تهدیدات امنیتی، معماری و طراحی ایمن شبکه ها و زیرساخت سازمانی

ایمان مجتهدین یزدی mojtahedin@cert.um.ac.ir

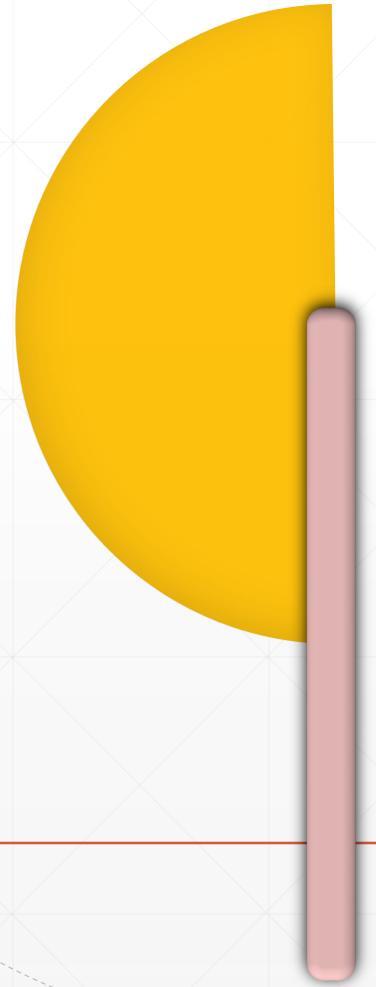
کارشناس آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

سازمان فنآوری اطلاعات ایران – مرکز ماهر – تابستان ۱۳۹۵

(کارگاه آموزشی مدیران و کارشناسان فنآوری اطلاعات – ارومیه – استان آذربایجان غربی)

Outline

- Introduction
- Network Architecture
- Network Security Device



Outline

- **Introduction**
  - Access Control Security
- **Network Architecture**
  - Hierarchical Network Design
  - Access
  - Distribution
  - Core
  - Collapsed
  - Flat Network
- **Network Security Device**
  - Firewall
  - UTM
  - Proxy
  - NAT
  - DMZ
  - IDS/IPS
  - VPN
  - …

قانون جرایم رایانه ای

- **فصل یکم جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی**
- **مبحث یکم دسترسی غیرمجاز**
- **ماده ۱** – هرکس به طور غیرمجاز به داده ها یا سیستم های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.
- **مبحث دوم شنود غیرمجاز**
- **ماده ۲** – هرکس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

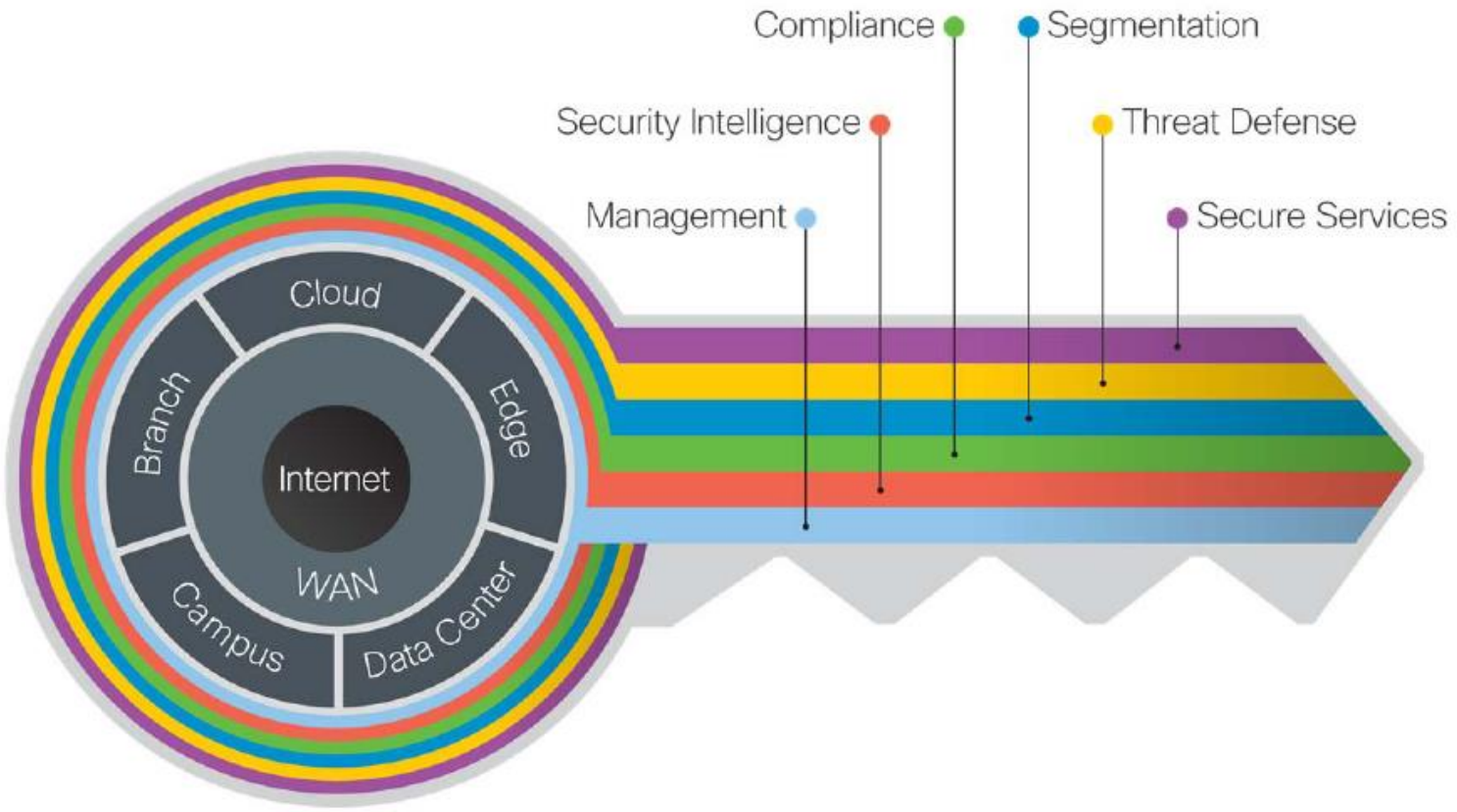
Introduction – هدف از پرداختن به موضوع امنیت در شبکه

- **CIA**
  - Confidentiality (محرمانگی داده ها)
  - Integrity (تمامیت و یکپارچگی داده ها)
  - Availability (در دسترس بودن داده ها)

به عبارتی :

- **کسب اطمینان از اینکه اطلاعات فقط در دسترس افراد مجاز قرار دارد.**
- **تامین صحت، دقت و کامل بودن اطلاعات و روش های پردازش آنها.**
- **کسب اطمینان از اینکه امکان دسترسی به اطلاعات مجاز در هر زمان و از هرمکان برای افراد مجاز مهیا باشد.**

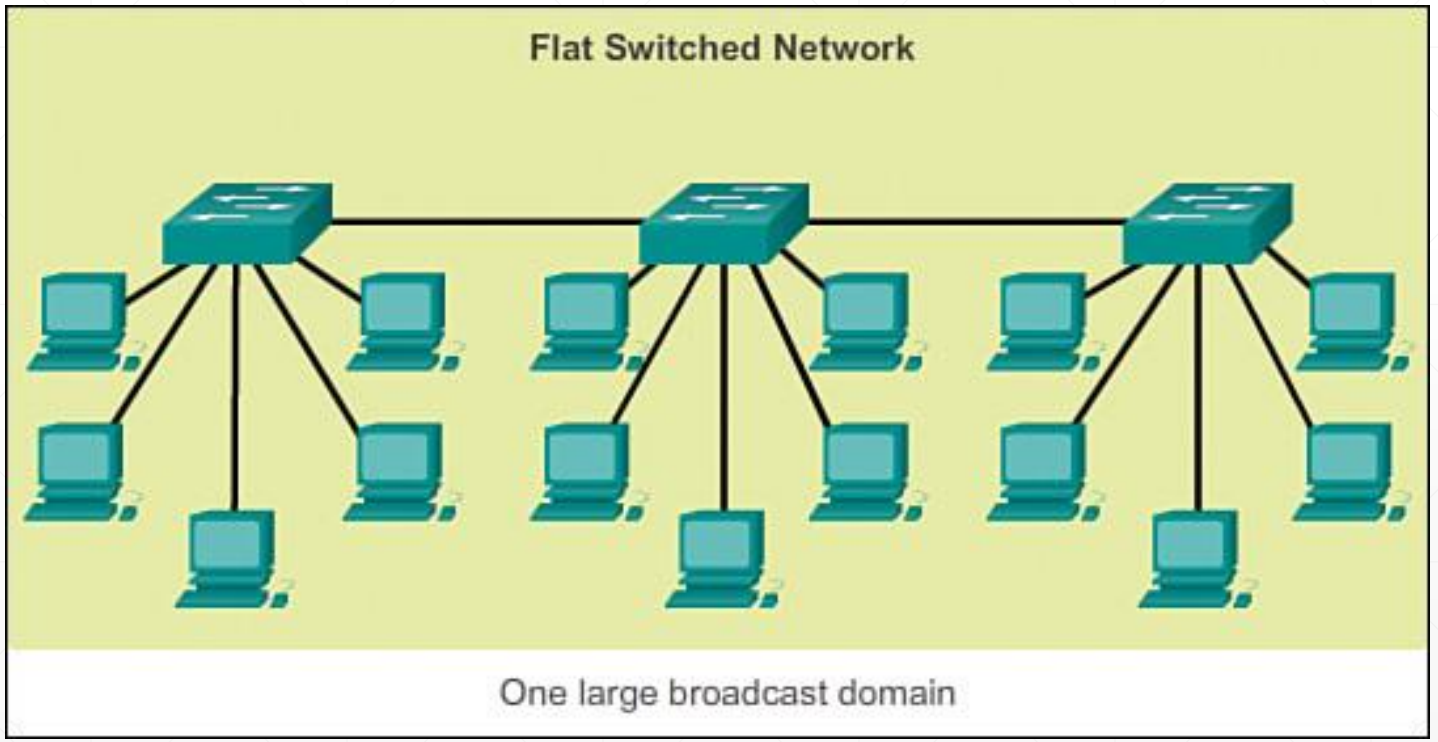
Network Design Layer



- از پیش نیاز های مقوله امنیت، فراهم نمودن معماری و همبندی صحیح اجزای شبکه است.
- یکی از این اجزای، انتخاب، چیدمان و همبندی تجهیزات اکتیو شامل سوئیچ ها، روتر ها، فایروال ها و مواردی از این دست می باشد که شرکت سیسکو معماری سه لایه را در پاسخ به این نیاز ارائه نموده است.

Network Design Layer

- Flat Network
  - The topology of a flat network is not segmented or separated into different broadcast
- **Problems:**
  - Poor security
  - No redundancy
  - Scalability and speed



Network Design Layer

- **Segmentation**

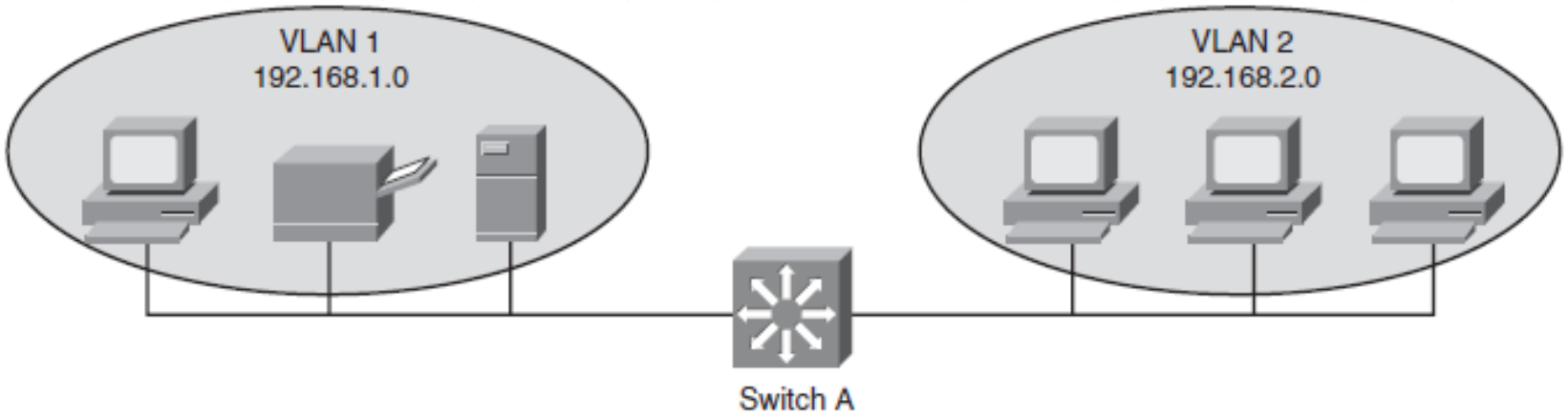
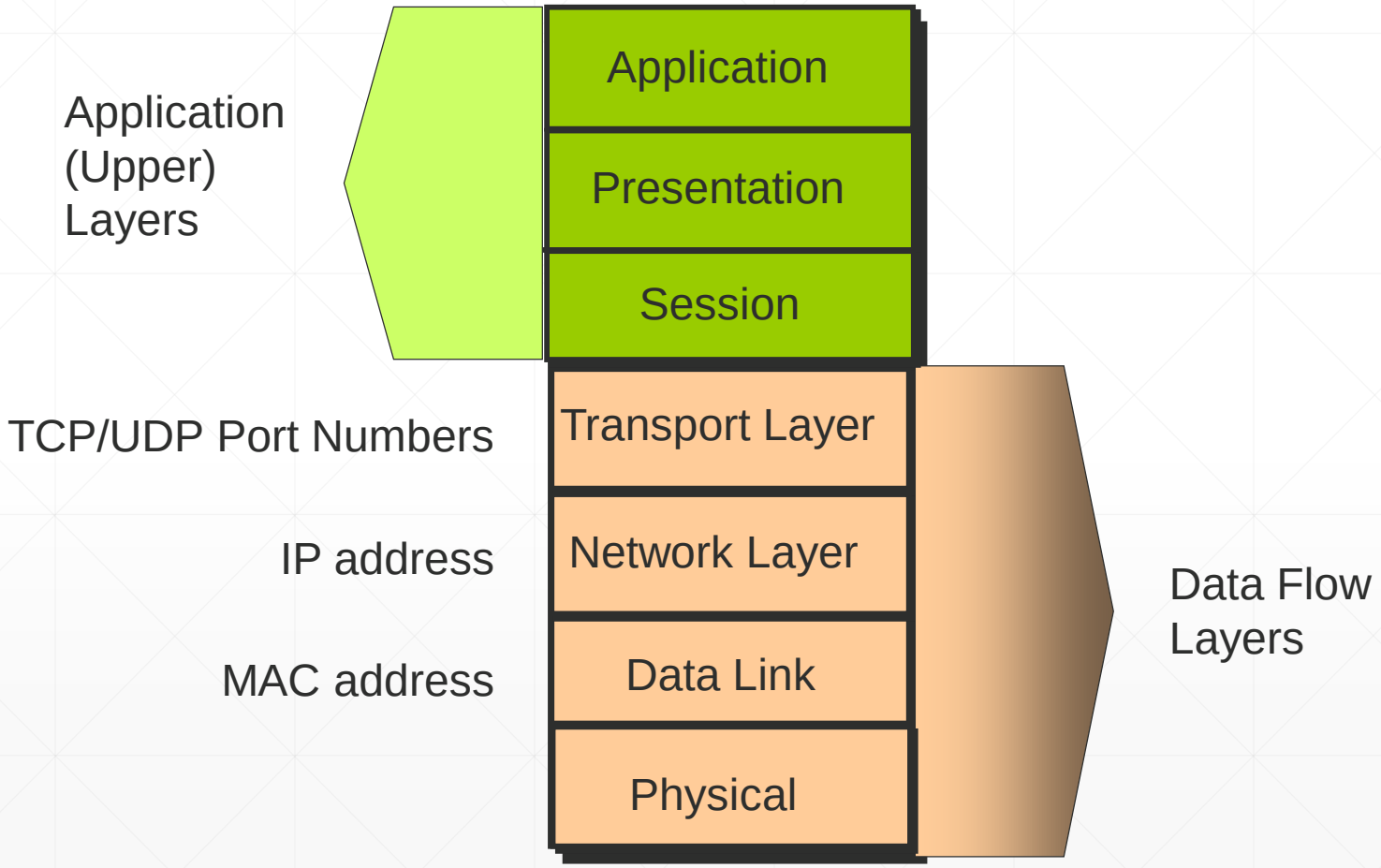


Figure 12-2 *Example of Network Segmentation*

OSI Model Overview



Network Design Layer

- **Modular network design**

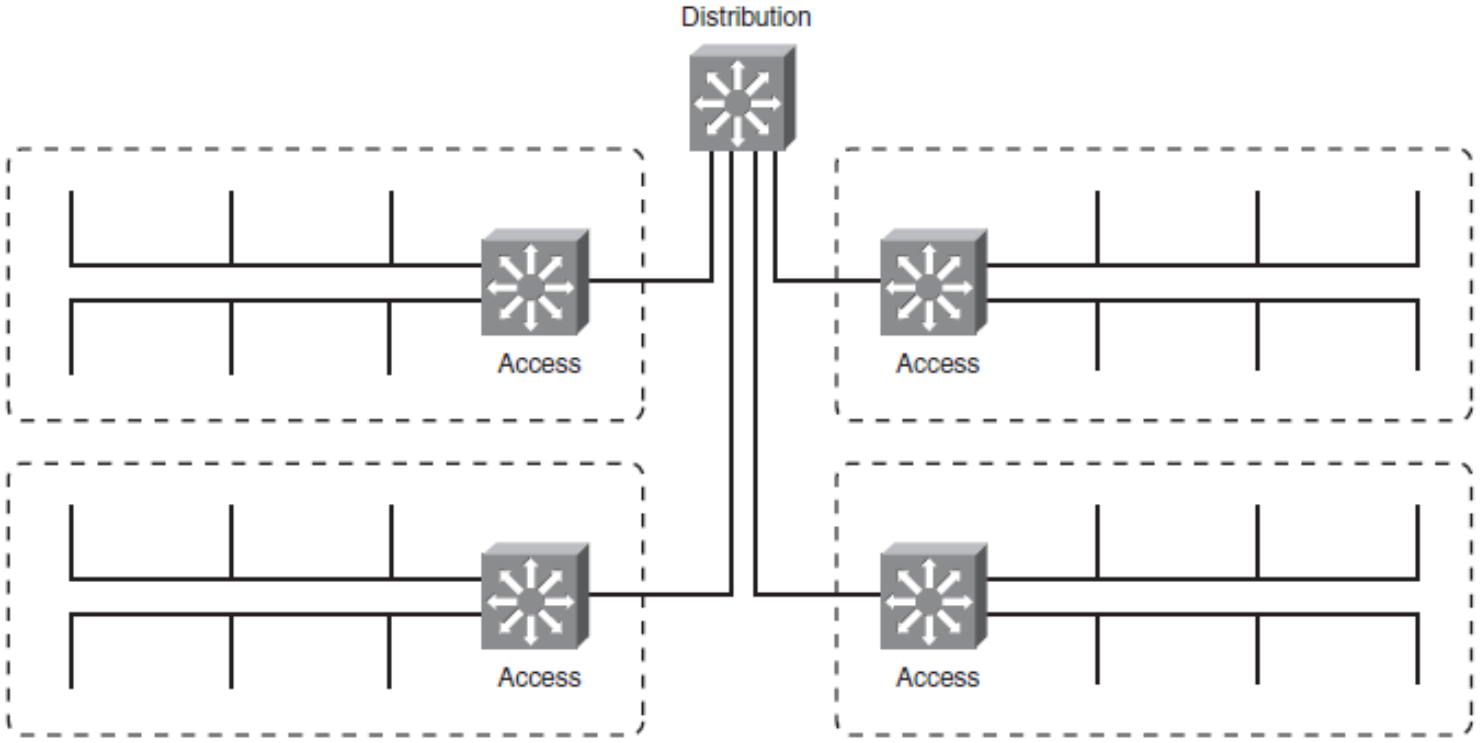


Figure 12-5 *Two-Layer Network Hierarchy Emerges*

Network Design Layer

- Modular network design to answer scalability and speed requirements .

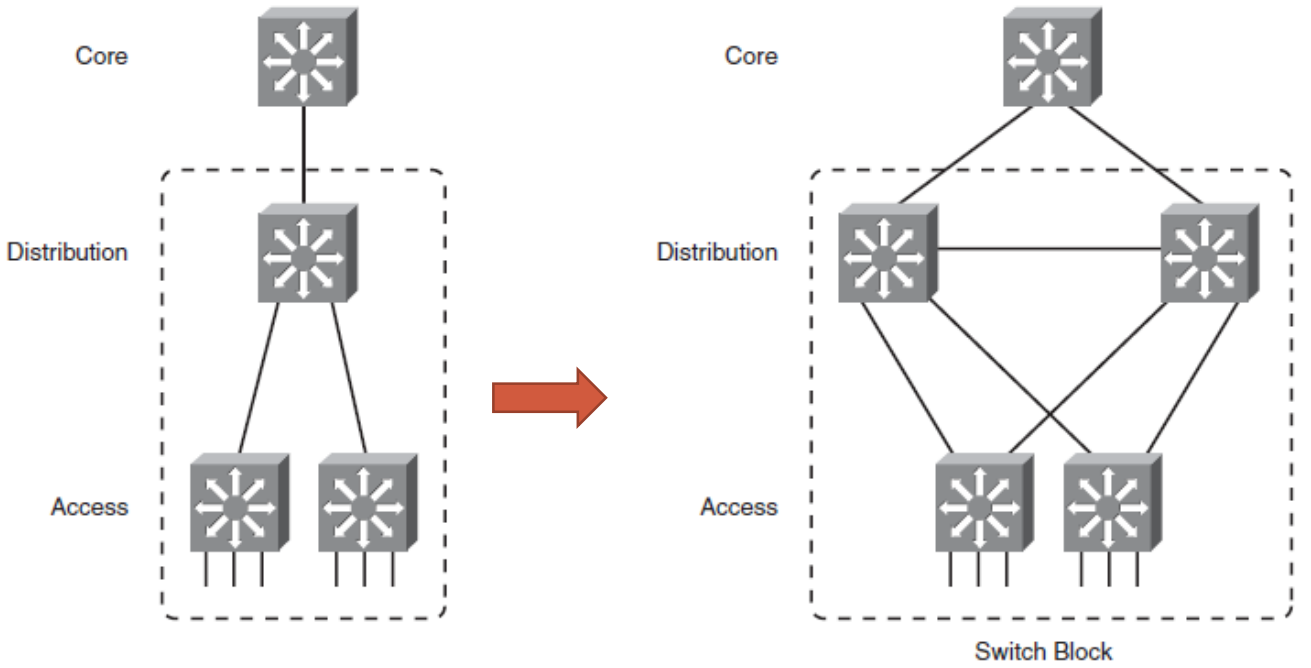


Figure 12-7 *Improving Availability in the Distribution and Access Layers*

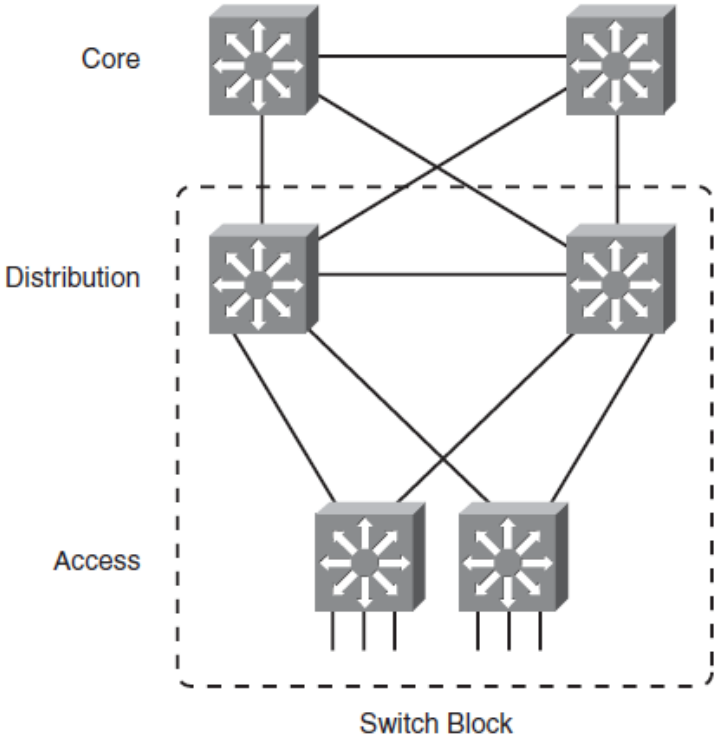
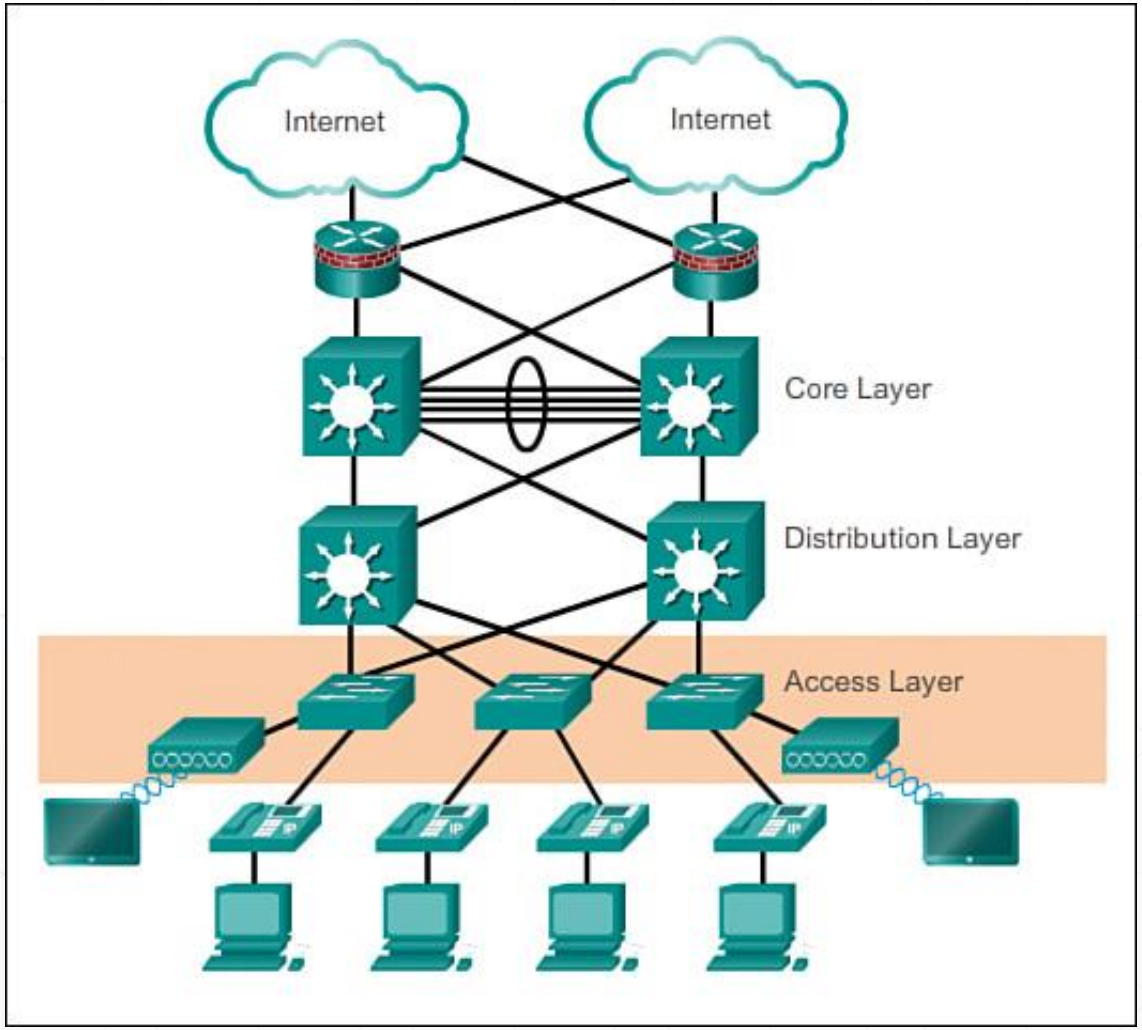


Figure 12-8 *Fully Redundant Hierarchical Network Design*

Network Design Layer

- Hierarchical Network Design
  - Access
  - Distribution (Aggregation)
  - Core



Hierarchical Network Design

- Access-Layer:
  - Low cost per switch port
  - High port density
  - Scalable uplinks to higher layers
  - User access functions such as VLAN membership, traffic and protocol filtering, and quality of service (QoS)
  - Resiliency through multiple uplinks

Hierarchical Network Design

- Distribution Layer:
  - Aggregation of multiple access-layer devices
  - High Layer 3 throughput for packet handling
  - Security and policy-based connectivity functions through access lists or packet filters
  - QoS features
  - Scalable and resilient high-speed links to the core and access layers

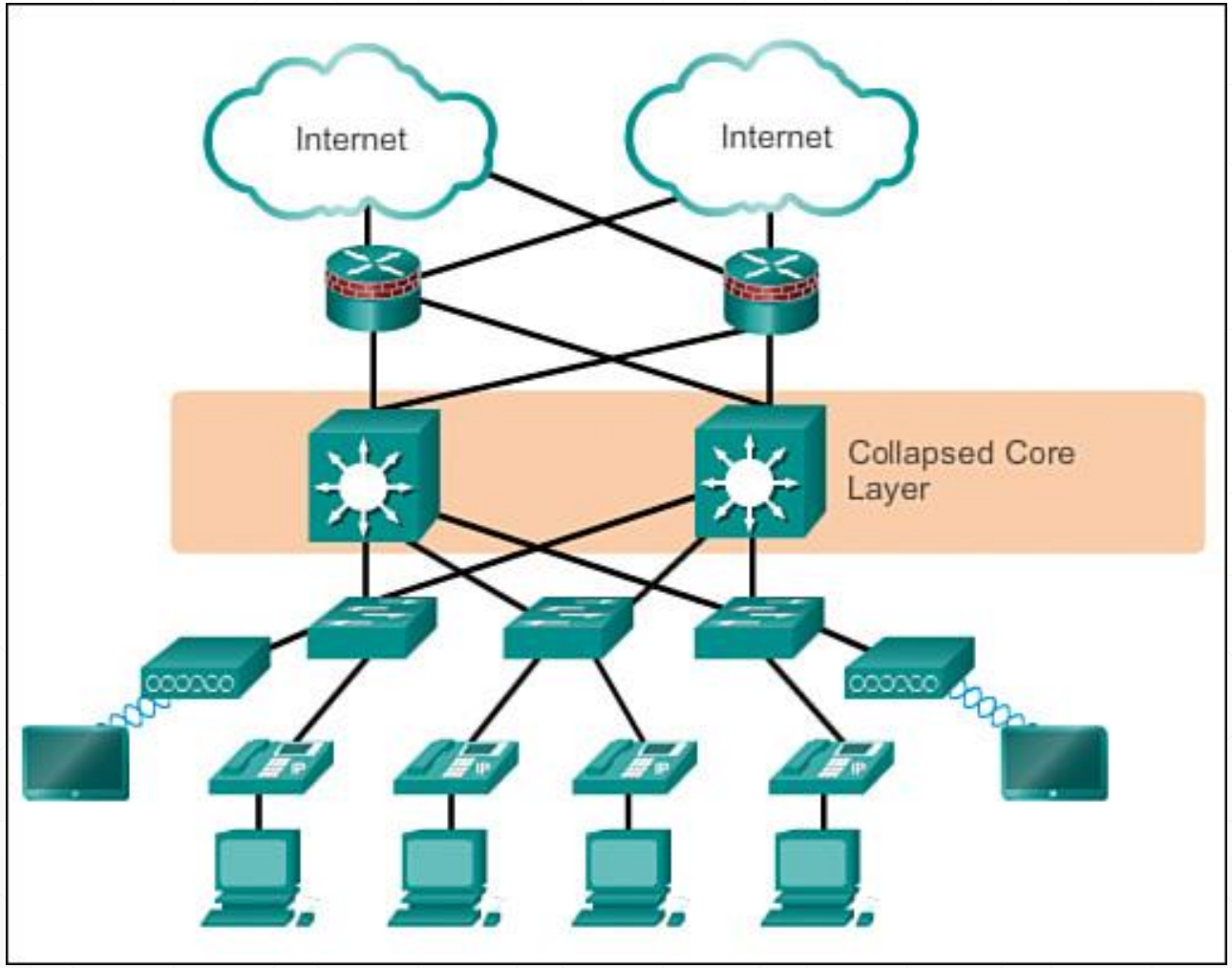
Hierarchical Network Design

- Core Layer:
  - Very high throughput at Layer 3
  - No costly or unnecessary packet manipulations (access lists, packet filtering)
  - Redundancy and resilience for high availability
  - Advanced QoS functions

Cisco Nexus 7200

Network Design Layer

- Collapsed Core Design



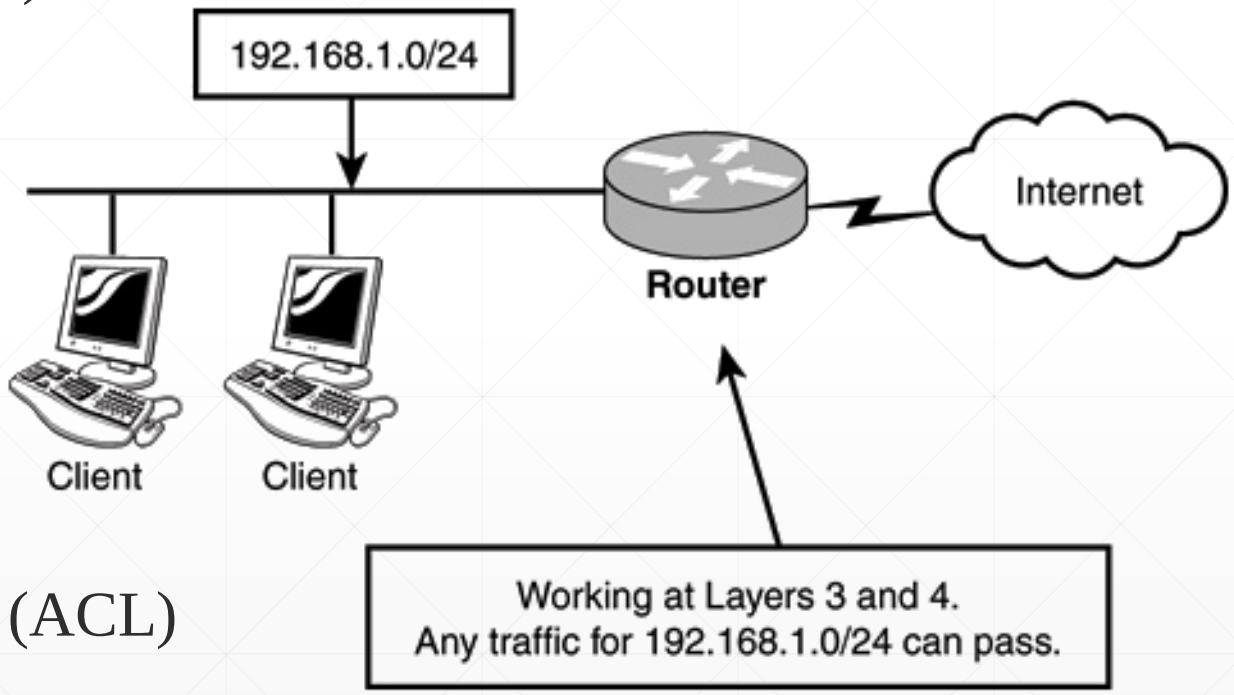
Firewall

Firewall

- firewall: An introduction to firewalls
  - A firewall is a hardware or software system that prevents unauthorized access to or from a network

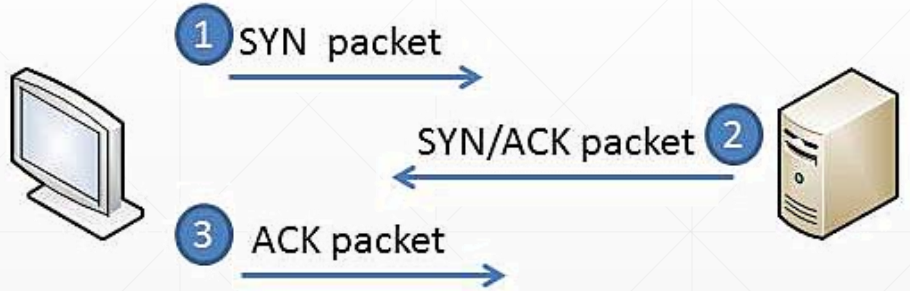
Firewall

- Firewall Type
  - Packet Filtering (Up to Layer 4)
    - نسل اول
    - Source IP address
    - Source port
    - Destination IP address
    - Destination port
    - OSI Transport Layer
  - Extended Access Control Lists (ACL)



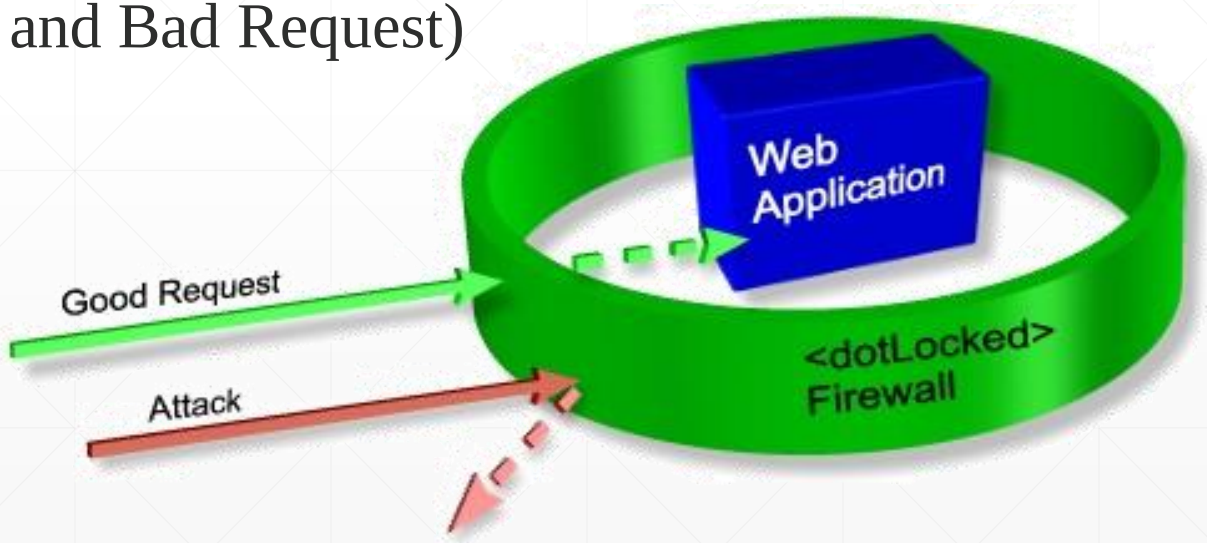
Firewall

- Firewall Type
  - Circuit level Gateway
    - نسل دوم
    - Layer 4, Transport layer, TCP Specific
    - Monitor TCP handshaking between packets (SYN,SYN-ACK,ACK)
    - For example: TCP interception mechanism in Multilayer switches.



Firewall

- Firewall Type
  - Application level Gateway (ALG)
  - Web Application Firewall (WAF)
    - نسل سوم
    - Layer 7, Application Attack (Good and Bad Request)
    - Deep packet inspection (DPI)



UTM

UTM

- UTM (Unified Threat Management)
- USM (Unified Security Management)
- Integrated security solutions

- Multiple security functions:
  - network firewalling, network intrusion prevention, antivirus (AV)
  - anti-spam, VPN, content filtering, load balancing, data loss prevention and …

UTM

- **Key advantages (مزایا)**
  - کاهش پیچیدگی در پیاده سازی
  - سهولت در بهره برداری: Plug & Play Architecture, Web-based GUI for easy management
- **Key Disadvantages (معایب)**
  - Single point of failure for network traffic, unless HA is used
  - Single point of compromise if the UTM has vulnerabilities
  - Potential impact on latency and bandwidth when the UTM cannot keep up with the traffic

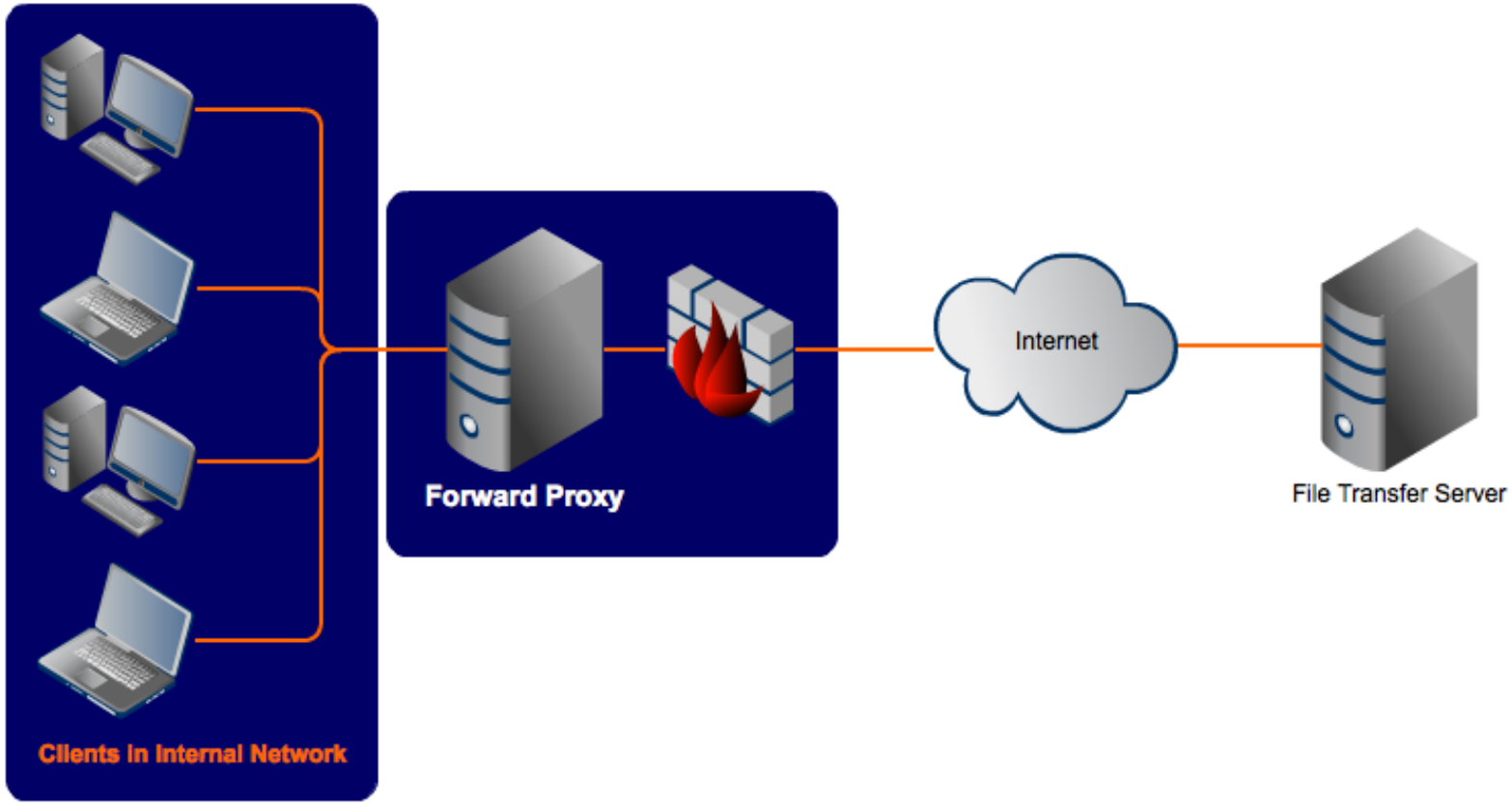
Proxy

Proxy

- تعریف :a proxy is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- کاربرد ها :Monitoring ,filtering and Security(Firewall), Caching, Bypassing filters
- انواع :Types of proxy
  - **Forward proxies**: Internet Sharing
  - **Reverse proxies**: Load balancing, authentication

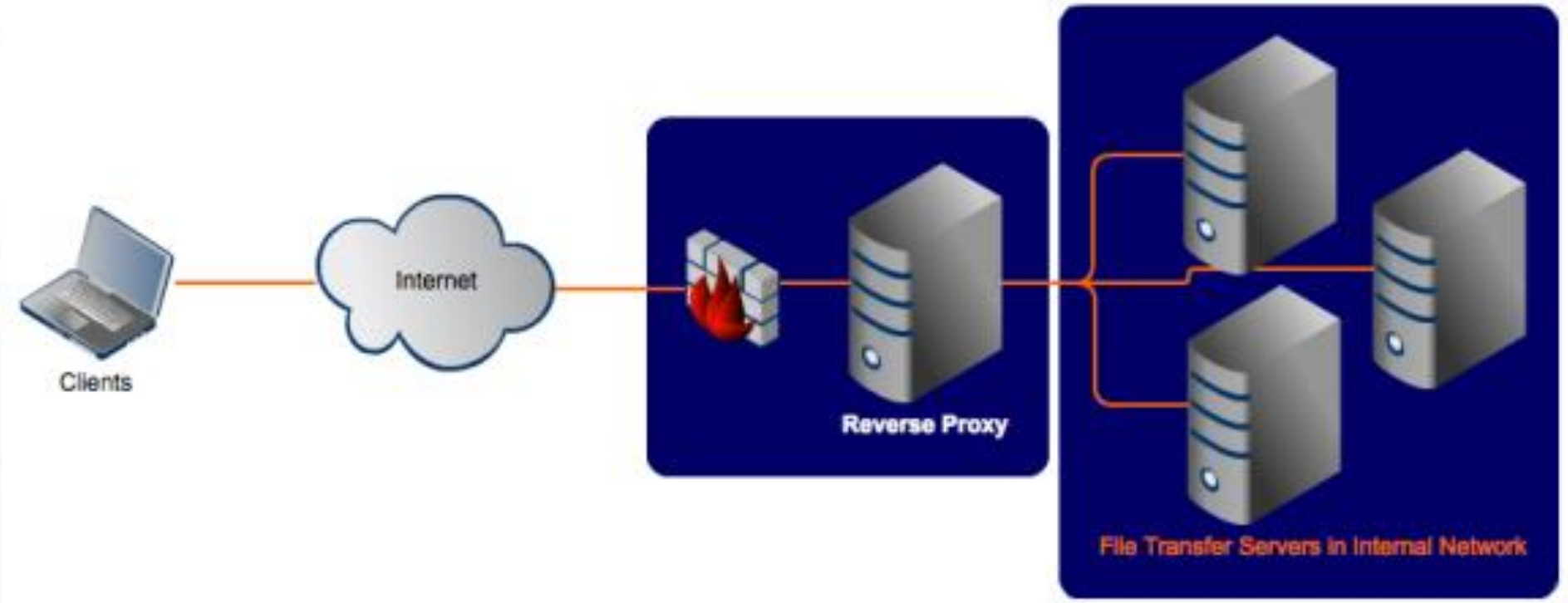
Forward proxies

- Internet Sharing
- Monitoring
- Security
  - Content Filtering



Reverse proxies

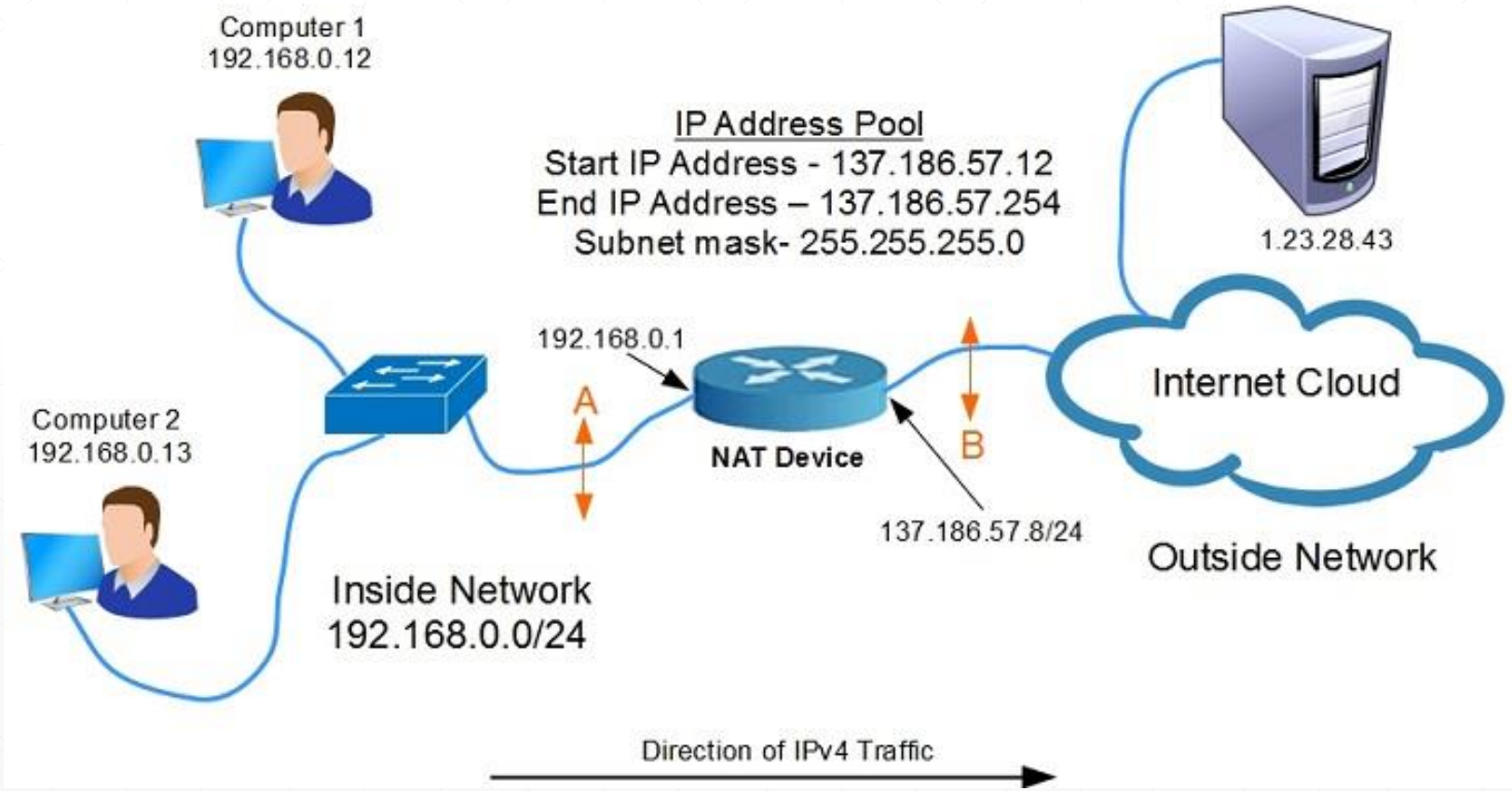
- Load balancing, authentication, Web Publishing, Application Firewall



NAT

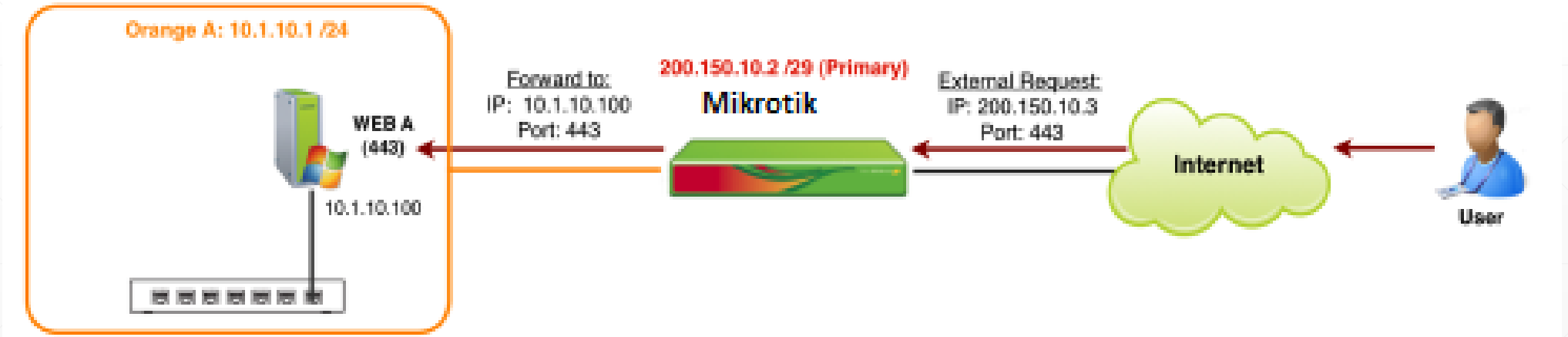
NAT

- NAT (Network Address Translation)



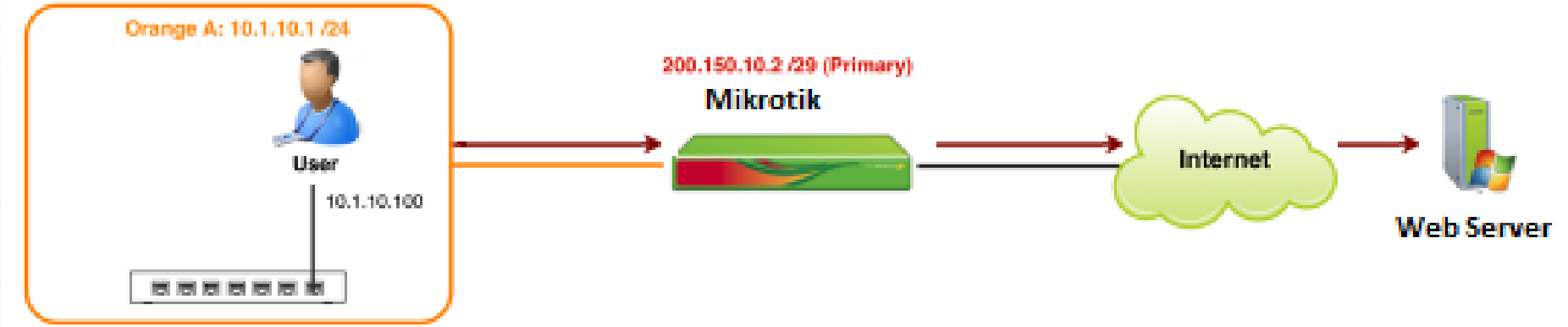
NAT

- DNAT
  - Destination network address translation (DNAT):publish a service, port forwarding, DMZ



NAT

- SNAT
  - Source network address translation (SNAT): connection tracking and filtering ,Internet Sharing
  - Masquerade: Type of SNAT , one-to-many



NAT Advantage and Disadvantage

- Advantages of NAT:
  - provide an **additional layer of security** by making the original source and destination addresses hidden.
  - provides **increased flexibility** when connecting to the public Internet.
- Disadvantages of NAT:
  - a **processor and memory resource** consuming technology, for all incoming and outgoing
  - may cause **delay** in IPv4 communication
  - cause loss of end-device to end-device IP **traceability**
  - Some **technologies and network applications** will not function

DMZ

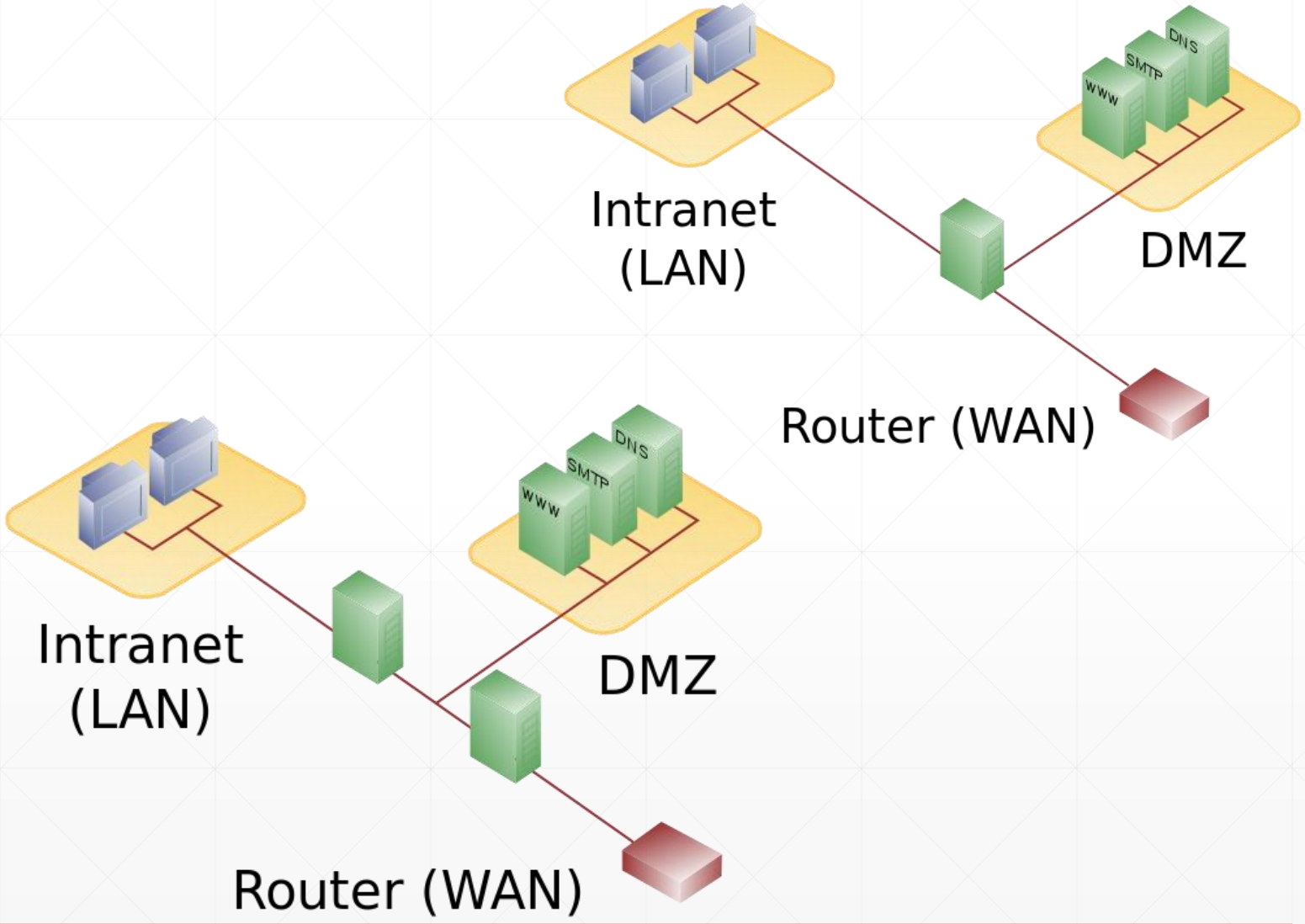
DMZ

- DMZ (De-Militarized Zone)
  - is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks.
  - Web Server, E-Mail Server, FTP, …
  - **وقتی لازم است اطلاعات یک سرور، هم از داخل و هم از خارج شبکه در دسترس باشد**

- MZ (Militarized Zone)
  - Private network Zone Include Servers and DB.

DMZ

- DMZ Architecture:
  - Single Firewall
  - Dual Firewall
    - front-end
    - back-end



IDS\IPS

IDS\IPS

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Intrusion Detection and Prevention Systems (IDPS)

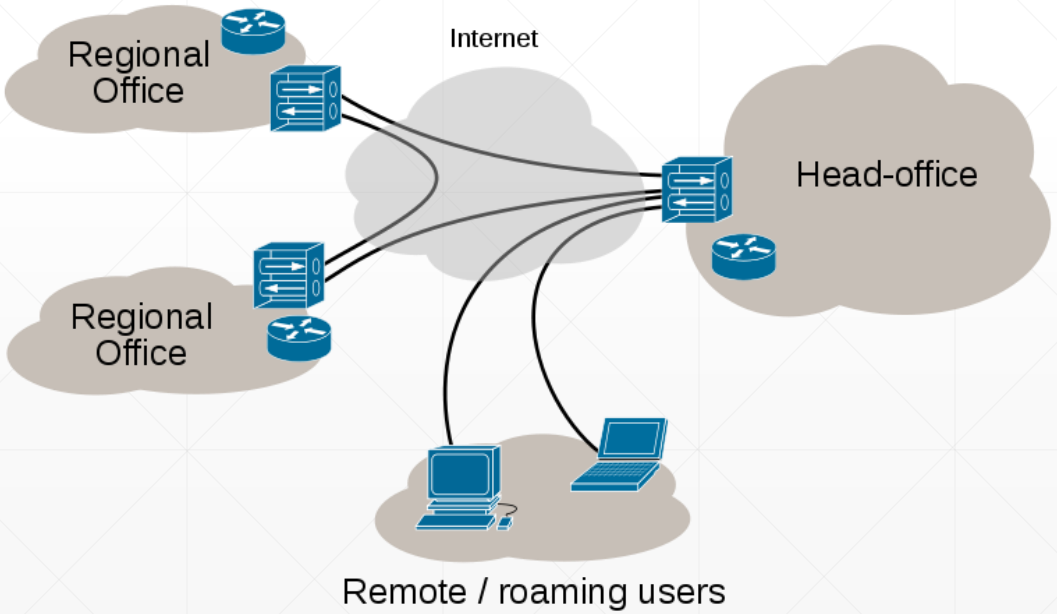
FW/IDS Event

- Alert Type!:
  - True Positive: : Attack – Alert
  - False Positive: : No attack – Alert
  - False Negative: : Attack - No Alert
  - True Negative: : No attack - No Alert

VPN

VPN

- زمانی که بخواهید از میان محیط عمومی، یک دسترسی ایمن وقابل اعتماد فراهم نمایید
- Virtual Private Network (VPN)
  - extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks



VPN

- VPN systems may be classified by:
  - The protocols used to tunnel the traffic
  - Whether they offer site-to-site or Client-to-Site connectivity
  - The levels of security provided (Encrypted or Unencrypted)
  - Network Layer, such as Layer 2 or Layer 3 or Layer 7 (PPOE or IP-SEC or WebVPN like cisco clientless SSL VPN)

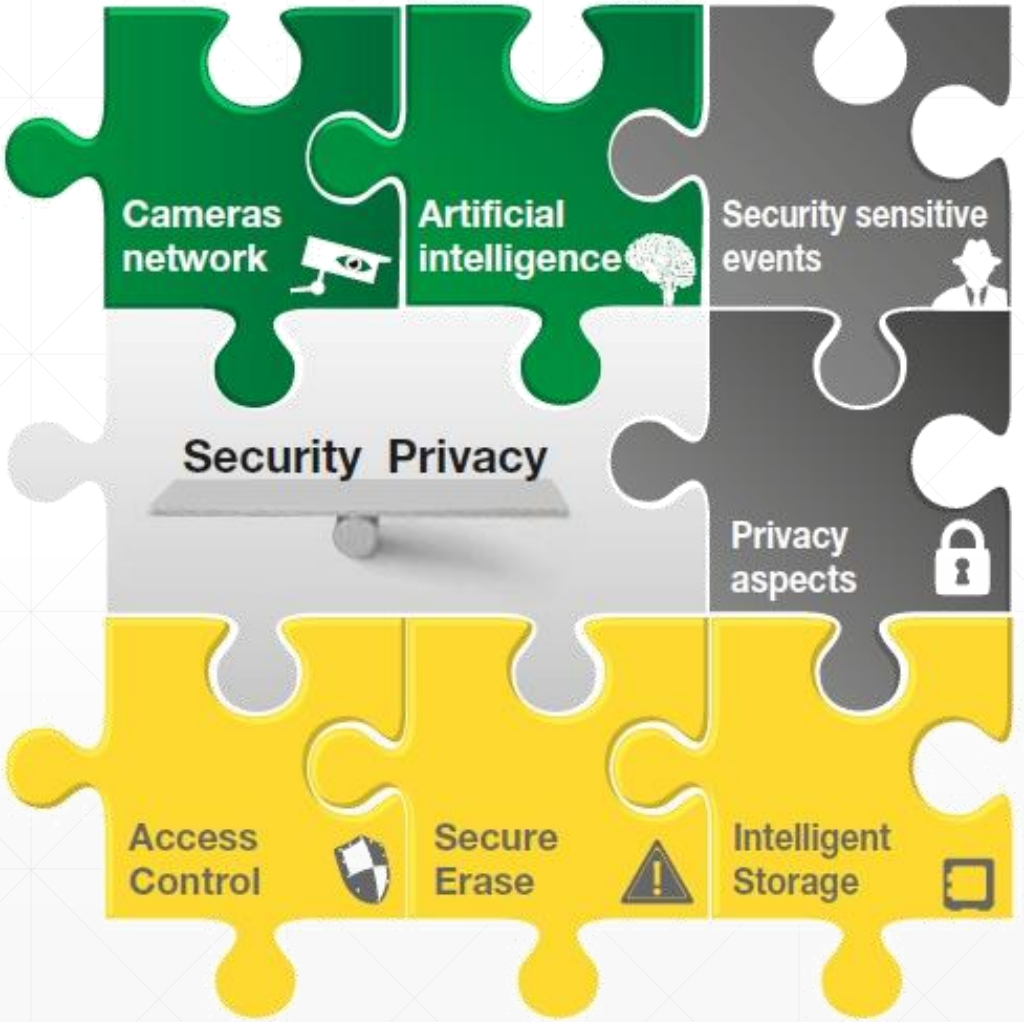
VPN

- Tunneling Protocols:
  - PPTP (Point-to-Point Tunneling Protocol)
  - PPP (Point-to-Point Protocol)
    - PPPOE (Point-to-Point Protocol over Ethernet)
    - PPPOA (Point-to-Point Protocol over ATM)
  - L2TP (Layer 2 Tunneling Protocol)
  - L2F (Layer 2 Forwarding)
  - **IPSec** (Internet Protocol Security)
  - SSTP (Secure Socket Tunneling Protocol)
  - GRE (Generic Routing Encapsulation)
  - OpenVPN …

Conclusion

- **Defense in Depth**: (also known as Castle Approach) is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system

Security is Puzzle …



Questions ?

Thanks for your Attention