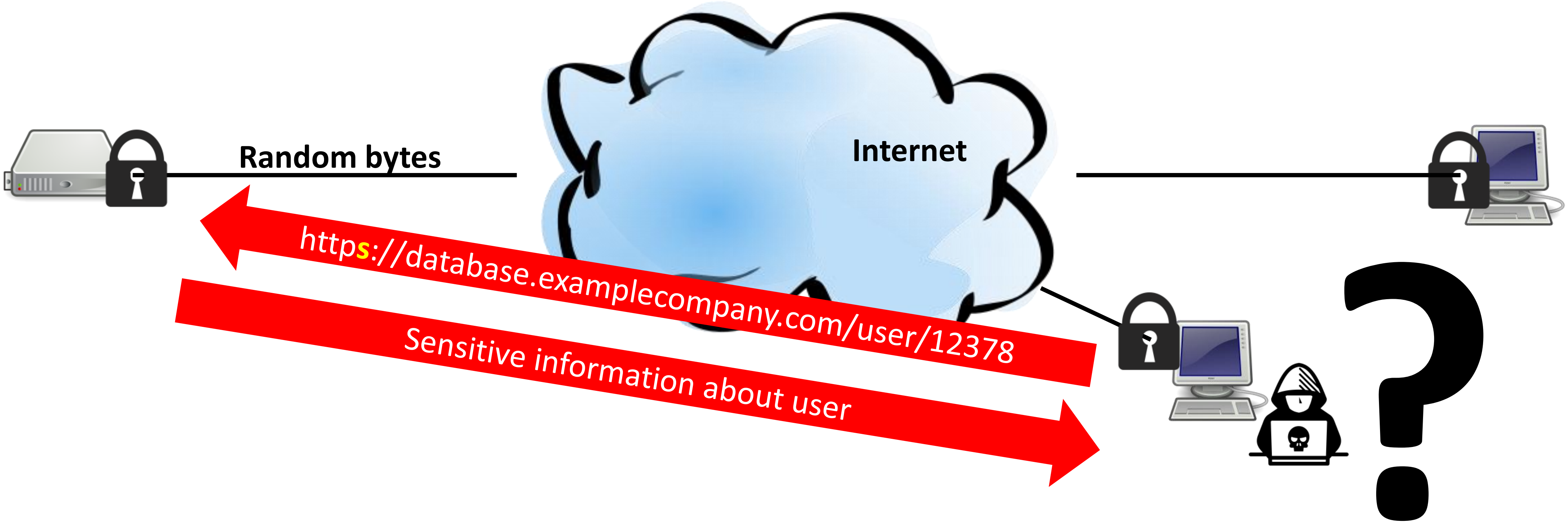
Prof. Ítalo Cunha

昆山杜克大学
DUKE KUNSHAN UNIVERSITY

End-to-end encryption


https://database.examplecompany.com/user/12378
Random bytes
Internet
Sensitive information about user

User authentication

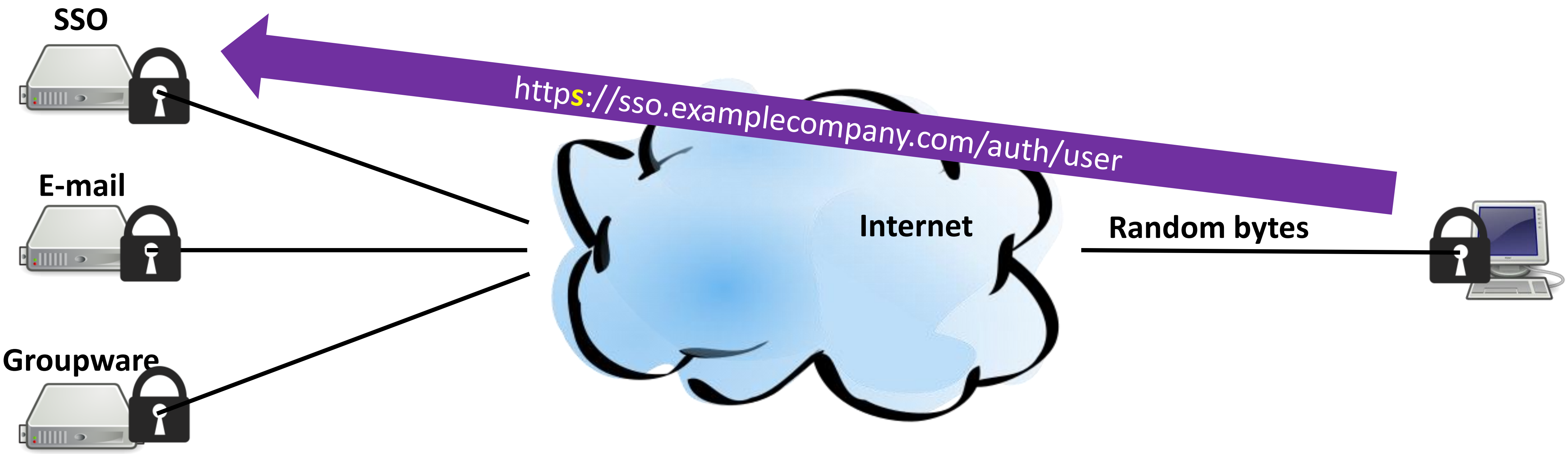


Random bytes
Internet
https://database.examplecompany.com/user/12378
Sensitive information about user
?

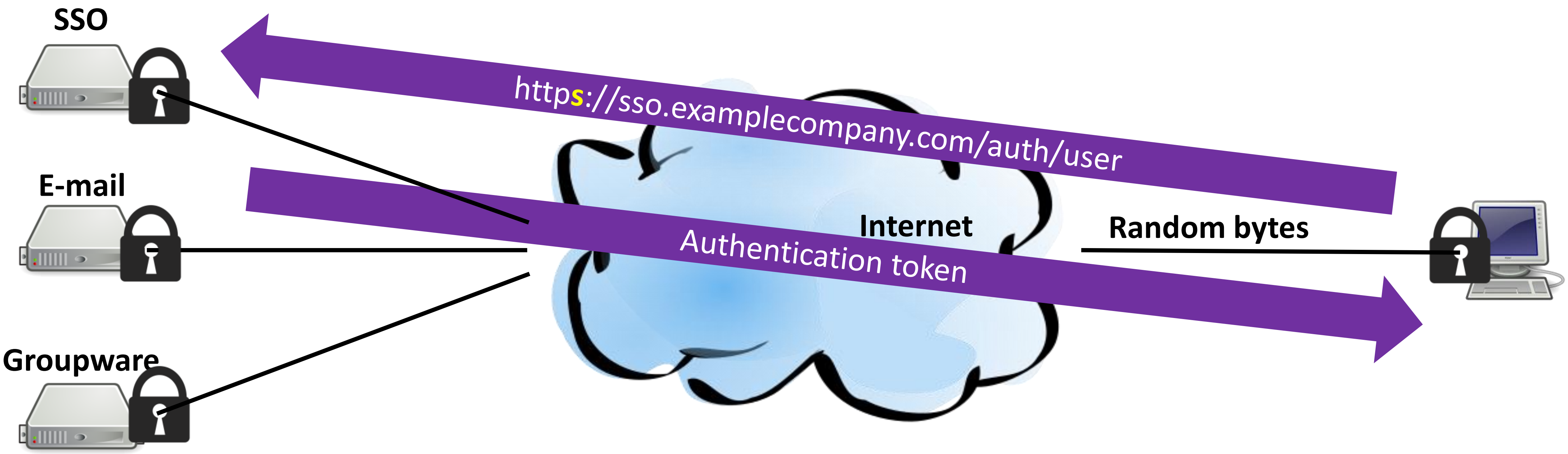
Zero-trust model

- All users are considered malicious/unauthorized until authenticated
- Many virtual machines, many microservices
    - Using an application might involve requests to multiple services
    - Juggling multiple accounts and typing password everywhere gets annoying
- Identity management (IdM)
    - Give each user *one* account and assign privileges/capabilities
    - Have a single point for authentication (Single Sign On, SSO)

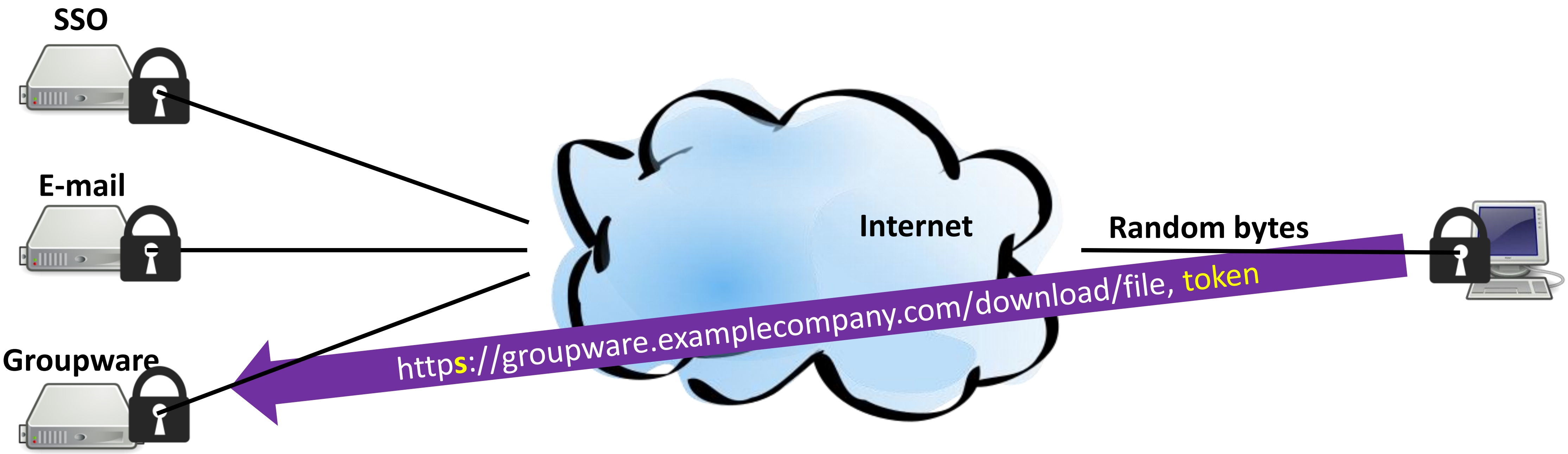
Single Sign On



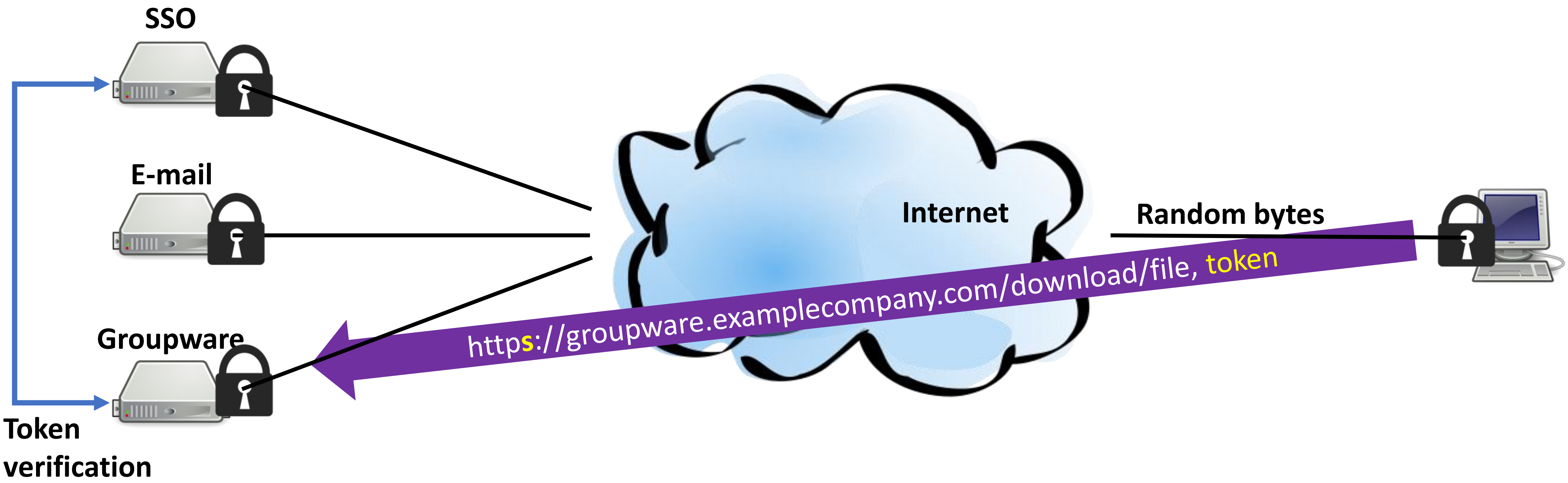
Single Sign On



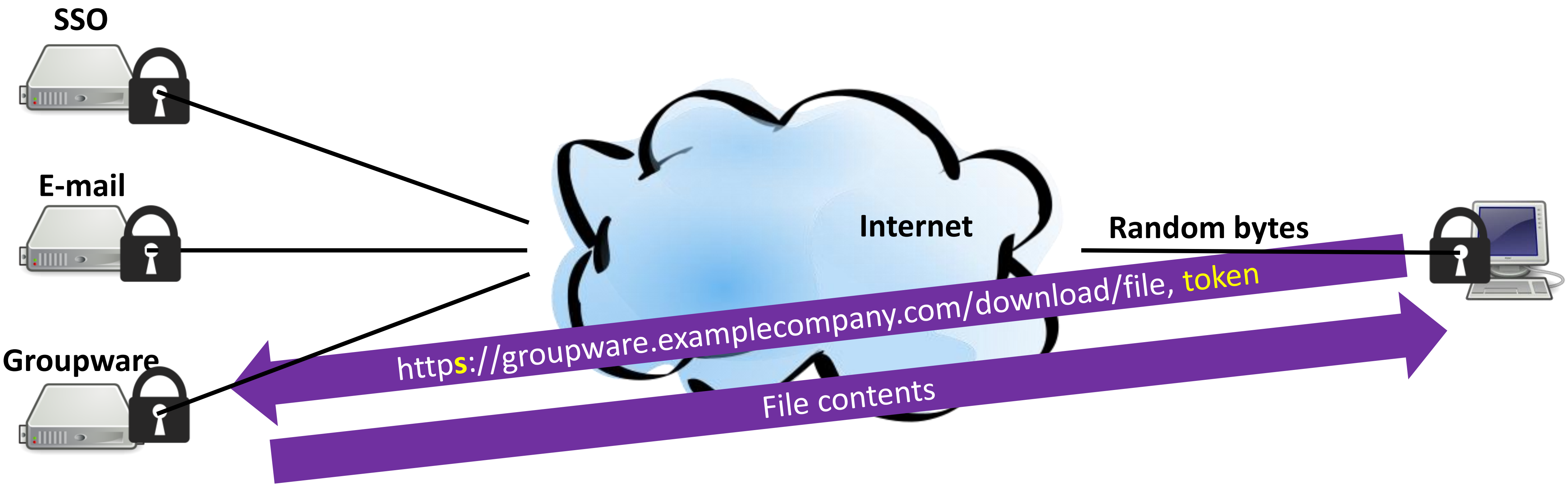
Single Sign On



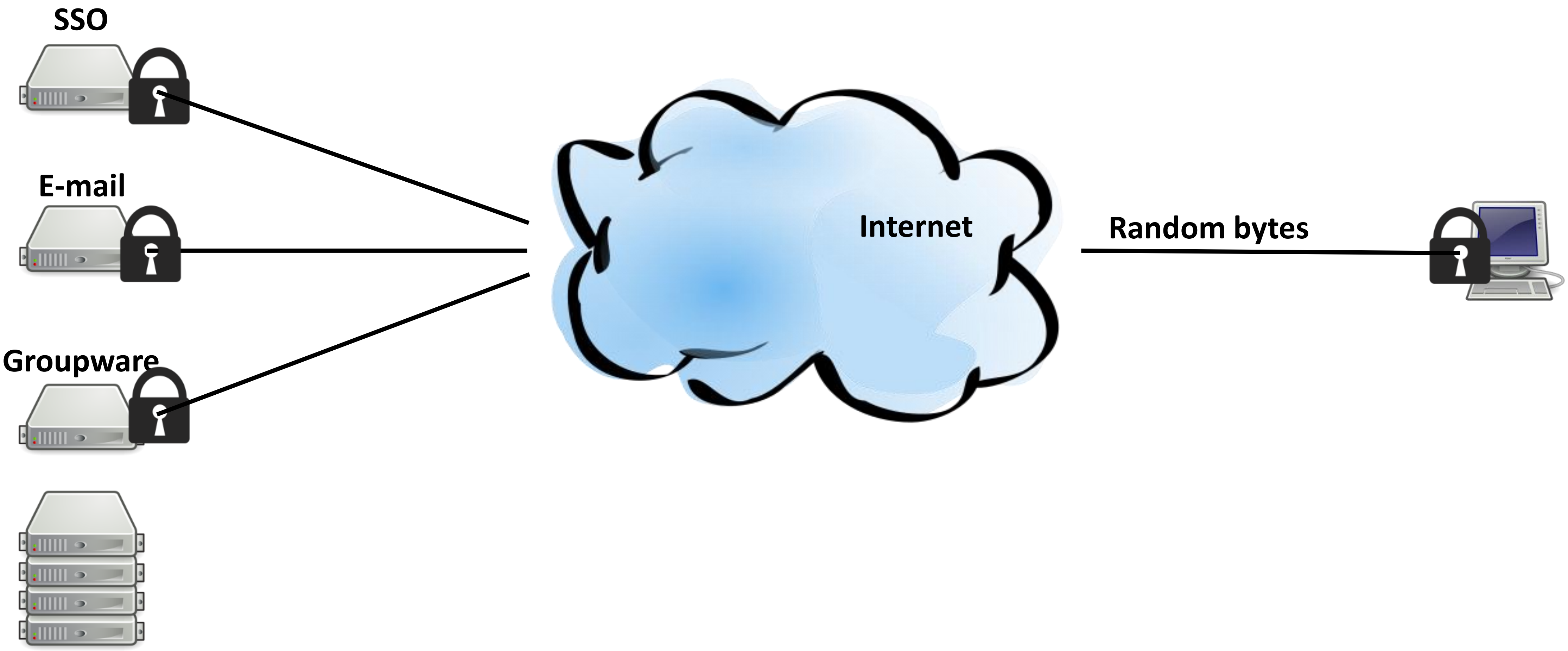
Single Sign On



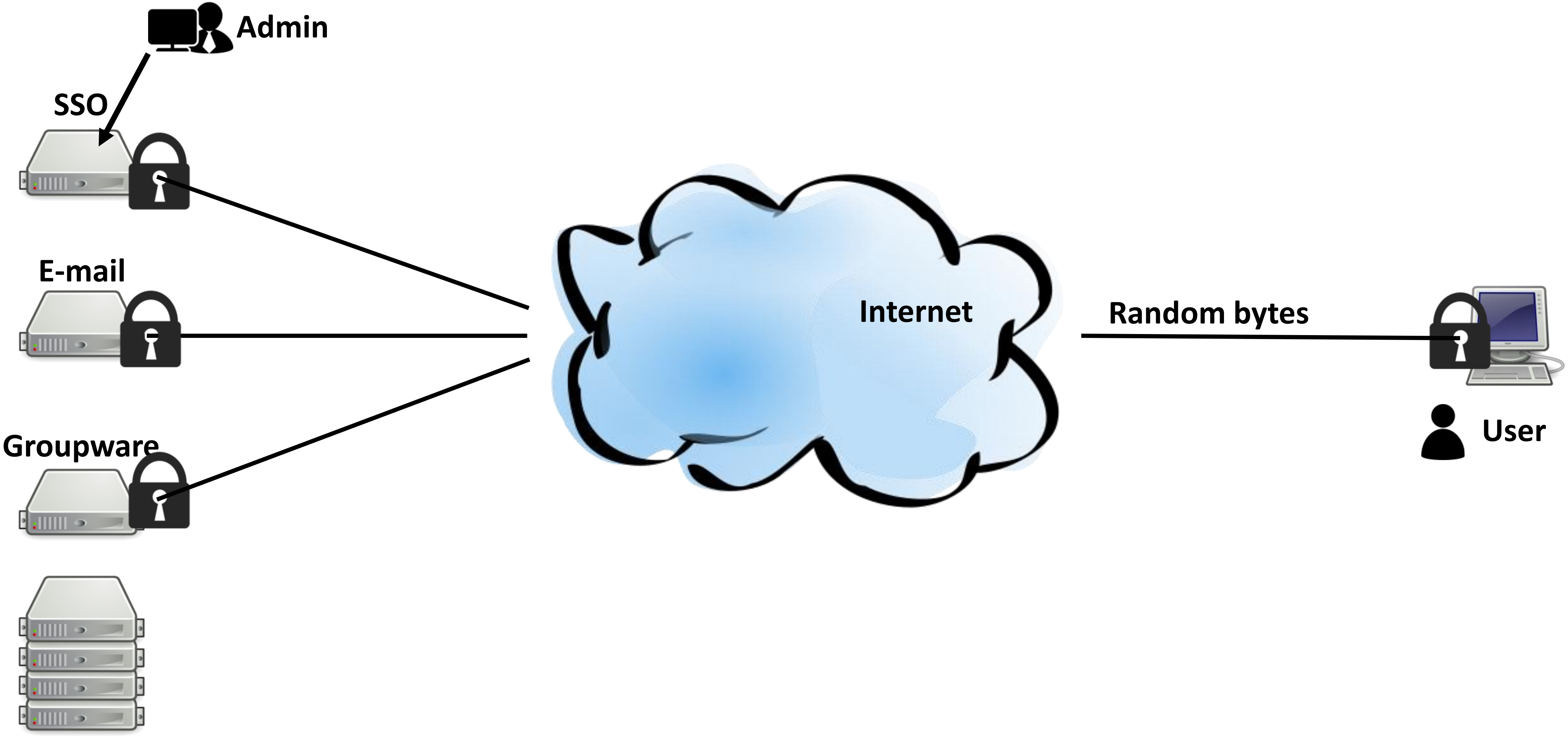
Single Sign On



Single Sign On



Single Sign On



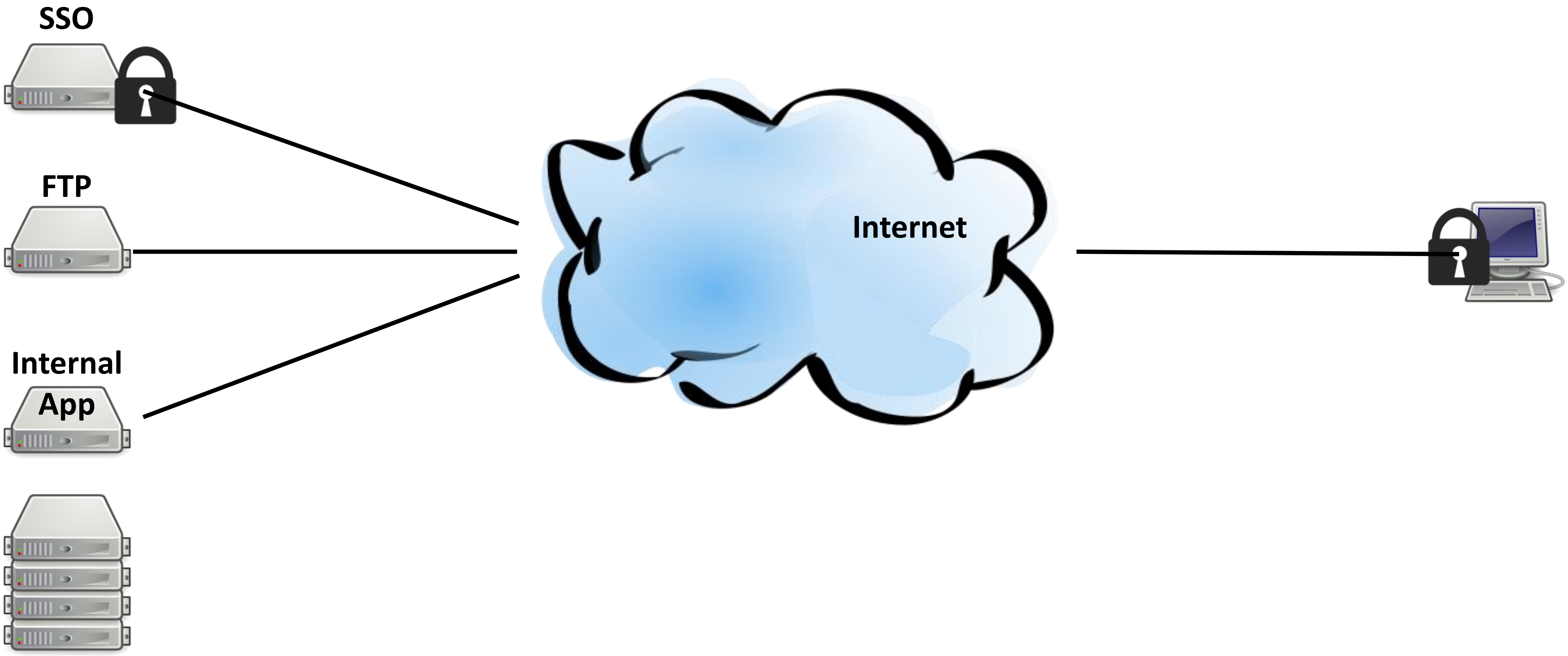
CompSci 401: Cloud Computing

Virtual Private Networks

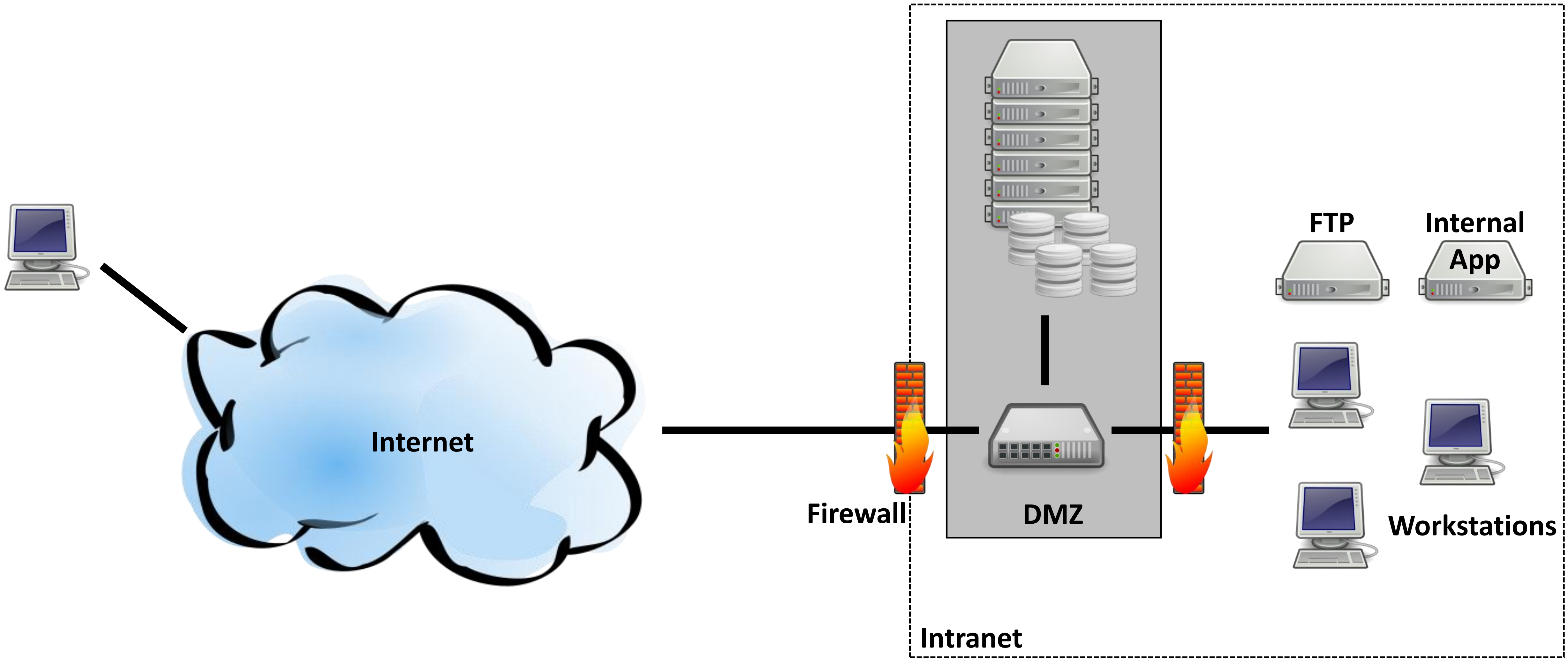
Prof. Ítalo Cunha

昆山杜克大学
DUKE KUNSHAN UNIVERSITY

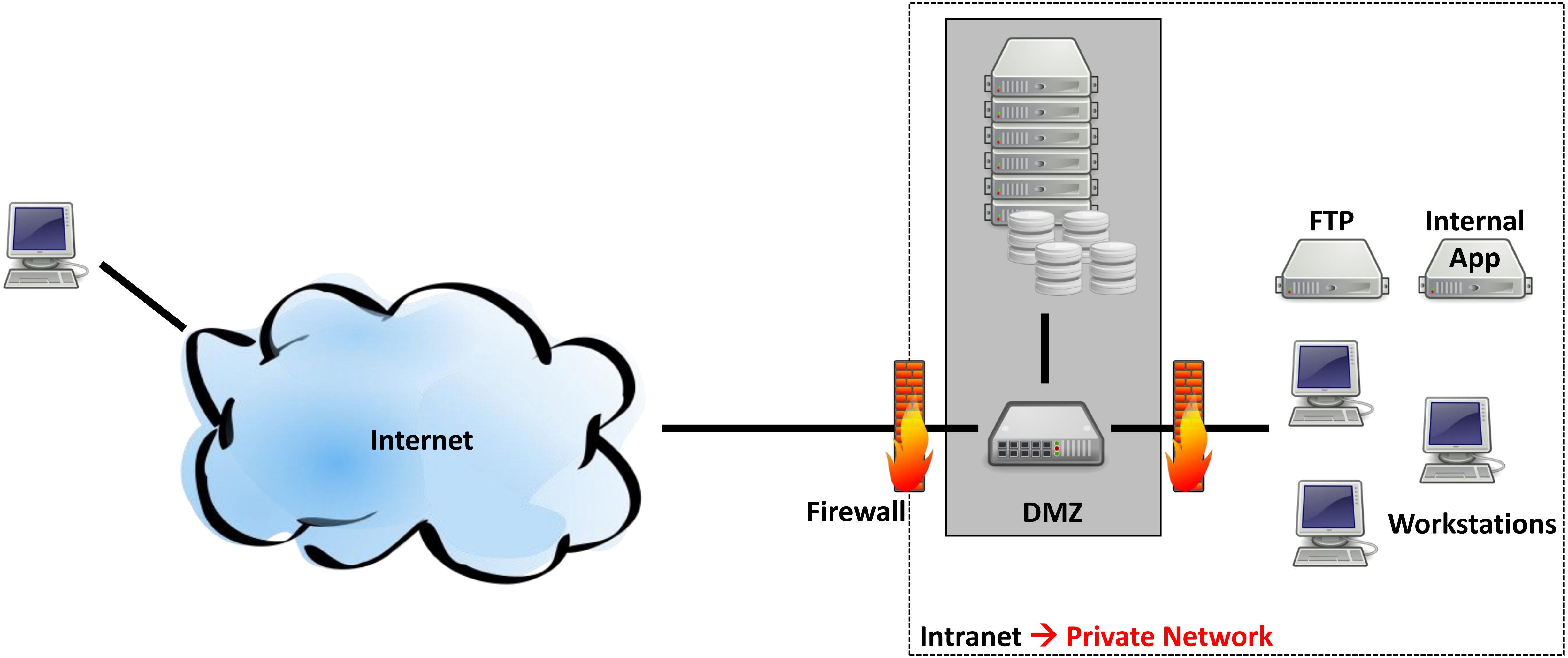
What about applications lacking security?



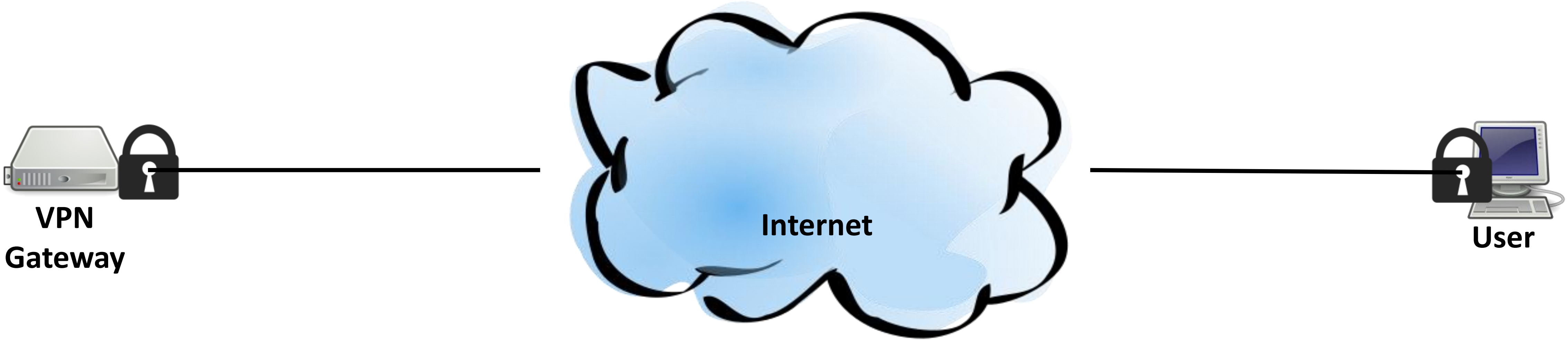
Security in Local Infrastructures



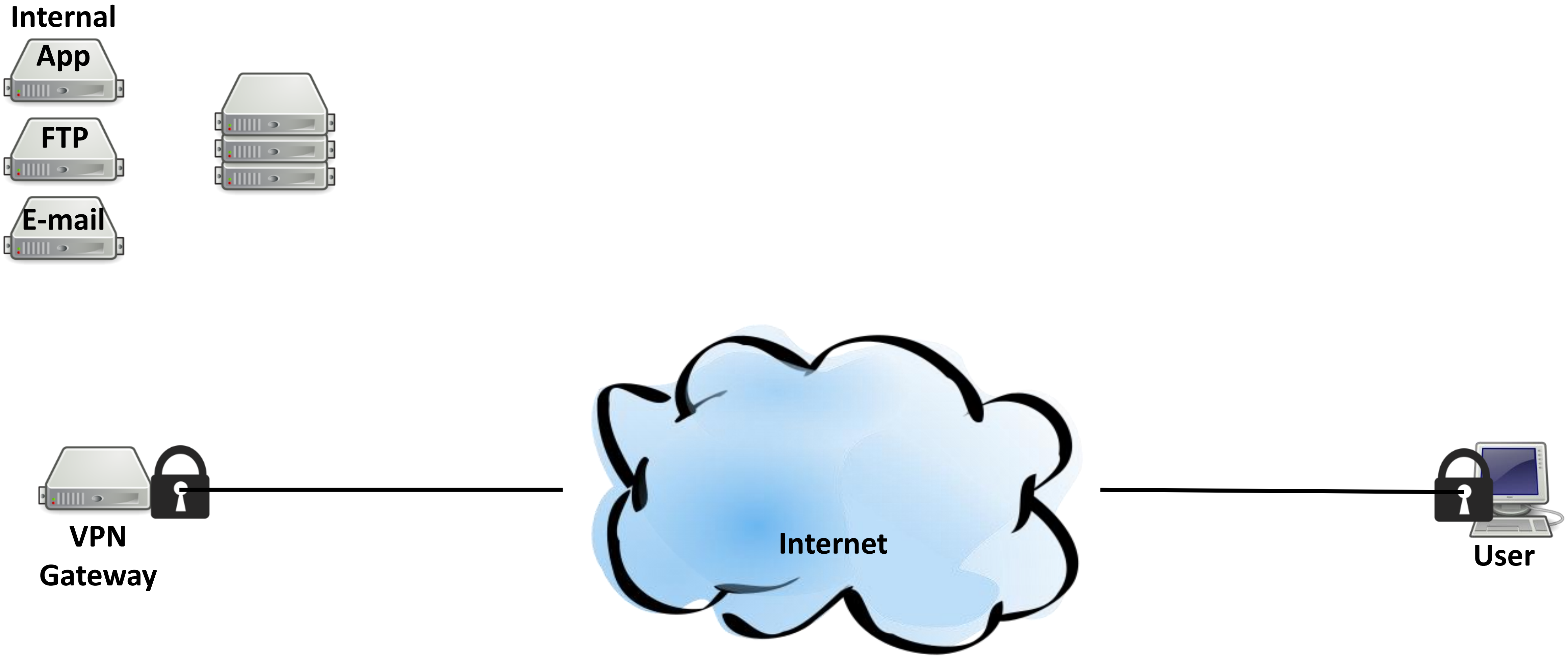
Security in Local Infrastructures



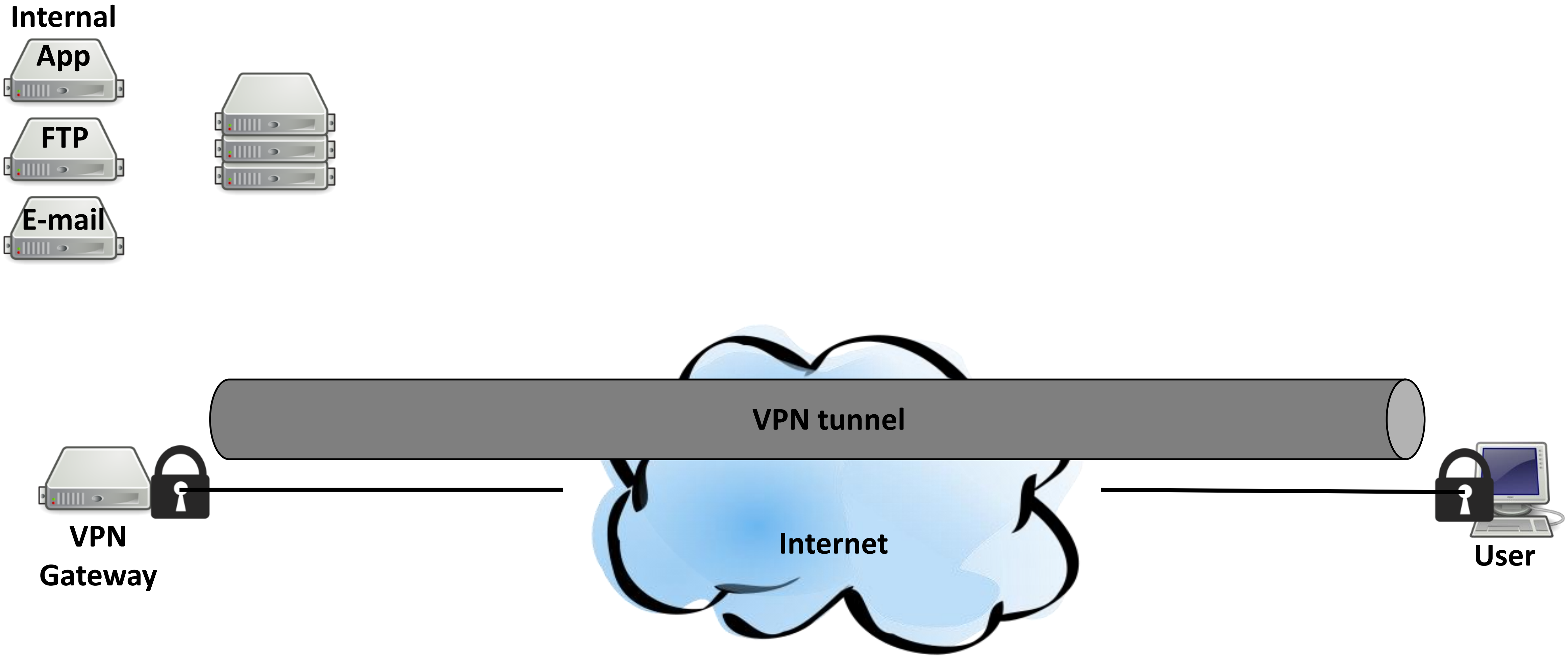
Virtual Private Network



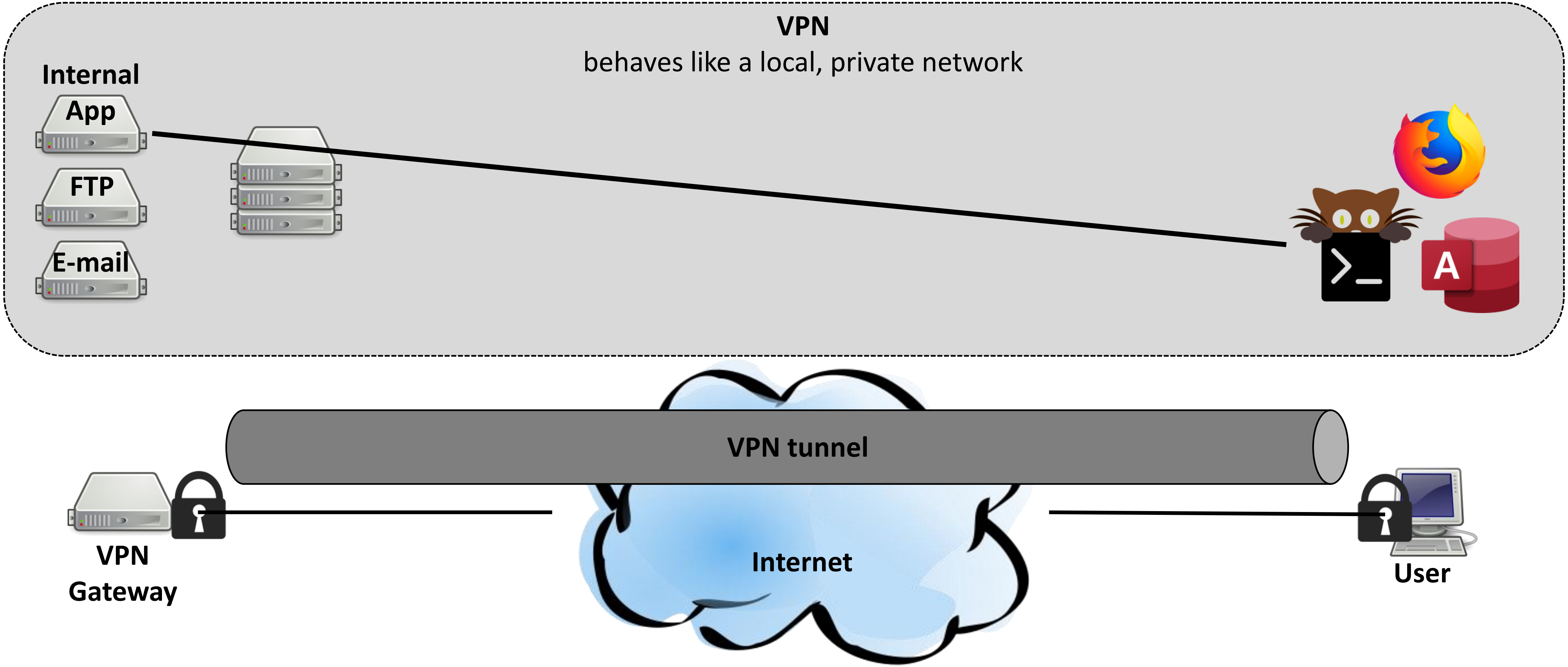
Virtual Private Network



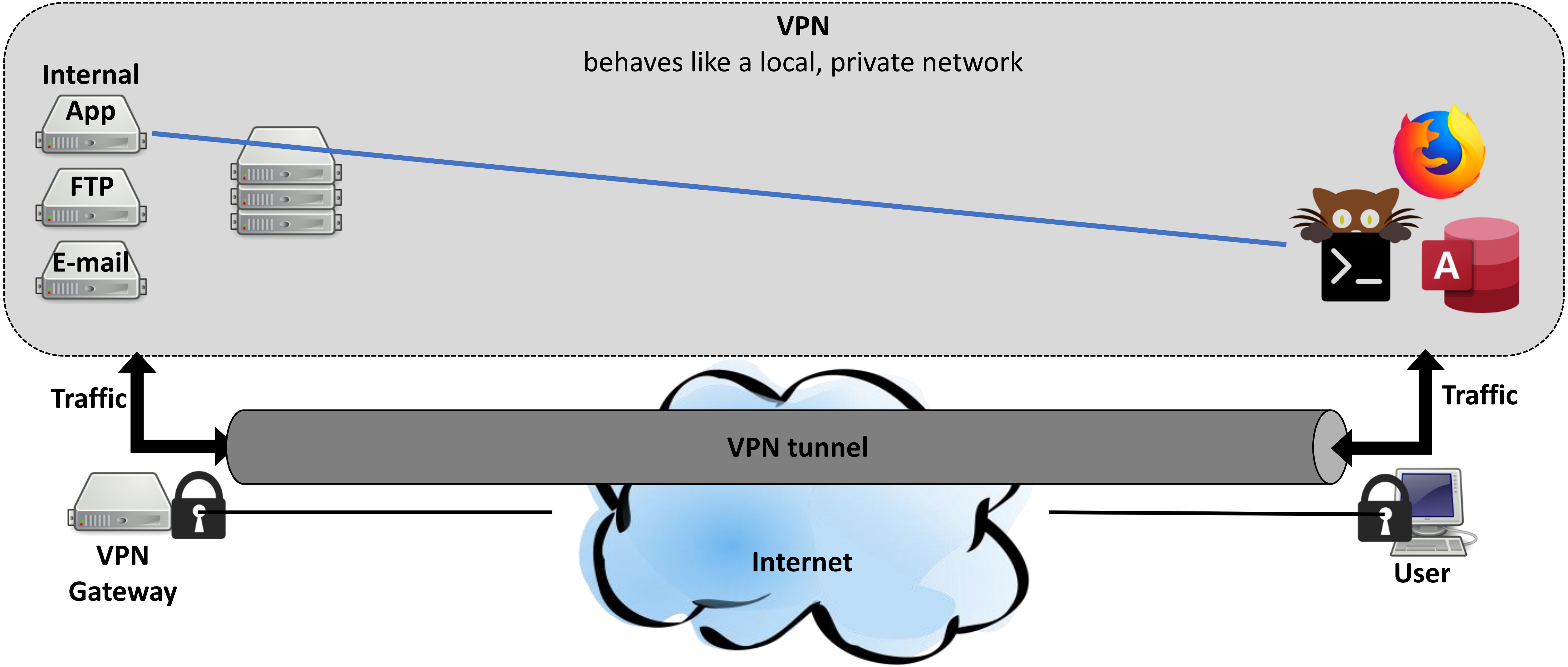
Virtual Private Network



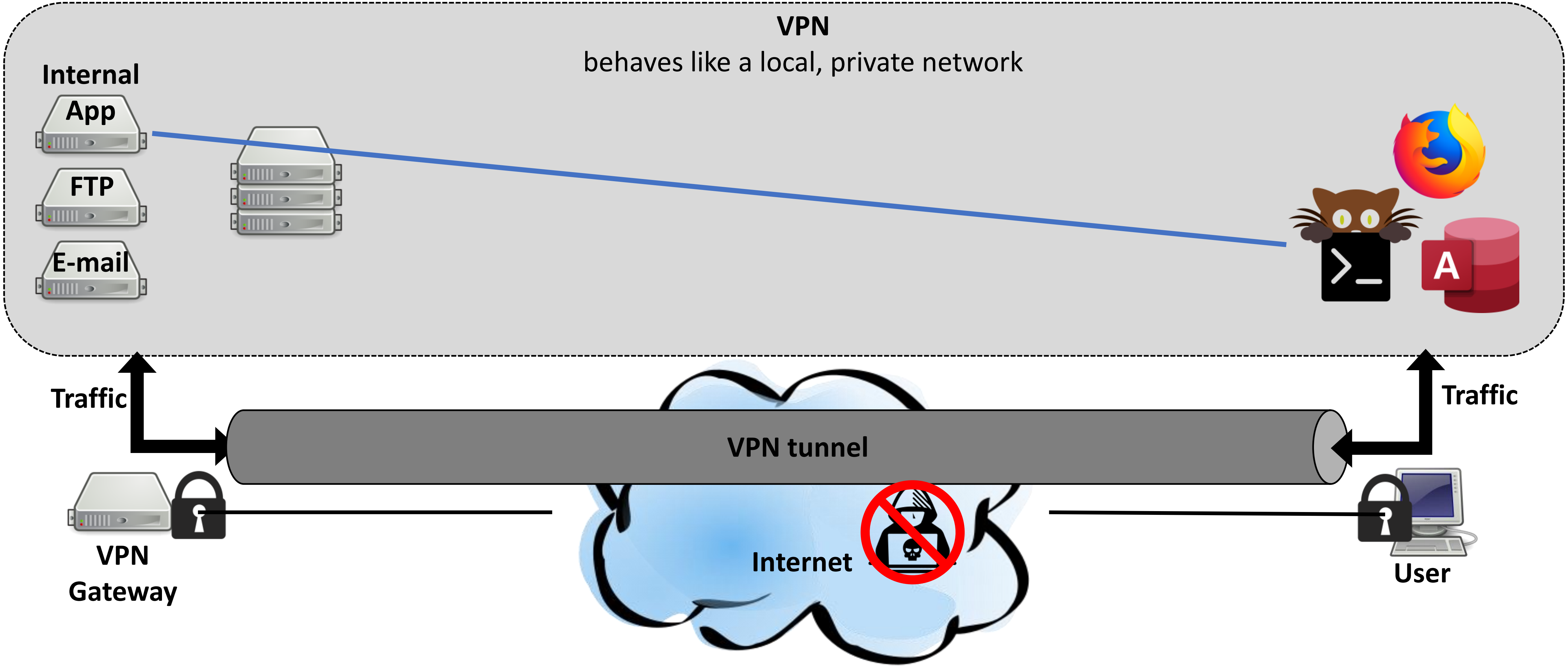
Virtual Private Network



Virtual Private Network

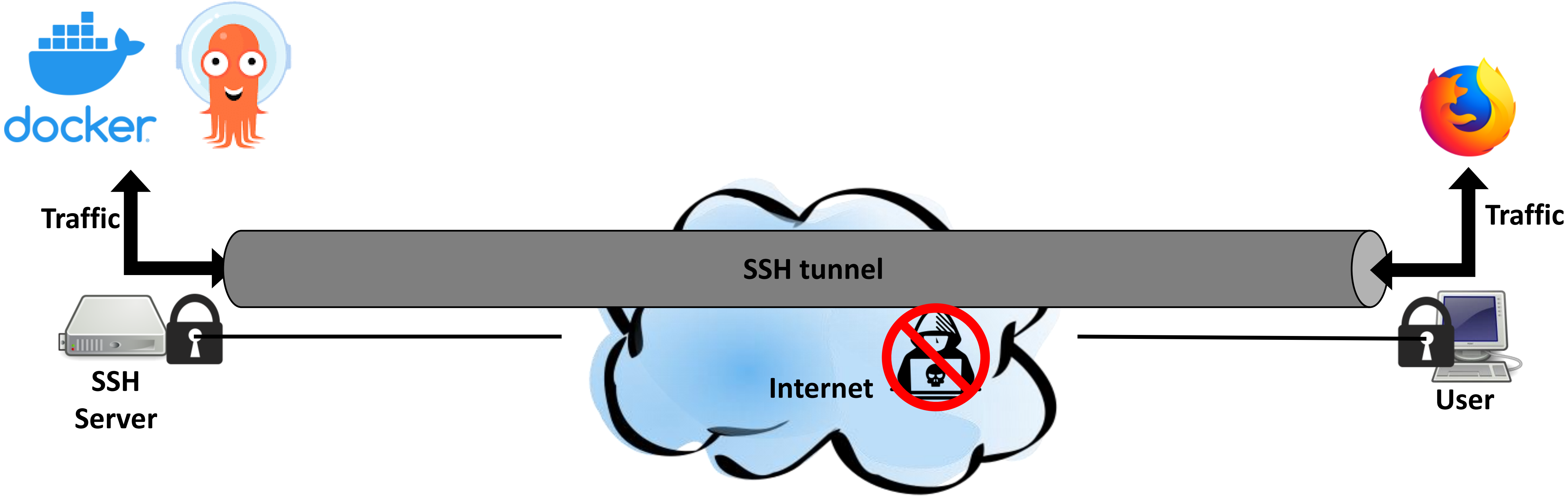


Virtual Private Network



SSH tunnels

- Simpler, but some concepts in common with VPNs
  - Does not create a local, private network
  - Only allows communication between specific IP:port pairs


docker
Traffic
SSH tunnel
Traffic
SSH
Server
Internet
User