

# Network Design Elements

Christopher Rees

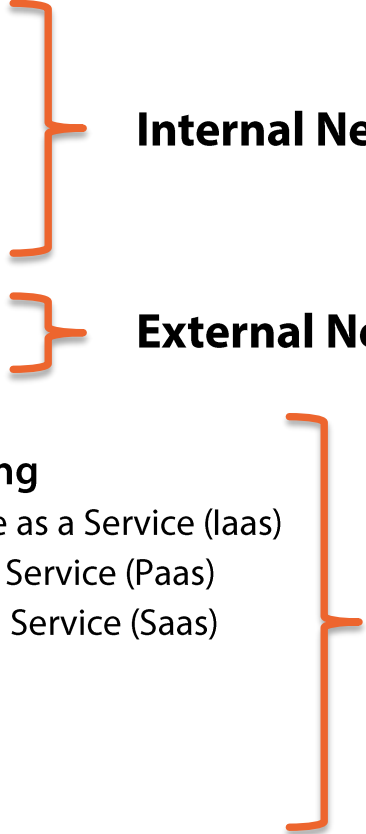
<https://www.linkedin.com/in/cdrees>

@cdrees



**pluralsight**   
hardcore dev and IT training

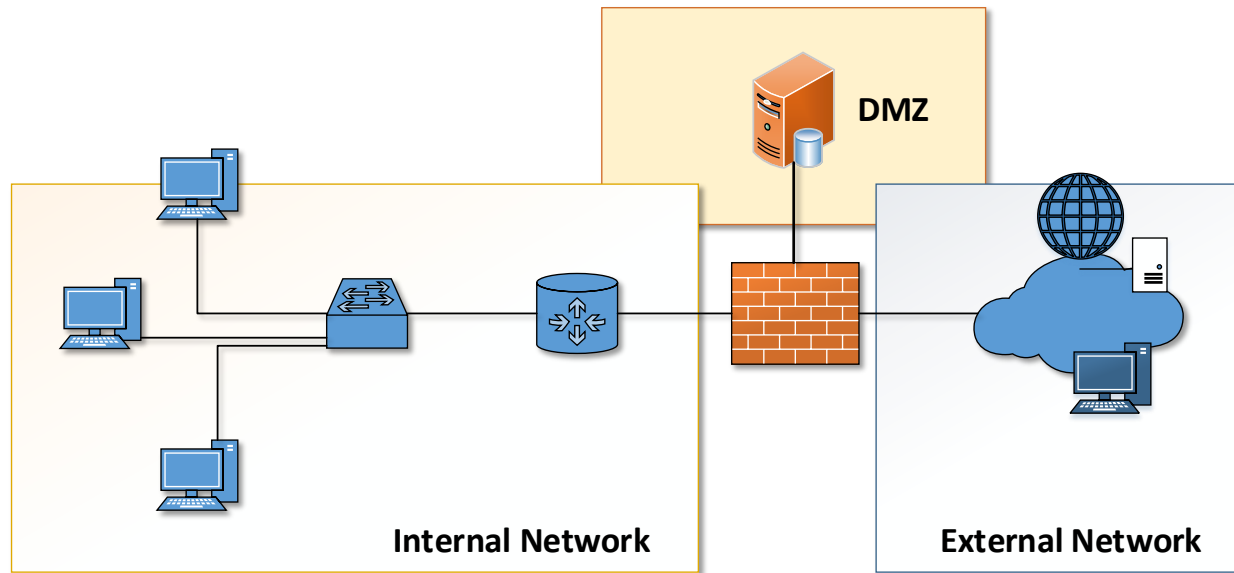
# Module Overview

- DMZ
  - Subnetting
  - VLAN
  - NAT
  - Telephony
  - Remote Access
  - NAC
  - Virtualization
  - Cloud Computing
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)
    - Private
    - Public
    - Hybrid
    - Community
  - Layered Security / Defense in Depth
- Internal Network Security**
- External Network Security**
- Virtualized / Cloud Concepts**
- 
- ```
graph LR; subgraph Internal_Network_Security [Internal Network Security]; DMZ; Subnetting; VLAN; NAT; Telephony; end; subgraph External_Network_Security [External Network Security]; Remote_Access[Remote Access]; NAC; end; subgraph Virtualized_Cloud_Concepts [Virtualized / Cloud Concepts]; Virtualization; Cloud_Computing[Cloud Computing]; end; Layered_Security[Layered Security / Defense in Depth];
```

# DMZ

- **DMZ (Demilitarized Zone)**

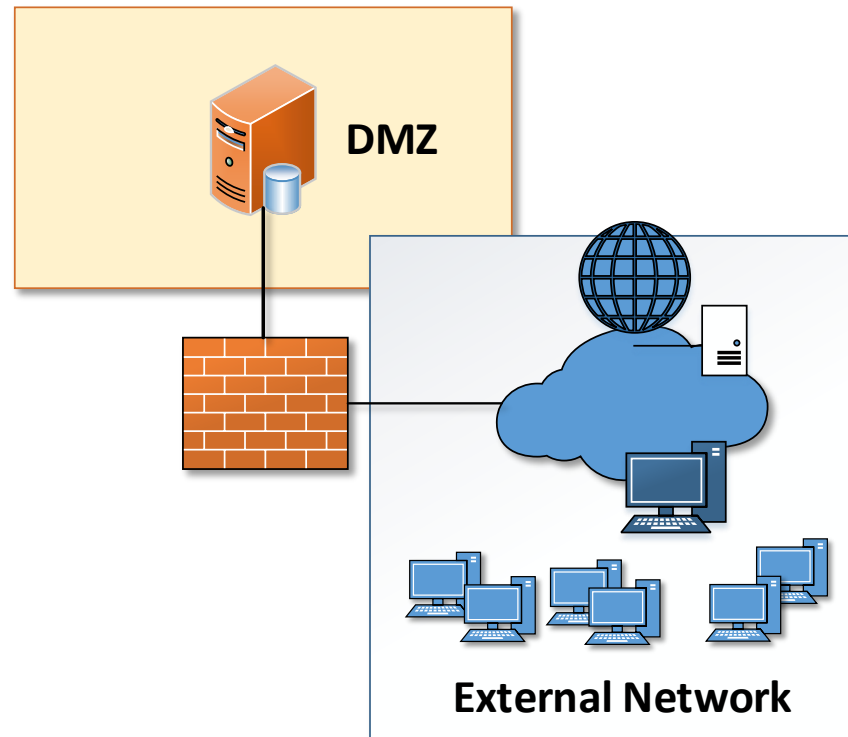
- Area of a corporate network that is accessible from external networks
- Used to provide **public facing** resources
- Sometimes referred to a **"Bastion Host"**



# DMZ

## ■ Typical DMZ Servers and Services

- HTTP (80)
- HTTPS (443)
- External DNS (53)
- SMTP Gateway (25)
- Public FTP Server (21)



# Subnetting

- **Subnetting breaks a larger network into smaller “sub” networks**
  - Used to reduce collisions and increase security

| Class    | Subnet Mask                     | # of Hosts per Network | # of Networks | Start-End Address           |
|----------|---------------------------------|------------------------|---------------|-----------------------------|
| <b>A</b> | 255.0.0.0                       | 16 Million             | 127           | 10.0.0.0 – 126.255.255.255  |
| <b>B</b> | 255.255.0.0                     | 65,000                 | 16,000        | 128.0.0.0-191.255.255.255   |
| <b>C</b> | 255.255.255.0                   | 254                    | 2 Million     | 192.0.0.0-223.255.255.255   |
| <b>D</b> | Reserved for multicast groups   |                        |               | 224.0.0.0 – 239.255.255.255 |
| <b>E</b> | Reserved for future use and R&D |                        |               | 240.0.0.0 – 254.255.255.254 |

# Private Address Ranges

- Each class of IP address has a private address range
  - Defined by **RFC 1918 (IPv4)** and **RFC 4193 (IPv6)**
  - Not routable on the Internet
  - Used for private, internal use
  - Many companies will have the **same private addresses** (i.e. 10.x.x.)
  
- Private Ranges
  - **Class A**
    - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - **Class B**
    - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - **Class C**
    - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

# Reducing Congestion



Imagine trying to have a **conversation** with someone  
**4 or 5** tables away!

# Reducing Congestion

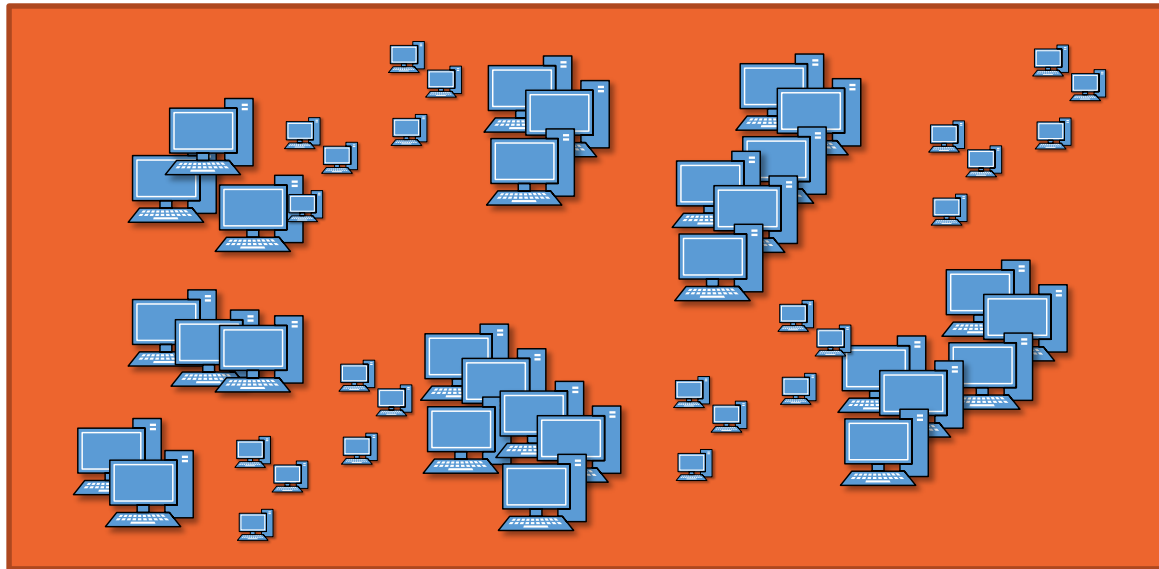


By having multiple, **smaller rooms**, there are less people per room, less noise and congestion. The people in one room can't **listen in** on other room's conversations



# Subnetting Example

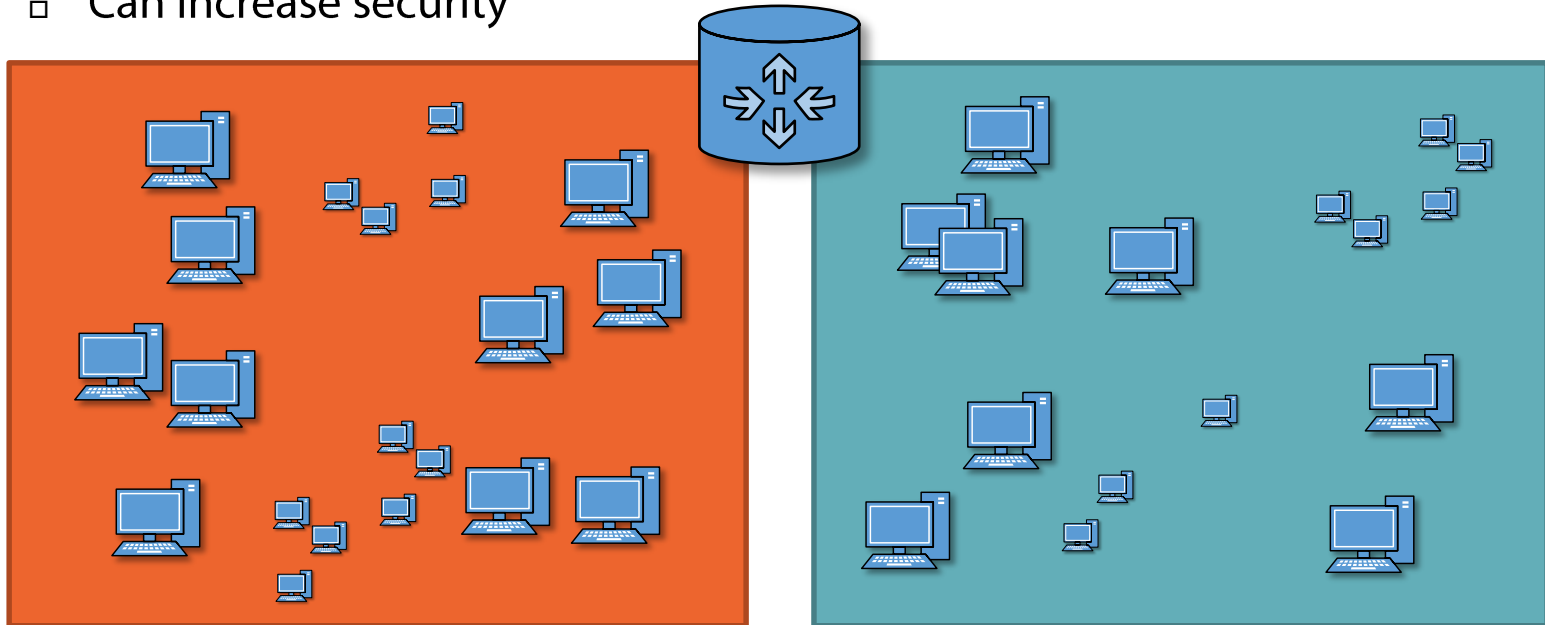
- **Breaking a large network into smaller sub-networks**
  - Reduces congestion
  - Improves flow of traffic
  - Can increase security



**One big network, **LOTS** of traffic, **collisions** and limited security**

# Subnetting Example

- Breaking a large network into smaller sub-networks
  - Reduces congestion
  - Improves flow of traffic
  - Can increase security



**Two smaller networks, reduced traffic, fewer collisions and increased security**

# Subnetting Example

- **Network 10.0.0.0**
  - Class A Network (16 million possible hosts)
  - Too large and unmanageable
- **Subnet into smaller networks by borrowing bits from the net mask**
  - Example: Default subnet of 255.0.0.0
  - We'll borrow bits from the net mask (255.x.x.x)
    - More networks with fewer hosts per network

10.0.0.0/8 (too big)

11111111.00000000.00000000.00000000

10.x.x.0/24 (more manageable)

11111111.11111111.11111111.00000000

# Subnetting Example

- 10.0.0.x/8

- 11111111.00000000.00000000.00000000



The diagram shows the binary representation of the IP address 10.0.0.x. The first octet is 11111111, and the next three octets are 00000000. A black bracket under the first octet is labeled 'Network'. An orange bracket under the remaining three octets is labeled 'Hosts'.


Network Hosts

$$2^8 = 256$$

(0-255)

- 10.x.x.x/24

- 11111111.11111111.11111111.00000000

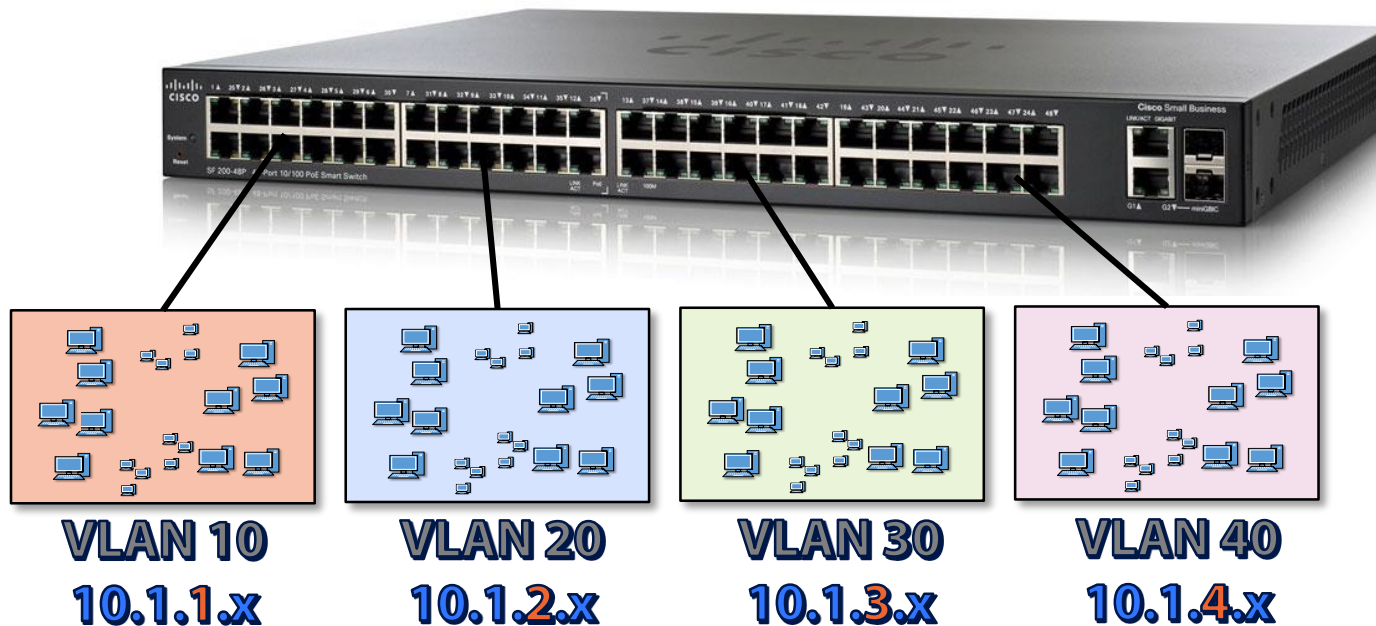


The diagram shows the binary representation of the IP address 10.x.x.x. The first three octets are 11111111, and the last octet is 00000000. A black bracket under the first three octets is labeled 'Network'. An orange bracket under the last octet is labeled 'Hosts'.

Network Hosts

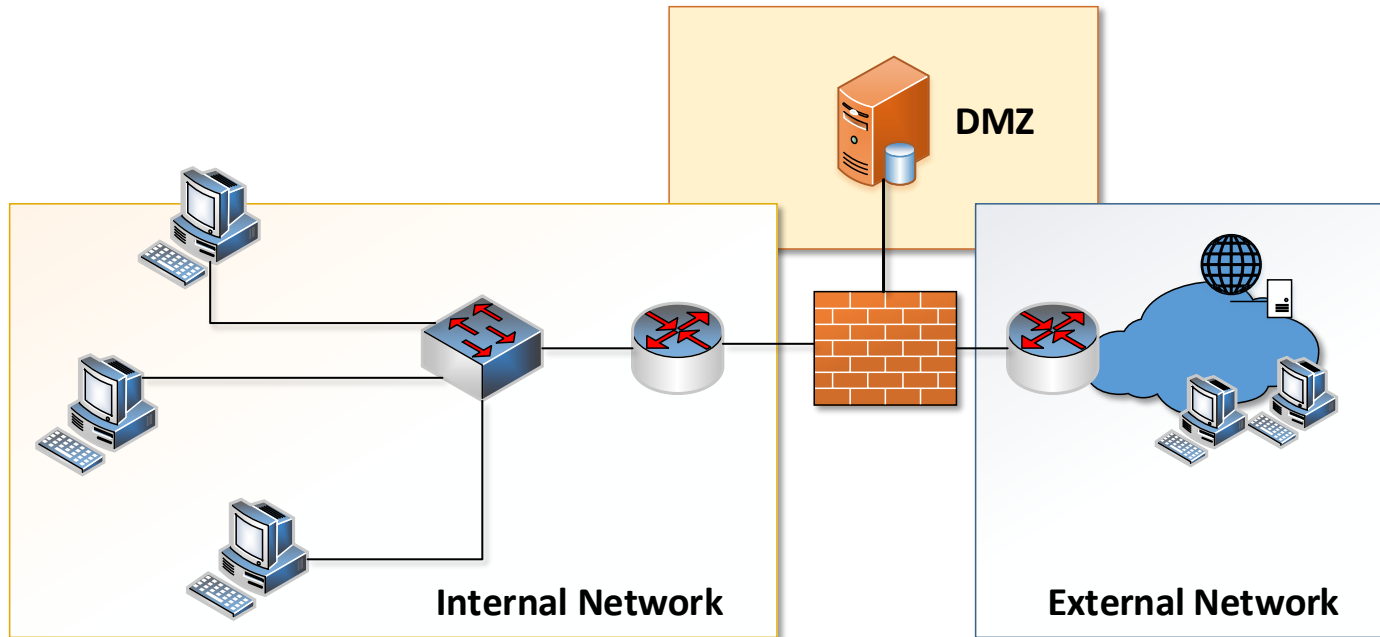
# VLAN

- **Virtual Local Area Network (VLAN)**
  - Goes hand in hand with subnetting
  - As we break a network up into smaller networks, we can assign each sub-network to it's own VLAN
    - VLAN is a layer 2 concept
    - IP Networks are a layer 3 concept

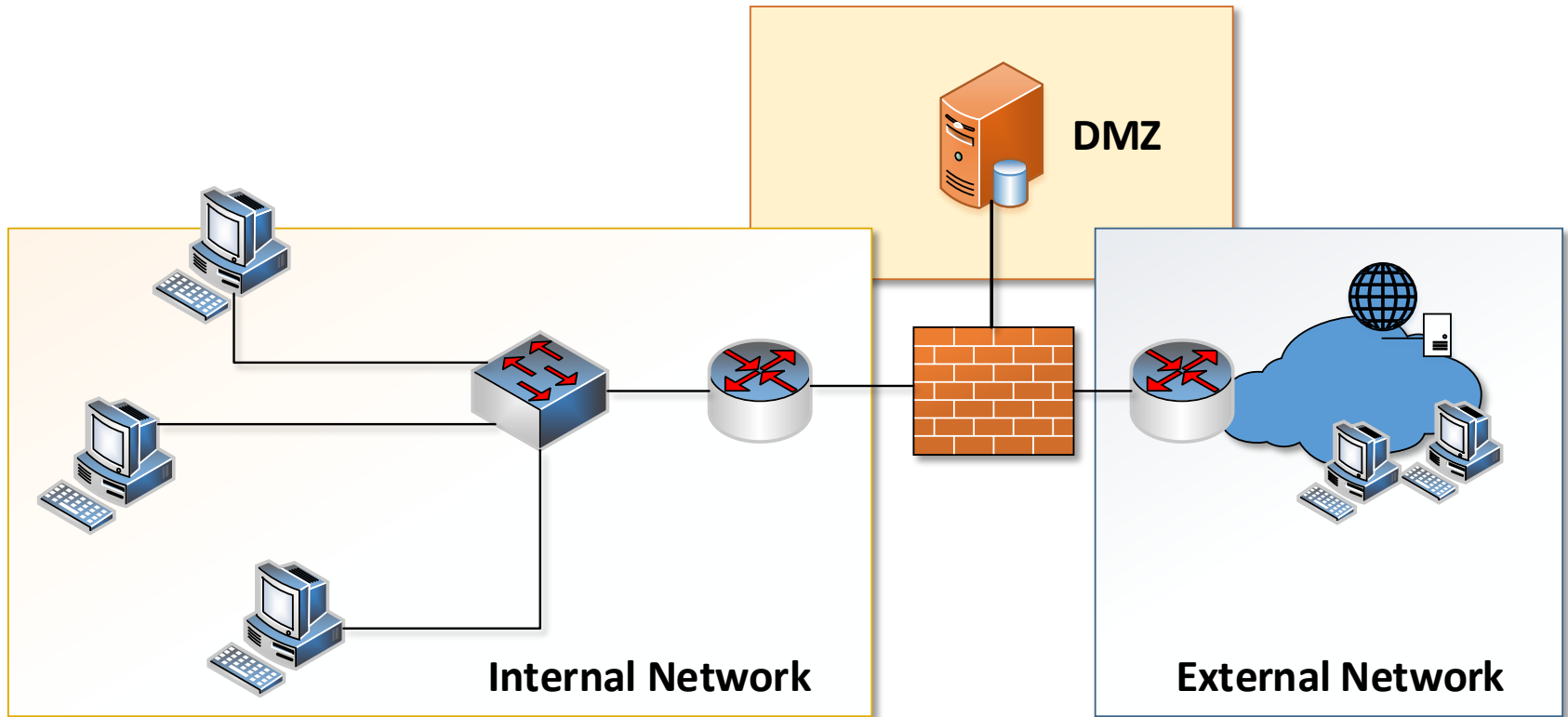


# NAT

- **Network Address Translation (NAT)**
  - Mask (Hide) the private IP address form the internal network as it goes out into the public external network



# NAT Example



**10.0.1.15/24 -> 25.1.15.0/28**

**Subnet Mask of 255.255.255.240**  
**16 IP addresses / 14 Hosts Available**  
**25.1.15.0 – 25.1.15.15 (Range)**  
**25.1.15.1 – 25.1.15.14 (Usable Hosts)**

# NAT and PAT

- **NAT**

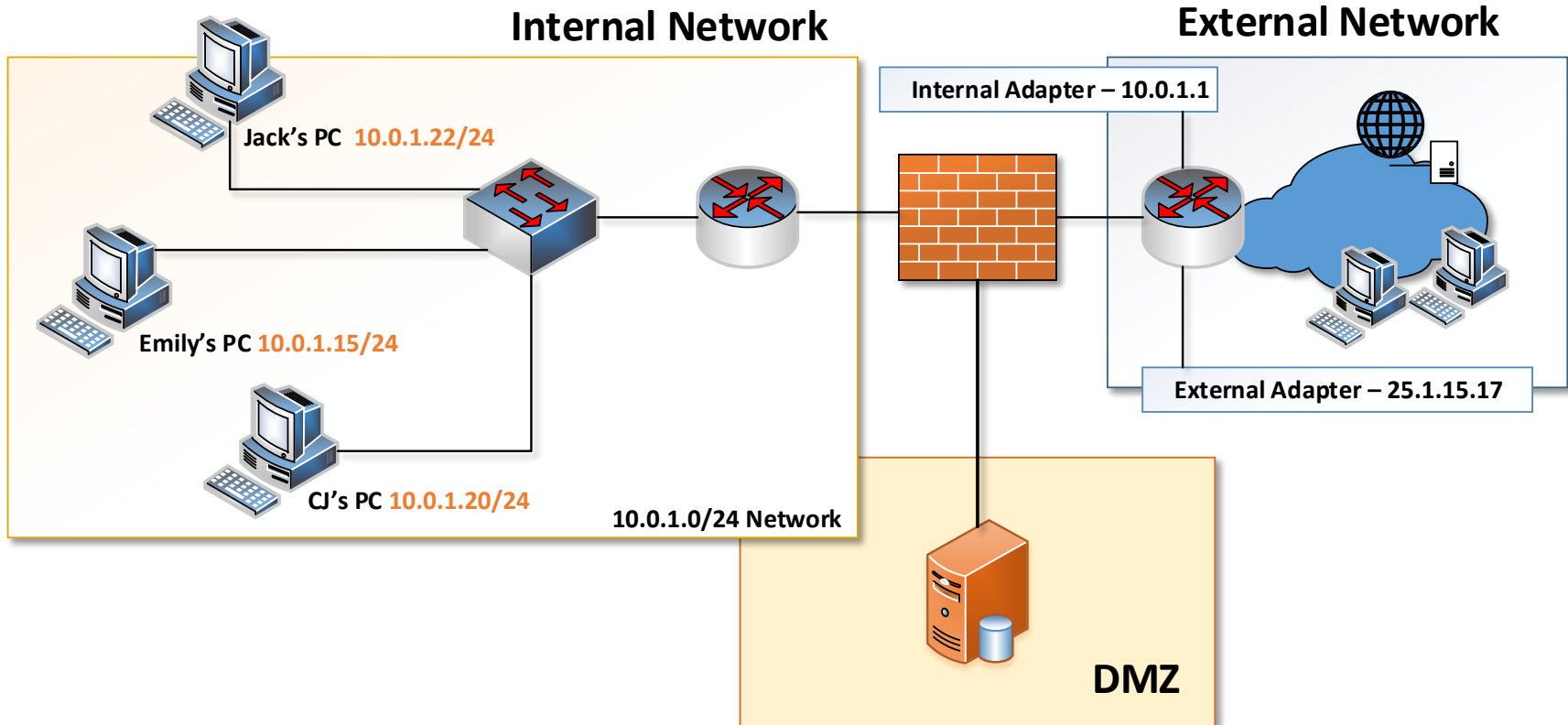
- 1 to 1 mapping
- Not necessarily scalable in very large environment depending on IP block

- **PAT (Port Address Translation)**

- Firewall or NAT/PAT device keeps track of internal requests and maps them to a single external IP
- Uses PORTS to keep track connections and traffic



# Port Address Translation (PAT)



10.0.1.22:80 → 25.1.15.17:13389 → Destination Address

10.0.1.15:80 → 25.1.15.17:14240 → Destination Address

# Telephony

- **Telephony is IP based voice communication (VoIP)**
  - Susceptible to the same types of attacks and outages as computer traffic
  - VoIP traffic is more sensitive to network fluctuations
    - Latency can cause stutter or dropped packets
- **Traffic should be segmented with VLANs**
  - VoIP outage doesn't affect data network and vice-versa
  - QoS can be applied to VoIP traffic
  - Increases security



# Module Overview

- DMZ
  - Subnetting
  - VLAN
  - NAT
  - Telephony
  - Remote Access
  - NAC
  - Virtualization
  - Cloud Computing
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)
    - Private
    - Public
    - Hybrid
    - Community
  - Layered Security / Defense in Depth
- Accessing Corporate Resources Remotely**

# Remote Access

- **Accessing corporate resources remotely**
  - Tele-commuters
  - Work from home
  - Road Warriors
  - Branch locations
  
- **VPN access enables access to some or all corporate resources**
  - Authenticate via RADIUS or some authentication
    - Two-factor, token, etc.
    - Network Admission Control my quarantine workstation or device until compliant

# NAC

- **Network Access Control or Network Admission Control**
  - Refers to a set of policies that define a minimal set of requirements each device must have before being allowed on the network
    - Anti-virus installed and up to date
    - Certain OS / Patch level
    - Applications
  - Becoming more important as BYOD becomes more and more prevalent
    - Good Messaging
    - Mobile Iron
    - Airwatch
- **Devices can be denied access or placed in a secure zone until minimal requirements are met**

# Virtualization

- **Virtualized infrastructure**
  - Workstations
  - Servers
  - Storage
  - Networking
  
- **Major Players in the Virtualization Space**
  - Vmware
  - Microsoft Hyper-V
  - KVM
  - Oracle

# Virtualization

- Taking the capabilities and “personality” of a physical device and converting to a virtual representation
  - Can perform the same functions as its physical counterpart
  - Lower infrastructure costs
  - Increased licensing costs (hypervisor license)

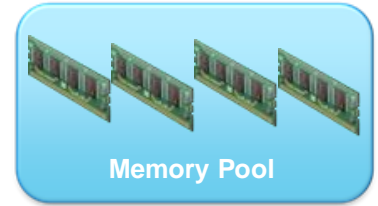
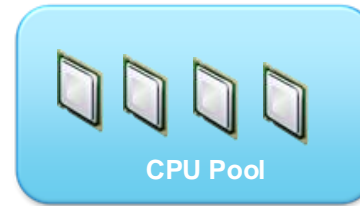


Traditional Server



Virtualized (VMware)

# VMware Example





## Vmware vCenter – Main Screen

## Vmware vCenter – Guest Information

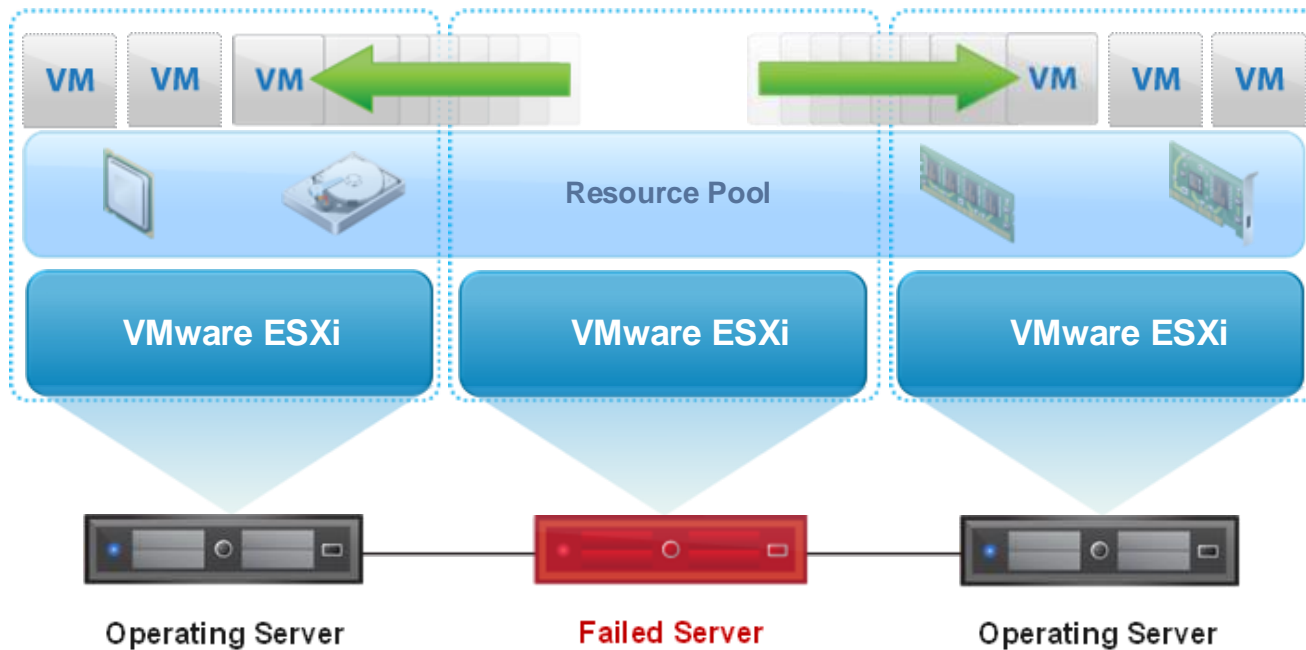
# Cloud Computing

- **Virtualization of infrastructure, platform and services**
  - Automation and self-service
  - Reduced time to market
  - Increased speed to develop and deliver
- **Cloud Computing**
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
    - Private
    - Public
    - Hybrid
    - Community



# “X” as a Service...

- “[Insert Buzzword] as a Service”
  - Virtualization and Commoditization of almost every layer of the IT “Stack”
  - Provides for quicker deployment along with increased HA/DR



# Infrastructure as a Service

- **IaaS allows for distribution and consumption of resources as a service**
  - Multiple users can utilize the same infrastructure (multi-tenant)
  - Allows for elastic scaling as needs and demands increase/decrease



**Compute**



**Network**



**Storage**

- **Typically priced using a utility model**
  - Shifts spend from CAPEX to OPEX
- **Can be private or public (or both)**

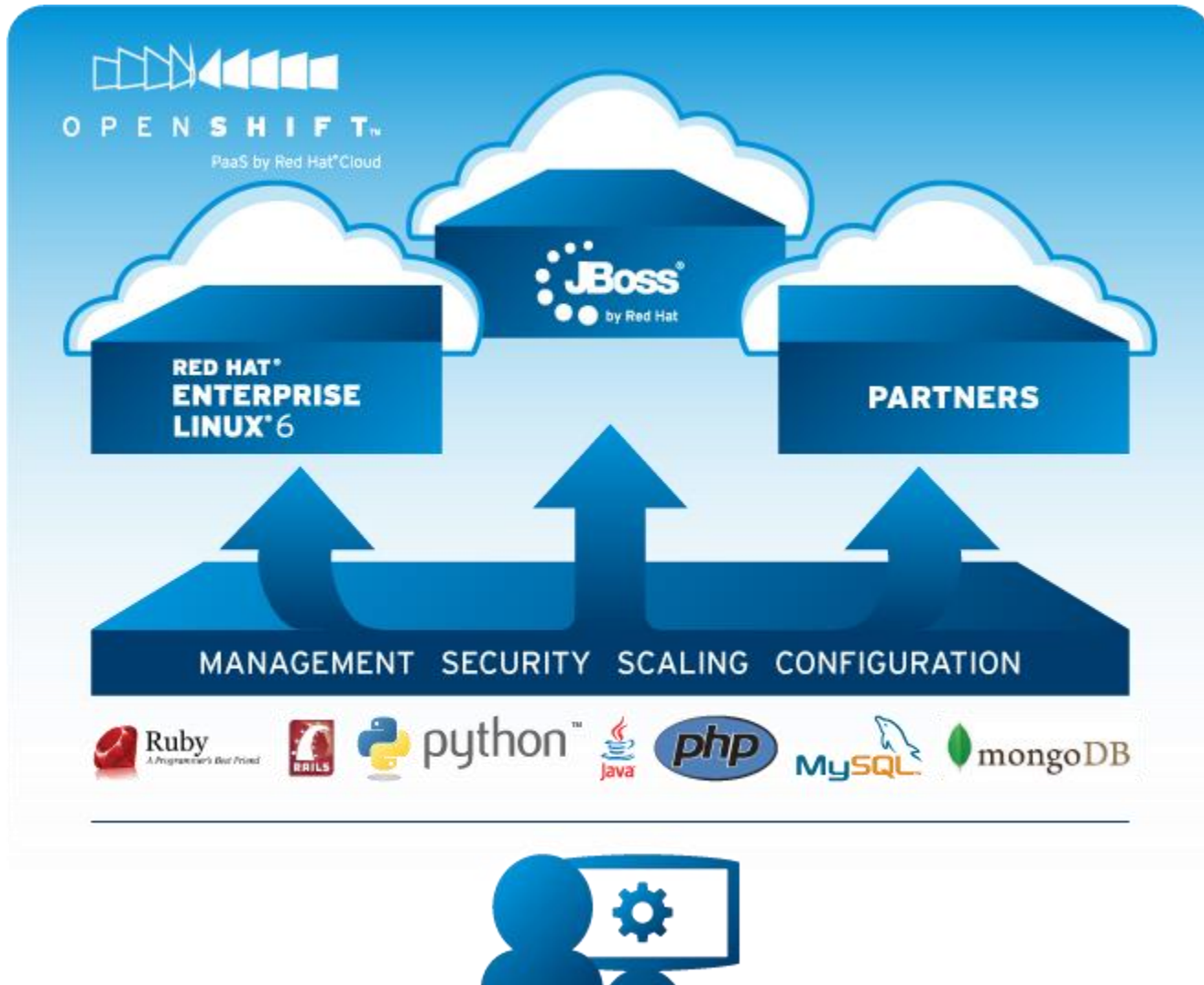
# Platform as a Service

- A **PaaS environment** is comprised of computational resources (i.e. test/dev environments) that be easily created and configured
  - No need to order, acquire, rack/stack hardware, configure network, IP addresses, load balancers, VLANs, install software, configure, etc.
  - Test environments can be quickly created, expand as needed, run tests, report and tear down on demand
  - Multi-tenant – where many users can use the same set of resources

## Example **PaaS** Providers

- AWS Elastic Beanstalk
- Windows Azure
- Heroku
- Force.com
- Google App Engine
- Apache Stratos
- Openstack (Redhat)
- Cloud Foundry (Pivotal)

# Platform as a Service



# Software as a Service

- **SaaS (Software as a Service)**
  - Applications that are provided on demand
    - No setup, installation, configuration required
    - Examples: Salesforce, Office 365, Google Apps

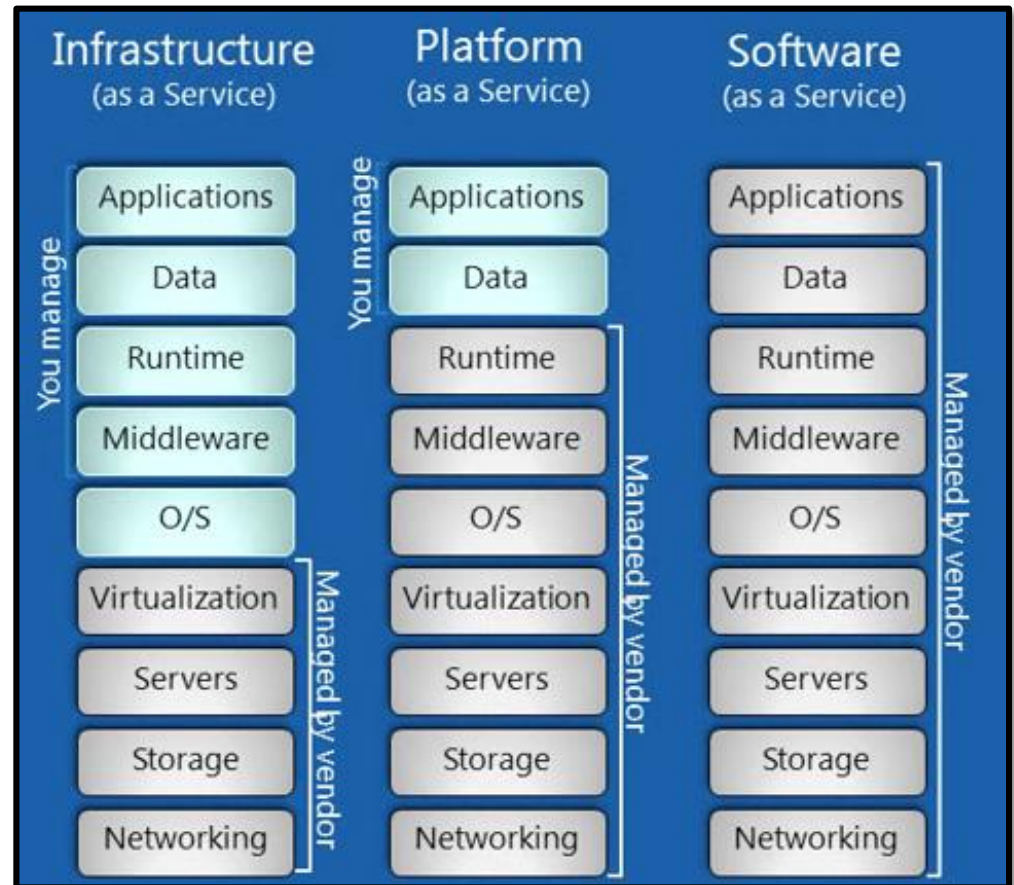




# IaaS, PaaS and SaaS Differentiators

- **Infrastructure as a Service**
  - You manage the OS up
- **Platform as a Service**
  - You manage the Data up
- **Software as a Service**
  - You manage nothing

*If you're running a Private Cloud, then you are "the vendor" customers are the managers*



# Types of Clouds

- **Private**

- You manage everything on internal resources
  - Could be IaaS, PaaS and/or SaaS

- **Public**

- Cloud provider manages resources (hosted)
- You control the data

- **Hybrid**

- Public and Private mix
- Resources are typically created internal (private) and then scaled (elastic) as needed

- **Community Cloud**

- Resources are **shared** among several groups/companies/organizations
- Can be public or private but costs are spread across members

# Layered Security / Defense in Depth

- **Multi-tiered approach to security**
  - Physical Security
    - Guards
    - Locks
    - Cameras
    - Badge Access areas
  - Technological Security
    - Network access controls
    - Desktop/Server access controls
      - Strong passwords
      - RBAC
    - Anti-virus
    - Malware detection
    - Intrusion detection/prevention systems



# Module Review

- DMZ
  - Subnetting
  - VLAN
  - NAT
  - Telephony
  - Remote Access
  - NAC
  - Virtualization
  - Cloud Computing
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)
    - Private
    - Public
    - Hybrid
    - Community
  - Layered Security / Defense in Depth
- Internal Network Security**
- External Network Security**
- Virtualized / Cloud Concepts**
-