Security Strategies in Web Applications and Social Networking

Chapter 5

Mitigating Risk When Connecting to the Internet

Learning Objective and Key Concepts

Learning Objective

- Describe best practices for connecting to the Internet and securing a network perimeter.

Key Concepts

- Web site risks, threats, and vulnerabilities
- Different approaches to Web hosting
- Best practices while connecting to the Internet
- Protecting the LAN-to-WAN Domain

Web Site Risks

- What are risks?
  - **Risk** concerns the deviation of results of future events from their expected results. Technically, the value of those results may be positive or negative.

Web Site Threats

- Something that is a source of danger
  - Declaration of an intention or a determination to inflict harm

Web Site Risks and Threats

- Hackers
- Malware
- Personal attacks

Web Site Risks and Threats (Cont.)

- Offensive and inappropriate material
- E-mail attacks
- Predators

Web Site Vulnerabilities

- In computer security, the term vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

Web Site Vulnerabilities (Cont.)

- End user
- Security
- Port
- Software
- Malware

External vs. Internal Web Site Hosting

External	Internal
Economy of scale	Control
Liability on the vendor	Additional cost
Expertise	Immediate support

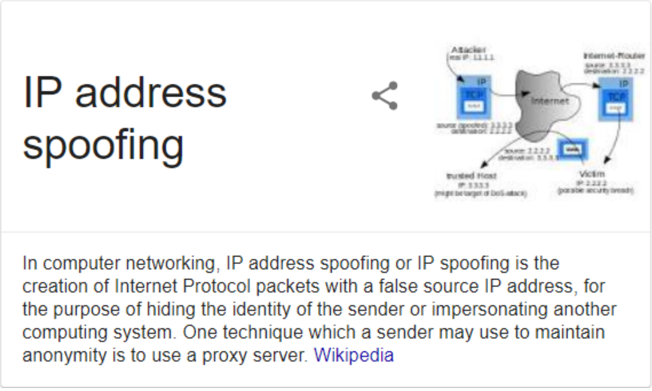
RIsk
Threat
Vulnerability
attack

disk storage spaces
bandwidth available
technical support
POP3 email
email forwarding
email aliases

WHOIS and DNS

- **WHOIS**: A query or response protocol that is widely used for querying databases in order to determine the registrant or assignee of the Internet resources
- **Domain Name System (DNS)**: Used for naming computers, services, and other objects on a network

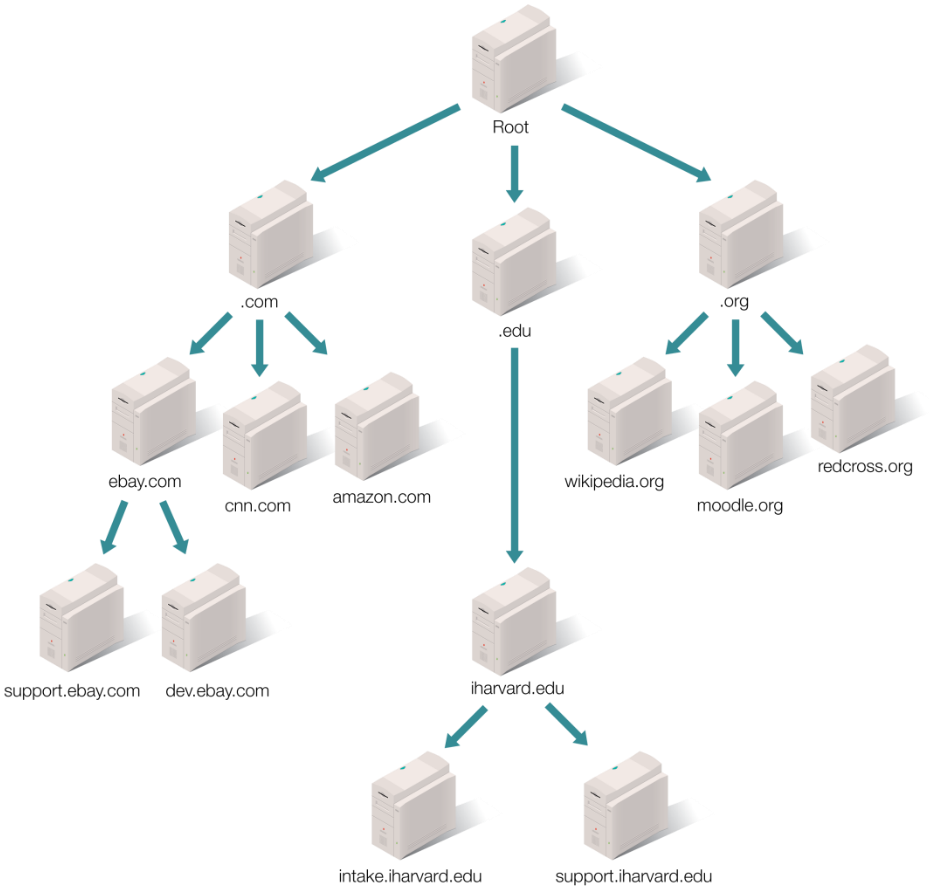
can become DoS using spoofing, use ip addr of the victim and repeatedly send reqs



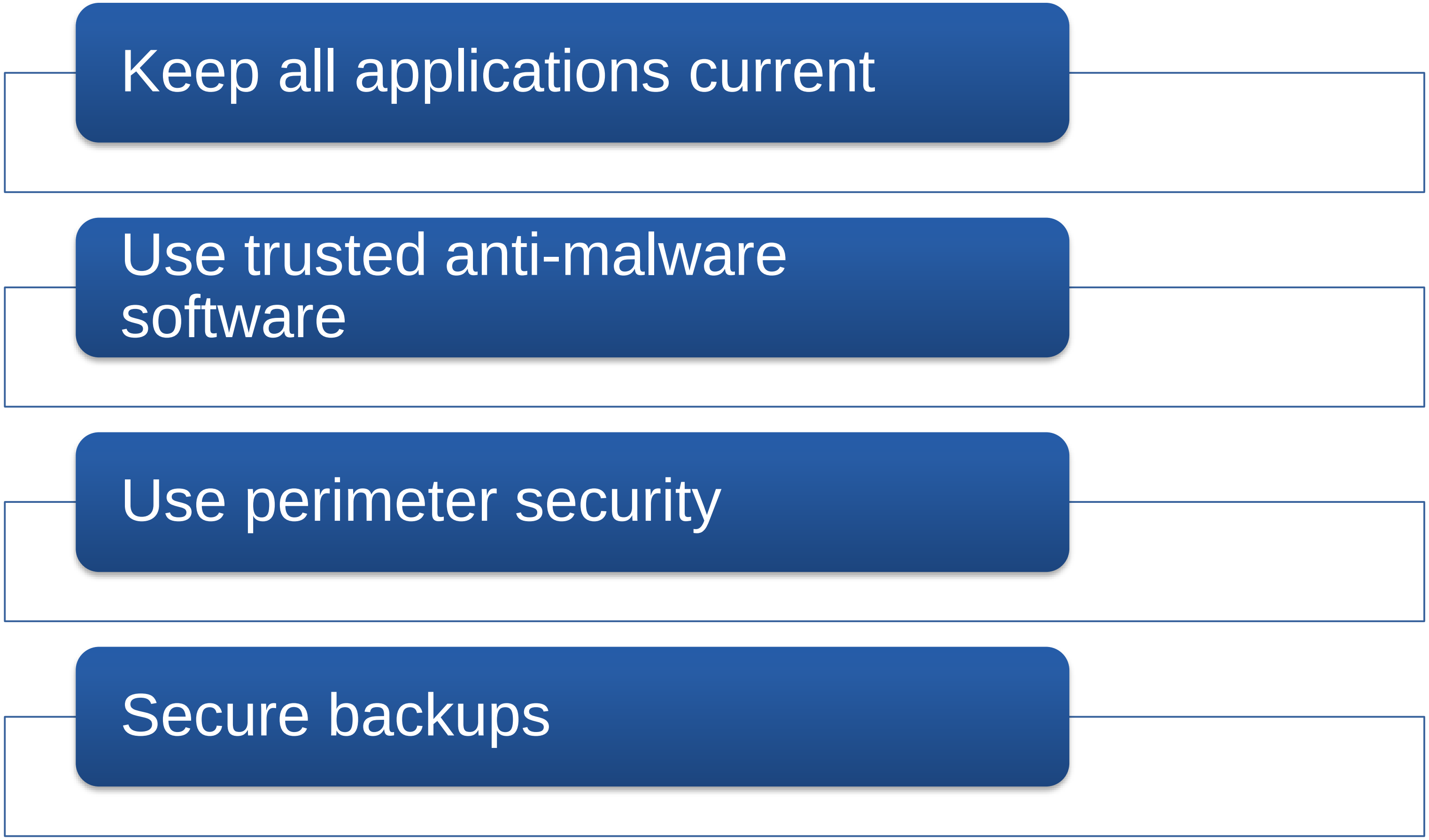
IP address spoofing

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system. One technique which a sender may use to maintain anonymity is to use a proxy server. Wikipedia

Sample of the DNS organization of the Internet



Best Practices for Connecting to the Internet



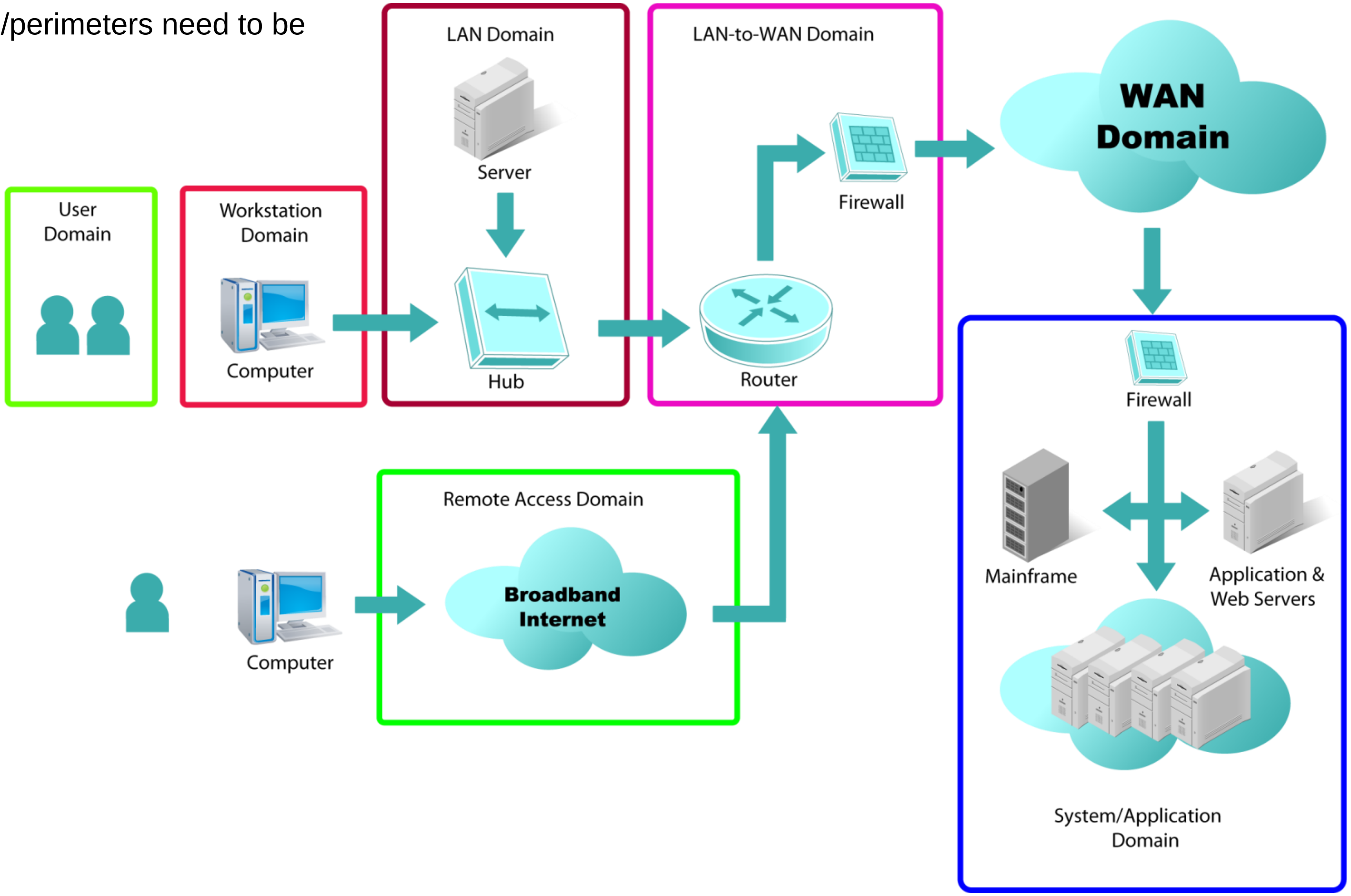
- Keep all applications current
- Use trusted anti-malware software
- Use perimeter security
- Secure backups

Best Practices for Connecting to the Internet (Cont.)

- Use secure passwords
- Report cybercrime
- Protect personal information
- Use data encryption

Seven Domains of a Typical IT Infrastructure

all the edges/perimeters need to be secured



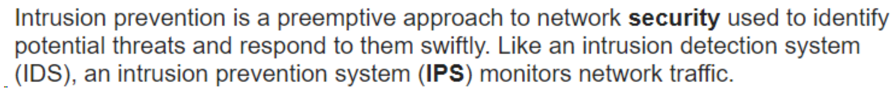
LAN-WAN Domain

- Web site security issues typically relate specifically to the local area network (LAN)-wide area network (WAN) domain.
- The following slides discuss some Web site security strategies in this domain.

Perimeter Defense and Firewalls

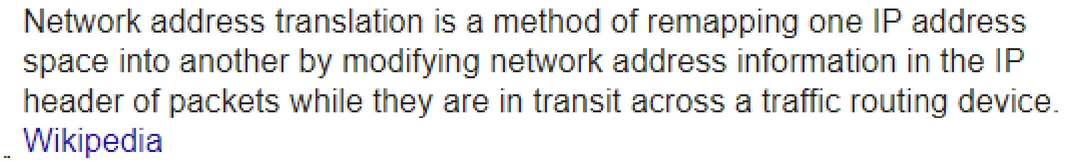
- **Perimeter defense**: A defense of the outside “edge” of a computer network
- **Firewall**: A technological barrier designed to prevent unauthorized or unwanted communications between sections of a computer network

content filtering for viruses, flagged them for threats
IDS-intrusion detection systems in the firewall
IPS-intrusion prevention system



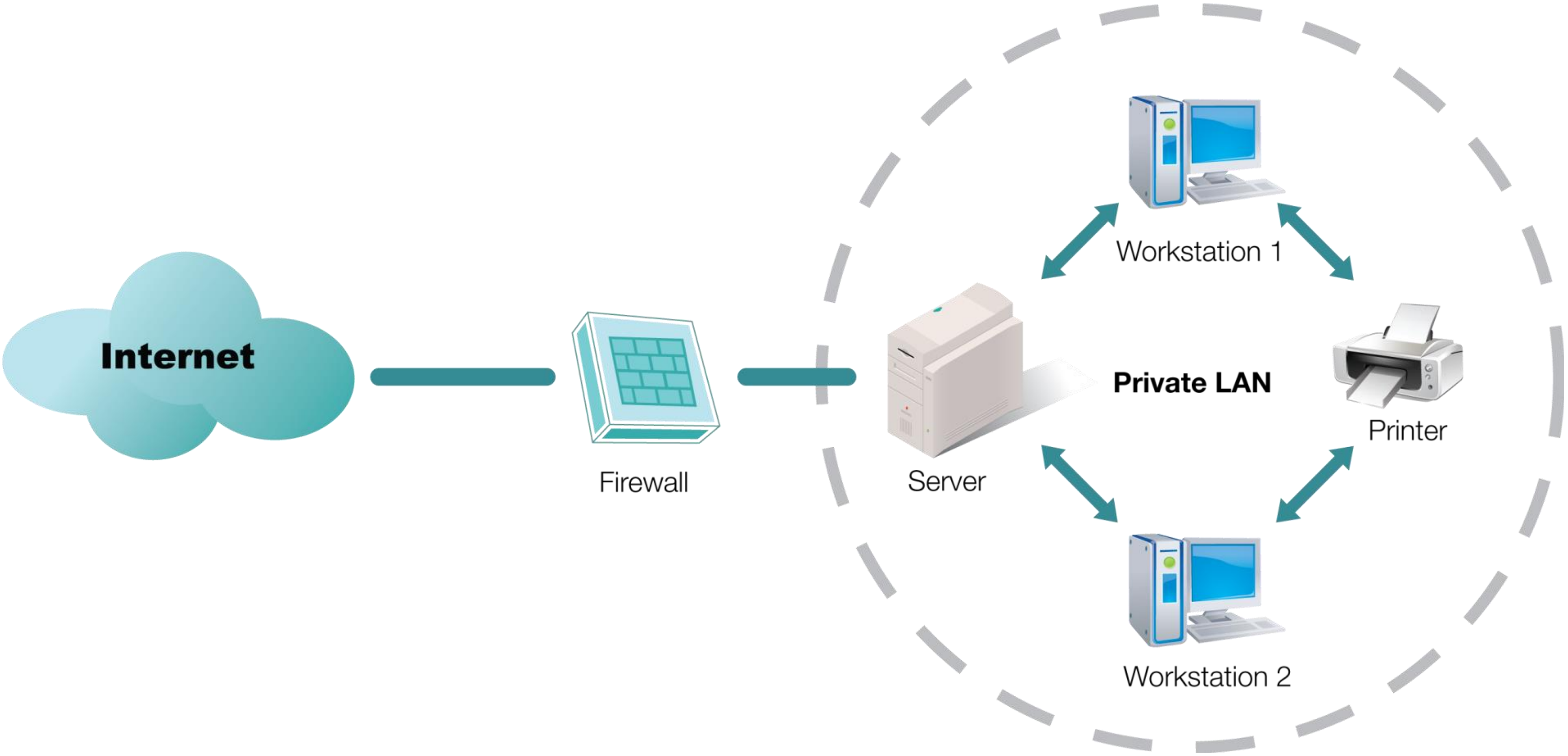
Intrusion prevention is a preemptive approach to network **security** used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (**IPS**) monitors network traffic.

network addr translation

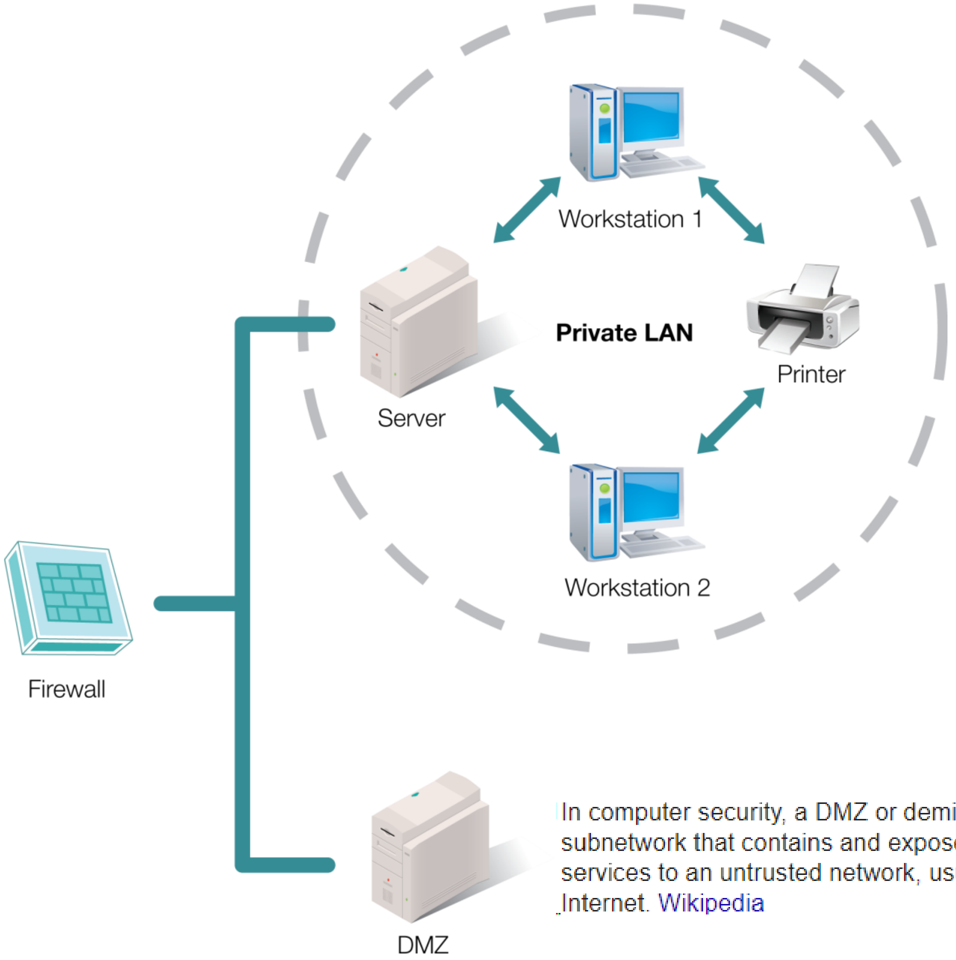


Network address translation is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
Wikipedia

A Standard Network Firewall Configuration

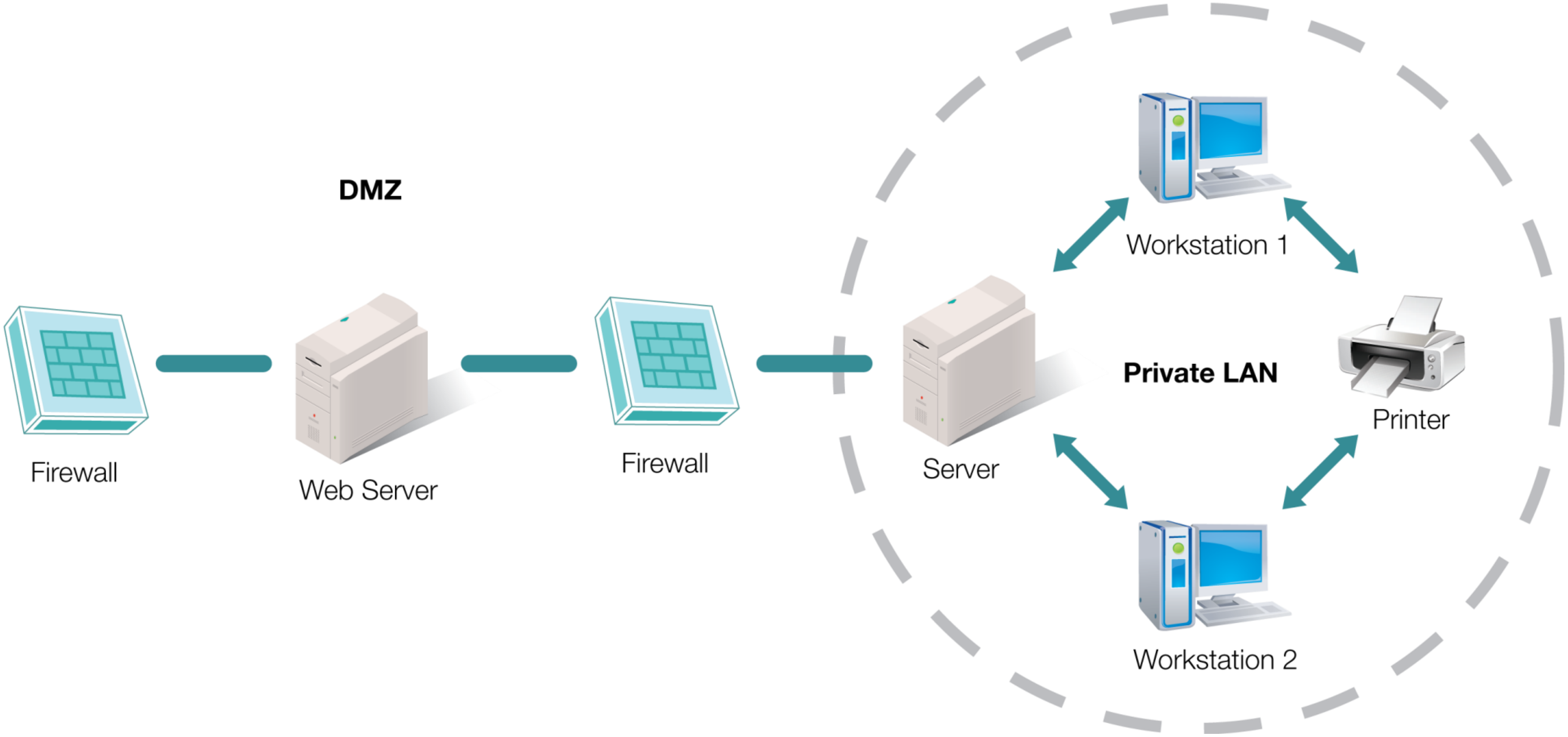


A DMZ Using a Three-homed Firewall Configuration



In computer security, a DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. Wikipedia

A DMZ Using an N-tier Firewall Configuration

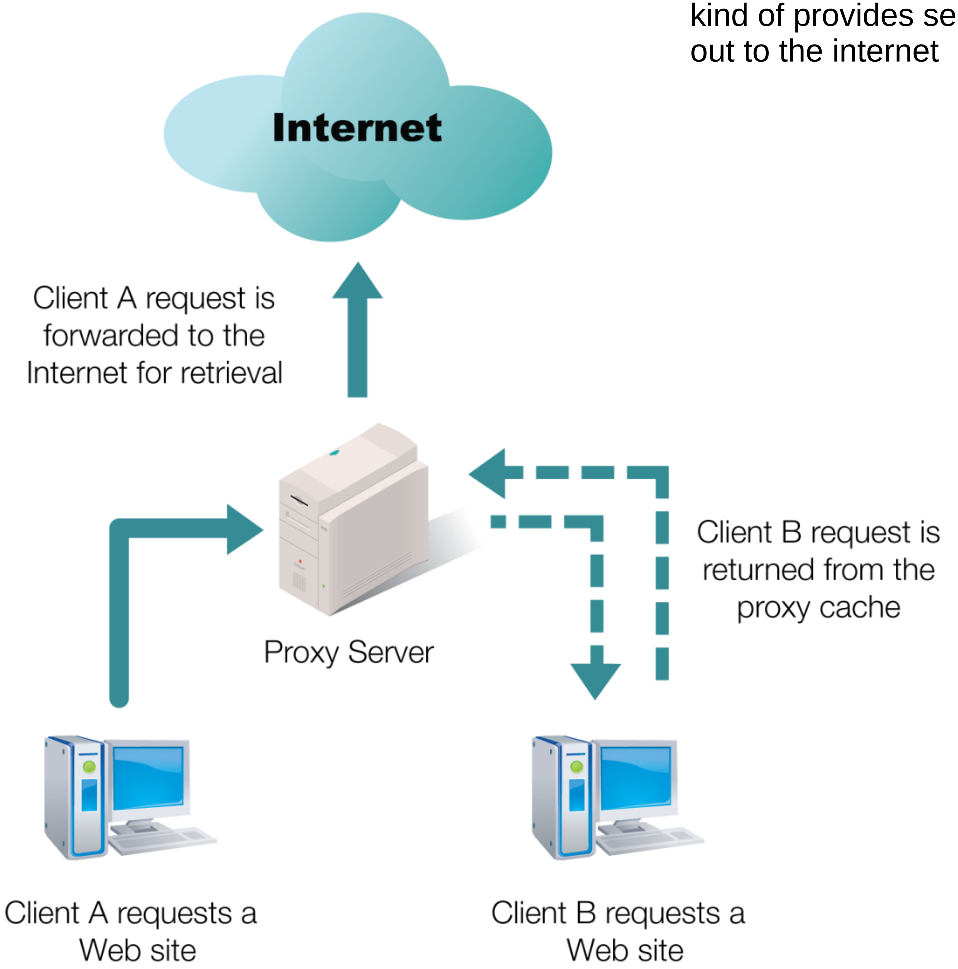


DMZs and Proxy Servers

- A demilitarized zone (DMZ) is a physical or logical sub network that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
- A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

A Proxy Server

kind of provides security as u do not need to reach out to the internet


Internet
Client A request is forwarded to the Internet for retrieval
Proxy Server
Client B request is returned from the proxy cache
Client A requests a Web site
Client B requests a Web site

IDS and IPS

comes bundled with firewall

- **Intrusion Detection Systems (IDS)**: Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity.
- **Intrusion Protection Systems (IPS)**: It provides policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted.

Data Leakage

- Data leakage issues arise from e-mail, IM, and other Internet channels.
- With the proliferation of mobile technology, data loss occurs frequently, whether accidentally or maliciously.

Summary

- Web site risks, threats, and vulnerabilities
- Different approaches to Web hosting
- Best practices while connecting to the Internet
- Protecting the LAN-to-WAN Domain