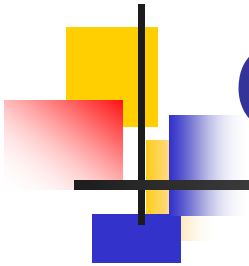


Overview

Domain 1: General Security Concepts

- M1: Introduction to Information Security
  - Key Security Concepts and Models
- M2: Cryptography
  - Encryption, Symmetric/Asymmetric Cryptography, Key Management

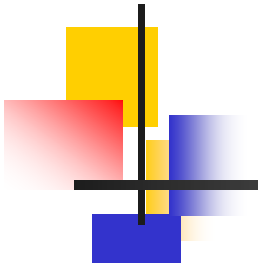
Domain 2: Security Threats, Vulnerabilities, and Mitigations

- M3: Threat, Attacks, Vulnerability, and Mitigations
  - Types of Threats, Attacks, and Vulnerabilities, Mitigation Techniques

Domain 3: Security Architecture

- M4: Cloud Computing
  - Could computing, Virtualization, and Cloud Security Controls
- **M5: Network Security**
  - **Secure Network Design, Network Security Devices, Network Security Techniques**

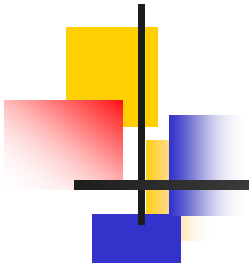
UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.



M5. Network Security

- TCP/IP Network Basic
  - TCP/IP Family Protocol and OSI 7 Layers
- Network Security Devices
  - Firewalls: Types of Firewalls, Firewall Processing Modes, Firewall Implementation (Firewall Architectures)
  - Intrusion Detection and Prevention System (IDPS): Types of IDPSs: N-IDPS and H-IDPS, IDPS Detection Methods
- Network Security Techniques
  - Virtual Private Networks (VPN)
  - Zero Trust Network Access

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.



Network Basic

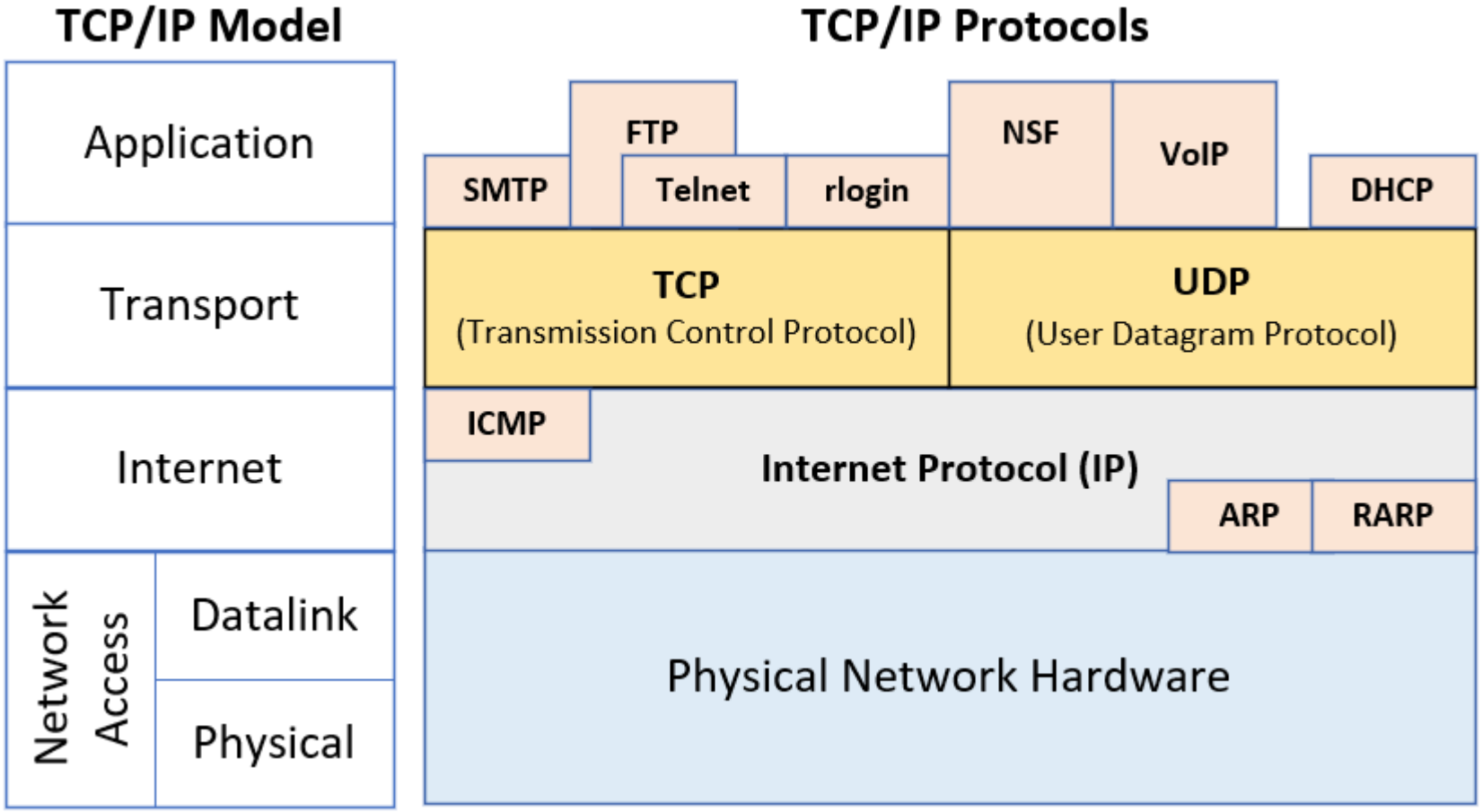
Data Communication Frameworks

- Protocol: A set of rules that govern communication between hardware and/ or software components
  - Open System: A system can communicate with any other system that follows the specified standards, formats and semantics

- Two major data communication frameworks
  - OSI (Open Systems Interconnection) 7 Layer Reference Model – by ISO
  - TCP/IP (Transmission Control Protocol/Internet Protocol) Suite

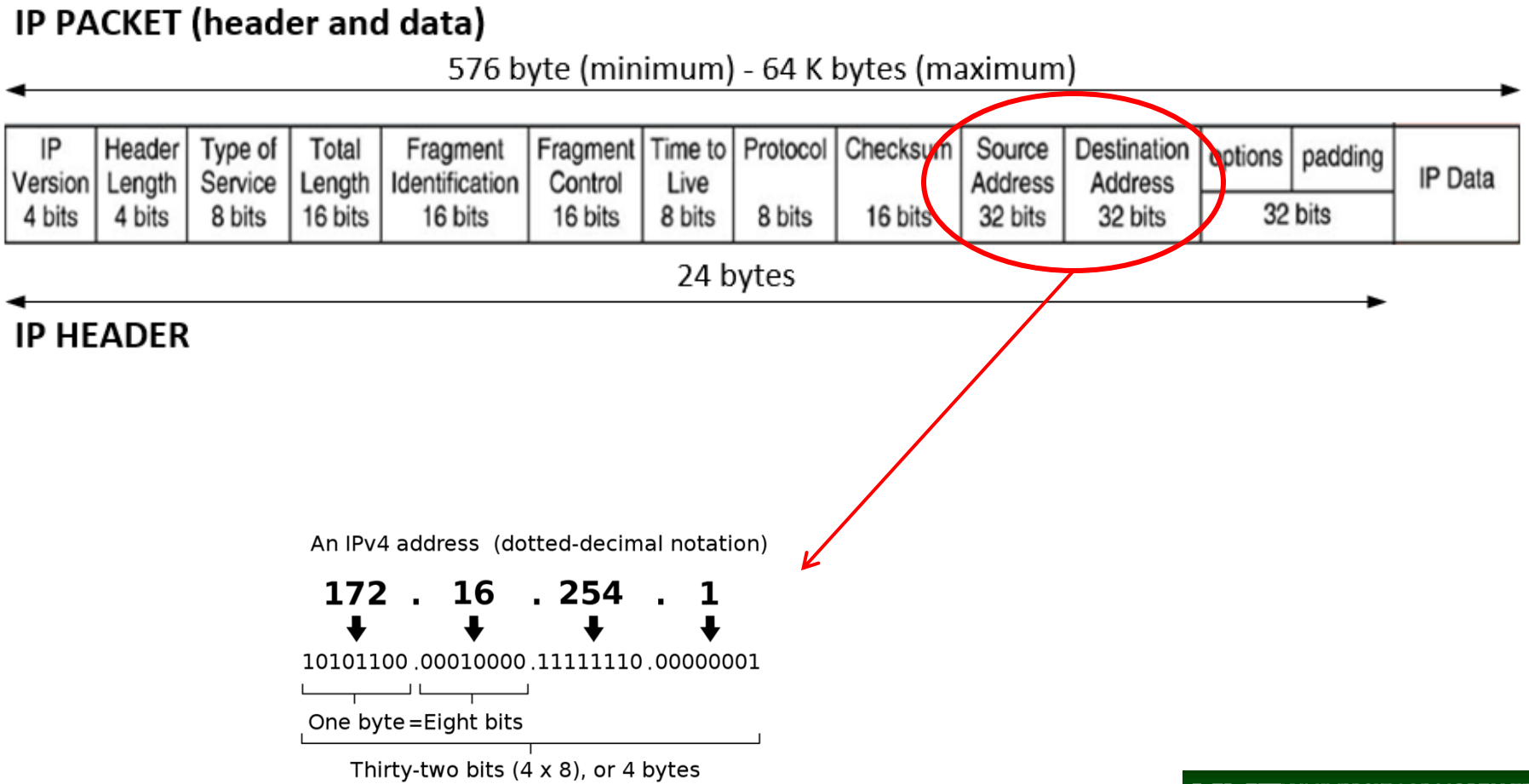
UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

TCP/IP Family of Protocols



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

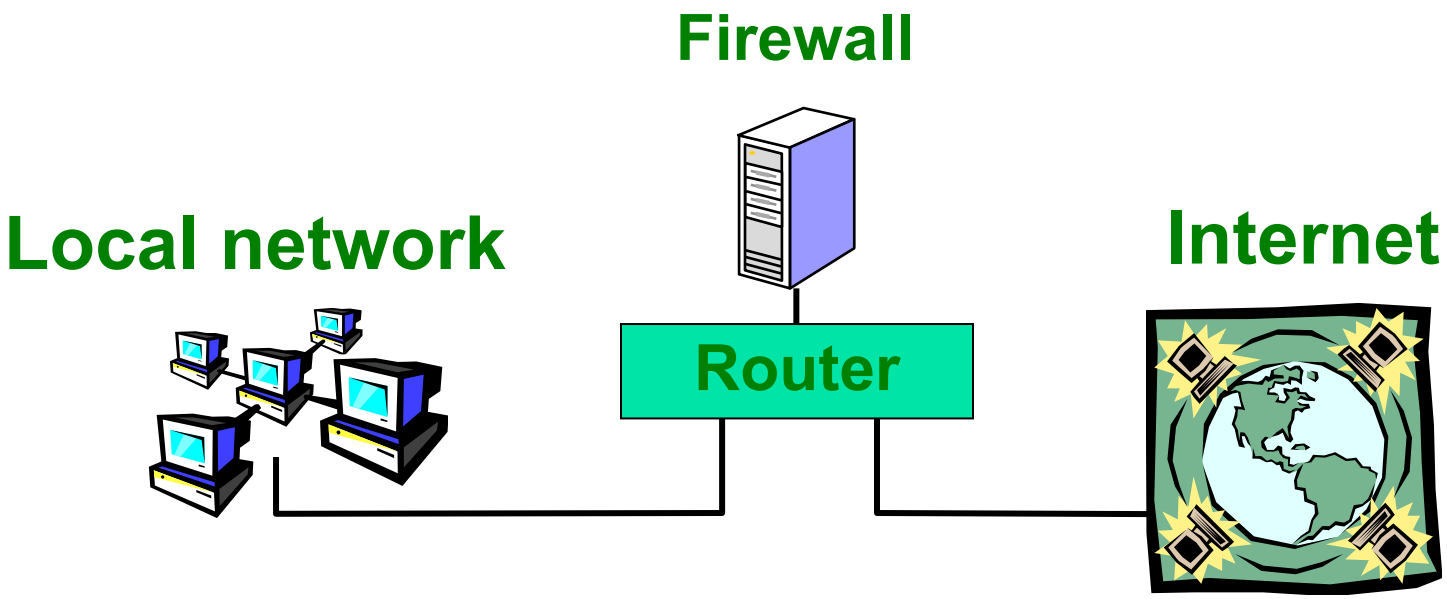
IPv4 Packet Structure



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Basic Firewall Concept

Separate local area net from the Internet

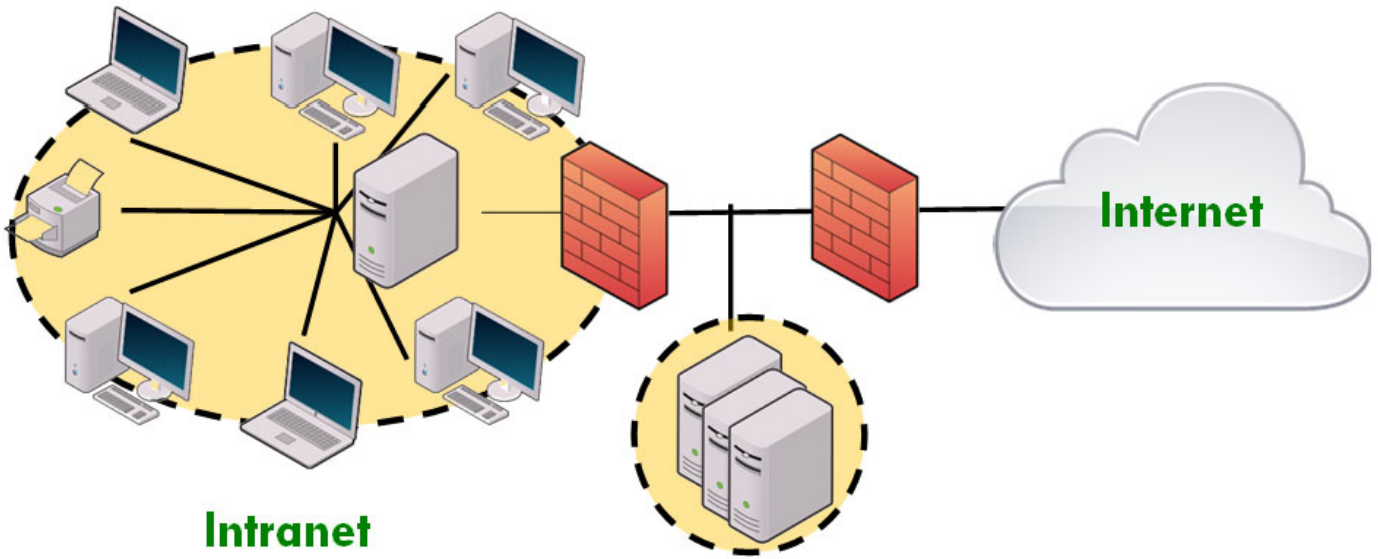


All packets between LAN and internet routed through firewall

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Intranet

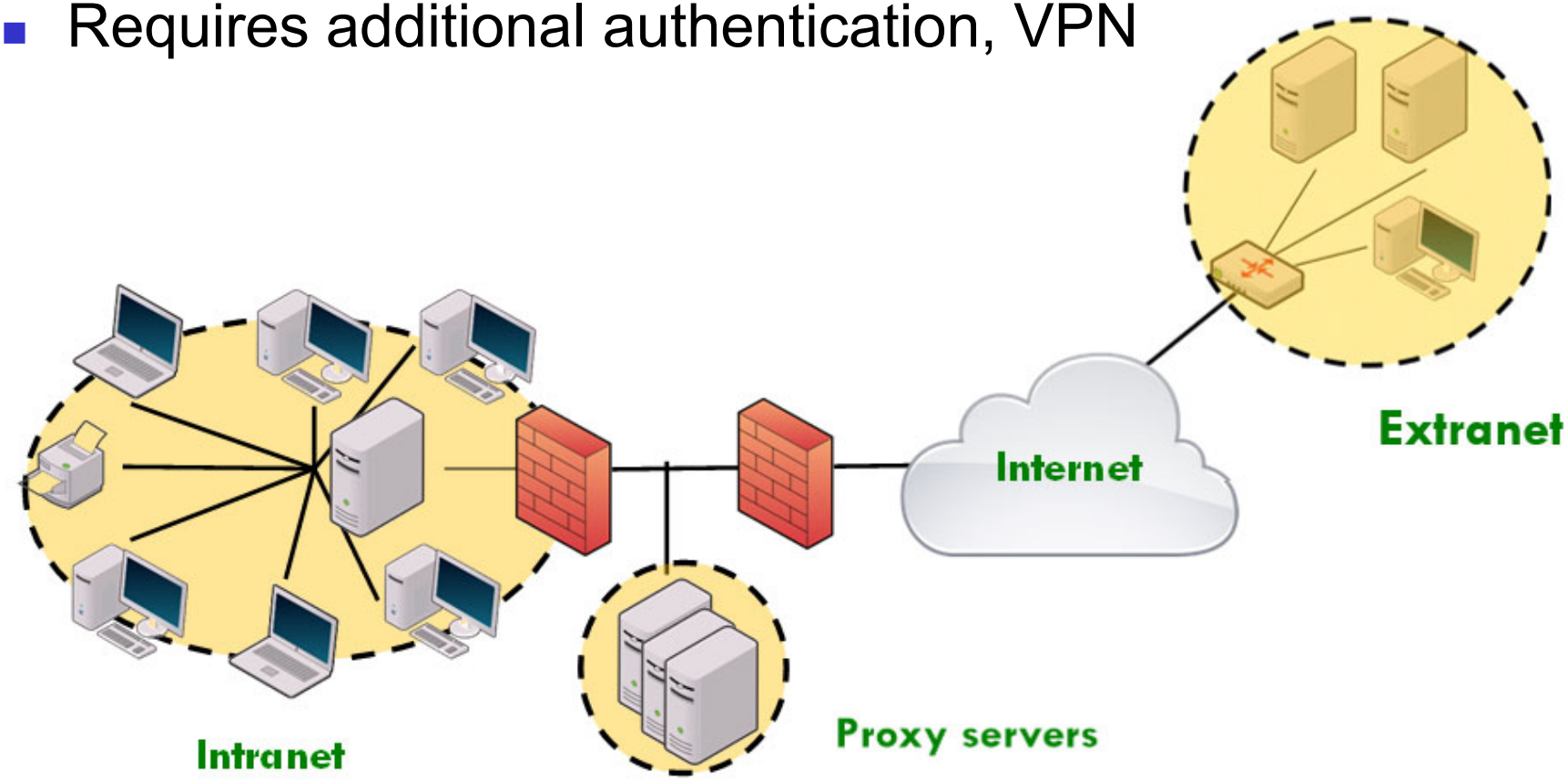
- Internal, private network
- Employees only
  - Sharing computing resources



TY OF NORTH TEXAS
power of ideas.

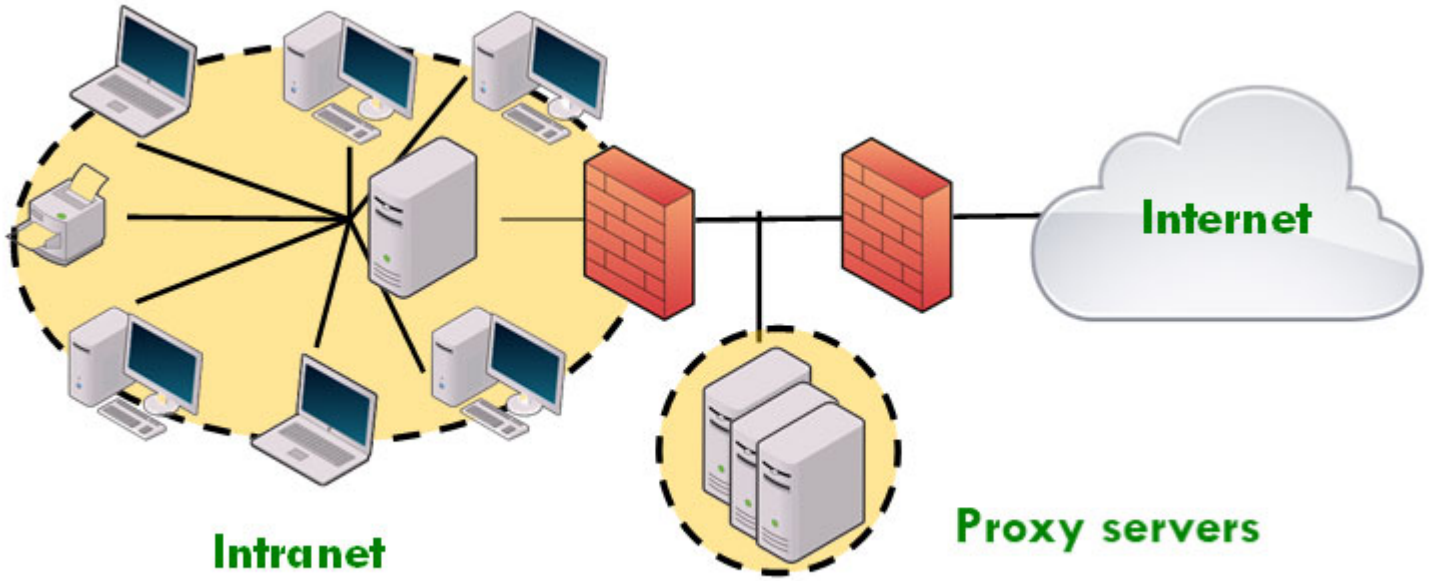
Extranet

- A private network for partners
  - Remote vendors, suppliers
- Requires additional authentication, VPN



DMZ (Demilitarized Zone)

- Additional layer of security between the internet and Intranet
- Public access to public resources
- Not on organization's intra network (intranet)



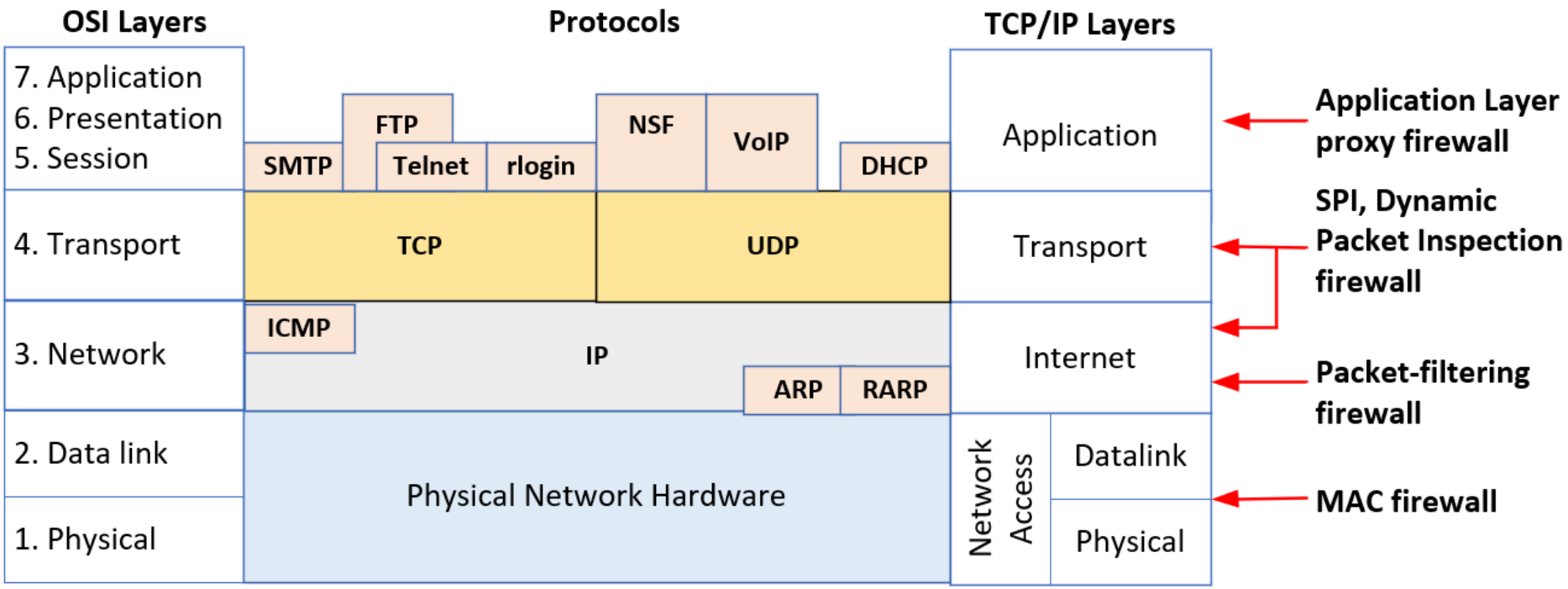
OF NORTH TEXAS
er of ideas.

Firewall Processing Modes

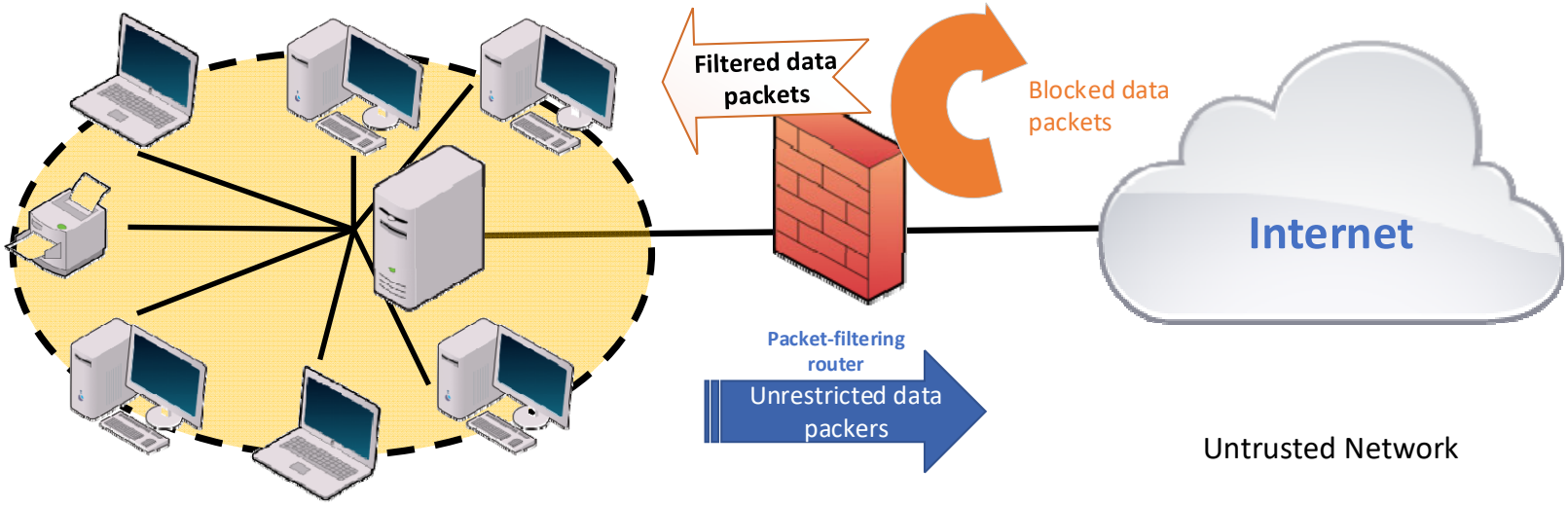
- Five processing modes that firewalls can be categorized by are:
  - Packet filtering (Network IP layer)
  - MAC layer (Data Link layer)
  - Dynamic packet inspection (TCP/IP Layer)
  - Proxy servers (Application layer)
  - Hybrids

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

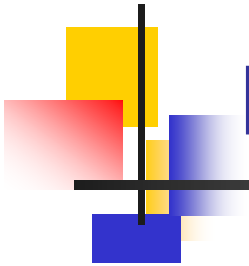
Firewall Types & OSI Model



Packet Filtering Firewall



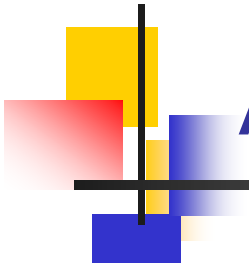
Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow



MAC Layer Firewalls

- Designed to operate at the MAC (media access control) layer of OSI network model
- Able to consider specific host computer's identity (i.e., MAC address) in its filtering decisions
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.



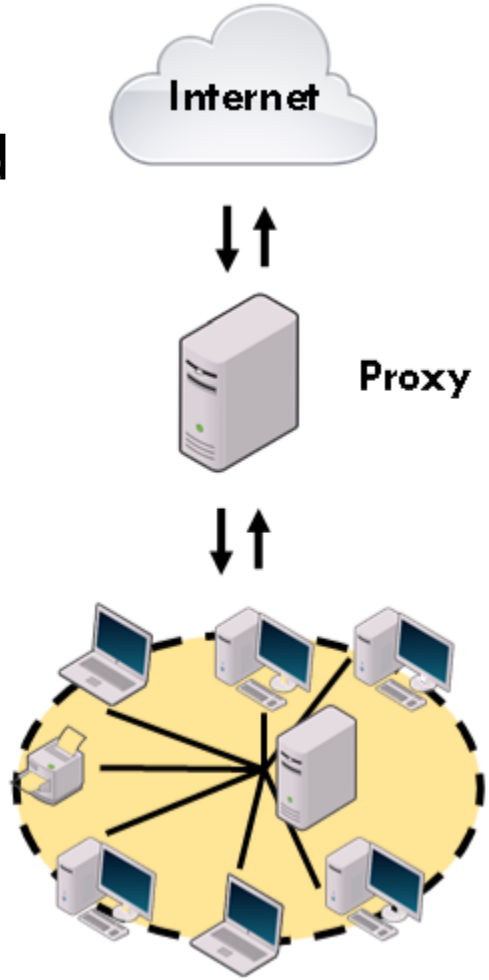
Application Gateways

- Frequently installed on a dedicated computer; also known as a proxy server, application proxy, bastion host, sacrificial host)
- Placed in unsecured network (e.g., DMZ)
- Additional filtering routers can be implemented behind the proxy server, further protecting internal systems

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Proxy Firewalls (Proxy Servers)

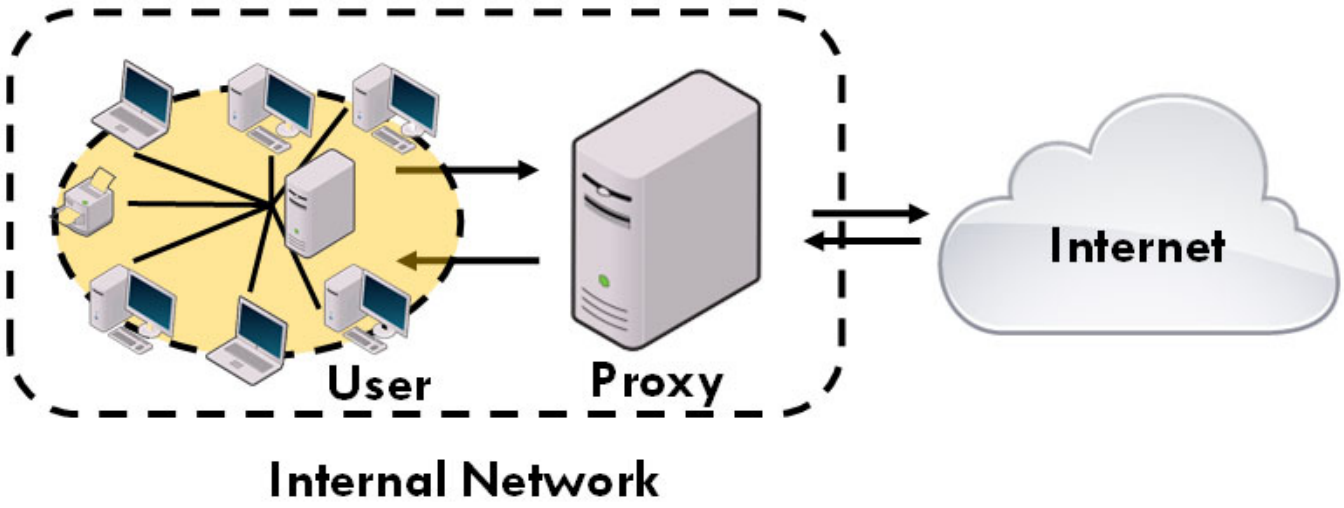
- Proxy servers (a.k.a., application gateways) receives user requests and sends the request on their behalf (the proxy)
- Common uses:
  - cache frequently accessed information
  - scan content (catch/defeat malware)
  - filter URLs (block websites)
  - control web access
  - authenticate users
- Two types of proxy servers
  - Forward proxy and backward proxy



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Forward (internal) proxy

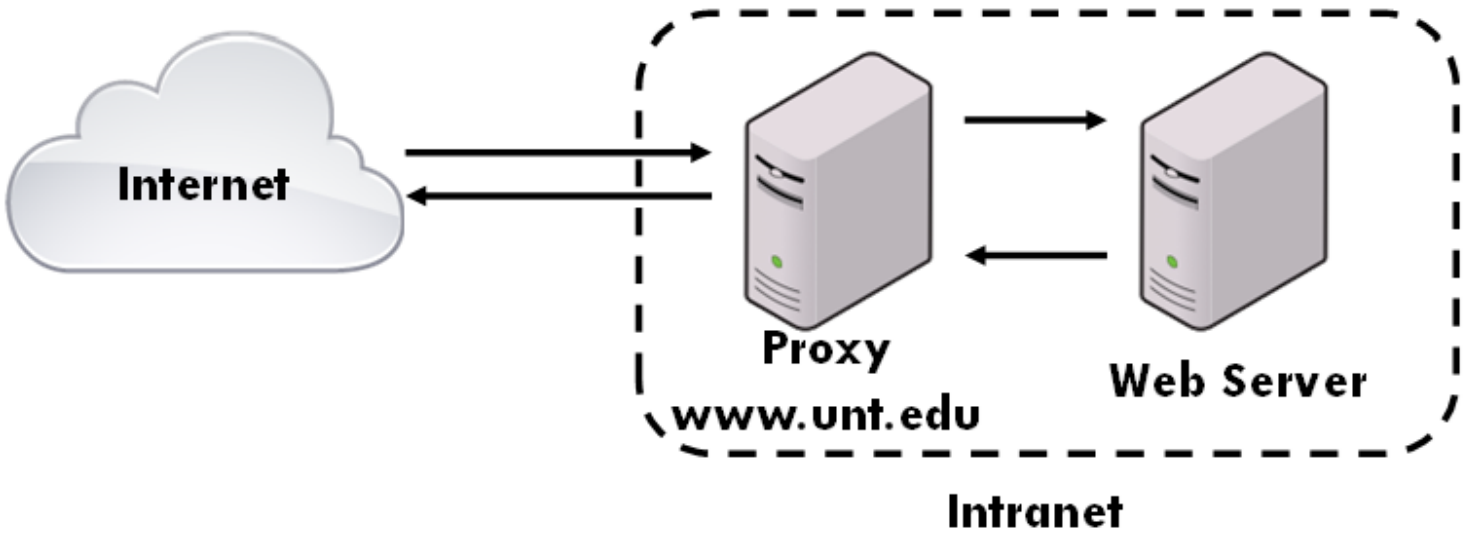
- Used for content filter and control user access to the internet
- Primary focus to restrict internal users to access external non-business material or deny incoming span



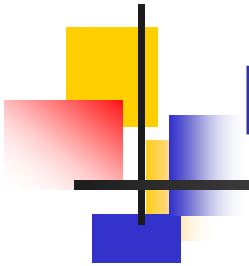
UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Reverse Proxy

- Traffic from the internet to internal service
- Outside world interacts with proxy, not actual web server



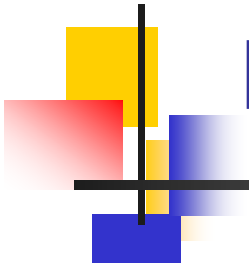
UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.



Hybrid Firewalls

- Combine elements of other types of firewalls; i.e., elements of packet filtering and proxy services, or of packet filtering and circuit gateways
- Alternately, may consist of two separate firewall devices; each a separate firewall system, but are connected to work in tandem

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.



Firewall Architectures

- Firewall devices can be configured in a number of network connection architectures
- Configuration that works best depends on three factors:
  - Objectives or needs of the network
  - Organization's ability to develop and implement architectures
  - Budget available for function

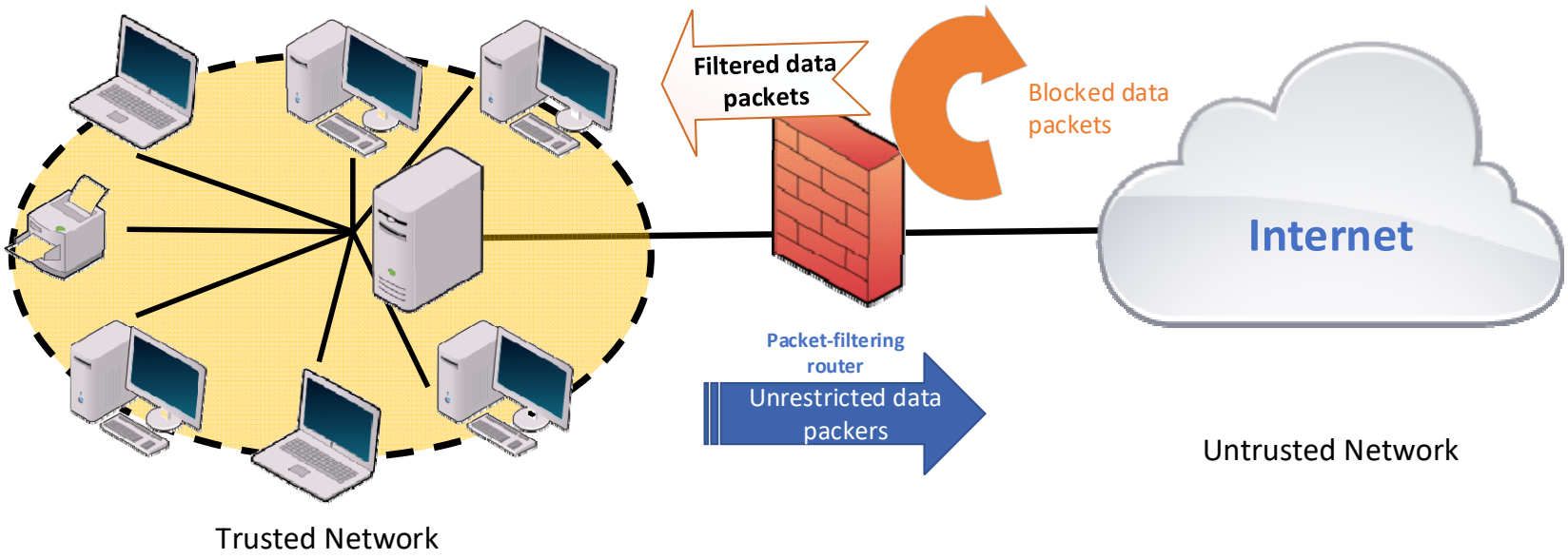
UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

Four Common Firewall Architectures

- Simple Packet filtering firewalls (routers)
  - Many of these routers can be configured to reject packets that organization does not allow into network
- Screened host with network address translator
  - Combines packet filtering router with separate, dedicated firewall such as an application proxy server
- Dual-homed bastion host firewalls
  - Two network interface cards (NICs): one connected to external network, one connected to internal network
- Screened subnet firewalls with DMZ
  - Commonly consists of two or more internal bastion hosts behind packet filtering router, with each host protecting trusted network

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

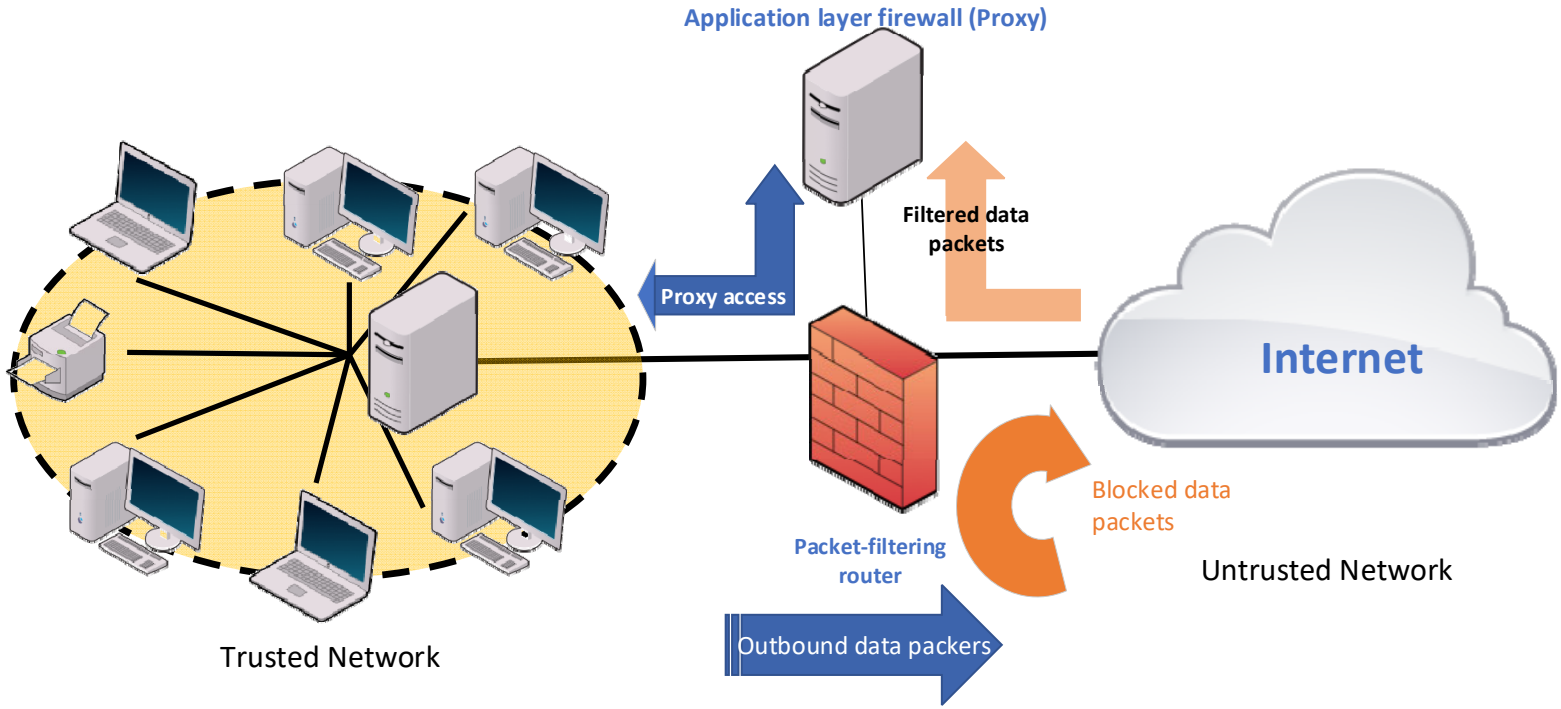
Simple Packet Filtering Firewall



Advantage: Simple but effective way to lower the risk from external attack.

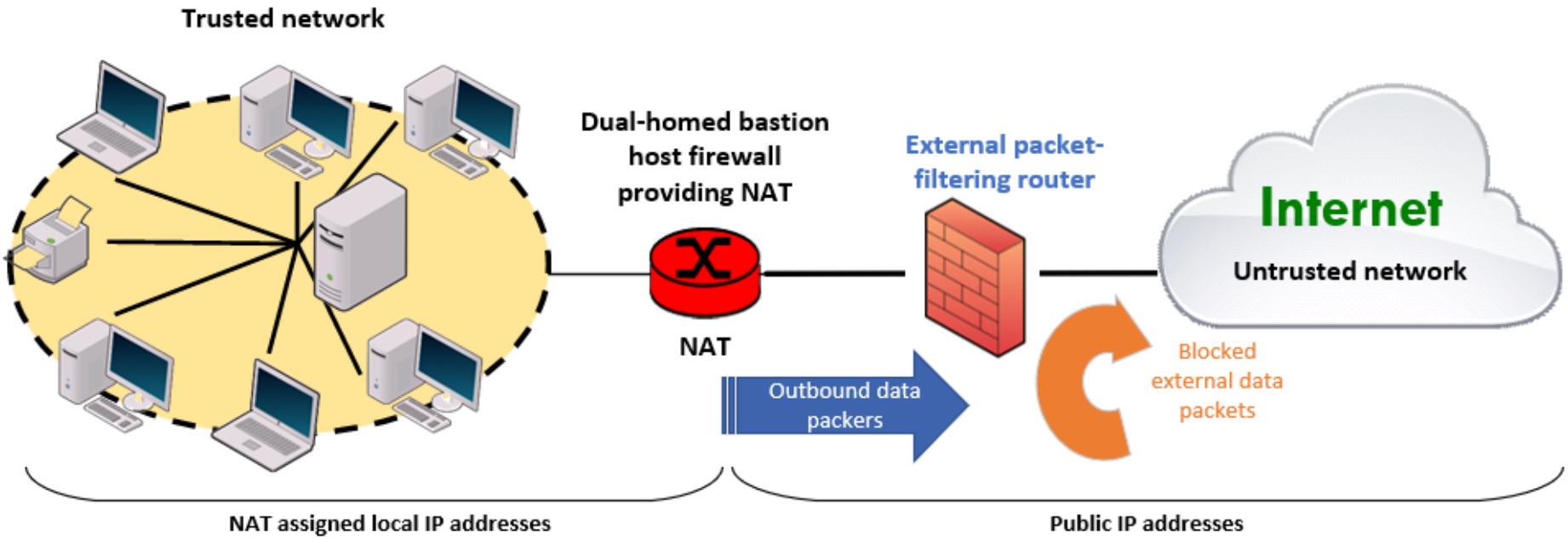
Drawbacks include a lack of auditing and strong authentication, and degrading network performance

Screened Host Firewalls



Allows router to pre-screen packets to minimize traffic/load on internal proxy and separate host (a.k.a. an application proxy, bastion host, sacrificial host) to examine an application layer protocol (e.g., HTTP). It can be a target for external attacks.

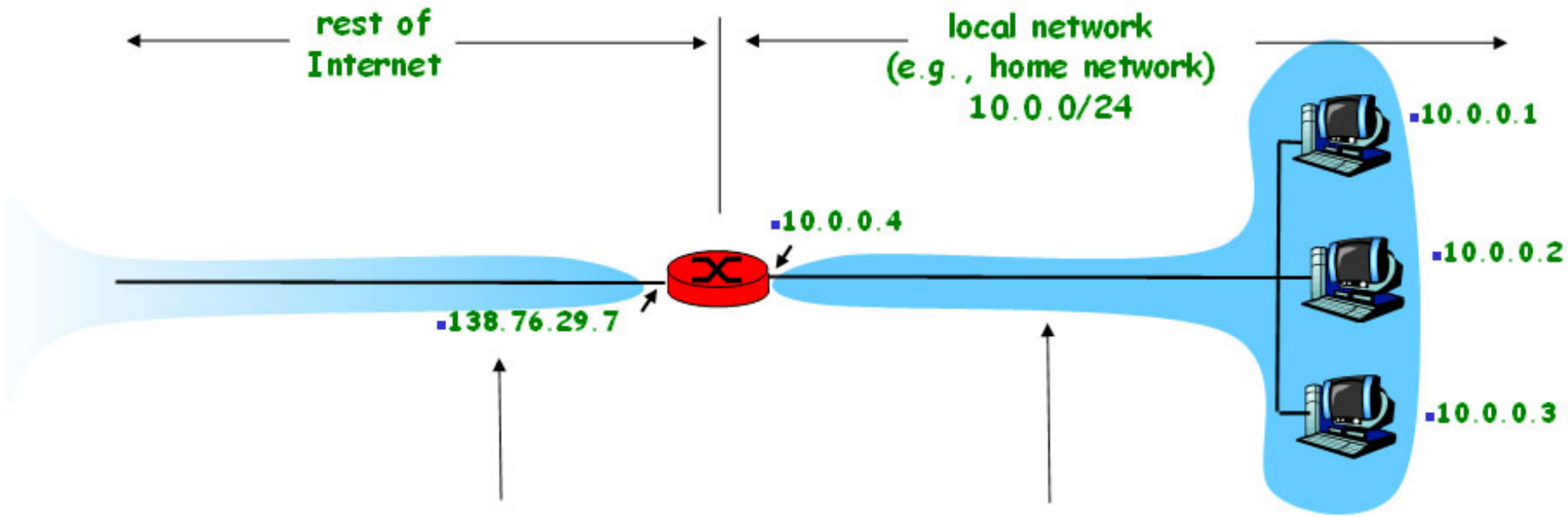
Dual-Homed Bastion Host Firewalls



Use of network address translation (NAT) creates another barrier to intrusion from external attackers

Strong overall protection with minimal expense

Network Address Translation (NAT)



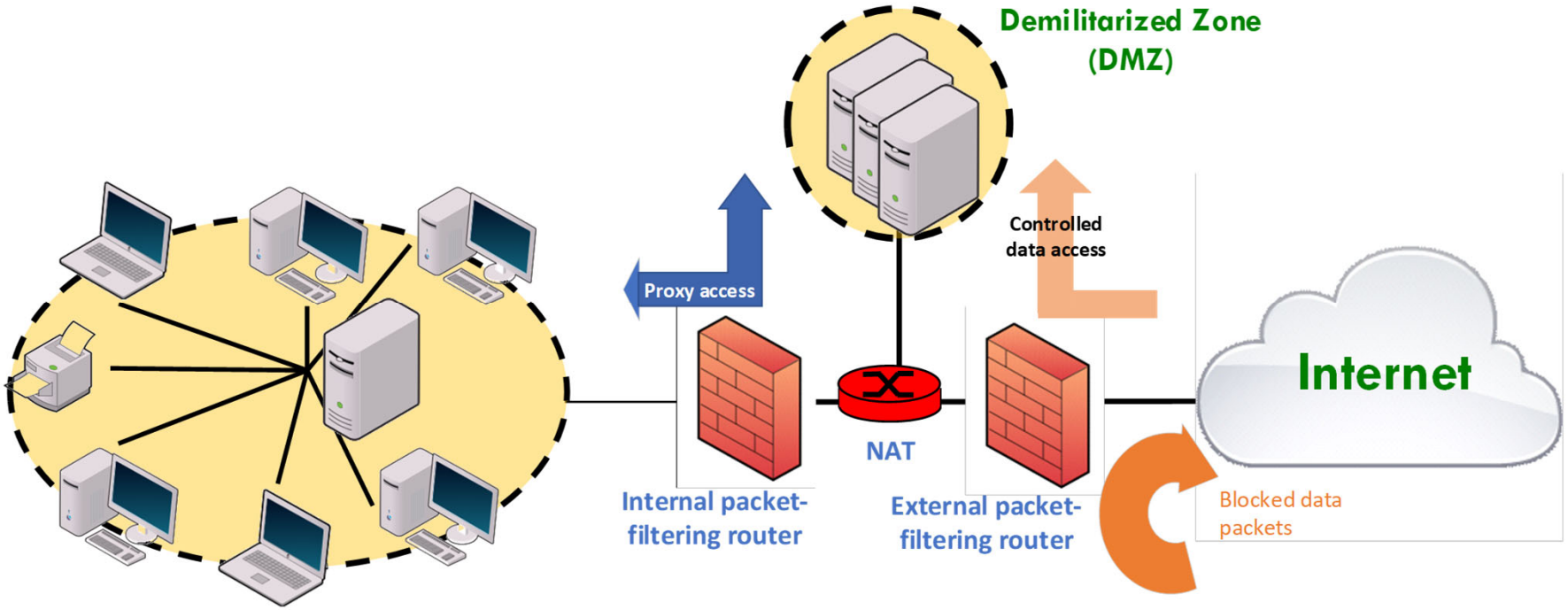
All **datagrams** ***leaving*** **local network have same single source NAT IP address: 138.76.29.7, different source port numbers**

destination in this network have 10.0.0/24 address for source, destination (as usual)

Illustration: Kurose and Ross

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Screened Subnet Firewalls (with DMZ)



Dominant architecture used today

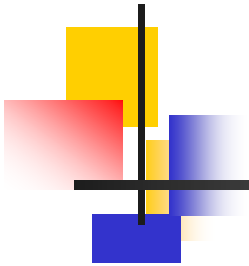
Protect the internal networks by limiting external connections

Create an area of known as an extranet

Selecting the Right Firewall

- When selecting firewall, consider a number of factors:
  - What firewall offers right balance between protection and cost for needs of organization?
  - What features are included in base price and which are not?
  - Ease of setup and configuration? How accessible are staff technicians who can configure the firewall?
  - Can firewall adapt to organization's growing network

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.



Intrusion Detection Systems

- Monitor network traffic searching for signs of potential malicious activities
  - Unusual logins, botnet traffic, SQL injections, malformed packets, etc.
- Alert administrators to suspicious activities
- Require someone to monitor and take appropriate actions

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

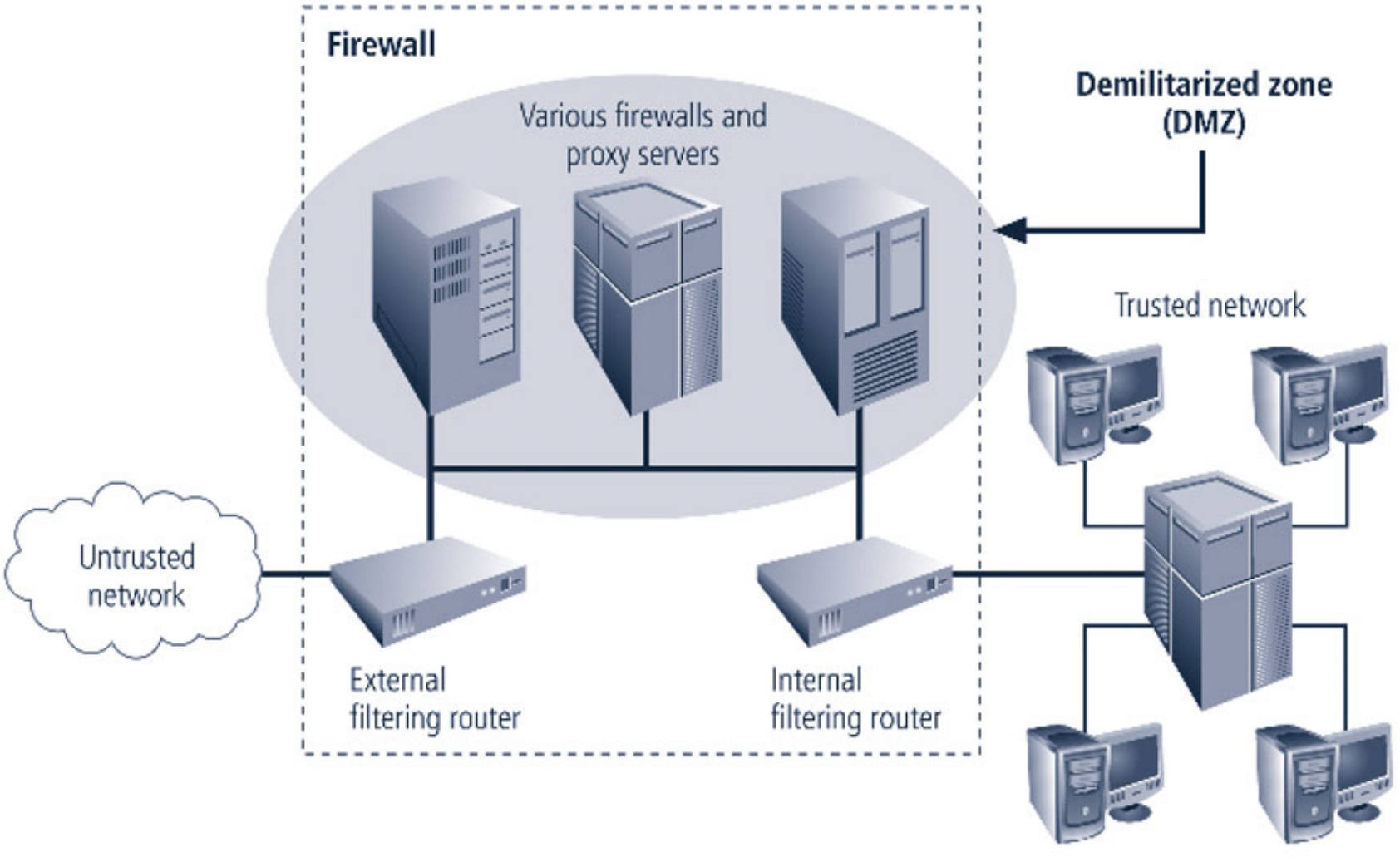
Intrusion Prevention Systems

- After receiving alert of suspicious activities, block suspicious activity automatically

- Intrusion Detection and Prevention System (IDPS) can detect an intrusion and also prevent that intrusion from attacking the organization.

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Firewalls, Proxy Servers, and DMZs

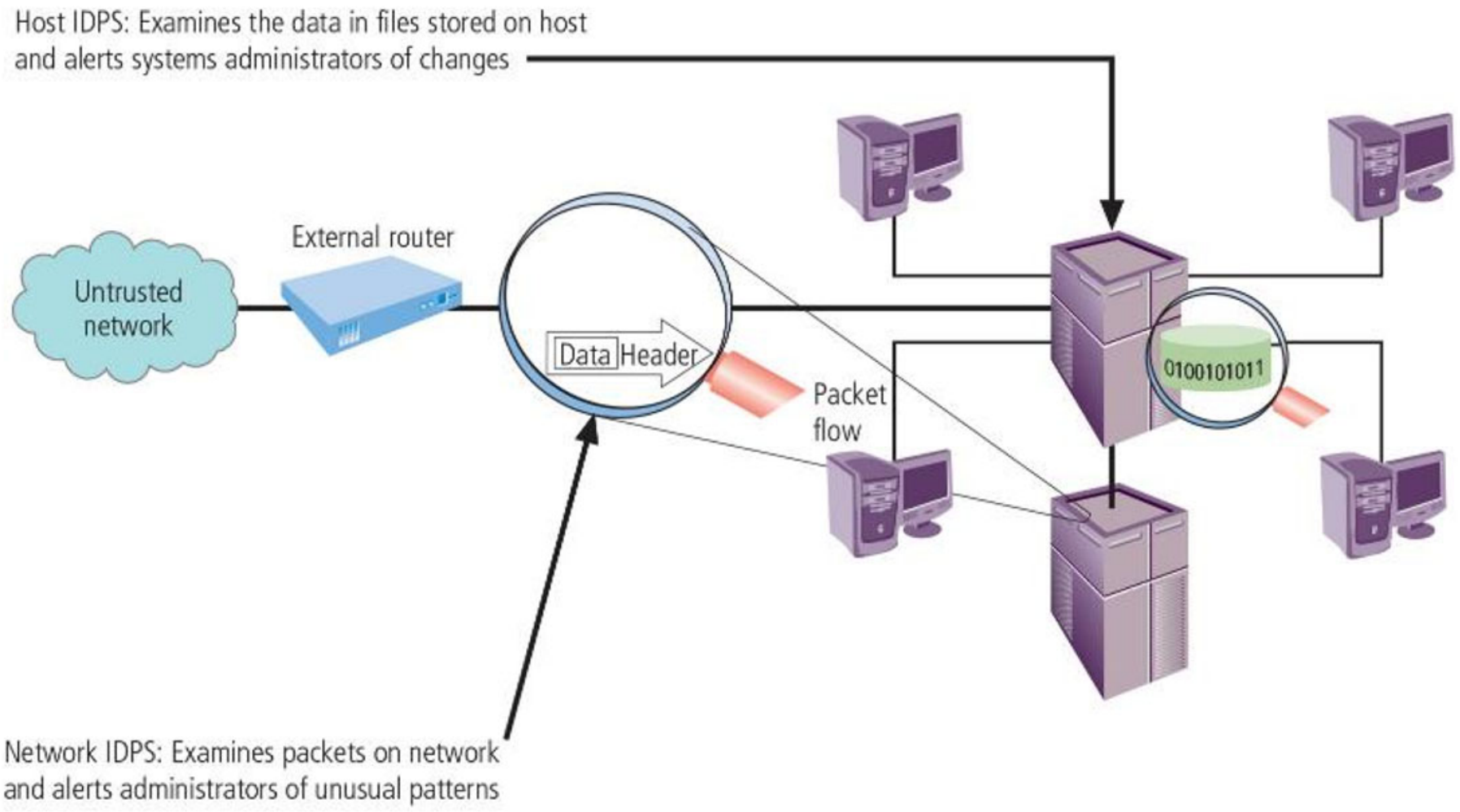


Two Operation Types of IDPS

- Network-based (examines packets on network)
  - Resides on computer or appliance connected to segment of a network; looks for signs of attacks
  - When examining packets, a NIDPS looks for attack patterns
- Host-based (examines the data stored on host)
  - Resides on a particular computer or server and monitors activity only on that system → system integrity verifiers

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

Intrusion Detection and Prevention Systems



Two subtypes of NIDPS

- Wireless NIDPS
  - Monitors and analyzes wireless network traffic
- Network behavior analysis (NBA) systems
  - Examine network traffic to identify problems related to the flow of traffic
  - Offer intrusion prevention capabilities
  - Types of events commonly detected include DoS attacks, scanning, worms, unexpected application services, policy violations

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

NIDPS (cont'd.) 1/2

- Advantages of NIDPSs
  - Good network design and placement of NIDPS can enable an organization to monitor a large network with few devices
  - NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
  - NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

NIDPS (cont'd.) 2/2

- Disadvantages of NIDPSs
  - Cannot analyze encrypted packets
  - Require access to all traffic to be monitored
  - Can become overwhelmed by network volume and fail to recognize attacks
  - Cannot reliably ascertain if attack was successful or not
  - Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

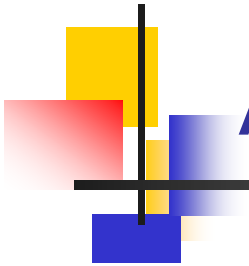
Host-Based IDPS (HIDPS)

- Resides on a particular computer or server (host) and verifies activity only on that system

  → **system integrity verifier**

- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Advantage over NIDPS: can usually be installed in a way that it can access encrypted information when traveling over network

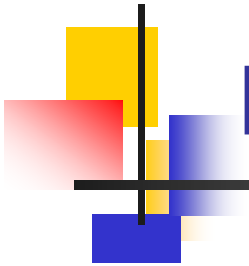
UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.



Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Can access encrypted traffics because HIDPS functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.



Disadvantages of HIDPSs

- Require more management effort to install, configure, and operate
- Can use large amounts of disk space for the host OS audit logs
- Vulnerable both to direct attacks and attacks against host operating system (e.g., susceptible to some denial-of-service attacks)
- Can inflict a performance overhead on its host systems
- Does not detect multi-host scanning, nor scanning of non-host network devices

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

IDPS Detection Methods

- Signature-based (a.k.a. knowledge-based) IDPS
  - Examine data traffic in search of patterns that match known signatures
- Anomaly-based (a.k.a. behavior-based) IDPS
  - Compare network traffic to the traffic that is known to be normal (called clipping level)
- Stateful protocol analysis (SPA) IDPS
  - Compares predetermined normal profiles against observed traffic
- Log file monitors (LFM)
  - Reviews log files generated by servers and network devices

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

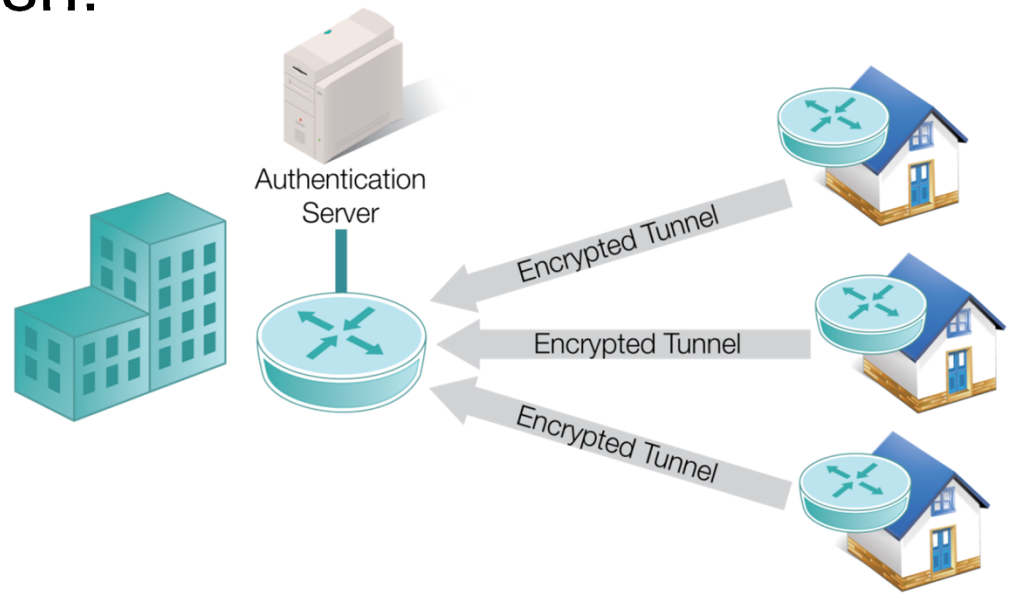
IDPS Response Behavior

- IDPS responses can be classified as active or passive
  - Passive response: setting off alarms or notifications, collecting passive data through SNMP traps
  - Active response: collecting additional information about the intrusion, launching response software, modifying the network environment, taking action against the intrusion
- Many IDPSs can generate routine reports and other detailed documents.

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

Virtual Private Networks (VPNs)

- Private and secure network connection between systems that uses data communication capability of unsecured and public network
- VPN must accomplish:
  - Encapsulation
  - Encryption
  - Authentication



CISCO VPN:
https://www.youtube.com/watch?v=jJdW0_yB9vo

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

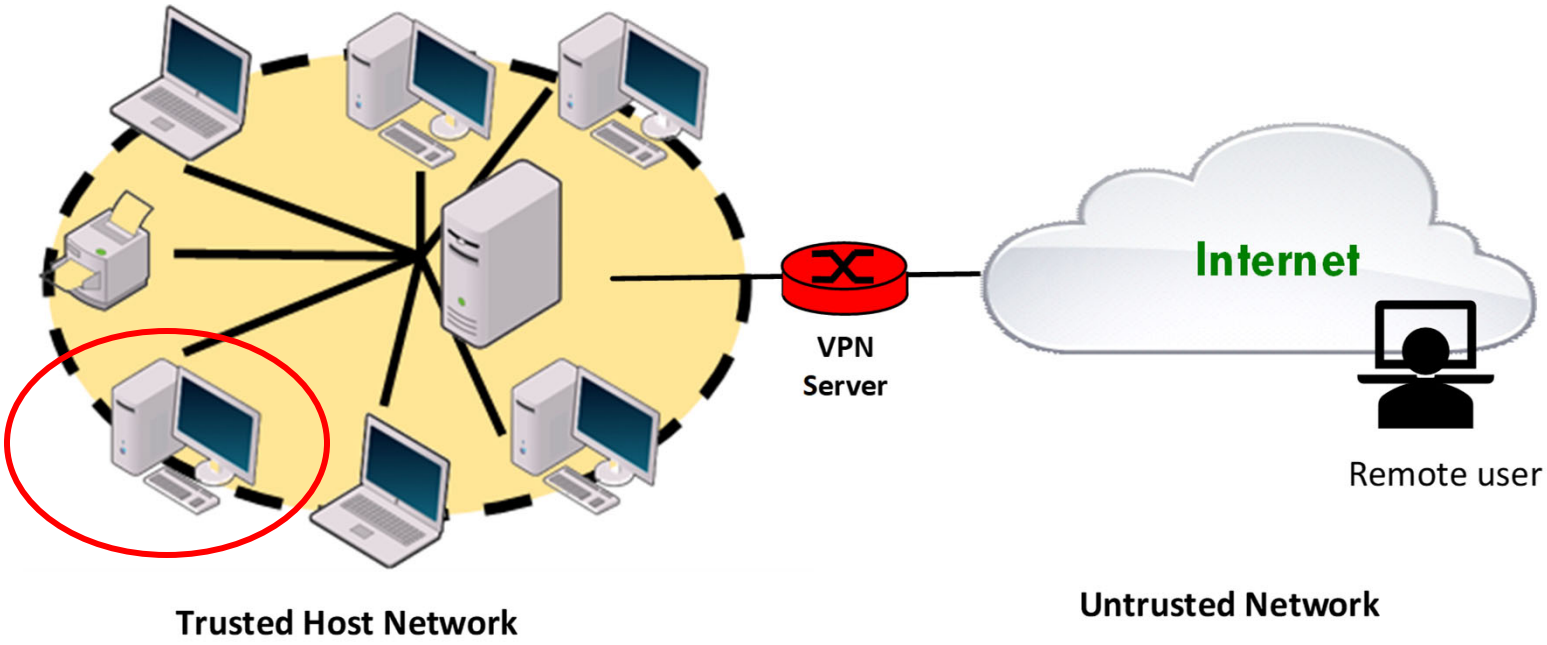
Virtual Private Networks (cont.)

- Three major VPN protocols
  - IPSec (Internet Security Protocol)
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)

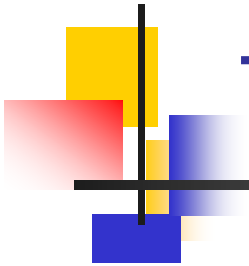
- Two types of VPN mode
  - Transport Mode: The data within an IP packet is encrypted, but the header information is not
    → Only data is encrypted
  - Tunnel Model: the entire packet is encrypted

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Transport Mode of VPN



- **Allows remote user to establish secure link directly with remote host, encrypting only data contents of packet not header information**



Transport Mode (remote access VPN)

- Allows remote user to establish secure link directly with remote host, encrypting only data contents of packet not header information
- Two popular uses:
  - End-to-end transport of encrypted data
  - Remote access worker connects to office network over the Internet by connecting to a VPN server on the perimeter

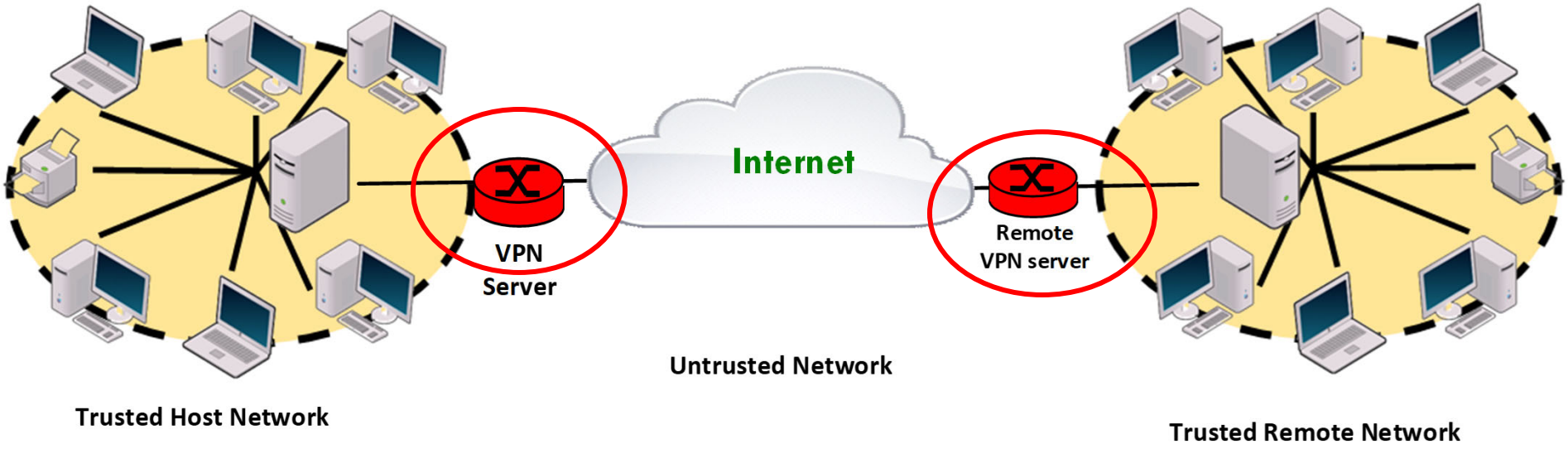
UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

Tunnel Mode (site-to-site VPN)

- Organization establishes two perimeter tunnel servers which act as encryption points, encrypting all traffic that will traverse unsecured network
- Primary benefit to this model is that an intercepted packet reveals nothing about true destination system
  - Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server

UNT UNIVERSITY OF NORTH TEXAS Discover the power of ideas.

Tunnel Mode of VPN



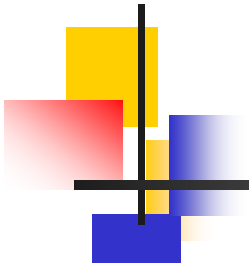
- **Primary benefit to this model is that an intercepted packet reveals nothing about true destination system**

Zero-Trust Network Access (ZTNA)

- Only authorized entities can access resources, regardless of whether they are inside or outside the organization's network.

- The Key Concepts of ZTNA
  - Identity-based Access Control using MFA - No one is trusted by default
  - Least privilege access – granting the minimum level of necessary access
  - Continuous verification - Never Trust, Always Verify
  - Microsegmentation

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.



Summary

- Network Basic
  - TCP/IP Family Protocol and OSI 7 Layers
- Network Security Devices
  - Firewalls: Types of Firewalls (Forward and Reverse Firewalls), Firewall Processing Modes (packer filtering, MAC layer, Dynamic stateful firewalls, proxy servers)
  - IDPS: Types of IDPS, Detection Methods
- Network Security Techniques
  - Virtual Private Networks (VPN)
  - Zero Trust Network Access

UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.